OFFERTA TECNICA

Procedura Ristretta

"Acquisizione dei servizi di firma digitale, marcatura temporale e conservazione sostitutiva dei documenti informatici, nonché di posta elettronica certificata, supporto, formazione ed help desk a favore della Regione del Veneto e degli Enti Locali del Veneto, degli Enti e Agenzie Regionali"

REGIONE DEL VENETO

Tec 1/2014
CIG 6266165AEE

PRESENTATA DA

Aruba PEC S.p.A.

Sommario

1 INTRODUZIONE

Gli ultimi anni sono stati caratterizzati da un sempre maggior impegno della Pubblica Amministrazione nell'attuazione di progetti volti alla profonda revisione organizzativa, finalizzata a migliorare i livelli di efficienza, efficacia ed economicità della propria azione ed a ottimizzare così le proprie capacità di risposta alle istanze della società civile.
La Regione del Veneto ha fortemente investito su sistemi deputati alla divulgazione delle informazioni, alla trasparenza amministrativa, alla semplificazione dei processi, all'erogazione dei servizi per i cittadini e le imprese e alla cooperazione tra le P.A..
In questo contesto di grande innovazione dei sistemi di comunicazione e di informatizzazione della P.A. e dei processi amministrativi s'inserisce il progetto della Regione, volto alla diffusione e al consolidamento dell'uso della Firma Digitale, della Firma Remota, della PEC e soprattutto della Conservazione tra gli Enti Locali veneti, gli Enti e le Agenzie Regionali.
Aruba PEC S.p.A. con il presente documento e la propria offerta tecnica intende rispondere alla gara fornendo il proprio know how nel settore e la propria esperienza maturata in progetti analoghi.

Oltre ai dispositivi e ai certificati di firma e di autenticazione, Aruba PEC metterà, pertanto, a disposizione di Regione del Veneto e degli Enti Aderenti degli strumenti volti a gestire l'intero ciclo di vita dei servizi erogati, oltre ad un pannello di monitoraggio evoluto che permetterà in modo semplice ed immediato di tenere sotto controllo, a più livelli, le prestazioni e i volumi dell'intera fornitura.
Aruba PEC S.p.A. oltre ad ospitare i sistemi hardware necessari alla messa on line dei servizi, in caso di aggiudicazione, garantirà il regolare funzionamento dei sistemi, eseguendo la diagnosi e rimozione di eventuali malfunzionamenti.
Sarà inoltre garantito l'adeguamento a versioni/release successive delle componenti applicative e dei prodotti software facenti parte della soluzione.
Aruba PEC fornirà tutto il supporto tecnico normativo e documentale a Regione del Veneto e agli Enti interessati nell'adesione ai servizi oggetto della convenzione. A titolo esemplificativo, verrà fornita consulenza e supporto per il processo di istituzione degli Enti che ne faranno richiesta quali Enti Emettitori di Carta Nazionale dei Servizi.

Quali ulteriori servizi migliorativi a corredo della fornitura, oltre a quelli espressamente richiesti dal Capitolato tecnico, Aruba PEC metterà a disposizione:

- Il sito web informativo di supporto al servizio;

- La consulenza agli Enti nelle fasi di adesione alla convenzione in modo da garantire la scelta dei servizi e soprattutto dei processi più idonei alle proprie esigenze;

- La fornitura dei servizi di comunicazione per promuovere l'iniziativa, corredata da una serie di eventi informativi/formativi tra gli Enti.

Aruba PEC garantisce che tutti i servizi oggetto della presente gara risponderanno in pieno a tutti i requisiti minimi previsti dal Capitolato Tecnico di gara, eventualmente oggetto di miglioramenti come descritto nel proseguo dell'offerta tecnica, e si impegna a soddisfare tutti i requisiti previsti dal Capitolato e dai documenti di gara anche se non esplicitamente citati e dettagliati nel presente documento.
Le immagini contenute nel presente documento riportate a titolo esemplificativo sono da considerarsi indicative.

1.1 DESCRIZIONE DELL'AZIENDA

Nata nel 2006 Aruba PEC S.p.A. è Ente Certificatore accreditato presso l'AgID e presente nell'elenco pubblico dei gestori di Posta Elettronica Certificata.
La validità dei servizi offerti e il continuo sviluppo di nuovi prodotti e tecnologie, hanno consentito ad Aruba PEC di affermare e consolidare la propria presenza sul mercato divenendo il primo Gestore in Italia per numero di servizi attivati, superando i 4.000.000 di caselle PEC registrate.
Aruba PEC da anni opera nel settore delle smartcard CNS e firma digitale, contribuendo attivamente alla digitalizzazione delle P.A.
Dal 02/12/2014 è iscritta nell'Elenco dei Conservatori accreditati tenuto da AgiD.

Certificazioni
ARUBA PEC S.p.A. ha conseguito la certificazione di sicurezza ISO 27001:2013 e la certificazione di qualità ISO 9001:2008.

Aruba PEC S.p.A. da anni opera nell'ambito delle CNS ed è azienda leader nel settore delle smartcard/token USB di firma ed autenticazione essendosi aggiudicata numerosi contratti per la produzione di CNS e di Tessere Sanitarie e per la fornitura dei relativi certificati.
L'azienda è inoltre il principale Gestore PEC con oltre 4milioni di caselle attive e da fine 2014 si è accreditata nell'elenco dei Conservatori, confermandosi un player importante anche per questo servizio.

La seguente tabella riporta le principali esperienze maturate da Aruba PEC e dal Gruppo Aruba in importanti progetti relativi ai servizi offerti in gara:

Esperienza	***Descrizione***
Trenitalia S.p.A. Accordo Quadro per la Fornitura di Servizi: PEC – Posta Elettronica Certificata, Firma Digitale e Conservazione Digitale a Norma	A partire dal 2013 Trenitalia S.p.A. conserva con Aruba PEC SpA alcune classi documentali: messaggi di Posta Elettronica Certificata (progetto Super) ad oggi per un totale di circa n. 21.650.000 messaggi; Lettere di Vettura progetto relative alla Business Unit Cargo che ha conservato circa n. 400.000 documenti LdV; già contrattualizzati ed entro fine anno in conservazione, tutte le Fatture Elettroniche Passeggeri a partire dal 2007 per un totale di circa 7.500.000 di documenti; a breve verrà attivata anche la conservazione di tutti i contratti di appalto Trenitalia a partire da Gennaio 2015. I documenti sono stati conservati sino al termine dell'anno 2014 sul vecchio sistema di conservazione e da gennaio 2015 sul nuovo sistema di conservazione conforme al DPCM del 3 Dicembre 2013.
Regione Basilicata	Aruba PEC ha fornito un servizio di conservazione sostitutiva per i dati sanitari e amministrativi del RIS-PACS regionale. Ad oggi hanno aderito le seguenti aziende: Aziende ASP (Azienda Sanitaria Potenza) ASM (Azienda Sanitaria Matera); Azienda Ospedaliera Regionale San Carlo di Potenza; I.R.C.C.S. CROB (Istituto di Ricovero e Cura a Carattere Scientifico) di Rionero in Vulture; Dati amministrativi per la Regione Basilicata (Atti e delibere,

	protocollo informatico, ecc.).
Vodafone Omnitel BV	Aruba PEC ha fornito un servizio di conservazione a norma delle caselle di posta elettronica certificata e relativi allegati (contratti tra Vodafone e Agenzie firmati digitalmente).
Infocamere e progetto Camere di Commercio Italiane (Gara Infocamere 2013). Stiamo inoltre procedendo al rinnovo del progetto dopo che l'RTI si è aggiudicato la nuova gara del 2015.	Nel 2013 il RTI composto da Aruba PEC, Actalis s.p.a. e Infocert si è aggiudicato la gara indetta da Infocamere per il servizio di Certification Authority di tutte le Camere di Commercio d'Italia. Nell'ambito della gara è stato fornito a tutte le camere di commercio il CMS che permette di gestire il ciclo di vita delle CNS, che sono emesse in diverse modalità (diretta immediata presso lo sportello della Camera di Commercio o centralizzata presso il centro servizi Aruba). Sono state emesse **271.000** smart card CNS e **110.000** Token USB CNS . Nell'ambito di questa Gara Aruba PEC ha anche fornito il software di firma e verifica utilizzato dagli utenti delle Camere di Commercio
Infocamere e progetto Camere di Commercio Italiane (Gara Infocamere 2011)	Nel 2011 il RTI composto da Aruba PEC e Actalis si è aggiudicato la gara indetta dal Infocamere per il servizio di Certification Authority di tutte le Camere di Commercio d'Italia. Nell'ambito della gara è stato fornito a tutte le camere di commercio il CMS che permette di gestire il ciclo di vita delle CNS, che sono emesse in diverse modalità (diretta immediata presso lo sportello della Camera di Commercio o centralizzata presso il centro servizi Aruba). Sono state emesse **545.000** smart card CNS e **114.000** Token USB CNS. Nell'ambito di questa Gara Aruba PEC ha anche fornito il software di firma e verifica utilizzato dagli utenti delle Camere di Commercio
CNS Regione Basilicata	Fornitura di **45.000** CNS di dispositivo Token USB con memoria, Card Management System per la gestione del ciclo di vita del certificato, Sito Web tematico, Campagna multicanale di promozione/comunicazione.
Consiglio Nazionale Geometri	Aruba PEC ha fornito oltre **40.000** Token USB con memoria ai Geometri italiani. I dispositivi includono sia un certificato di Firma Digitale con Ruolo sia un certificato CNS con Ente Emettitore il Consiglio Nazionale Geometri.
Fondazione Italiana Geometri	Aruba PEC ha fornito oltre 100.000 caselle di posta elettronica certificata di tipologia Standard.
Consiglio Nazionale degli Ingegneri	Aruba PEC ha fornito oltre **6.500** Token USB agli Ingegneri italiani.
Consiglio Nazionale degli Architetti	Aruba PEC ha fornito oltre **10.000** Token USB agli Architetti italiani
Progetto dSign dell'Università degli Studi di Napoli Federico II	Aruba PEC si è aggiudicata la gara per il progetto dSign dell'Università degli Studi di Napoli Federico II per la fornitura di **3.200** kit di firma digitale completi di Token USB e Sim card analoghi a quelli che verranno erogati al Ministero in caso di aggiudicazione della gara in oggetto.
Forniture di TS-CNS per le regioni Friuli e Sicilia (gara SOGEI del 2009)	Aruba PEC si è aggiudicata la gara per la fornitura delle TS-CNS per le regioni Friuli e Sicilia. Ad oggi sono state emesse circa 840.000 carte. La CA utilizzata per l'emissione delle **840.000** carte è stata

	generata ed è mantenuta da Aruba PEC.
Forniture di TS-CNS Regione Toscana (gara SOGEI del 2009) RTI Actalis e Aruba PEC	A seguito dell'aggiudicazione delle gara SOGEI per la fornitura delle carte TS-CNS per Regione Toscana, Aruba PEC ed ACTALIS (società Gruppo Aruba) hanno fornito, a fronte di un contratto per 4.000.000, circa **3.900.000** carte. Le carte sono di tipo dual Interface. La CA utilizzata per l'emissione delle 3.900.000 carte è stata generata ed è mantenuta da Aruba PEC.
TS-CNS Regione Sardegna	Nel corso del 2011, Aruba PEC ha prodotto per SOGEI e consegnato **1.300.000** carte per i cittadini della Regione Sardegna. Le carte sono di tipo dual Interface. La CA utilizzata per l'emissione delle 1.300.000 carte è stata generata ed è mantenuta da Aruba PEC.
TS-CNS Regione Valle d'Aosta	Nel corso del 2011 Aruba PEC ed ACTALIS hanno prodotto per SOGEI e consegnato **110.000** carte per i cittadini della Regione Autonoma Valle d'Aosta. Le carte sono di tipo dual Interface. La CA utilizzata per l'emissione delle carte è stata generata ed è mantenuta da Aruba PEC.
CNS Arma Dei Carabinieri (Gara IPZS)	Aruba PEC si è aggiudicata la gara indetta da IPZS e ha prodotto circa **127.000** carte CNS. Nell'ambito di questa Gara Aruba PEC ha anche fornito il software di firma e verifica utilizzato dall'Arma dei Carabinieri
Carta operatori sanitari Regione Toscana	Aruba, nell'ambito dell'erogazione della gara di Gestione delle CSE di Regione Toscana, ha fornito agli operatori sanitari nel 2011 circa **60.000** CNS, oltre a **5.700** carte per gli Enti di Regione Toscana e 2.200 tesserini per i dipendenti.
Convenzione DCS software, società che opera con gli Ordini Forensi	Aruba PEC ha fornito oltre **22.500** Token USB, con caratteristiche tecniche e funzionali analoghe a quelli che verranno erogati a Regione del Veneto in caso di aggiudicazione della gara in oggetto, agli Avvocati italiani tramite la convenzione con la società DCS Software

La tabella seguente evidenzia quali sono i punti di forza della soluzione progettuale che Aruba PEC ha descritto nel presente documento tecnico.

Cod.	Punti di forza della soluzione progettuale proposta	Paragrafo in cui è descritta
0	Aruba PEC S.p.A. è Ente Certificatore accreditato presso il DigitPA, presente nell'elenco pubblico dei gestori di Posta Elettronica Certificata e Conservatore accreditato	**1.1**
1	Rete di Account Commerciali distribuita sul territorio come interfaccia dedicata per gli Enti regionali, utile a fornire supporto per la gestione di specifici aspetti contrattuali e/o richieste fuori standard durante il corso della fornitura	**1.2**
2	Sito Web dedicato alla Regione del Veneto contenente presentazioni e modulistica necessaria per i servizi della fornitura di gara	**1.2.1.b**
3	Pannello Unico di gestione dei servizi	**1.2.1.a**
4	Percorso formativo dedicato al personale degli Enti regionali – organizzato da un'apposita Segreteria Didattica – e gestito da Formatori Esperti attraverso seminari e/o workshop sia nella fase di avvio che durante il corso della fornitura	**6**
5	Al fine di incentivare l'adesione degli Enti e la diffusione dei servizi oggetto del presente bando, Aruba PEC organizzerà, senza oneri	**6**

	aggiuntivi, **7 workshop dedicati al progetto**, 1 per Provincia.	
6	Fornitura di un sistema CMS, Card Management System, che permetterà gestire in autonomia da parte degli Enti le attività di richieste ed emissione dei kit di firma	**2.1.1**
7	I moduli di richiesta PDF per la sospensione/revoca del servizio di Firma Remota da sottoporre al Titolare - automaticamente prodotti dal CMS - potranno essere sottoposti a firma grafometrica	**2.1.1.b**
8	Per consentire la firma grafometrica **Aruba PEC abiliterà 100 postazioni** mettendo a disposizione della Regione e degli Enti Aderenti **100 tavolette grafometriche** (incluse nell'offerta).	**2.1.1.b**
9	Riconoscimento del richiedente del servizio di Firma tramite procedura di identificazione con webcam su sessione videoconferenza Aruba PEC fornirà dunque la piattaforma d'identificazione e la possibilità di utilizzo illimitato, per tutta la durato del contratto e relative estensioni da parte della Regione e/o degli Enti aderenti interessati che attraverso i propri incaricati potranno effettuare il riconoscimento a distanza, utile ad es. in caso di presenza di sedi distaccate ecc.	**2.1.1.b**
10	Aruba PEC metterà a disposizione personale incaricato all'emissione live di kit/dispositivo sul territorio regionale - con un preavviso massimo di 2 giorni. Aruba PEC garantirà l'emissione di 50 appuntamenti nella modalità illustrata, fermo restando che sarà la Stazione Appaltante a decidere chi potrà goderne e quando.	**2.1.1.b**
11	Smartcard personalizzata per emissione Certificati. Possibilità di personalizzare il supporto plastico e la grafica in quadricromia su richiesta di ogni Ente Aderente	**2.2**
12	Token USB personalizzati per servizi di Firma digitale. Possibilità di personalizzare graficamente i dispositivi (guscio plastico esterno) in accordo con ciascun Ente Aderente.	**2.2**
13	Token USB da 8GB	**2.2**
14	Scratchcard contenenti codici Pin e Puk personalizzate per la fornitura	**2.2**
15	Possibilità di attivazione del servizio di firma remota in abbinamento a diverse tipologie OTP a scelta dell'Ente/richiedente.	**2.3**
16	Token Mobile OTP (APP Mobile) personalizzato con il logo di Regione del Veneto.	**2.3**
17	Fornitura di servizi di firma che rispettino oltre alle caratteristiche minime anche le caratteristiche migliorative richieste dal capitolato	**2.6**
18	Chiusura di una casella PEC in autonomia da parte dell'Ente, con conseguente tempo di attivazione e chiusura che può ridursi dalle 48 ore a pochi minuti.	**3.1**
19	Servizio di PEC con 2 tipologie di caselle con dimensioni superiori: tipologia STANDARD con dimensione 8 GB e con spazio archivio 24 GB; tipologia AVANZATA con dimensione 14 GB e con spazio archivio 24 GB	**3.2**
20	Singola casella PEC con caratteristiche più performanti: numero di messaggi invio/ricezione illimitati; numero massimo destinatari per messaggio pari a 1.000; dimensione massima del singolo messaggio con allegato pari a 100	**3.2**

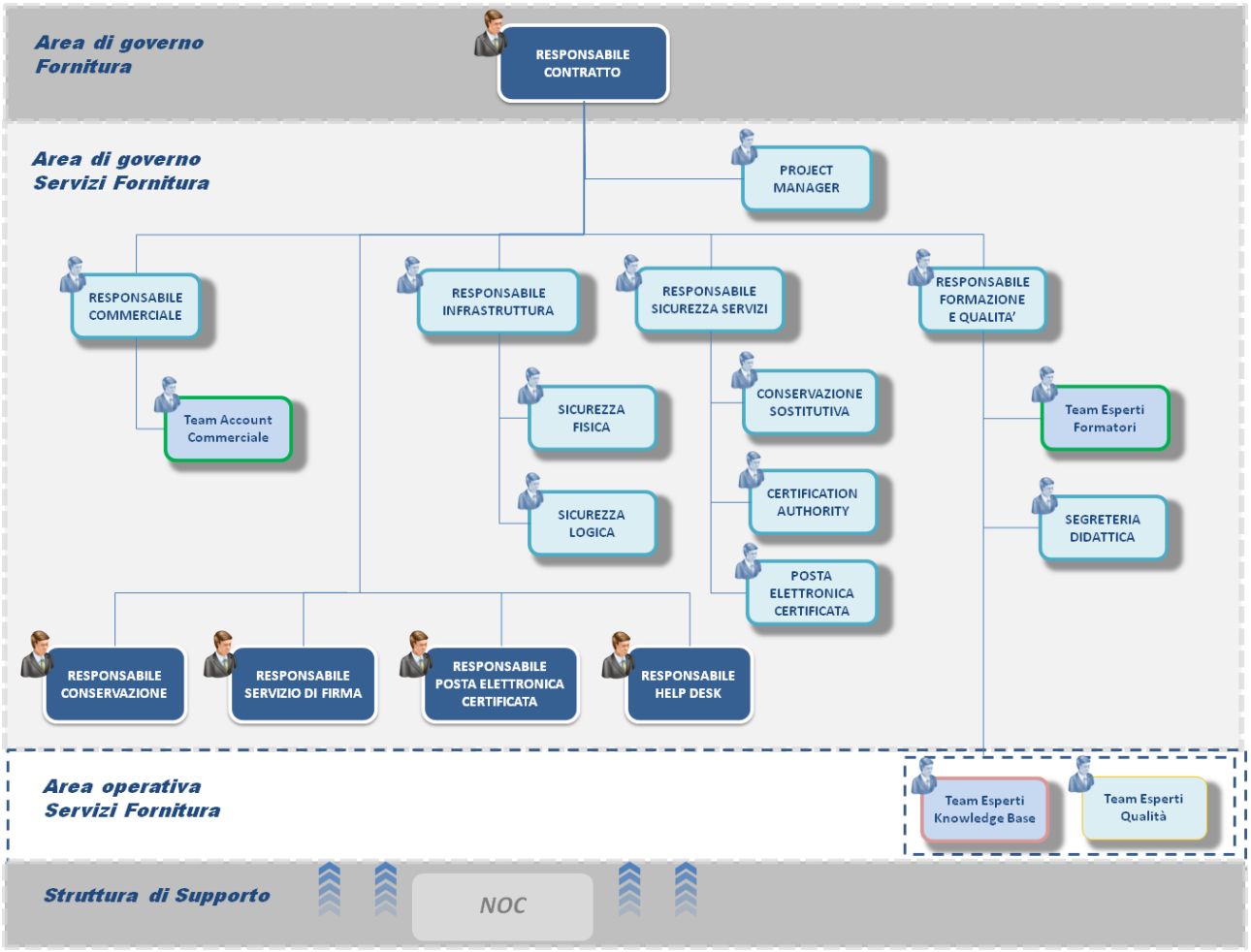
	MB	
21	Servizio di PEC con servizi opzionali aggiuntivi: possibilità di incrementare lo spazio allocato sulla casella o sull'archivio per step di 1 GB; APP mobile per la consultazione ed utilizzo della casella PEC per i principali smartphone/tablet; notifica al titolare per avviso via email al raggiungimento di specifiche soglie di occupazione della propria casella; possibilità per il titolare di scaricare i log delle transazioni per uno specifico messaggio; possibilità di impostare ogni casella PEC in modalità multiutenza (cioè diverse persone possono utilizzare una stessa casella accedendo con le proprie credenziali)	**3.2**
22	Possibilità di gestire la saturazione dell'archivio sia scaricando i messaggi presenti, sia inviandoli in conservazione	**3.1.2**
23	Disponibile modalità di invio dei documenti soggetti a Conservazione digitale a norma tramite i canali: FTPS, PEC, HTTPS e Web Services.	**4.1**
24	Garanzia di immodificabilità e staticità dei documenti conservati a norma , tramite l'adozione di applicazioni software in grado di esibire i documenti nei formati ammessi e di garantire l'accesso ai documenti informatici nel lungo periodo.	**4.1**
25	Sistema di reportistica per il servizio di Conservazione a norma capace di analizzare in maniera granulare l'archivio della singola società o Ente aderente.	**4.1**
26	Il sistema di Conservazione di Aruba PEC è ospitato presso i data center di Aruba SpA, pertanto la soluzione offerta risulta scalabile ed affidabile in quanto risulta essere ridondato e resiliente ai guasti (grazie alla funzionalità di HA e Fault Tollerance).	**4.3**
27	Il sistema di Conservazione – al fine di garantire la massima sicurezza – consente l'accesso agli utenti soltanto apposite personali ed univoche credenziali, che vengono richieste tramite pagine web basate sul protocollo SSL. Oltre alle credenziali indicate – l'accesso da parte di ciascun utente prevede una ulteriore autenticazione tramite OTP.	**4.3**
28	Il Servizio di Conservazione prevede l'utilizzo di Backup geografico nel sito Disaster Recovery del data center di Aruba – finalizzato alla creazione e conservazione di copie di sicurezza dei dati, in duplice copia sincrona.	**4.3**
29	Il servizio Help Desk in fornitura è conforme allo standard ITIL v3 ed è tuttora dimensionato a soddisfare costante livello di supporto ad oltre migliaia di persone.	**5.1**
30	Il canale di contatto telefonico tramite Numero Verde del servizio Help Desk prevede l'uso di un centralino IVR, in grado di instradare automaticamente la chiamata al centro di competenza adeguato - in base alla tipologia di servizio su cui è richiesta l'assistenza da parte di ciascun utente.	**5.1**
31	Il centralino IVR del servizio Help Desk consente di configurare ed inserire "messaggi di intro" durante la fase di risposta all'utente. Tali messaggi comunicano le news relative ai servizi erogati (es. nuovi servizi disponibili, ecc.) e/o messaggi di preavviso in merito ad aggiornamenti e/o eventi pianificati sui sistemi (che potrebbero avere impatti sulla normale operatività).	**5.1**
32	Il servizio Help Desk metterà a disposizione per ciascun utente la	**5.1**

	possibilità di contatto outbound su richiesta. A tale proposito viene infatti predisposto - all'interno delle varie sezioni delle FAQ il servizio Call me back – con un tempo di richiamata entro 10 minuti dalla richiesta di contatto.	
33	Al di fuori di tale fascia oraria Aruba PEC continua comunque a garantire la ricezione di: richieste tramite i canali di Posta Elettronica e Portale Web e Fax; segnalazioni per malfunzionamenti e/o problemi di sicurezza attraverso i sistemi di monitoraggio interni; comunicazione di interventi e/o fermi servizio pianificati.	**5.1**
34	Il Servizio di Help Desk manterrà - per tutta la durata contrattuale - la banca dati relativa alla registrazione di tutte le segnalazioni ricevute (Trouble Ticket).	**5.1**
35	Il servizio di Help Desk - qualora si verifichino richieste massive e/o transitori picchi di attività - si adopera ad attingere risorse dal Team Esperti Qualità e dal Team Esperti KB - al fine di organizzare Focus Group - in forma di seminari e workshop - dedicati agli utenti della Regione del Veneto.	**5.1**
36	Il servizio di Help Desk – qualora l'assistenza non sia in grado di risolvere la problematica una volta raggiunto il 2°livello – effettua opportuna escalation verso gli esperti funzionali di tematica presenti all'interno dei Centri di Supporto. Nel frattempo viene incaricata una risorsa del Team di Operatori di 2° Livello a ricoprire temporaneamente il ruolo di Case Manager, che funge da interfaccia verso i Centri di Supporto, con lo scopo di seguire a livello procedurale la risoluzione del problema ed a seguito assicurare a livello operativo l'evasione della richiesta.	**5.1**
37	Tutti i servizi saranno erogati tramite i Data center sicuri del Gruppo Aruba certificati ISO 27001	**1.2.2**
38	Possibilità di attivare servizi di firma digitale e PEC in modalità massiva	**2.1.1. e 3.1.4**
39	Durata quinquennale dei certificati di firma e autenticazione a bordo di smartcard e token	**2.2**

Per una più agevole individuazione degli elementi migliorativi della soluzione, abbiamo inserito all'interno del documento il seguente simbolo: ☞

1.2 ORGANIZZAZIONE DEL FORNITORE: COMPITI E SERVIZI EROGATI DA CIASCUN FORNITORE

Il **modello organizzativo della fornitura per Regione del Veneto** si distingue in tre aree specifiche: l'**Area di governo Fornitura**, l'**Area di governo Servizi Fornitura** e l'**Area operativa Servizi Fornitura**.



L'**Area di governo Fornitura** è costituita dalla figura del **Responsabile Contratto** Aruba PEC.

All'interno dell'**Area di governo Servizi Fornitura** sono presenti le seguenti figure:

- ✓ **Project Manager** – è garante della fornitura dei servizi sottoscritti dagli Enti della Regione del Veneto e il principale punto di contatto per questi ed organo di staff al **Responsabile Contratto**. Rappresenta il punto di contatto diretto per i **Responsabili di area** ed il punto di riferimento trasversale per i **Responsabili di servizio**.
- ✓ **Responsabile Commerciale** – è supervisore della gestione commerciale e supporto agli **Enti della Regione del Veneto** che hanno aderito al contratto di fornitura. Nello specifico si avvale del **Team Account Commerciale** che funge da interfaccia con i **referenti degli Enti della Regione del Veneto** qualora insorgano richieste fuori standard e/o sia necessario revisionare accordi specifici per la fornitura dei servizi sottoscritti nel contratto. . E' prevista la presenza di Account Commerciali distribuiti nel territorio della Regione del Veneto al fine di poter fornire supporto dedicato agli Enti della Regione del Veneto.
- ✓ **Responsabile Infrastruttura** – è supervisore della sicurezza dell'infrastruttura del data center Aruba su cui vengono ospitati i servizi previsti nella fornitura di gara. Garantisce il corretto funzionamento ed adeguata manutenzione degli apparati/sistemi infrastrutturali nel rispetto degli standard si **Sicurezza Fisica** e di **Sicurezza Logica**.
- ✓ **Responsabile Sicurezza Servizi** – è supervisore degli standard e policy di sicurezza necessarie a garantire la corretta erogazione dei servizi. Nello specifico garantisce l'adeguato mantenimento dei livelli di sicurezza per il **servizio di Conservazione, Certification Authority e PEC** oggetto della fornitura in gara.
- ✓ **Responsabile Formazione e Qualità** – rappresenta il responsabile del livello di competenze e della qualità operativa svolta durante l'erogazione e manutenzione dei singoli servizi oggetto della fornitura. Tale figura interagisce con ciascun **Responsabile di servizio** e garantisce il miglioramento continuo di processi/procedure utili a perfezionare il

livello di servizio dell'intera fornitura. Si avvale di un **Team Esperti Formatori** che vengono ingaggiati per erogare formazione agli utenti della Regione del Veneto in occasione di seminari e/o workshop. Viene supportato inoltre da una **Segreteria Didattica** avente lo scopo di organizzare e pianificare percorsi formativi dedicati agli utenti della Regione del Veneto.

Il **governo della fornitura dei servizi** è infine garantito dalle figure dei **Responsabili di servizio**, che svolgono il ruolo di supervisione e coordinamento dell'erogazione e fruizione dei servizi contrattualizzati da ciascun Ente della Regione del Veneto:

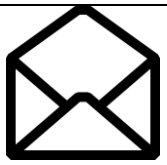
- **Responsabile Conservazione**
- **Responsabile Servizio di Firma**
- **Responsabile Posta Elettronica Certificata**
- **Responsabile Help Desk**

L'**Area operativa Servizi Fornitura** ha infine la responsabilità di fornire operativamente i servizi agli utenti di riferimento della Regione del Veneto e degli Enti aderenti, la cui organizzazione è descritta nel dettaglio per singolo servizio all'interno della specifica sezione della presente offerta tecnica.

1.2.1 STRUMENTI E INTERFACCE PER LA FORNITURA

L'intera fornitura viene personalizzata con **strumenti ed interfacce dedicate** ai servizi, al fine di consentire un adeguato monitoraggio e controllo al personale della Regione del Veneto e degli Enti Aderenti.
Nello specifico riepiloghiamo di seguito i principali strumenti ed interfacce che verranno fornite a supporto:

	✓ **Sito Web dedicato** – sito dedicato al progetto, contenente la presentazione generale per i singoli servizi, la sezione delle FAQ esterne, la sezione contenente la modulistica di contratto e l'area download che mette a disposizione software e driver utili all'utilizzo dei dispositivi di fornitura. Per dettagli si rimanda al par. 1.2.1.b.
	✓ **Pannello Unico di Gestione e Monitoraggio** – pannello di gestione dei servizi erogati. Il pannello contiene una consolle di monitoraggio attraverso la quale è possibile controllare lo stato di avanzamento dei servizi (sia a livello aggregato che di singolo Ente regionale). Il pannello prevede sezioni dedicate per singolo servizio, all'interno delle quali è possibile visualizzare il valore SLA, lo stato di consegna degli apparati di fornitura, lo stato della contabilità, la gestione delle anagrafiche e la possibilità di esportare appositi report/statistiche. Per la descrizione del pannello si rimanda al Capitolo 7.
	✓ **Strumenti di Gestione Operativa –** strumenti necessari per l'operatività di alcuni servizi quali la Conservazione a norma (DocFly) e la firma digitale e remota (**CMS – Card management System)**
	✓ **Portale Web Help Desk** – piattaforma di trouble ticketing per la gestione delle richieste di assistenza da parte degli utenti della Regione del Veneto e degli Enti aderenti – avvenute tramite i canali di contatto via Ticket, Email, Fax o Numero Verde. Per dettagli si rimanda al Capitolo 5.

	✓ **Canali di Supporto** – canali di contatto tra i referenti della Regione del Veneto finalizzati a fornire ulteriore supporto negli ambiti di **formazione dedicata** e gestione **aspetti contrattuali**. Tali canali di contatto prevedono l'interazione della Regione del Veneto con l'area di formazione (segreteria didattica e formatori esperti) e l'area commerciale (account di riferimento per gli Enti regionale). Il canale commerciale in particolare rappresenta il punto di contatto dedicato per ciascun Ente della Regione del Veneto, con cui poter interagire direttamente ad approfondire aspetti contrattuali specifici e/o gestione fuori standard nell'ambito della fornitura.

1.2.1.a. PANNELLO UNICO DI GESTIONE

Come valore aggiunto Aruba PEC offre a tutti gli Enti interessati, la possibilità di richiedere e gestire i servizi, attraverso un **Pannello Unico di Gestione** , un prodotto consolidato che è in produzione da anni e gestisce migliaia di clienti, partner, rivenditori tra pubbliche amministrazioni, aziende private, ecc.
Ferma restando la possibilità di richiedere l'attivazione dei servizi ad Aruba PEC che si incaricherà di processare le richieste mediante il proprio centro servizi, la presenza di un pannello di amministrazione condiviso consente ai responsabili della Regione e degli Enti Aderenti, fino a quelli degli Enti Associati, di tenere sotto controllo l'andamento dei servizi, le richieste effettuate da ogni Ente, il monte delle caselle PEC attivabili, ecc.

La possibilità di usare uno strumento online consente inoltre di ridurre drasticamente i tempi di attivazione dei servizi: dalle 48 ore richieste dal capitolato è possibile passare a pochi minuti.

Il pannello unico permette quindi di gestire tutta la fase di richiesta ed autorizzazione del servizio e, in alcuni casi anche l'attivazione dello stesso. Ad esempio, come descritto nel capitolo relativo alla posta elettronica certificata, attraverso il pannello è possibile gestire l'intero ciclo di vita di una casella PEC: dalla richiesta, fino all'attivazione e alla successiva chiusura.

Fermo restando che l'iter autorizzativo potrà sempre avvenire attraverso il Pannello Unico, per quanto riguarda la firma digitale, la firma remota, la conservazione a norma, data la peculiarità dei servizi, verranno utilizzati due strumenti specifici per la gestione operativa:

- ✓ il Card Management System (CMS)
- ✓ Il sistema di Conservazione, DocFly

Il **Card Managementi System**, descritto al paragrafo 2.1.1, consente di emettere certificati di autenticazione (CNS), firma digitale, firma remota, gestendone l'intero ciclo di vita e dialogando con il dispositivo fisico per la generazione delle chiavi private e l'installazione dei certificati, una volta ottenuti dalla Certification Authority.
DocFly, dal canto suo, permette di gestire l'intero ciclo di vita della conservazione sostitutiva nel rispetto della normativa di riferimento.

Riportiamo, di seguito, uno screenshot del Pannello Unico di Gestione nel quale si può notare la presenza di una sezione (TAB) per ogni servizio con le funzionalità specifiche per ciascuno di essi.

Come è possibile vedere sono presenti le sezioni relative a:

- PEC
- Firma digitale
- Marcatura temporale
- Conservazione a norma (DocFly)
- Certificati SSL.

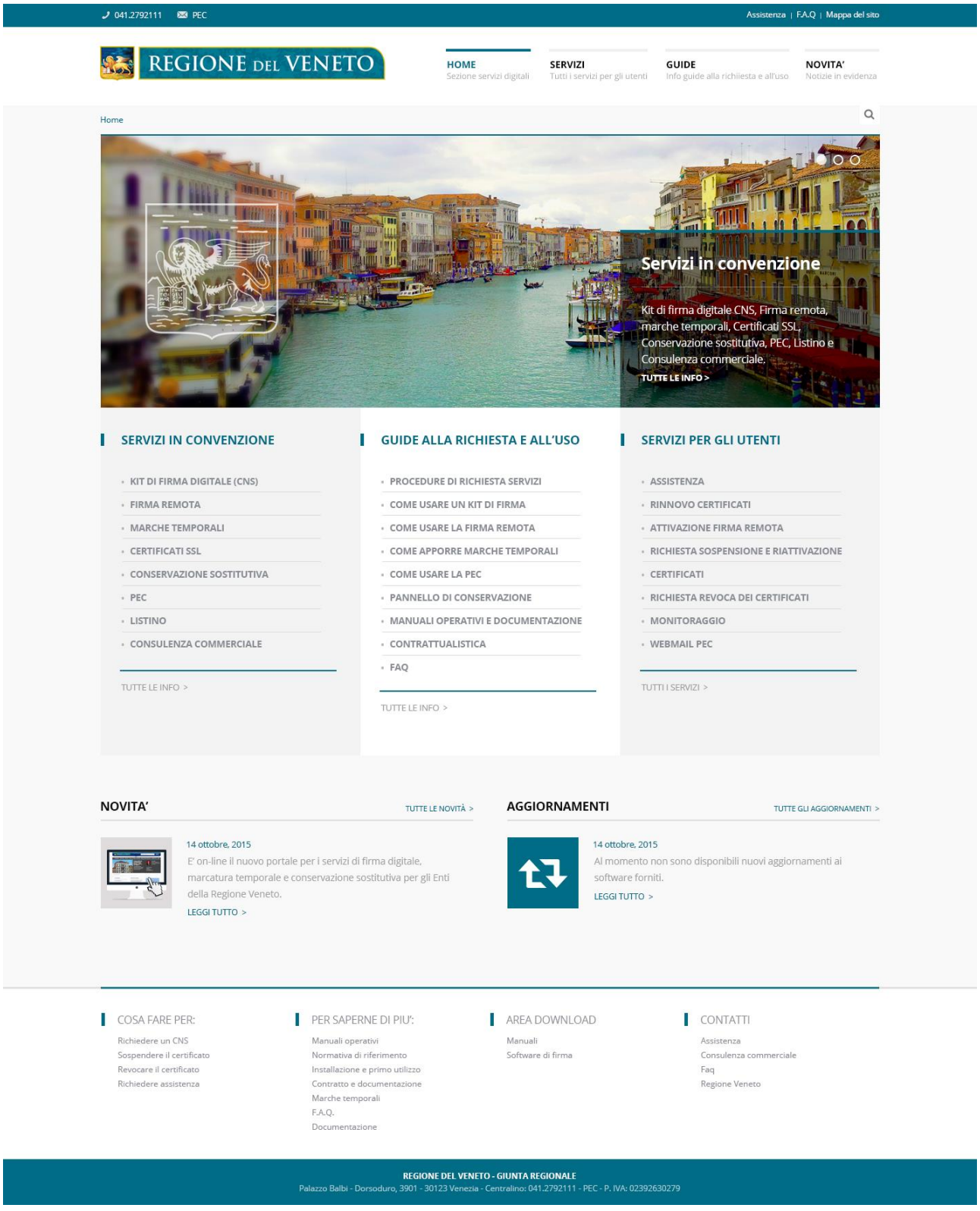
All'interno di ogni sezione verranno visualizzate le sole funzionalità specifiche per la stazione appaltante e per l'utente che si è autenticato sul pannello.
Nell'esempio riportato sopra le voci relative alla PEC sono da considerarsi indicative. Nel caso specifico della Regione del Veneto verranno previste le funzionalità di richiesta di attivazione di caselle STANDARD o AVANZATE, con la possibilità di aggiungere le opzioni "multiutenza", "conservazione", etc.

All'interno del pannello unico sarà presente una sezione contenente la Consolle di Monitoraggio che consente di tenere sotto controllo il funzionamento e l'andamento dei servizi erogati. Per i dettagli si veda il relativo capitolo 7.

1.2.1.b. SITO WEB A CORREDO DELLA FORNITURA

Al fine di garantire il massimo successo dell'iniziativa di Regione del Veneto e di fornire nel modo più semplice ed intuitivo possibile informazioni e dettagli sui servizi erogati agli Enti e agli utenti finali, Aruba PEC predisporrà un portale web informativo dedicato al progetto.
Tale strumento permetterà non solo di mettere a disposizione un unico centro di reperimento delle informazioni sui servizi ma anche di guidare gli utenti nelle procedure di adesione ed attivazione, mettendo a disposizione anche una consulenza commerciale fornita da Aruba PEC che permetterà d'incentivare gli enti ad aderire ed intraprendere ed accelerare il processo di digitalizzazione

A titolo di esempio, riportiamo di seguito un'ipotesi di grafica e di contenuti che andranno a popolare il sito web. L'impianto grafico definitivo e le funzionalità del sito saranno poi concordate con Regione del Veneto durante le fasi di start up del progetto.



Il sito web, redatto in lingua italiana, sarà un valido supporto informativo per gli utenti che intendono aderire al servizio, i quali vi potranno trovare guide, manuali, FAQ e strumenti di gestione dei servizi. Aruba PEC s'impegna ad occuparsi della redazione dei documenti e delle altre informazioni correlate ai servizi offerti, che dietro l'assenso di Regione del Veneto saranno pubblicati.

Il sito sarà erogato dall'infrastruttura di Aruba PEC che ne curerà anche la manutenzione e gestione per la durata del contratto, garantendo comunque adeguato supporto tecnico.
Qualora lo desideri, Regione del Veneto potrà occuparsi direttamente della gestione dei contenuti, in completa autonomia. In tal caso Aruba PEC, oltre al supporto tecnico necessario, fornirà anche un'adeguata formazione sull'utilizzo del Content Management System messo a disposizione al personale che verrà coinvolto dalla Regione.

Sul sito web saranno adottate da Aruba PEC una serie di misure atte a garantire un adeguato livello di **sicurezza**, particolarmente per quanto riguarda le fasi di dialogo con la C.A. e d'interazione con i dispositivi. In sintesi:

- ad eccezione delle aree puramente informative del sito, tutte le risorse (URL) del sito coinvolte in operazioni on-line saranno accessibili solo su **canale sicuro SSL/TLS** con chiavi di sessione di almeno 128 bit;
- le componenti attive integrate sul sito web (es. applet Java) saranno **firmate digitalmente**, con certificato emesso da una CA riconosciuta;
- nello sviluppo del sito saranno adottate tecniche riconosciute di **secure coding**;
- i **certificati** degli utenti saranno **verificati** in termini di autenticità e di validità, prima di essere accettati nel contesto delle operazioni on-line che lo richiedono;
- dopo l'autenticazione utente, ove prevista, la **sessione** avrà una durata limitata nel tempo;
- prima del suo passaggio in produzione, il sito web sarà sottoposto ad un **Vulnerability Assessment** (VA).

STRUTTURA DEL SITO

Sul sito saranno disponibili le seguenti informazioni:

- informazioni generali sui servizi, sui dispositivi e sul software applicativo;
- manuali, procedure e istruzioni per l'uso dei prodotti e dei servizi;
- istruzioni per la sospensione e riattivazione diretta (on-line) dei certificati;
- istruzioni per richiedere la revoca dei certificati;
- istruzioni per il rinnovo dei certificati di prossima scadenza;
- istruzioni per la gestione e l'utilizzo del dispositivo;
- documentazione tecnica di riferimento;
- normativa di riferimento;
- modulistica;
- software di utilità.

Il sito web sarà strutturato in modo da garantire semplicità e chiarezza. Le informazioni in esso contenute sono essenziali, raccolte per sezioni tematiche e riproposte nelle varie aree del sito in modo tale che siano facilmente raggiungibili dai visitatori.

Per un'immediata individuazione delle informazioni si ipotizza la suddivisione del sito web in 3 macro aree:

- Servizi in convenzione
- Guide alla richiesta e all'uso
- Servizi per gli utenti

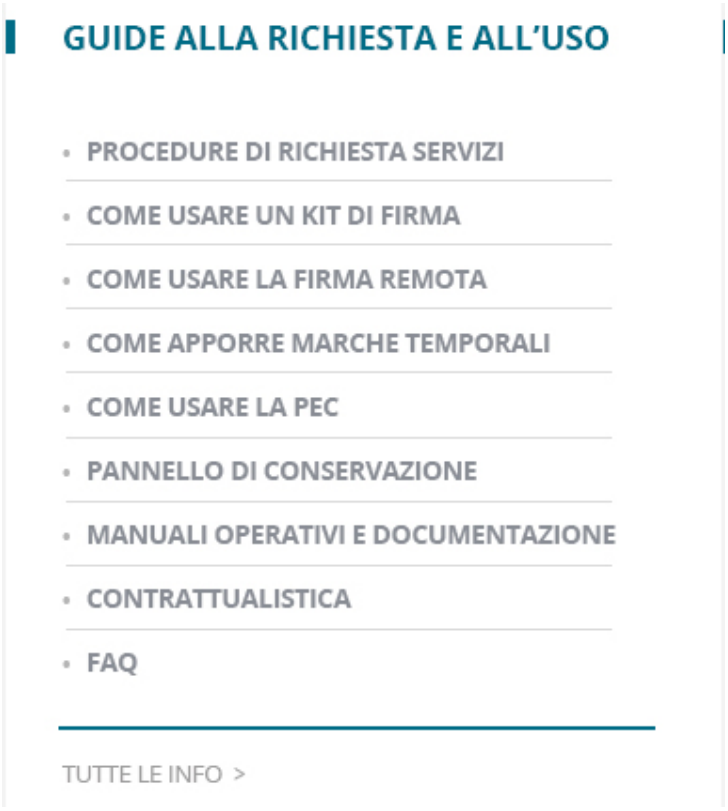
Servizi in convenzione
In questa sezione sarà possibile recuperare maggiori informazioni riguardo ai servizi messi a disposizione degli enti con la convenzione, ai possibili impieghi, ai processi di emissione e alla normativa di riferimento.

In particolare sarà possibile approfondire i seguenti aspetti:

- Informazioni, normativa di riferimento e casistiche di utilizzo dei servizi offerti:
  - Kit di firma digitale (CNS)
  - Firma Remota
  - Marche temporali
  - Certificati SSL
  - Conservazione sostitutiva
  - PEC
- Listino
- Consulenza commerciale

Questa sezione permetterà soprattutto agli utenti che non hanno ancora aderito alla convenzione di ricevere maggiori informazioni sui prodotti e servizi offerti e sui loro possibili impieghi. Oltre al listino di riferimento sarà possibile richiedere una consulenza commerciale che aiuterà l'Ente nell'analisi delle sue esigenze e nella scelta dei servizi più adatti.

Guide alla richiesta e all'uso
Questa sezione conterrà tutte le informazioni utili alle procedure da seguire per la richiesta dei servizi e al loro utilizzo. Sarà pertanto maggiormente destinata agli Enti che hanno già deciso di aderire alla convezione o hanno già richiesto l'attivazione, anche se i contenuti saranno pubblici e raggiungibili da chiunque acceda al sito.



Qui sarà dunque possibile trovare approfondimenti sui seguenti aspetti:

- Procedure di richiesta servizi
- Come usare un kit di firma
- Come usare la firma remota
- Come apporre Marche temporali
- Come usare la PEC
- Pannello di conservazione
- Manuali Operativi e documentazione
- Contrattualistica
- FAQ

Il valore aggiunto di questa sezione sarà quello di fornire tutta la modulistica e contrattualistica necessaria all'Ente per aderire al servizio: quindi una volta esaminate le caratteristiche dei servizi offerti e deciso di aderire potrà direttamente scaricare il materiale necessario e seguire la procedura prevista. In caso di ulteriori dubbi potrà richiedere una consulenza commerciale fornita da Aruba PEC.

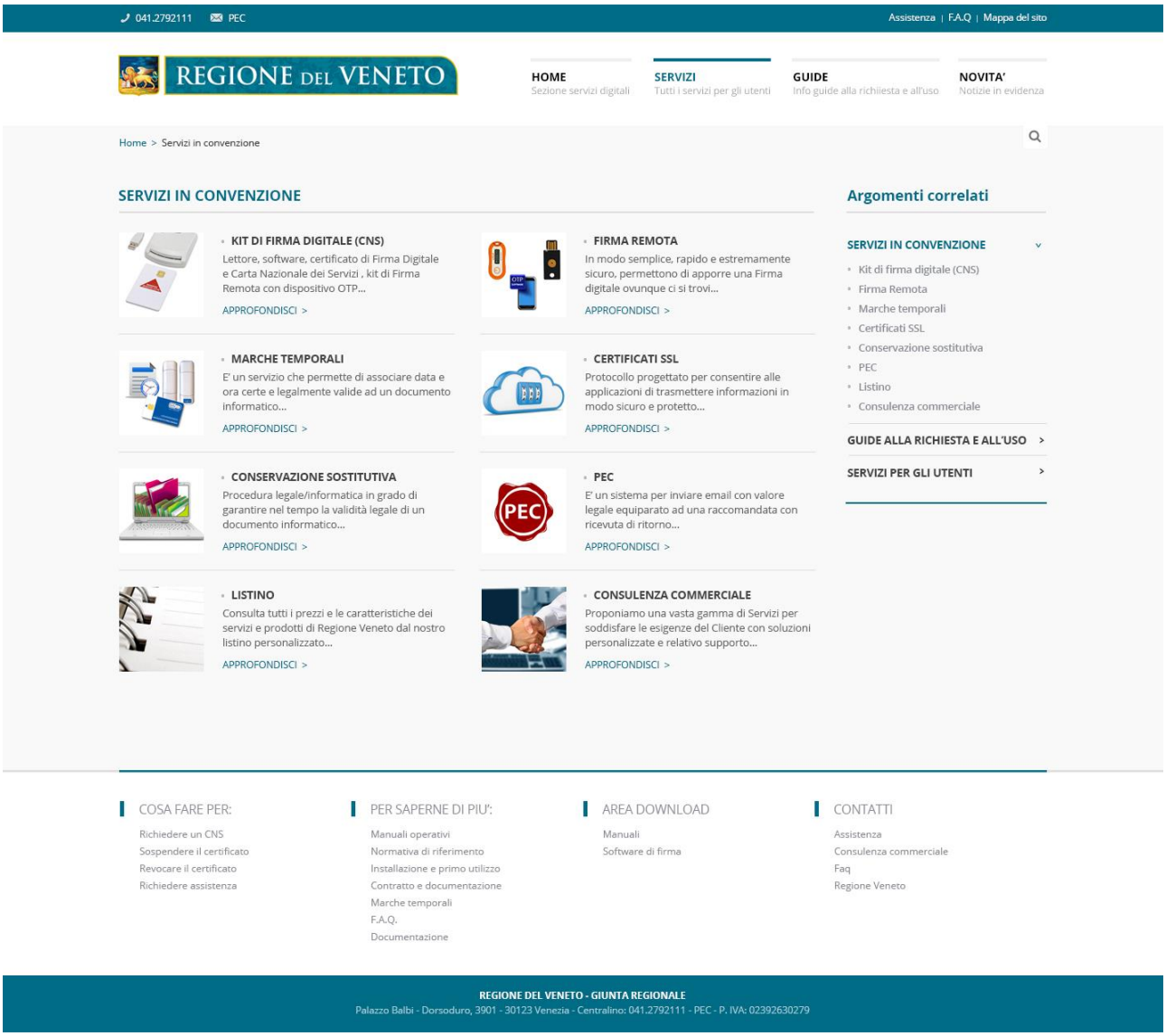
Servizi per gli utenti
Questo sezione fornirà spiegazioni sulle procedure da seguire per la gestione del ciclo di vita dei certificati di firma e fornirà i collegamenti diretti sia al pannello di monitoraggio complessivo dei servizi che della webmail PEC.

All'interno di questa sezione sarà possibile trovare le informazioni necessarie a:

- Assistenza
- Rinnovo certificati
- Attivazione firma remota
- Richiesta sospensione e riattivazione certificati
- Richiesta revoca dei certificati
- Monitoraggio
- Webmail PEC

Cliccando il titolo della sezione si raggiungerà una pagina riepilogativa di tutti i contenuti presenti in quella determinata sezione.
Accanto ai vari contenuti sarà presente una piccola introduzione che permetterà di comprendere meglio le informazioni che saranno presenti nella pagina dedicata.

Ad esempio, cliccando su Informazioni sui Servizi in Convenzione si arriverà ad una pagina simile alla seguente, che permetterà di avere un'anteprima sul contenuto ricercato:



Per garantire la massima raggiungibilità dei contenuti il portale proporrà il link agli stessi anche nell'header. Inoltre il footer proporrà i medesimi contenuti sotto un'altra veste in modo da soddisfare tutte le possibili ricerche e curiosità dell'ente.

Sarà inoltre presente una sezione per la ricerca dei contenuti e la mappa del sito web, in modo che tutte le informazioni siano facilmente rintracciabili dai cittadini interessati al servizio.

Per facilitare la navigazione sarà presente sotto l'header il percorso di navigazione (il cosiddetto *Bread Crumbs*) che permetterà al navigatore di individuare rapidamente la sezione dove si trova e tornare alle precedenti, ad essa collegate.

Informazioni presenti

Il sito web verrà popolato con una serie di contenuti forniti da Aruba PEC, che potranno essere modificati tramite il back end di gestione messo a disposizione.

Oltre ai contenuti, Aruba PEC predisporrà i documenti e manuali utili per l'utilizzo dei servizi da parte degli utenti.

In particolare verranno predisposti almeno i seguenti manuali:

- Manuale operativo CNS: il manuale operativo CNS è il documento che contiene le regole e le procedure operative che governano l'emissione della Carta Nazionale dei Servizi (CNS) e dei relativi certificati. Tale documento deve essere obbligatoriamente predisposto dalla P.A. che emette la CNS.
- Manuali operativi dei certificati di sottoscrizione (firma digitale): il manuale operativo del certificato di sottoscrizione ha lo scopo di illustrare e definire le modalità operative adottate dalle Certification Authority nell'attività di certificazione.
- Manuali operativi dei certificati di sottoscrizione con firma remota: il manuale operativo del certificato di sottoscrizione ha lo scopo di illustrare e definire le modalità operative adottate dalle Certification Authority nell'attività di certificazione.
- Certificate Policy CNS: è il documento che descrive la policy ovvero le regole generali relative all'emissione ed all'utilizzo dei certificati di autenticazione per la Carta Nazionale dei Servizi erogati dal Certificatore accreditato.
- Manuale operativo DocFly: il manuale guida del sistema di conservazione sostitutiva vuole essere per l'utente un valido strumento ai fini di un corretto utilizzo del Pannello di gestione del sistema di conservazione digitale a norma DocFly. All'interno del presente documento sono trattati, pertanto, gli argomenti relativi alla gestione e navigazione all'interno del Pannello Web e le procedure di acquisizione dei documenti da sottoporre a conservazione, tramite l'utenza "Master", con l'intento di soddisfare le esigenze dell'utente che potrà sfruttare al meglio le potenzialità offerte da DocFly.
- Specifiche tecniche DocFly: si tratta del documento tecnico che descrive, nel dettaglio, i canali di integrazione previsti per il sistema di conservazione digitale a norma DocFly e il corretto utilizzo su ciascuna delle interfacce
- Modulistica: il sito sarà inoltre popolato con la modulistica che la Stazione Appaltante riterrà necessaria, quale ad esempio il modulo di revoca dei certificati, i contratti di adesione, atto di affidamento del processo di conservazione, scheda di conservazione, etc...

Tutte le funzioni presenti nel sito saranno di facile ed immediato utilizzo e dotate di documentazione semplice, completa e sempre aggiornata.

Il Portale predisposto sarà navigabile, oltre che dai pc, anche per mezzo di dispositivi mobili quali Smart Phone e tablet, mentre ne sarà garantita una naturale fruibilità anche a quelle classi di utenti svantaggiate. Il sito web pertanto rispetterà tutte le normative in materia di accessibilità di seguito riportate come approfondimento.

Approfondimento – Accessibilità

Si forniranno di seguito informazioni circa l'erogazione, la fruibilità e la qualità dei sistemi informatici nell'ambito del progetto sulla comunicazione elettronica certificata tra il cittadino e le Pubbliche Amministrazioni in relazione alla definizione di accessibilità che viene data nelle specifiche del Dec. Min. 8 lug 2005 : "*la capacità dei sistemi informatici, nelle forme e nei limiti consentiti dalle conoscenze tecnologiche, di erogare servizi e fornire informazioni fruibili, senza discriminazioni, anche da parte di coloro che a causa di disabilità necessitano di tecnologie assistive o configurazioni particolari*".

Il sito web messo a disposizione sarà basato su un Content Management System, che permetterà di modificare, sostituire, rimuovere o aggiungere contenuti e pagine web.
Per poter eseguire quest'attività di aggiornamento è stata prevista un'apposita area di amministrazione del portale a cui potrà accedere solo il personale autorizzato alle modifiche.
L'accesso al pannello di amministrazione avverrà tramite un qualunque browser web digitando l'indirizzo a cui è stato pubblicato il sistema, accedendo alla sezione di amministrazione.
Attraverso l'area amministrativa, quindi, si potranno non solo modificare i contenuti già presenti nel sito, ma creare nuove pagine web, inserire nuove immagini e prevedere nuovi testi.
I profili di accesso previsti saranno di tipo:

- **Amministratore**, in grado di gestire qualsiasi elemento costituente il portale;
- **Redattore**, abilitato alla sola gestione e aggiornamento dei contenuti.

I contenuti iniziali e tutta la documentazione inerente il servizio verranno comunque inseriti nel portale web direttamente dal personale tecnico di Aruba PEC; eventuali e successive integrazioni potranno essere effettuate dallo stesso personale, su indicazione della Regione, o direttamente da quest'ultima una volta entrata in possesso delle credenziali di accesso.

SERVIZIO DI CONSULENZA COMMERCIALE

Quale ulteriore valore aggiunto Aruba PEC garantirà la possibilità di richiedere una consulenza commerciale/informativa sui servizi offerti dalla convenzione.
Più che una consulenza volta ad incentivare l'acquisto dei servizi questo strumento messo a disposizione gratuitamente permetterà agli Enti di valutare insieme ad un esperto le proprie esigenze, di analizzare insieme i processi lavorativi e le procedure necessarie all'adesione ai servizi e alla loro attivazione.
Riteniamo che questo possa essere un valido strumento per garantire il successo dell'iniziativa e contribuire alla diffusione della digitalizzazione tra gli Enti Veneti.

1.2.2 DESCRIZIONE DEI DATA CENTER

Aruba PEC erogherà i servizi oggetto del presente bando attraverso i data center del Gruppo, **certificati ISO 27001**. I data center sono ubicati in territorio italiano.
L'infrastruttura sarà attiva e disponibile in modalità **H24, 365 giorni all'anno** e garantirà la disponibilità sia dei server (fisici/virtuali) che degli elementi network nel data center in conformità a quanto richiesto dal Capitolato Tecnico. La gestione e la manutenzione ordinaria della stessa non produrrà disservizi all'utente. Eventuali fermi programmati per manutenzione straordinaria verranno concordati e autorizzati dall'Amministrazione.
I Data Center assicurano la garanzia dei livelli di sicurezza previsti dalle normative vigenti ed in particolare, come descritto nei capitoli successivi, offriranno:

- un ambiente sicuro e protetto (sicurezza fisica);
- garanzia di riservatezza, integrità e disponibilità delle informazioni trattate (sicurezza logica);
- l'impiego di mezzi idonei e l'adozione di processi e procedure per la gestione sicura delle informazioni (sicurezza organizzativa).

I servizi ed i sistemi coinvolti soddisferanno pienamente:

- Legge 82/2005 e sue successive integrazioni "Codice dell'amministrazione digitale";
- D. Lgs. 196/2003 "Testo unico delle disposizioni in materia di privacy" (in particolare quanto previsto per gli Amministratori di Sistema).

1.2.2.a. DATA CENTER PRIMARIO

Di recentissima apertura, il nuovo data center di Aruba è uno dei pochi in Italia a rispondere ai requisiti tecnici previsti dalla normativa **ANSI/TIA 942-A** necessari a garantire i livelli di uptime

propri del **Rating IV (ex Tier)**: tutta l'infrastruttura è ridondata in modo da poter funzionare anche in caso di guasto nei sistemi elettrici e di condizionamento. Inoltre l'impianto elettrico è stato realizzato in modo che qualsiasi componente dello stesso possa essere rimossa per guasti o manutenzione senza che nessun sistema subisca disservizio. L'azienda e il data center sono certificati **ISO27001** per la sicurezza delle informazioni.
Il data center, che ha una superficie pari a 4.000 mq dedicata alle sole sale dati e locali di presidio, è progettato per contenere a pieno regime circa 40.000 server in 1.100 armadi rack, per una potenza elettrica assorbita dai soli server ed apparecchiature informatiche di circa 4,5 MW, in ridondanza **2*n**.

Adiacenti all'edificio principale, ma separati da esso per motivi di sicurezza, si trovano:

- un ulteriore edificio che ospita i **Power Center** che alimentano i server ed il sistema di condizionamento
- una costruzione per ciascuno dei due rami dell'impianto (distanti 6 metri dai **Power Center**) - dedicate ad ospitare le batterie di alimentazione del sistema **UPS**

Tutti gli edifici rispondono alle normative sismiche. La scelta di separare i Power Center e i locali batterie dal resto del data center è stata adottata per annullare il rischio che eventi accidentali a queste componenti possano influire sul regolare funzionamento del data center o danneggiare i server.

La progettazione e realizzazione del **data center Aruba** è avvenuta seguendo le direttive impartite dall'ANSI/TIA 942-A per rispondere al massimo livello di Rating ovvero il 4. Il data center è stato infatti costruito in modo che qualsiasi componente necessaria per il funzionamento dei server ospitati possa venire meno, per guasto o necessità di manutenzione, senza che il servizio ne risenta, attraverso la ridondanza di tutti i componenti a servizio dell'alimentazione elettrica e del raffrescamento dei server (quali ad esempio trasformatori, UPS, STS, gruppi elettrogeni Diesel, Chiller, unità di condizionamento).

Tutto ciò viene garantito indipendentemente dalla presenza o meno di forniture e fattori esterni, prevedendo all'interno del data center stesso scorte (in primis di carburante per i gruppi elettrogeni Diesel, ma anche di tutto il resto che fosse necessario) per poter funzionare per nel caso in cui le forniture di energia elettrica o altre utenze dall'esterno risultassero interrotte.
In ultimo, la possibilità di usufruire di un network di datacenters multipli distribuiti su territorio nazionale e all'estero consente di realizzare piani di Disaster Recovery e Business Continuity per i sistemi "mission critical" che li richiedono.

Le sale dati sono dotate di sistemi di condizionamento e la connettività è ridondata in modo da garantire la massima affidabilità e il massimo uptime dell'infrastruttura. Il **data center** è monitorato e **presidiato 24h su 24h, 365 giorni all'anno** e l'accesso alla struttura è permesso solo a seguito di riconoscimento e registrazione.

Altre informazioni salienti:

- **5 MW** di **potenza elettrica ridondata**, più 2 MW per il condizionamento;
- Oltre **80 Gb/s** di **connettività Internet** (almeno il doppio della capacità trasmissiva necessaria per garantire continuità e qualità dei servizi);
- **interconnessione col data center IT2** attraverso cavi privati multi-fibra, su due percorsi differenti;
- impianto **antincendio** automatico a gas inerte;
- impianto di **condizionamento**;
- sistema di **rilevamento liquidi**;
- impianto **antintrusione**;

- **controllo accessi fisici**.


L'accesso alla struttura è permesso solo a seguito di riconoscimento e registrazione.

1.2.2.b. DATA CENTER SECONDARIO

Questo data center ha una superficie di circa **2000 m²** e può ospitare **fino a 10.000 server** (attualmente ne ospita circa 7.500). Dispone di **3 sale dati** comprendenti in totale circa 500 armadi atti ad ospitare server con una capacità totale di oltre 250 TB. Ogni sala dati è provvista di:

- **alimentazione elettrica protetta e ridondata** su 2 linee indipendenti;
- **connettività Internet ridondata e distribuita** (in modo da garantire il massimo della sicurezza perimetrale e ambientale e prevenire così ogni eventuale perdita di dati).
- impianto **antincendio** automatico a gas inerte;
- impianto di **condizionamento**;
- sistema di **rilevamento liquidi**;
- impianto **antintrusione**;
- controllo accessi fisici.

È inoltre presente un apposito locale nel quale sono allocati esclusivamente gli UPS ed i quadri di distribuzione generale dell'energia elettrica.


Anche questo data center dispone di un **NOC** (**Network Operation Center**) dove operatori qualificati garantiscono **monitoraggio e assistenza 24hx7, 365 giorni/anno**.

Per quanto riguarda la **connettività**: questo Data Center è interconnesso ai backbone dei principali provider nazionali di accesso (ossia providers che forniscono collegamenti agli utilizzatori finali), quali Telecom Italia, Wind ed Eutelia. A tali provider è stato scelto di abbinare due dei principali carrier internazionali, Cogent Communications ed Interoute, in modo da instradare in modo ottimale il traffico con l'estero. A completamento delle interconnessioni, questo data center è collegato sol MIX (Milan Internet Exchange) e col NAMEX (Nautilus Mediterranean eXchange point), i principali NAP (Neutral Access Point) nazionali. Tale assetto consente di ottimizzare gli instradamenti, a prescindere dalla provenienza/destinazione del traffico, con importanti effetti in termini di performance.
Il **sistema elettrico** garantisce la continuità dell'energia ed è costituito da:

- due gruppi elettrogeni diesel da 1540 kVA cadauno funzionanti in parallelo (potenza totale 3080 kVA), che si attivano in caso di mancanza di energia elettrica di rete;
- 5 UPS a batterie da 500 kVA cadauno funzionanti in parallelo (potenza totale di 2500 kVA), con ridondanza di tipo almeno n+1 a pieno carico – necessarie a garantire l'alimentazione, la protezione e l'isolamento dei server, degli apparati di networking e delle linee elettriche;
- due trasformatori MT-BT separati da 2500 kVA ciascuno, di cui ogni trasformatore alimenta uno dei due rami che costituiscono l'impianto elettrico (con ridondanza di tipo 2*n).

Ogni sala dati dispone di due linee elettriche separate che si dividono ulteriormente a livello di quadro di fila, cosicché ogni singolo armadio rack dispone di 4 linee di alimentazione separate 230V 16A monofase.

1.2.2.c. GESTIONE DELLA SICUREZZA ED AFFIDABILITÀ

Aruba PEC è azienda certificata ISO 27001 pertanto svolge le proprie attività ponendo al centro la sicurezza dei dati. I data center che verranno utilizzati per il servizio offrono le massime garanzie di sicurezza fisica, logica ed organizzativa come descritto nei successivi paragrafi.

Piano di Disaster Recovery
Aruba PEC ha sviluppato e adotta appositi piani di Disaster Recovery e Business Continuity allo scopo di gestire e mediare i rischi cui può essere soggetta.
Tali documenti definiscono ed elencano le azioni da intraprendere prima, durante e dopo una condizione di emergenza per assicurare il ripristino (Disaster Recovery) e la continuità (Business Continuity) dei servizi erogati. Vengono inoltre elaborati piani per progetti specifici qualora il cliente, come in questo caso, li richieda.
Essi forniscono indicazioni e dove possibile istruzioni passo-passo atte ad assicurare la continuità dei servizi critici di Aruba PEC anche in presenza di eventi indesiderati che possano causare il fermo prolungato dei sistemi informatici.
Il datacenter che costituisce il sito primario è situato in un'area classificata come di "basso rischio idrogeologico", inoltre l'edificio è completamente antisismico ed è posto ad un piano rialzato dal livello stradale, in modo da risultare maggiormente protetto alle calamità naturali. L'intero Datacenter è continuamente monitorato sia in sede locale che in più sedi remote ed è dotato delle soluzioni di sicurezza più avanzate descritte in seguito. La struttura è inoltre collegata direttamente con un secondo Datacenter, sempre di proprietà di Aruba, che rappresenta la sede di Disaster recovery.

Il Piano di Disaster Recovery è stato redatto tenendo presente le "Linee Guida per il disaster recovery delle PA" dell'Agenzia per l'Italia Digitale, ex DigitPA ed è dunque ispirato al ciclo di Deming (Plan, Do, Check, Act) prevedendo, dopo la fase iniziale di studio/analisi del contesto, il disegno della soluzione tecnologico-organizzativa che meglio risponde alle esigenze di continuità richieste, la realizzazione e il mantenimento della soluzione. Tale piano verrà dettagliato maggiormente in fase di setup dell'infrastruttura.

1.2.2.d. LA SICUREZZA FISICA DEI DATA CENTER

Nelle due strutture che verranno messe a disposizione per l'erogazione dei servizi viene data grande importanza alla sicurezza degli ambienti e dei dati in essi contenuti. Per questo sono presenti tutta una serie di sistemi che permettono di garantire integrità degli ambienti e dei servizi.

In entrambi i Data Center è prevista la presenza di personale nel NOC h24 x 7 x 365, che, anche agli ausili dei sistemi di monitoraggio, antintrusione e di videosorveglianza, è in grado di effettuare un efficace controllo fisico degli accessi.

Sicurezza Fisica Data Center Primario

L'edificio è stato progettato ponendo la massima attenzione alla **sicurezza fisica degli accessi**:

- le **porte esterne** sono di tipo blindato;
- le **finestre** e le **superfici vetrate esterne** a piano terra sono dotate di vetro antiproiettile dello spessore di 21 mm;
- le **griglie per il passaggio dell'aria** necessaria al raffreddamento della sala dati sono protette da sbarre trasversali in acciaio del diametro di 20 mm.

L'**accesso dei visitatori** avviene attraverso una "**bussola**" a due ante rotanti e interbloccate, analoga a quelle normalmente utilizzate negli istituti bancari - anch'essa dotata di vetri anti-proiettile da 21 mm di spessore. Una volta avuto accesso all'interno, è presente una seconda barriera, costituita da varchi motorizzati. Per attraversare tali varchi è necessario essere accreditati alla antistante Reception, con lo scopo di ottenere un badge abilitato. Per la registrazione dei visitatori, è istituito un apposito registro conservato in conformità con quanto previsto dalla **normativa ISO 27001**.
Superata la barriera dei varchi motorizzati, si trova davanti la sala dati principale, delimitata da una parete in vetro antiproiettile da 21 mm. L'accesso, consentito solo al personale abilitato, avviene tramite porte scorrevoli di sicurezza assoggettate al controllo accessi. L'intero stabile è circondato da una resede che lo separa su tutti i lati dalle altre proprietà, e protetto da una recinzione rigida in metallo dell'altezza di 260 cm. La struttura è presidiata e sorvegliata 24x7x365.

Accesso controllato tramite autenticazione

Il **data center** è dotato di un **sistema di controllo accessi** esteso a tutti i varchi, sia esterni (ingresso principale, uscite di sicurezza, magazzini, locali tecnici) che interni (sale dati, locali tecnici, uffici). Il riconoscimento è basato su un doppio criterio di autenticazione, mediante l'utilizzo di una tessera di prossimità e la digitazione di un pin. Il sistema di gestione degli accessi prevede la possibilità di abilitare e disabilitare le singole tessere in base alle aree, agli orari ed ad altri parametri, in modo da garantire sia la massima sicurezza degli ambienti che la necessaria fluidità degli accessi. E' possibile generare dettagliati report (per utente, per varco, per data) in modo da ricostruire con la massima precisione - se necessario - i percorsi effettuati da ogni singolo visitatore.

Impianto anti-intrusione

L'edificio è dotato di un **sistema anti-intrusione** che utilizza sensori volumetrici a doppia tecnologia, assieme a sensori a contatti su infissi e sensori di vibrazione sui vetri delle sale dati.
L'impianto è integrato da sistemi evoluti di analisi delle immagini rese disponibili dall'impianto di video-sorveglianza (trattato di seguito). La resede esterna è protetta tramite barriere a raggi infrarossi applicate lungo tutto il perimetro della recinzione esterna. L'impianto anti-intrusione è integrato con il sistema di controllo accessi.

Impianto di video-sorveglianza

L'**impianto di video-sorveglianza** è costituito da un cospicuo numero di telecamere (oltre 120) posizionate sia all'interno dell'edificio (lungo tutti i punti di passaggio e all'interno dei locali

sensibili) che all'esterno (lungo la recinzione, sulla copertura dell'edificio e nella zona dove sono ubicati i gruppi elettrogeni). Le telecamere utilizzate sono di tipologie diverse in base alle diverse esigenze derivanti dai singoli posizionamenti (angolo e distanza di visuale, tipologia di illuminazione, ecc). Le immagini vengono rese disponibili in real-time al personale di presidio mediante appositi monitor presenti all'interno del **NOC**.
Tutte le immagini acquisite vengono immagazzinate tramite videoregistratori digitali, situati in ambienti protetti e conservate per 24H, come previsto dalle vigenti **normative in ambito Privacy**.

Impianto rilevamento fumi e spegnimento incendio

Tutto l'edificio è dotato di un **sistema di rilevamento dei fumi** costituito da sensori ottici posizionati in ambiente, sotto al pavimento flottante e sopra il controsoffitto. I sensori sono collegati tra loro in loop e mediante cavo antifiamma, in modo da garantire il loro funzionamento anche in caso di interruzione di un collegamento. Sono stati previsti opportuni sensori in grado di verificare la presenza di fumo all'interno delle condotte per il ricambio dell'aria degli ambienti.
La gestione dell'impianto è demandata ad una centrale a 6 loop, con il compito di rilevare i segnali provenienti dai sensori, attivando gli allarmi ottici e acustici, nonché provvedendo all'attivazione dell'impianto di spegnimento mediante apposite unità di spegnimento. Le aree sensibili e/o a maggiore rischio (2 sale dati, 2 sale tlc, 6 power center, 6 sale trasformatori MT e 2 sale quadri MT) sono dotate di sistema di spegnimento a gas inerte (Azoto).

Il **metodo di spegnimento** è quello della diluizione d'ossigeno, ottenuto mediante una scarica di un'adeguata quantità di azoto in grado di ridurre la percentuale di ossigeno dal 23% presente normalmente in atmosfera al 12% circa, valore che non consente la combustione. Tale scarica non rappresenta un pericolo per la salute delle persone eventualmente ancora presenti nell'ambiente al momento della scarica (comunque annunciata con un anticipo di 60 secondi da allarmi acustici e ottici) e preserva gli apparati consentendo la continuità nell'erogazione dei servizi.
I gruppi elettrogeni di emergenza presenti, posizionati all'esterno, sono dotati di impianti di rilevazione e di spegnimento incendi (ad anidride carbonica) dedicati e autonomi. Tali gruppi sono dotati inoltre di sistema di intercettazione del carburante, in grado di interrompere l'afflusso in caso di incendio. E' inoltre presente la normale dotazione di estintori portatili e carrellati.

Impianto di rilevamento liquidi e sistema antiallagamento

I vari locali dell'edificio sono dotati di sensori per il **rilevamento della presenza di liquidi**, posizionati sotto il pavimento flottante. Per quanto riguarda la possibilità di allagamento derivante da rottura delle tubazioni per l'acqua dei servizi igienici (o dalla dimenticanza di rubinetti aperti), è stato previsto un sistema costituito da sensori (flussostati e rilevatori di presenza) e da una logica che, nel caso in cui venga rilevato il flusso di acqua in assenza di persone all'interno dei singoli servizi igienici, provvede all'interruzione dell'erogazione dell'acqua nel medesimo ambiente tramite l'attivazione di una elettrovalvola, eliminando la possibilità di riversamento di acqua a terra.
Le eventuali problematiche derivanti da alluvioni sono scongiurate, in quanto la struttura è ubicata in zona pianeggiante ed in posizione rilevata di circa un metro rispetto al piano di campagna. In fase progettuale si è provveduto inoltre a evitare il posizionamento di impianti strategici o di parte di essi a quota inferiore a tale valore: ciò esclude la necessità di sistemi anti-allagamento dotati di pompe idrauliche.

Sicurezza degli apparati

I server dislocati presso il Centro Servizi saranno dotati di meccanismi di sicurezza fisica utili ad impedire il furto locale dei dati. Gli armadi rack sono tutti dotati di sportelli metallici con serratura a chiave e i supporti di memorizzazione contenenti dati sono conservati in luogo sicuro. Gli apparati attivi di rete saranno posizionati in armadi di cablaggio con chiusura a chiave che inibisce l'accesso fisico ai dischi locali e ne impedisce la rimozione.

BMS

Tutti gli impianti sopradescritti, assieme agli impianti e sistemi strategici (gruppi elettrogeni, ups, quadri elettrici, condizionamento di potenza) e agli impianti standard (illuminazione, condizionamento uffici) sono supervisionati da un sistema **BMS** (**Building Management System**) a mappe, in grado di gestire tutti gli eventi e gli allarmi, di interpretarli e di assegnare loro le opportune priorità, generando le conseguenti notifiche in modo da ridurre al massimo i tempi di interpretazione e individuazione degli eventi. Il **BMS** - controllato dal personale di presidio del **NOC** (**Network Operation Center**) - è accessibile anche da remoto ed in grado di provvedere alla notifica degli allarmi tramite i consueti canali (e-mail, SMS, ecc).

Sicurezza fisica Data Center Secondario

La **sicurezza fisica** del **data center** secondario viene garantita attraverso:

- un sistema di video-sorveglianza che utilizza telecamere motorizzate per tenere sotto controllo i punti nevralgici della struttura;
- un sistema di allarme che rileva automaticamente eventuali vibrazioni o aperture non autorizzate di ingressi e di infissi;
- un impianto anti-intrusione – monitorato dal NOC - che utilizza rilevatori di presenza a doppia tecnologia (micro-onde e raggi infrarossi), contatti magnetici e barriere a raggi infrarossi per proteggere le zone in cui gli ambienti sono suddivisi e prevenire l'apertura non autorizzata di ingressi ed infissi;
- sistema di controllo accessi che permette l'accesso al solo personale autorizzato, dotato di badge con tecnologia RFID e codice PIN personale;
- un sistema anti-incendio a gas inerti (non tossici) - connesso a rilevatori di fumo posti sopra e sotto al pavimento flottante – che si attiva automaticamente inondando di gas solo la zona colpita;
- un sistema di rilevazione liquidi che permette di intercettare - dal NOC e tramite appositi allarmi acustici in loco - eventuali fuoriuscite di liquido dagli impianti tecnologici;
- un sistema centrale server per archiviare e consultare (da personale autorizzato tramite accesso protetto) qualsiasi accesso ai locali, che solo avviene attraverso RFID associato a codice numerico.

Anche nel sito secondario, i server saranno dotati di meccanismi di sicurezza fisica utili ad impedire il furto locale dei dati: gli armadi rack sono provvisti di sportelli metallici con serratura a chiave; i supporti di memoria dati sono conservati in un luogo sicuro ed i server sono protetti da un apposito sportello con chiusura a chiave (come inibizione dell'accesso fisico e della rimozione).

1.2.2.e. SICUREZZA ORGANIZZATIVA COMUNE AI DUE DATA CENTER

Aruba PEC garantisce inoltre la sicurezza organizzativa delle strutture, che verrà adeguata in caso di evoluzioni delle normative. Il sistema di registrazione dei log per tutti i servizi erogati è infatti conforme alle normative vigenti e verrà adeguato in caso di evoluzioni.
A tale proposito viene garantito che:

- i processi attuati per il monitoraggio e la rilevazione di eventuali intrusioni o anomalie sono regolati e descritti all'interno del **Piano di Sicurezza dei Data Center**;
- l'accesso alle informazioni riservate dell'Amministrazione sarà permesso solo a personale autorizzato, in conformità al **D.Lsg. 196/2003** e successive modifiche;
- l'erogazione di servizi e dei sistemi coinvolti sia conforme alla **Legge 82/2005** (Codice Amministrazione Digitale).

Aruba PEC garantisce che tutti gli apparati necessari all'erogazione dei servizi saranno gestiti solo da personale univocamente individuato e che gli aspetti di sicurezza vengano attuati in base a procedure documentate. All'interno del piano della sicurezza delle strutture, redatto sulla base delle linee guida della certificazione ISO27001, sono documentati:

- accesso fisico delle persone agli edifici in cui sono situati apparati;
- accesso fisico delle persone ai locali contenenti apparati;

- regole per l'accesso da parte di personale esterno (fornitori, addetti alla manutenzione, visitatori, etc.);
- gestione degli strumenti per l'accesso ad eventuali casseforti ed armadi blindati (combinazioni delle casseforti, chiavi degli armadi, etc.);
- gestione degli archivi cartacei (regole per la conservazione, modalità di consultazione, eventuale registrazione degli accessi, etc.);
- gestione di situazioni anomale;
- ripristino dell'interruzione dell'erogazione di energia elettrica;
- procedure di backup e di restore;
- procedure di escalation.

Le **postazioni di lavoro** si trovano in uffici interdetti all'accesso del pubblico. Le postazioni condivise, messe a disposizione della clientela, risiedono su reti e uffici separati (sale riunioni attrezzate), e sono dotate di opportune limitazioni di accesso.
Per l'**accesso alle postazioni di lavoro**, i dipendenti dispongono di token hardware personali protetti da apposito **PIN** associato a credenziali nella forma nome.cognome e password, di tipo strong, conosciute solo dagli stessi. Attraverso l'**Active Directory aziendale** è possibile offrire cambio password con obbligo di password in base a policy standard condivise.
L'accesso ai server viene garantito attraverso le stesse credenziali personali sia per ambienti windows che per ambienti linux. Le password vengono mantenute nella massima riservatezza e non possono essere trascritte.
Tutti i log di accesso ai server sono centralizzati su un apposito server. Ogni notte viene generato un report e mandato all'addetto di controllo dei report. Esso con cadenza giornaliera controlla tale report e verifica la regolarità degli accessi, verificando che non ci siano accessi da reti esterne, che non ci siano accessi con esito negativo e che non ci siano accessi di personale che non aveva motivo di accedere. Se la verifica ha avuto esito positivo vengono eseguite verifiche sui controlli e informato immediatamente il responsabile della sicurezza.

1.2.2.f. SICUREZZA LOGICA DEI SISTEMI E DEGLI APPARATI

I protocolli ed i servizi utilizzati per la gestione degli apparati (SNMP, RADIUS, NTP, Log, LDAP) vengono erogati solo verso le reti di management mediante l'utilizzo di ACL (Access Control List). All'interno delle reti dedicate, se il protocollo/servizio lo supporta, è in ogni caso necessario autenticarsi.
Tutti i protocolli previsti per l'accesso ed il controllo dei sistemi sono di tipo sicuro cifrato, prevedendo ssh, https o rdp.
All'interno dei singoli apparati i servizi non necessari vengono disattivati e quelli necessari vengono erogati solo verso le interfacce che richiedono che tali servizi vengano resi disponibili.
Le politiche e le conseguenti architetture e configurazioni di rete adottate garantiscono fra l'altro:

- L'impossibilità di effettuare IP spoofing da un qualsiasi utente connesso direttamente alla rete
- L'impossibilità di effettuare attacchi smurf, fraggle, land tramite limitazione nell'accesso agli indirizzi di broadcast e filtraggio dei pacchetti che riportano un indirizzo sorgente palesemente scorretto
- La capacità di reagire tempestivamente a qualsiasi tipo di attacco alle proprie infrastrutture anche tramite la possibilità di configurare in qualsiasi punto della rete qualsiasi regola di filtraggio atta a mitigare il fenomeno evidenziato

Gli enti/gruppi che operano sulla configurazione dei sistemi hanno diverse esigenze in termini di necessità d'accesso alle classi d'apparati. L'autorizzazione all'accesso alla configurazione di un apparato è nominale, non di gruppo. L'accesso ad una specifica classe d'apparati dipende dall'appartenenza dell'utente ad uno specifico gruppo. L'associazione dell'utenza al Gruppo permette di confinare l'accesso degli utenti ai soli apparati la cui gestione è in carico al Gruppo. Sulla base di tale appartenenza, l'utente potrà autenticarsi sull'apparato utilizzando una login ed

una password personali nel caso di apparati con tecnologia IP mentre per quanto riguarda apparati di trasporto (SDH e DWDM) l'autenticazione si esegue a livello dei sistemi di gestione. Sono stati inoltre introdotti dei meccanismi di gestione delle password (lunghezza minima, presenza di caratteri numerici, ecc.) di enable e delle password locali in modo da ottenere un bilanciamento tra l'esigenza di avere un adeguato livello di sicurezza e le esigenze di implementazione/gestione delle linee guida.
L'inserimento di un nuovo utente in un gruppo deve essere richiesto dal responsabile del gruppo stesso. La richiesta deve pervenire via e-mail all'apposita casella di posta nel caso della rete IP o all'amministratore di rete nel caso di accesso agli apparati di rete di Trasporto.
Successivamente alla configurazione dell'utente, sarà inviata e-mail di conferma all'utente stesso ed al responsabile del gruppo. La rimozione di un utente da un gruppo deve essere richiesta dal responsabile del gruppo stesso. La richiesta deve pervenire via e-mail all'apposita casella di posta nel caso della rete IP o all'amministratore di rete nel caso di accesso agli apparati di rete di trasporto.
Successivamente alla rimozione dell'utente, sarà inviata e-mail di conferma all'utente stesso ed al responsabile del gruppo. Le password utilizzate dagli utenti dovranno seguire le seguenti regole:

1. Non inferiori agli 8 caratteri (in accordo con la legge delega 127/2001 Allegato B comma 7)
2. Non devono essere facilmente indovinabili. Nomi propri, nomi di prodotti, nomi di Clienti ecc.. sono da evitare
3. Devono contenere caratteri misti: minuscole, maiuscole, numeri, spazi, caratteri speciali (@, %, $ ecc.)
4. Non devono coincidere con le password utilizzate per altri servizi di rete.

L'utente viene invitato a cambiare con regolarità la sua password utente. Nel caso l'utente decidesse di non cambiare la propria password vengono adottate le seguenti misure:

- Trascorsi due mesi, dall'ultimo cambio di password effettuato, l'utente riceverà dei solleciti settimanali per cambiare la propria password
- Passati tre mesi, dall'ultimo cambio di password effettuato, l'utente non potrà accedere agli apparati e sarà obbligato ad utilizzare un'opportuna procedura via web che lo condurrà a modificare la propria password utente.

La procedura descritta nel presente paragrafo permette di sospendere gli account associati a fornitori o ai dipendenti non più presenti, nei casi in cui la cancellazione non sia stata segnalata debitamente dal responsabile di gruppo.

1.2.3 MANUTENZIONE SERVIZI

I servizi offerti saranno disponibili, 24 ore al giorno e 7 giorni su 7 nel rispetto degli SLA previsti dal capitolato e monitorati attraverso lo strumento fornito da Aruba PEC e descritto nel Capitolo 7.

I fermi programmati e gli interventi di manutenzione straordinaria, ossia le interruzioni del servizio necessarie per svolgere attività di manutenzione verranno preferibilmente effettuati nella fascia oraria notturna, previa comunicazione scritta agli Enti Aderenti, da inviare con un anticipo di almeno 5 giorni lavorativi.

Oltre ai servizi di help desk erogati nelle modalità descritte nel Capitolo 5, Aruba PEC si impegna a fornire manutenzione **Correttiva ed Evolutiva/Adeguativa** dei sistemi offerti per tutta la durata dell'appalto senza oneri aggiuntivi, fornendo tutti gli aggiornamenti necessari per adeguare le modifiche alle normative o correzioni di malfunzioni. Regione del Veneto e gli Enti Aderenti saranno tempestivamente informati di qualsiasi variazione dovesse rendersi necessaria alle informazioni precedentemente comunicate e agli oggetti del servizio.

Il servizio di manutenzione **Correttiva ed Evolutiva/Adeguativa** – per tutta la durata del contratto - comprende:

- l'aggiornamento dei prodotti software (software client) all'ultima versione;

- l'adeguamento e aggiornamento dei prodotti software (software client) a fronte di mutamenti legislativi e/o aggiornamenti dei sistemi, quali sistemi operativi, browser ecc.;
- l'adeguamento della piattaforma software (interfaccia, strumento di monitoraggio, sito ecc.) ed il rilascio di nuove versioni (a garanzia del mantenimento ottimale del livello di funzionamento dell'intero sistema);
- la tempestiva fornitura di informazioni e oggetti modificati nel caso vi fossero evoluzioni nei dispositivi o nelle librerie o nelle modalità di gestione correlate.

Viene inoltre garantito l'aggiornamento di tutte le informazioni fornite per l'erogazione dei servizi.

1.2.3.a. MANUTENZIONE CORRETTIVA

Per manutenzione correttiva si deve intendere l'attività volta alla rimozione dei difetti del software tramite sviluppo ed applicazione di modifiche. Per supportare i processi di diagnosi delle problematiche saranno previsti meccanismi di logging, sia lato server che lato client.

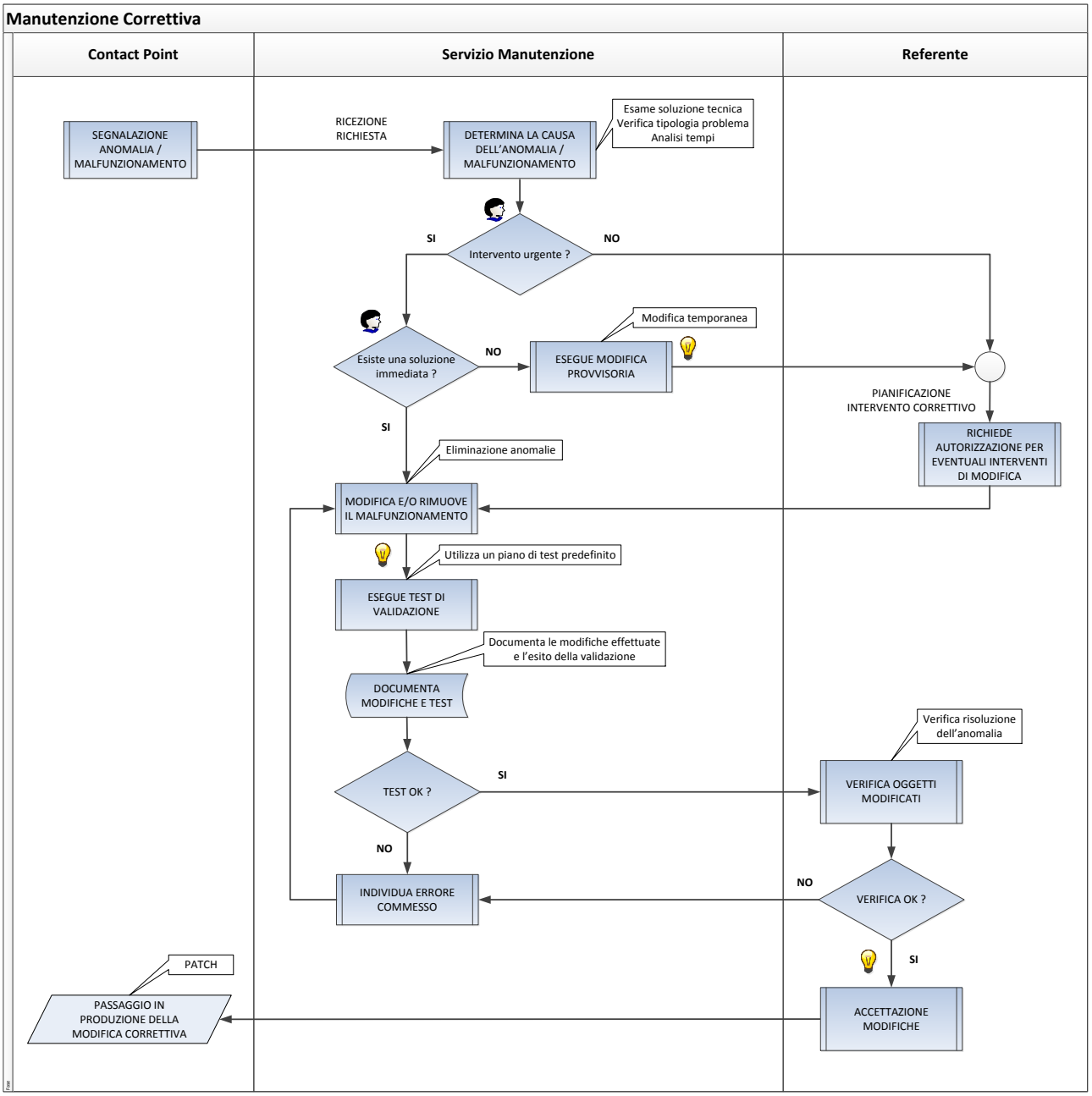
A fronte della segnalazione di un malfunzionamento Aruba PEC garantirà, nel rispetto degli SLA, di:

- comunicare la presa in carico del malfunzionamento;
- comunicare la data prevista di risoluzione del malfunzionamento riscontrato;
- procedere alla realizzazione della soluzione alla problematica riscontrata che verrà rilasciata in un ambiente di test, per verificare la corretta integrazione con i software o applicativi degli Enti nei casi necessari;
- concordare il rilascio della soluzione in produzione;
- comunicare l'avvenuto rilascio.

All'interno del processo di manutenzione correttiva vengono di seguito evidenziate, in particolare, le seguenti tre fasi:

- la presa in carico della problematica riscontrata;
- l'avvio degli interventi per correggere la problematica riscontrata;
- la fase di conduzione degli interventi.

Nel corso delle attività di analisi e/o rimozione di un malfunzionamento, la funzione di manutenzione correttiva, quando opportuno, fornirà al Help Desk le nuove soluzioni applicative da inoltrare agli utenti finali.
Nella seguente figura si riporta il diagramma di flusso relativo al processo di manutenzione correttiva:



1.2.3.b. MANUTENZIONE EVOLUTIVA E ADEGUATIVA

Tutti i prodotti e servizi oggetto della fornitura sono garantiti da Aruba PEC pienamente conformi alla normativa vigente in tema di Firma Digitale e di Carta nazionale di Servizi, Posta Elettronica Certificata e Conservazione Digitale a norma e in ogni caso a tutte le norme di riferimento citate nel Capitolato Tecnico.

Aruba PEC garantirà anche il continuo e completo adeguamento a variazioni di ambienti tecnologici e/o a sopravvenute variazioni normative dei servizi e dei prodotti.
Aruba PEC si impegna dunque a monitorare l'evoluzione della normativa applicabile ai prodotti e servizi oggetto della presente fornitura per individuare tempestivamente l'introduzione di nuove regole, requisiti, standard tecnici ecc. con impatto su quanto erogato alla Regione del Veneto e agli Enti Aderenti.

A tal fine Aruba PEC metterà a disposizione un ambiente di collaudo nel quale verranno rilasciate le diverse release di sistema al fine di eseguire gli opportuni test e procedere poi all'autorizzazione alla messa in produzione.

In particolare, Aruba PEC garantisce di:

- comunicare la necessità di adeguamento;
- comunicare il piano di adeguamento;
- procedere alla realizzazione necessaria;
- rilasciare la nuova release in ambiente di collaudo;
- rilasciare la nuova release in ambiente di produzione;
- comunicare l'avvenuto rilascio della soluzione.

Di seguito si riporta una descrizione del processo di manutenzione adeguativa e dell'organizzazione che verrà adottata per garantire gli adeguamenti entro in tempi previsti dalle normative di riferimento e comunque in data concordate con gli Enti.

Analisi delle modifiche

A fronte della rilevazione dell'esigenza di svolgere un'attività di manutenzione adeguativa sui prodotti e/o servizi forniti, Aruba PEC provvederà a comunicarlo a Regione del Veneto sottoponendo un documento di "Analisi delle Modifiche", nel quale saranno descritte le modifiche necessarie, il campo di applicazione, la criticità di ciascuna modifica e le eventuali alternative di implementazione, nonché il **piano di adeguamento** proposto per la attuazione delle modifiche.

Attuazione delle modifiche

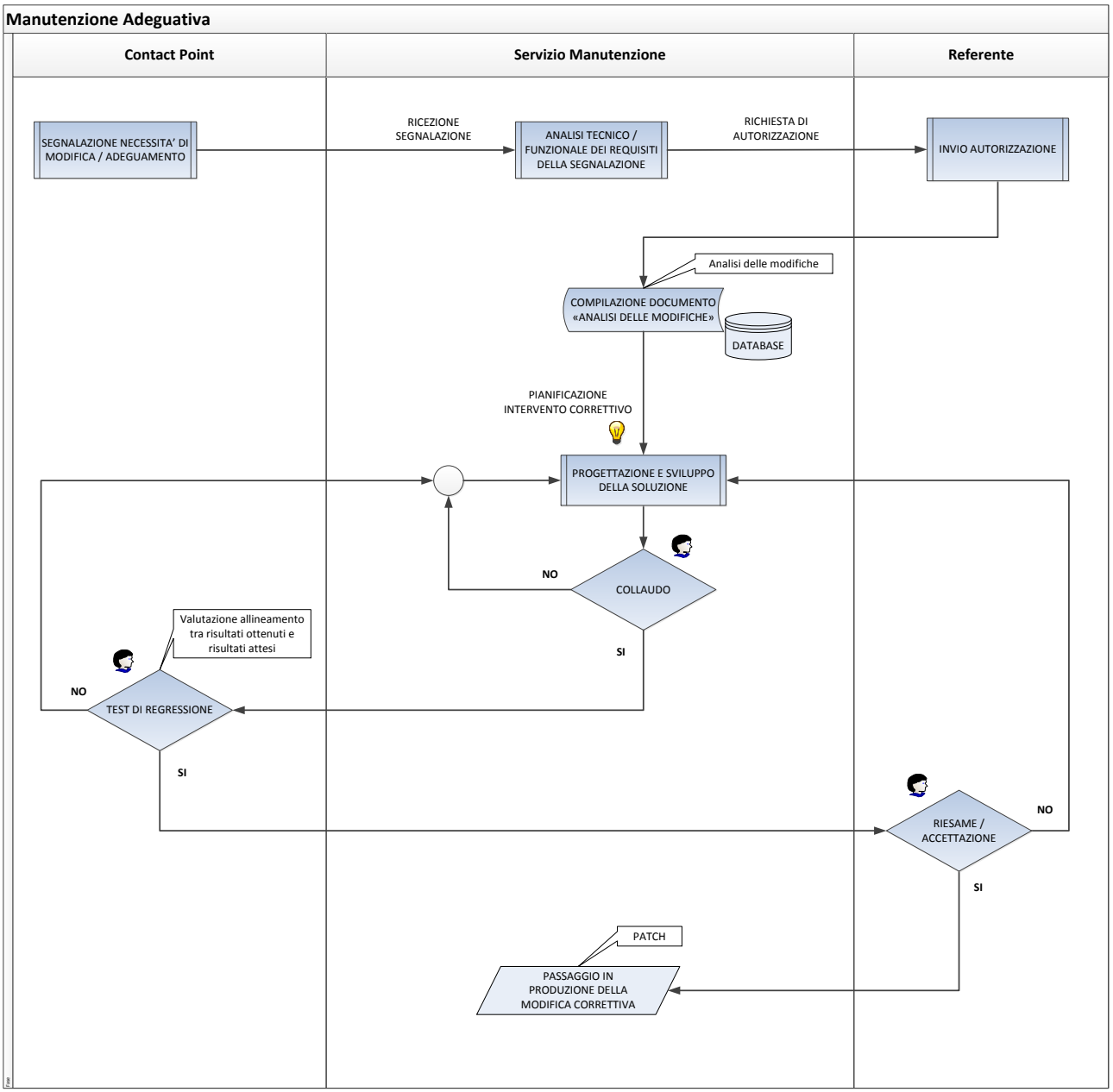
Aruba PEC realizzerà le modifiche previste dal Piano assicurando:

- che siano definiti, eseguiti e documentati i test (unitari, funzionali, di prodotto, di sistema, di non regressione) delle parti modificate e non modificate (unità software, componenti ed elementi di configurazione).
- il completo e corretto soddisfacimento dei requisiti nuovi o modificati, assicurando la permanenza del corretto funzionamento della soluzione rispetto ai requisiti originali non modificati (regression test).

Il risultato di suddette attività, dunque, consisterà nel software modificato / aggiornato / evoluto e nell'aggiornamento/correzione/integrazione della documentazione relativa.

L'attività sarà volta ad accertare l'integrità del sistema modificato attraverso verifiche, sulla base di tutte le registrazioni effettuate ed ai risultati delle prove eseguite.
Una volta conclusi i test con successo Regione del Veneto procederà ad autorizzare la messa in produzione della modifica e Aruba PEC, una volta effettuato l'aggiornamento, ne darà conferma.

Nella seguente figura riportiamo il diagramma di flusso relativo al processo di manutenzione adeguativa:



Aruba PEC attuerà le modifiche necessarie entro il termine concordato con Regione del Veneto, garantendo comunque l'aggiornamento entro le date prescritte dalla normativa.

2 SERVIZIO DI FIRMA DIGITALE, MARCATURA TEMPORALE E CERTIFICATO SSL

Aruba PEC, in caso di aggiudicazione, fornirà una serie di prodotti e servizi qualificati per favorire la diffusione della tecnologia della firma digitale nell'ambito dell'Amministrazione regionale e all'interno delle Pubbliche Amministrazioni Venete aderenti. In particolare verranno rilasciati:

- ✓ Kit per la firma digitale
- ✓ Servizio di firma remota
- ✓ Certificati SSL "wildcard" o per singolo server (per singolo DOMINIO)
- ✓ Marche temporali

I servizi offerti e gli strumenti messi a disposizione sono di seguito descritti: Aruba PEC garantisce il rispetto di tutte le caratteristiche minime e migliorative richieste dal capitolato tecnico.

Oltre alle caratteristiche dei prodotti e servizi offerti, di seguito si riporta una proposta di gestione delle richieste di attivazione/prenotazione e di rilascio degli stessi, con particolare riguardo al servizio di firma digitale, servizio che prevede una serie di obblighi imposti dalla normativa di riferimento che devono essere rispettati. Il processo proposto potrà comunque essere modificato in accordo con la Regione del Veneto in fase di avviamento del servizio.

Lo strumento che verrà messo a disposizione per la gestione ed emissione dei certificati è il CMS (Card Management System): tale strumento, già utilizzato in altre importanti forniture (CCIAA Italiane, Partner Aruba PEC, Regione Sardegna ecc.) e in parte personalizzato per questo progetto, permetterà agli Enti una completa autonomia nelle operazioni di richiesta e gestione dei servizi. Facciamo presente che il flusso degli ordini da parte degli Enti (prenotazione dei kit) potrà essere effettuato anche mediante il Pannello Unico di Gestione (si veda a tal proposito il par. 1.2.1.b).

La soluzione proposta, modulare e flessibile, consentirà diversi livelli di gestione e monitoraggio dell'operato di tutti gli attori coinvolti: un unico strumento permetterà quindi sia la semplice richiesta di emissione del kit da parte del Centro Servizi Aruba PEC, sia il rilascio live da parte dell'Ente stesso.

I processi proposti, frutto di un'attenta analisi delle esigenze e delle esperienze maturate in contesti analoghi, potranno essere ulteriormente personalizzati ed adattati a seconda delle richieste e delle necessità dei singoli Enti.

In ogni caso, per ogni servizio offerto Aruba PEC consegnerà a Regione del Veneto e all'Ente Aderente, con frequenza e modalità che saranno concordate, una relazione dettagliata per singolo Ente sullo stato e la quantità dei servizi attivati ed erogati. Tali dati potranno comunque essere reperiti in autonomia anche all'interno dello strumento di monitoraggio che verrà messo a disposizione della fornitura, come descritto nel Capitolo 7.

Aruba PEC garantisce il rispetto dei livelli di servizio richiesti nel par. 5.1.4 del Capitolato: i relativi dati verranno messi a disposizione all'interno dello strumento di monitoraggio che permetterà di avere una visione completa del rispetto degli SLA concordati.

I servizi offerti saranno disponibili, 24 ore al giorno e 7 giorni su 7 nel rispetto degli SLA previsti dal capitolato e monitorati attraverso lo strumento fornito da Aruba PEC e descritto nel Capitolo 7.

I fermi programmati e gli interventi di manutenzione straordinaria, ossia le interruzioni del servizio necessarie per svolgere attività di manutenzione verranno preferibilmente effettuati nella fascia oraria notturna, previa comunicazione scritta agli Enti Aderenti, da inviare con un anticipo di almeno 5 giorni lavorativi.

Tutti i servizi verranno erogati dai data center del Gruppo Aruba, che rispondono alle stringenti misure di sicurezza previste dalla normativa in materia e sono dotati di appositi sistemi di protezione logica e fisica al fine di impedire accessi non autorizzati, come descritto nel par. 1.2.2.

2.1 STRUMENTI E MODALITA' ORGANIZZATIVE PER LA GESTIONE DEL CICLO DI VITA DEL SERVIZIO

In questo capitolo vengono illustrati i flussi operativi attraverso i quali Regione del Veneto e gli Enti Aderenti saranno messi in grado di richiedere ed emettere i certificati, ferma restando la responsabilità del certificatore nell'identificazione del soggetto che richiede il certificato qualificato di firma anche se tale attività è delegata a terzi, anche ai sensi dell'art. 32, comma 4, del CAD, nonché del D.P.C.M. 22/2/2013.

Gli attori protagonisti dei diversi flussi di emissione sono:

Richiedente:	Colui che effettua la richiesta di rilascio dei certificati di Firma Digitale e CNS Like (o CNS)
Titolare:	Colui che ha ottenuto il rilascio dei certificati richiesti
Incaricato al riconoscimento (o IR):	Colui che effettua il riconoscimento de-visu del richiedente, compila la registrazione via Card Management System (CMS) e stampa il modulo di richiesta. Sottopone il modulo alla sottoscrizione del richiedente e lo controfirma.
Operatore di Registrazione (o ODR):	Colui che oltre a poter svolgere tutti i compiti tipici dell'IR, ha facoltà di perfezionamento (produzione dispositivi) delle richieste.
Centro Servizi Aruba PEC:	Il gruppo di lavoro che riceve, perfezionandole, le richieste provenienti da Regione del Veneto e/o dagli Enti Aderenti e/o loro incaricati. Ha in carico la produzione e della postalizzazione dei dispositivi.
Certification Authority	L'autorità che riceve ed esegue le richieste di emissione e gestione dei certificati

Una copia di tutte le richieste cartacee prodotte tramite uno qualunque dei flussi di seguito esposti, sottoscritta dal richiedente e controfirmata dall'operatore che effettua il riconoscimento, dovrà sempre entrare in possesso della C.A.
Nei paragrafi seguenti vengono illustrati i flussi di emissione gestiti dal sistema fornito, nella loro accezione standard. Alcuni dettagli potrebbero variare a seconda delle abilitazioni conferite tramite CMS sia a dell'Ente che a livello di singolo Operatore.

Di seguito una tabella che sintetizza le principali attività assegnabili ai vari attori coinvolti:

	Registrazione	Emissione	Attivazione Firma Remota	Sospensione Riattivazione	Revoca	Rinnovo	Gestione Uffici	Gestione Operatori
IR	✔							
OdR	✔	✔	✔	✔	✔	✔	✔	✔
Utenza ADMIN				✔	✔	✔	✔	✔
Centro Servizi		✔			✔		✔	✔

Titolare			✔	✔	✔	✔		

Il sistema, basato su una gerarchia di ruoli opportunamente profilati, consentirà l'accoglimento di qualsiasi istanza di monitoraggio, controllo ed operatività della Regione, degli Enti Aderenti ed eventuali Associati che si avvarranno dei servizi offerti.

Gli scenari di seguito illustrati includono diverse proposte di strutturazione degli Enti ed individuazione degli operatori di richiesta/rilascio, fermo restando la disponibilità di Aruba PEC ad accogliere diverse istanze di implementazione del servizio in fase di avvio, da concordare con la Stazione Appaltante.

Per l'emissione dei certificati di autenticazione di firma digitale e di firma remota e per la gestione del relativo ciclo di vita, viene messo a disposizione degli enti e del centro servizi di Aruba PEC, lo strumento **Card Management System** (CMS) di seguito descritto.

2.1.1 IL CMS (CARD MANAGEMENT SYSTEM)

Aruba PEC metterà a disposizione di Regione del Veneto e degli Enti aderenti uno strumento di semplice ed intuitivo utilizzo, dedicato al progetto, che permetterà in completa autonomia di:

- ✓ richiedere;
- ✓ gestire;
- ✓ monitorare;

i servizi oggetto di questo capitolo.

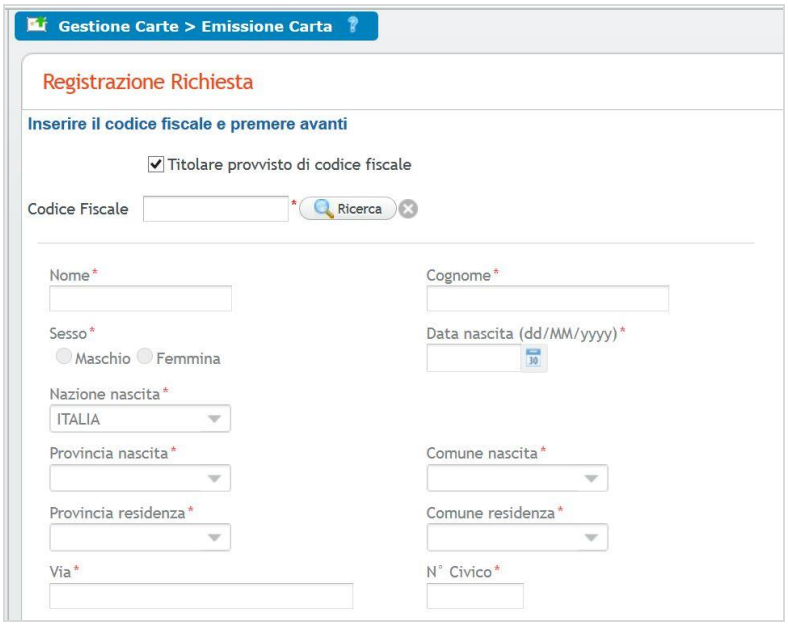
La soluzione, modulare e flessibile, consentirà diversi livelli di gestione e monitoraggio dell'operato di tutti gli attori e le utenze coinvolte.

L'accesso all'area sarà conferito via smartcard ai vari referenti individuati dagli Enti Aderenti, i quali potranno dunque disporre in maniera autonoma di tutti gli aspetti del servizio coinvolti, relativamente alle aree di propria competenza. Le smartcard necessarie all'accesso verranno fornite da Aruba PEC, incluse nella fornitura, a tutti gli operatori incaricati dagli Enti privi di tali dispositivi di autenticazione.

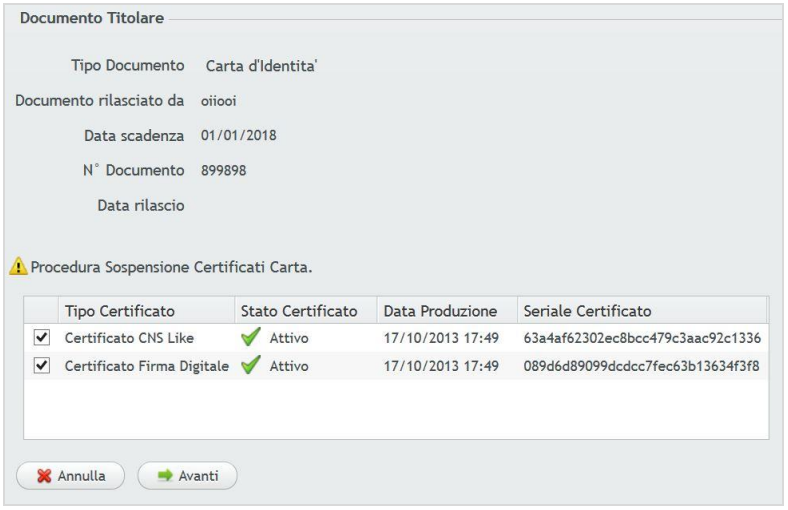
Riportiamo, di seguito alcune immagini del Card Management System.

Accesso al sistema:

Form di richiesta di emissione:



Richiesta di sospensione:



Affinché i vari attori coinvolti (Regione, Enti Aderenti, Enti Associati) siano formalmente in grado di richiedere dispositivi recanti a bordo certificati, sarà necessaria la precedente sottoscrizione di apposite convenzioni e mandati opportunamente redatti da Aruba PEC.

Il procedimento di rilascio dei certificati prevede infatti, in ogni caso:

1) riconoscimento de-visu del richiedente
ovvero l'attività di identificazione certa del richiedente, tramite esibizione del documento di riconoscimento; tale attività potrà essere svolta sia prima dell'invio della richiesta di emissione dei certificati, che al momento della consegna del kit eventualmente prodotti dal centro servizi Aruba PEC.

2) sottoscrizione della richiesta
ovvero raccolta della firma del richiedente sul modulo di richiesta fornito dalla Società/Certificatore. Lo stesso modulo viene sottoscritto anche dal riconoscitore e fatto pervenire ad Aruba, che ne curerà la conservazione.

3) invio della richiesta alla Società/Certificatore
ovvero inoltro dei dati di richiesta precedentemente raccolti i quali, in virtù della sottoscrizione del richiedente raccolta dal riconoscitore, legittimano l'emissione dei certificati da parte del Certificatore.

Le figure deputate allo svolgimento delle attività sopra elencate potranno essere:

- Incaricato al Riconoscimento (IR) per le attività 1 e 2;
- Operatore di Registrazione per l'attività 3 (l'OdR può comunque svolgere le funzioni di IR).

In fase di avvio del servizio Aruba PEC richiederà dunque la sottoscrizione dei documenti necessari alla formalizzazione dei ruoli:

Convenzione CDRL	Compilando e sottoscrivendo questo documento ogni Ente Aderente si configura come Centro di Registrazione Locale per la Certification Authority Aruba PEC, potendo così emettere e/o richiedere i certificati. All'interno dello stesso documento l'organizzazione individua la persona di riferimento per la gestione delle questioni tecnico/organizzative.
Incarico Odr	L'incarico andrà sottoscritto dal personale individuato dall'Ente Aderente preposto alla validazione ed effettivo invio delle richieste di certificato alla Certification Authority. Le stesse risorse verranno formate da Aruba secondo le modalità illustrate nel Capitolo 6.
Incarico IR	L'incarico andrà sottoscritto dal personale che l'Ente Aderente avrà individuato, tra le proprie risorse e quelle degli Enti Associati, come idoneo all'effettuazione del riconoscimento de-visu dei richiedenti, della raccolta della sottoscrizione dei moduli di richiesta ma non della validazione ed invio verso la Certification Authority Aruba. Anche in questo caso, il personale individuato riceverà adeguata formazione secondo i canali e le modalità più avanti (Capitolo 6).

Una volta raccolta la documentazione descritta, che potrà comunque aggiornarsi in corso di servizio con nuovi incarichi e/o convenzioni, sarà dunque formalmente instaurata la catena di deleghe ed autorizzazioni necessarie all'inoltro delle richieste di emissione presso la Certification Authority Aruba PEC.

Questo, in abbinamento alle funzionalità offerte dal sistema Aruba, consentirà l'implementazione di molteplici modalità di richiesta e rilascio dei certificati, così da andare incontro a qualsiasi necessità tecnico/organizzativa dei futuri Enti coinvolti. La flessibilità offerta da Aruba PEC nella gestione del processo di rilascio rappresenta un valore aggiunto in quanto permetterà la completa autonomia dell'Ente nelle procedure di richiesta ed, eventualmente, di emissione con una conseguente riduzione dei tempi di fornitura.

L'instaurazione della catena di deleghe permetterà infatti di accelerare i tempi di produzione dei kit: i 5 giorni necessari al rilascio partiranno infatti non dalla consegna della documentazione ad Aruba PEC, ma dall'invio della richiesta di produzione mediante l'interfaccia fornita.
I documenti verranno poi raccolti dalla c.a. con cadenza che verrà concordata con Regione del Veneto e/o gli Enti Aderenti.

2.1.1.a. CARATTERISTICHE DELL'INTERFACCIA MESSA A DISPOSIZIONE

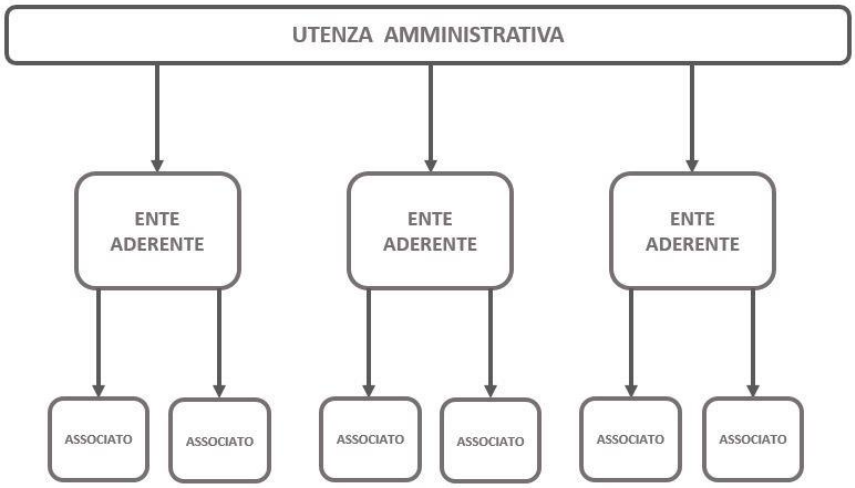
Il CMS, costruito intorno ai due *eventi* di richiesta ed emissione dei certificati, sarà in grado di recepire le richieste provenienti dai vari Enti coinvolti e porle all'attenzione del Centro Servizi Aruba, oppure consentire agli operatori l'immediato perfezionamento dei dispositivi.

Il sistema pertanto permetterà:

1) **Produzione dei certificati in carico al Centro Servizi Aruba PEC – singola o massiva** (tramite il caricamento di un file csv)
2) **Produzione dei certificati effettuata dal personale incaricato dagli Enti Aderenti**
3) *Eventualmente* **la produzione dei certificati effettuata dal personale incaricato dagli Enti Associati**

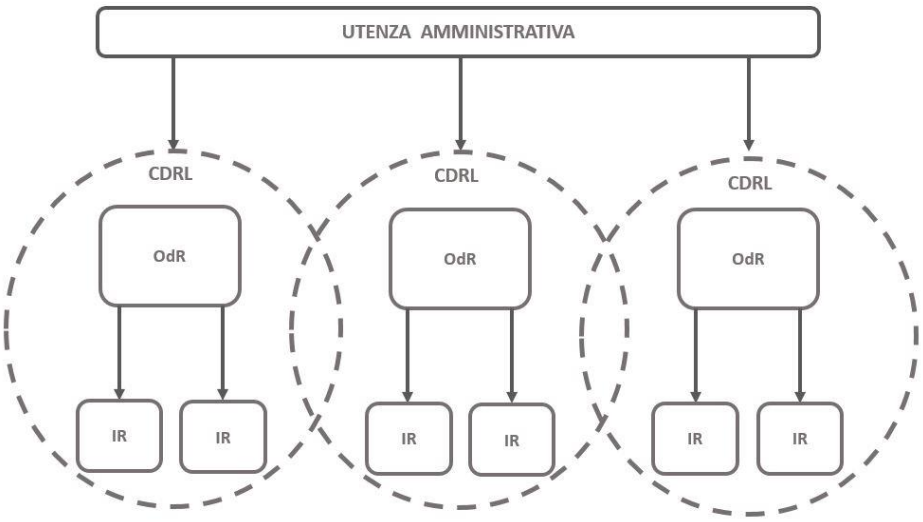
Lo strumento inoltre permetterà sia la sospensione, riattivazione e revoca dei certificati che il rinnovo degli stessi in prossimità della scadenza.

All'interno del sistema gli Enti potranno essere strutturati in maniera gerarchica ad opera dell'utenza amministrativa, dando luogo ad una puntuale organizzazione e monitoraggio del servizio, ad esempio:



Agli Enti così strutturati verrà attribuita la disponibilità operativa (numero e tipologia certificati richiedibili) concordata in fase di avvio, lasciando loro decidere a quale modalità di richiesta ed emissione aderire, tra quelle illustrate più avanti.

Le utenze di accesso saranno profilate di conseguenza, consentendo agli operatori individuati la sola registrazione delle richieste, l'inoltro alla Certification Authority Aruba o la produzione dei dispositivi on the spot.



L'accesso al sistema sarà subordinato a:
- censimento di un account operatore presso il sistema;
- autenticazione con smartcard, contenente un certificato di autenticazione in corso di validità.

Al login ogni operatore avrà a disposizione il panel di funzionalità associato alla propria utenza, ad esempio:

IR (ad esempio un operatore dell'Ente Associato)
- Funzionalità di registrazione;
- Funzionalità di ricerca;

relative ai servizi di propria competenza, con sola visibilità del proprio sportello operativo.

OdR (ad esempio un operatore dell'Ente Aderente)
- Funzionalità di registrazione;
- Funzionalità di emissione;
- Funzionalità di ricerca;
- Gestione ciclo di vita dei certificati;
- Gestione disponibilità certificati (assegnazione a sotto-Enti);

Con visibilità dell'operato del proprio Ente e di quelli ad esso afferenti.

Utenza Amministrativa (ad esempio un operatore regionale o di Aruba PEC)
- Funzionalità di registrazione;
- Funzionalità di emissione;
- Funzionalità di ricerca;
- Gestione ciclo di vita dei certificati;
- Gestione disponibilità certificati (assegnazione ai vari Enti);

Con visibilità dell'operato di tutti gli Enti.

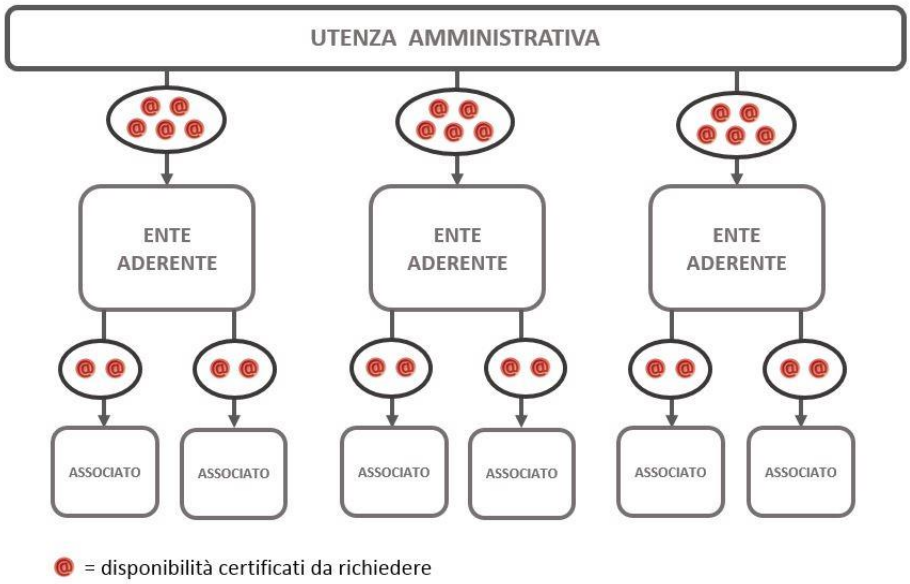
Gli step di registrazione ed emissione saranno del tutto indipendenti, ovvero una registrazione effettuata da un operatore, sia esso qualificato come IR o OdR, potrà essere inoltrata all'attenzione del Centro Servizi Aruba, perfezionata immediatamente da un operatore di tipo OdR oppure presa in carico dallo stesso in un secondo momento, senza alcun vincolo temporale e/o procedurale.

2.1.1.b. MODALITÀ DI RICHIESTA

Vengono di seguito illustrati i possibili scenari di richiesta offerti dalla soluzione proposta.
Ognuna delle opzioni potrà essere scelta dal singolo Ente Aderente, indipendentemente dalla scelta effettuata dagli altri Enti suoi pari.

1) Produzione dei certificati in carico al Centro Servizi Aruba PEC

Il CMS fornito da Aruba PEC consentirà l'attribuzione di un monte certificati, diviso per tipologia di dispositivo, da assegnare ai vari Enti Aderenti coinvolti.
Questi potranno decidere a loro volta quanta disponibilità assegnare ai rispettivi Enti Associati, dando luogo al seguente flusso di gestione della disponibilità dei certificati:

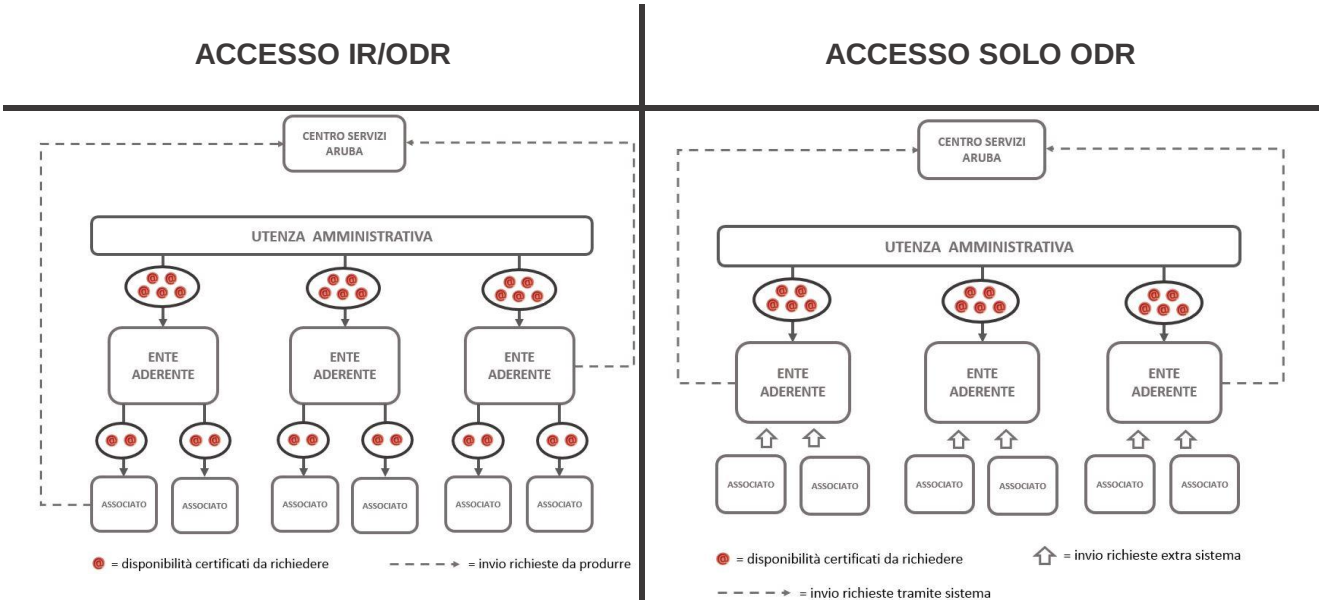


Una volta definito il monte certificati, gli operatori avranno la possibilità di:

- inserire i dati relativi ai titolari richiedenti;
- stampare i moduli di richiesta automaticamente compilati dal sistema, così da sottoporli a firma del richiedente;
- validare l'inoltro della richiesta verso la Certification Authority Aruba PEC;

fintantoché il monte certificati a disposizione, visibile all'accesso da ogni operatore, non risulterà esaurito.

Con questo semplice strumento, gli Enti Aderenti potranno decidere di volta in volta quanta disponibilità assegnare ai propri Enti Associati, monitorandone l'operatività.
Le richieste così registrate tramite sistema giungeranno in visione al Centro Servizi Aruba PEC, il quale si occuperà della produzione dei dispositivi, spedendoli al recapito concordato entro i limiti di tempo stabiliti dal capitolato (5 giorni, ad esclusione dei giorni festivi, dalla richiesta).
Se ritenuto opportuno la facoltà d'accesso potrà essere limitata ai soli Enti Associati (OdR), i quali si occuperanno dunque dell'inoltro ad Aruba sia per le richieste di proprio interesse che per quelle provenienti dagli Enti Associati di riferimento.



Lo scenario in questione prevede la produzione e la spedizione dei dispositivi in carico al Centro Servizi Aruba PEC, pur mantenendo in capo all'operatore le operazioni di:

- riconoscimento de visu del titolare;
- sottoscrizione del modulo di richiesta da parte del richiedente e del riconoscitore;
- inoltro della richiesta alla Certification Authority Aruba PEC tramite sistema.

1.1) Registrazione massiva

In alternativa alla registrazione puntuale di ogni richiesta all'interno del sistema sarà possibile, per gli Enti Aderenti che lo riterranno opportuno, avvalersi della ***funzione di registrazione massiva***.
Il sistema consentirà infatti il caricamento di un file csv, compilato secondo i criteri che verranno condivisi in fase di avvio e comunque contenente i dati relativi ai titolari/richiedenti.

Il contenuto di tale file verrà preso in carico dal sistema; questo effettuerà in tempo reale un controllo sulla validità formale dell'inserimento e:

- notificherà all'utente eventuali imperfezioni di compilazione;
- prenderà in carico le registrazioni correttamente trasmesse;

Dando immediata evidenza delle operazioni effettuate ovvero delle richieste inoltrate.

Queste, al pari degli inserimenti di cui al punto precedente, giungeranno subito in visione al Centro Servizi, il quale si occuperà della produzione/spedizione dei dispositivi.

	A	B	C	D	E	F	G	H
1	Nome	Cognome	Sesso	Codice Fiscale	Data di nascita	Luogo di nascita	Tipologia dispositivo	...
2	Mario	Rossi	M	rrrmmm70bo4a123z	04/02/1970	Torino	Smartcard	...
3								
4								

Gli eventi di produzione dei dispositivi portati a termine dal Centro Servizi verranno registrati e resi visibili agli operatori aventi accesso al sistema, in modo da consentire il monitoraggio puntuale di tutte le tempistiche ed i passaggi di stato (richiesta/lavorazione) inclusi nell'iter produttivo.

Emissione Live sul territorio, a cura del personale Aruba PEC

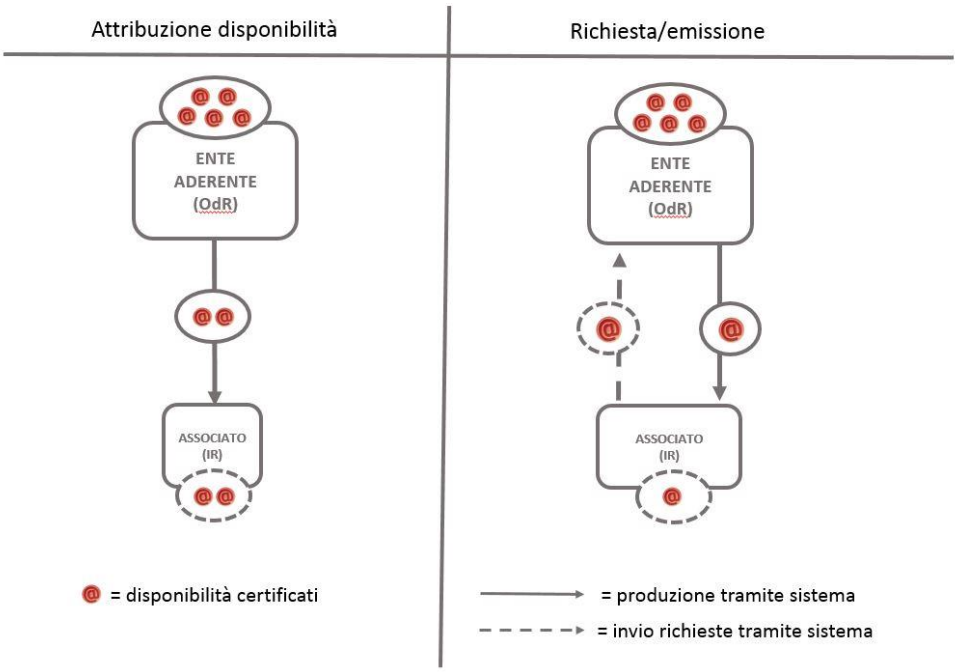
In aggiunta alle modalità sopra descritte, Aruba PEC metterà a disposizione personale incaricato

all'emissione live sul territorio regionale:
con un preavviso massimo di 2 giorni sarà infatti possibile richiedere la presenza di un operatore Aruba PEC che giunga sul posto ed emetta il kit/dispositivo richiesto, sollevando la Regione e/o gli Enti coinvolti da qualsiasi impegno tecnico e/o logistico. Pertanto, una volta ricevuta la richiesta, un incaricato Aruba PEC concorderà la data di rilascio live che avverrà entro 2 giorni lavorativi, salvo diverse esigenze dell'Ente.
Aruba PEC garantirà l'emissione di 50 appuntamenti nella modalità illustrata, fermo restando che sarà la Stazione Appaltante a decidere chi potrà goderne e quando.

2) Produzione dei certificati effettuata dal personale incaricato dagli Enti Aderenti

Per gli Enti Aderenti che si avvarranno di questa modalità il CMS consentirà l'emissione autonoma dei dispositivi sia per il proprio Ente che per conto degli Associati.

Come nello scenario precedente, le richieste potranno essere inserite a sistema dagli operatori accedenti, siano essi afferenti ad Enti Associati o Aderenti, ma solo gli account di tipo OdR potranno avere accesso alle funzionalità di emissione.



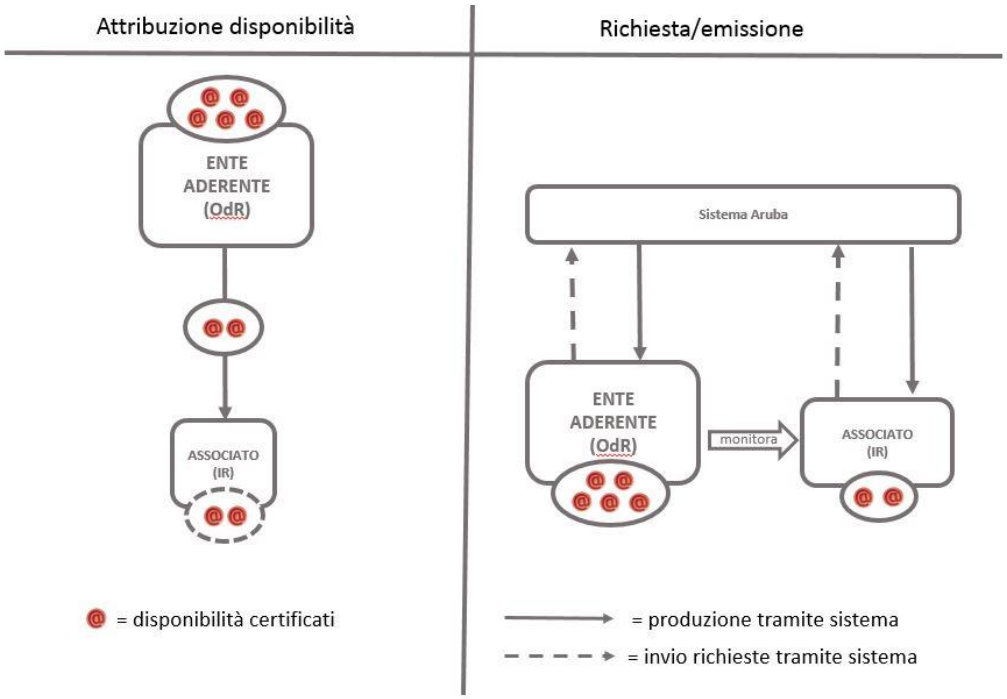
In questo modo verrà eliminata l'attesa imputabile ai tempi di lavorazione/spedizione Aruba PEC.
Gli operatori di emissione saranno preventivamente dotati degli opportuni dispositivi vergini, sulla base della tipologia e del numero richiesto, da produrre sul posto al momento della richiesta.
Gli operatori abilitati potranno dunque:

- produrre le richieste provenienti dagli Enti Associati;
- effettuare richieste e produzioni per proprio conto;
- attribuire agli enti associati il numero di certificati/dispositivi che possono richiedere (disponibilità);
- tenere traccia della propria attività e monitorare quella complessiva del proprio Ente Aderente;

- monitorare l'attività degli Enti Associati e la loro disponibilità residua.

3) Produzione dei certificati effettuata dal personale incaricato dagli Enti Associati

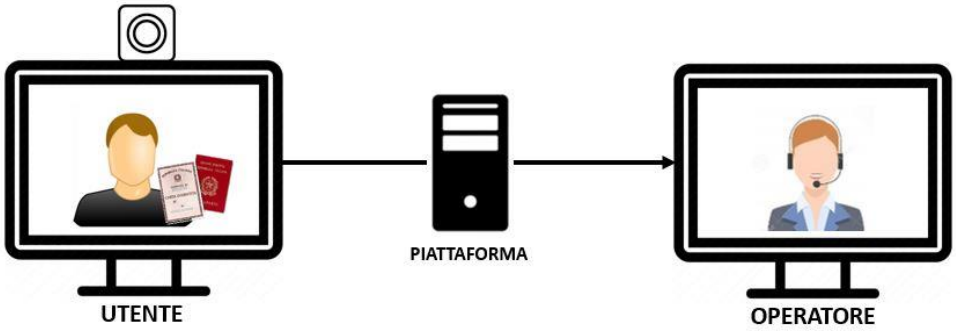
In ultima istanza il CMS potrà consentire l'effettuazione di richieste ed emissioni tanto al personale individuato dagli Enti Aderenti quanto a quello degli Enti Associati.
In questo modo tutti gli operatori accedenti saranno indipendenti nell'effettuazione di richieste ed emissioni di certificati, eliminando completamente tutti i possibili tempi di attesa.
Allo stesso tempo, gli operatori afferenti agli Enti Aderenti potranno mantenere visibilità dell'operato degli Associati, attribuendogli a monte la disponibilità di certificati concordata e monitorandone attività/residui in corso di esercizio.



Identificazione con webcam

In caso di aggiudicazione Aruba PEC metterà a disposizione uno strumento di riconoscimento del richiedente alternativo alla procedura de-visu finora illustrata.
Gli Enti del caso potranno infatti avvalersi della procedura di "identificazione con webcam", qualora questa possa venire incontro alle loro esigenze tecnico/operative.
Aruba PEC fornirà dunque la piattaforma d'identificazione e la possibilità di utilizzo illimitato, per tutta la durato del contratto e relative estensioni da parte della Regione e/o degli Enti aderenti interessati che attraverso i propri incaricati potranno effettuare il riconoscimento a distanza, utile ad es. in caso di presenza di sedi distaccate ecc.

In tale modalità l'identificazione del richiedente verrà effettuata mediante l'ausilio di un sistema di videoconferenza, prevedendo dunque che il Titolare in questione sia dotato di una webcam correttamente collegata ad un computer con sistema audio funzionante.



L'Incaricato al riconoscimento dell'Ente, eventualmente deputato a questa attività, sarà in grado di garantire l'autenticità della richiesta nel corso della sessione di videoconferenza.

L'Incaricato si accerterà dell'identità del richiedente tramite la verifica di un documento di riconoscimento in corso di validità (purché munito di fotografia recente e riconoscibile, firma autografa e di timbro, rilasciato da un'Amministrazione dello Stato).

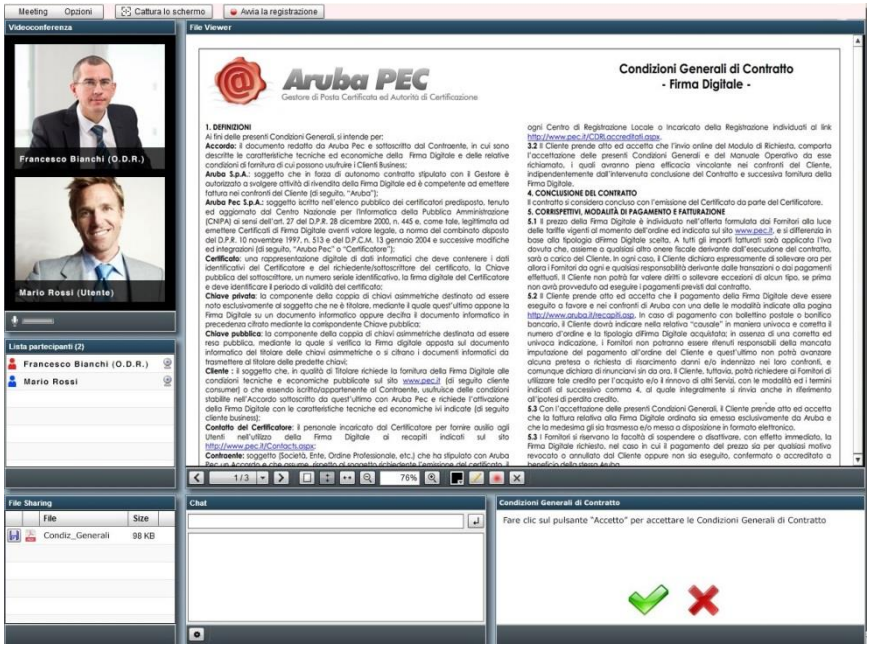
Al momento dell'identificazione il Titolare dovrà confermare:

- l'accettazione delle condizioni contrattuali e del trattamento dei dati personali per l'attivazione del servizio di firma e per il rilascio del certificato digitale, mostrate a video;

- i dati identificativi ed anagrafici registrati che verranno utilizzati anche per l'emissione dei certificati.

Per garantire la tutela e la gestione dei propri dati personali in piena aderenza al D.Lgs. 196/2003, ad ogni richiedente dovrà essere preventivamente fornita l'informativa sulla privacy chiedendo il consenso alla videoregistrazione ed al trattamento dei dati.

In ogni momento l'operatore avrà la possibilità, tramite appositi tasti di catturare le immagini, di iniziare una registrazione e di interromperla.



Terminata la sessione di videoconferenza il sistema provvederà, autonomamente, ad elaborare le tracce audio-video per la produzione del file .mp4 e relativi metadati (XML). I file così generati verranno inviati al sistema di conservazione che li archivierà per un periodo non inferiore a 20 anni secondo quanto indicato nell'art. 32, comma 3, lettera j) del CAD. Il sistema di conservazione sicura salverà i file cifrandoli con le chiavi pubbliche dei responsabili del servizio in modo da garantire che solo questi ultimi possano aver accesso al contenuto dei file multimediali.
L'operatore avrà facoltà di rifiutare il riconoscimento nel caso in cui giudichi non adeguata la registrazione o abbia dubbi sulla reale identità del richiedente.

Firma grafometrica

Come ulteriore elemento migliorativo, se ritenuto opportuno i moduli di richiesta PDF, automaticamente prodotti dal CMS, potranno essere sottoposti a firma grafometrica.

Un'apposita funzionalità del sistema richiamerà il software in grado di:

- prendere in carico il modulo di richiesta pdf;

- attivare il device grafometrico (tavoletta);

- implementare la procedura di firma grafometrica (apposizione della firma grafometrica del richiedente e firma dell'operatore);

- inviare il modulo così sottoscritto in conservazione a norma.

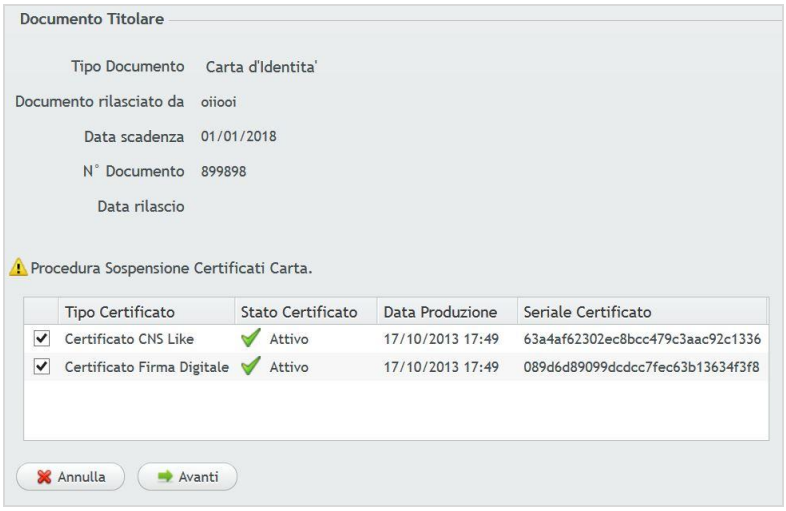
Questo scenario non prevedrà dunque la stampa di materiale cartaceo, sollevando gli Enti coinvolti dalla stampa, conservazione ed invio ad Aruba della modulistica sottoscritta.

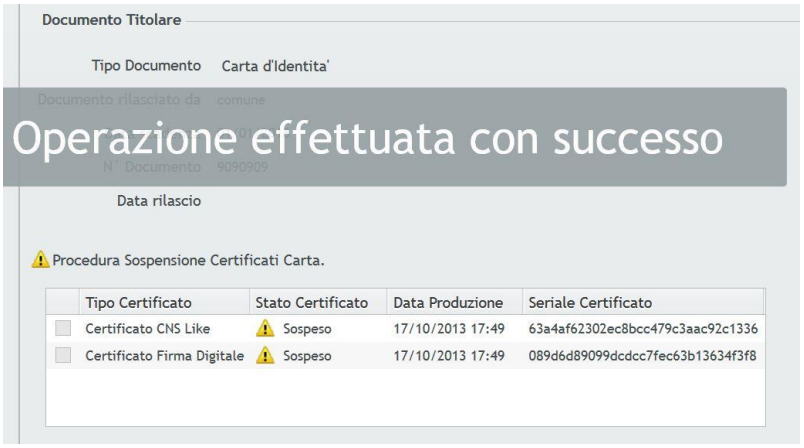
Al fine di agevolare l'adozione di questo strumento, di sicura utilità operativa per gli operatori interessati, **Aruba PEC abiliterà 100 postazioni** mettendo a disposizione della Regione e degli Enti Aderenti **100 tavolette grafometriche** (incluse nell'offerta).

2.1.1.c. SOSPENSIONE/RIATTIVAZIONE DEI CERTIFICATI

Attraverso lo stesso CMS gli operatori abilitati avranno la possibilità di gestire il ciclo di vita dei certificati di propria competenza, e dunque:
- sospendere;
- riattivare;
- revocare
i certificati dei titolari afferenti al proprio Ente di riferimento.

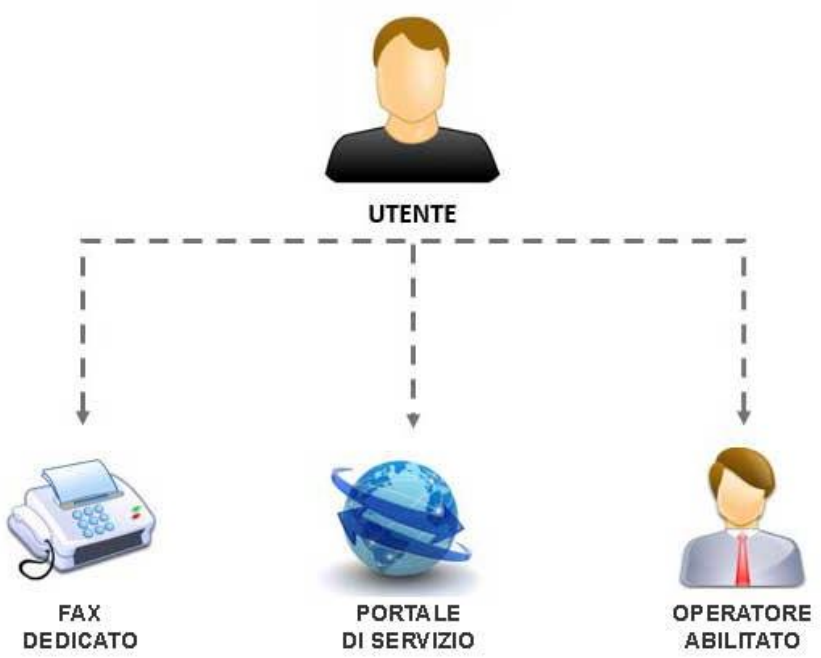
Richiesta di sospensione tramite CMS:





Le prime due operazioni, sospensione e riattivazione, saranno comunque esposte dal portale di servizio (par. 1.2.1.b); in questo modo i titolari potranno richiedere sospensione e riattivazione dei propri certificati in self-provisioning.

La stessa revoca potrà essere richiesta anche direttamente dal titolare alla Certification Authority, inviando per fax il modulo di richiesta revoca che verrà pubblicato sul portale di servizio.
In qualunque caso, lo stato dei certificati (attivo, sospeso, revocato) verrà automaticamente aggiornato all'interno del sistema, così da poter avere un riscontro reale sullo stato dei certificati, anche qualora questi vengano sospesi/riattivati/revocati da canali esterni al sistema.



Se ritenuto opportuno, le operazioni di life-cycle-management offerte dal sistema potranno prevedere la produzione automatica dei moduli di richiesta di sospensione/revoca, da sottoporre a firma del titolare.
In ogni caso, qualora gli Enti Aderenti si configurino come "Terzo Interessato" nei confronti dei titolari/certificati emessi, sarà possibile per gli operatori incaricati la sospensione e/o revoca dei certificati riconducibili alla propria organizzazione anche senza esplicita richiesta del titolare.

2.1.1.d. RINNOVO DEI CERTIFICATI

Aruba PEC garantisce il rinnovo tempestivo dei certificati di autenticazione e firma per tutta la durata del contratto e relative proroghe/estensioni. All'approssimarsi della scadenza dei certificati emessi la Certification Authority verrà inviata una email di avviso ai titolari ed ai relativi Enti, invitandoli a collegarsi presso la sezione "rinnovo" del portale di servizio (par. 1.2.1.b).

Qui, in modalità self-provisioning sarà possibile ottenere i nuovi certificati, siano essi su dispositivo fisico (Firma digitale, CNS) che remoto.

La procedura, alla quale avranno accesso i titolari, consterà di:

- cancellazione dei certificati a bordo del dispositivo (o HSM, in caso di firma remota);
- creazione di nuove chiavi crittografiche;
- invio della Certificate Signing Request alla Certification Authority Aruba PEC;
- generazione dei certificati richiesti;
- installazione dei certificati così prodotti a bordo del dispositivo;
- sovrascrittura del pin già noto al titolare.

Nel caso della firma remota le stesse operazioni avverranno all'interno dell'infrastruttura dedicata, senza alcuna evidenza locale per l'utente richiedente.
Le operazioni così effettuate genereranno l'evento "rinnovo" visibile all'interno del sistema da parte degli operatori autorizzati.
In fase di avvio del servizio potranno essere valutati con la Stazione Appaltante modifiche allo scenario proposto, inserendo eventuali ulteriori step (es. validazione, controllo…) ritenuti opportuni.

Se ritenuto opportuno, le stesse funzionalità di rinnovo esposte dal portale di servizio potranno essere fruite dalla stessa interfaccia di emissione, in modo tale che la procedura venga eseguita dall'operatore abilitato, in presenza del titolare richiedente.

2.1.1.e. APPROVVIGIONAMENTO ED AVVIO DEL SERVIZIO

Come illustrato nella pagine precedenti, l'avvio del servizio presuppone la sottoscrizione della modulistica predisposta da Aruba PEC, necessaria alla costituzione degli Enti come Centro di Registrazioni Locale Aruba ed al conferimento degli incarichi agli operatori individuati.

Tutta la documentazione sarà messa a disposizione della Regione all'avvio del contratto, in modo tale che la stessa Regione potrà disporne per configurarsi da subito come entità di rilascio operativa.
In seguito alla stipula del contratto verranno comunicati all'Ente Aderente i riferimenti del Responsabile del servizio di firma digitale e marcatura temporale, il quale raccoglierà le esigenze organizzative ed operative dell'Ente, consegnandogli dunque la documentazione necessaria all'avvio del tipo di operatività richiesta.
Se ritenuto opportuno gli stessi documenti potranno essere pubblicati in apposita area del portale di servizio (par. 1.2.1.b).

Una volta completata la raccolta dei documenti necessari all'avvio potranno essere assegnate le disponibilità di certificati e dispositivi ai vari Enti coinvolti, sulla base degli accordi intercorsi tra i vari Enti, la Regione ed Aruba PEC.
L'attribuzione del monte certificati/dispositivi a disposizione dei vari Enti potrà essere effettuata direttamente dal Centro Servizi Aruba PEC, il cui operato sarà comunque visibile dall'utenza amministrativa conferita alla Regione.
In maniera contestuale verranno create le entità "Ente Aderente/Ente Associato" all'interno dell'interfaccia. Il censimento degli operatori, profilati secondo gli accordi e la modulistica raccolti in fase di avvio, verrà effettuato dal personale Aruba PEC dedicato al servizio.

2.1.1.f. REPORTISTICA E MONITORAGGIO

Tutte le operazioni effettuata tramite l'interfaccia Aruba verranno tracciate e rese visibili agli operatori accedenti.
Ogni operatore avrà dunque in visione tutti i dati di sua pertinenza, dall'effettuazione delle richieste alla revoca, completi delle informazioni "autore", "data", "organizzazione", "sportello".

Utilizzando gli appositi filtri messi a disposizione sarà inoltre possibile effettuare ricerche puntuali (es. ricercare l'operazione x relativa al titolare y per il giorno z), oppure estrarre dati cumulativi funzionali alle esigenze di reportistica di ogni Ente, limitatamente al proprio livello gerarchico all'interno del sistema:

- l'utenza amministrativo/regionale avrà visibilità totale, ovvero dell'operato degli Enti Aderenti e di quelli associati;

- le utenze relative agli Enti Aderenti avranno in visione il tracciato del proprio operato ed il monitoraggio del lavoro degli Enti a loro associati;

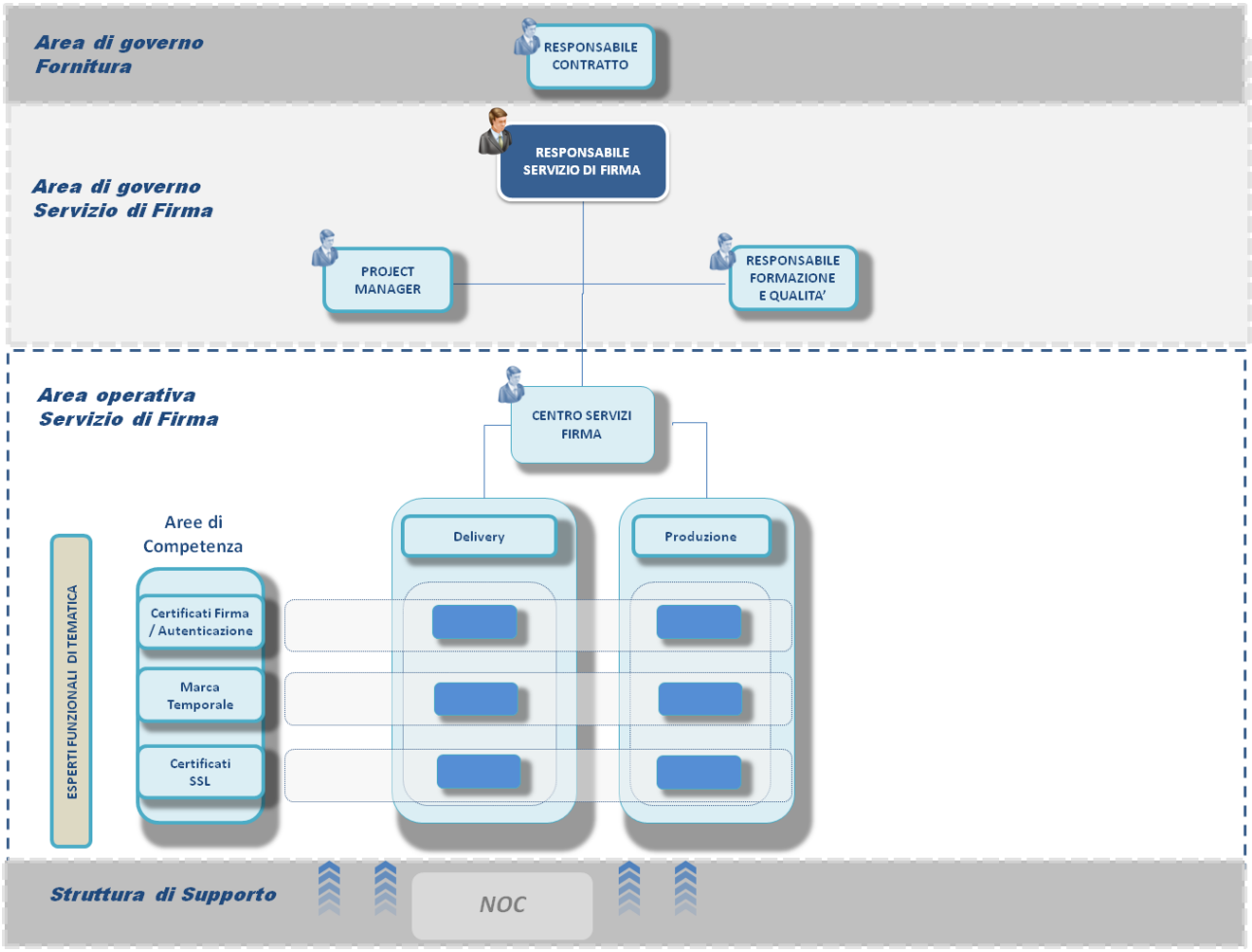
- la reportistica ed il monitoraggio degli Enti Associati sarà altresì limitata ai soli dati di diretta competenza.

Le informazioni salienti verranno raccolte all'interno della Consolle di monitoraggio, visibile dal Pannello Unico di Gestione in modo da fornire, ai responsabili regionali e degli enti aderenti un'immediata e sintetica overview sull'andamento e funzionamento dei servizi.

2.1.2 ORGANIZZAZIONE DEL SERVIZIO DI FIRMA

Per avviamento del servizio si intende la predisposizione di tutte le procedure, attività, ruoli, funzioni propedeutiche per la fruizione del servizio da parte dell'Ente Aderente. La conclusione delle attività di avviamento dovrà avvenire entro 3 mesi dalla firma del contratto.
Il servizio dovrà essere erogato fino all'ultimo giorno di validità del contratto.

All'interno del **modello organizzativo del Servizio di Firma** si distinguono due aree specifiche: l'**Area di governo** e l'**Area operativa**.



Ciascun utente della Regione del Veneto può usufruire del **Servizio di Firma** come centro di competenza identificato a gestire le richieste di firma remota, marca temporale e certificati SSL. L'organizzazione del **Servizio di Firma** prevede la sinergia tra figure professionali appartenenti a **due distinte aree funzionali**.

All'interno dell'**Area di Governo del Servizio di Firma** sono presenti le seguenti figure:

- ✓ **Responsabile Servizio di Firma** – è supervisore dell'intero **Servizio di Firma**. Coordina l'organizzazione e le attività svolte dal **Centro Servizi di Firma**, sia nella fase di avvio/gestione che nella fase di produzione dei dispositivi. Ha inoltre il compito di coinvolgere la figura del **Responsabile Formazione e Qualità** qualora sia necessario un miglioramento qualitativo sugli aspetti operativi. A seguito della firma del contratto il suo nominativo e i relativi recapiti (telefono, fax, mail) verranno comunicati formalmente all'Ente Aderente in modo da mettere in piedi tutte le attività propedeutiche all'avviamento del

servizio, quali ad es. definizione delle procedure, dei ruoli e delle funzioni, eventuali personalizzazioni grafiche ai dispositivi, pianificazione delle attività formative ecc..
Tale figura s'interfaccerà con "referente" appositamente individuato dagli Enti che curerà gli aspetti tecnologici ed amministrativi e i rapporti tra l'Amministrazione richiedente, Regione del Veneto e Aruba PEC. A tale "referente" verrà garantito l'accesso a tutte le informazioni sul servizio erogato al proprio Ente.
Oltre che con il Referente, il Responsabile del Servizio di Firma, o un suo incaricato, s'interfaccerà con l'ufficio interno all'Amministrazione deputato a seguire la pratica di rilascio e l'identificazione dei futuri titolari dello strumento di firma.

- ✓ **Responsabile Formazione e Qualità** – rappresenta il responsabile del livello di competenze e della qualità operativa svolta dal **Centro Servizi di Firma**. Tale figura interagisce con il **Responsabile Firma** e garantisce l'aggiornamento ed il miglioramento continuo di processi/procedure utili a perfezionare il livello di servizio.

L'**Area Operativa del Servizio di Firma** ha la responsabilità di fornire operativamente il servizio agli utenti di riferimento della Regione del Veneto e degli Enti aderenti. La dimensione organizzativa è basata sul seguente schema:

- La dimensione verticale è costituita dal team **Delivery** e dal team **Produzione** aventi il seguente compito
  - **Delivery** – rappresenta il team che si occupa della predisposizione dei servizi di firma – includendo la fase di avvio e l'eventuale revisione della loro pianificazione. Tale figura interagisce con il **Responsabile Centro Servizi Firma** e garantisce la corretta erogazione dei servizi di firma.
  - **Produzione** – rappresenta il team che si occupa della produzione dei dispositivi di firma: token, smart card, ecc. Tale figura interagisce con il **Responsabile Centro Servizi Firma** e garantisce la fornitura dei dispositivi agli utenti richiedenti.

- La dimensione orizzontale è organizzata in base alle aree funzionali e di competenza:
  - **Certificati di Firma / Autenticazione**
  - **Marca Temporale**
  - **Certificati SSL**

Le attività di fornitura su tali ambiti richiedono spesso l'interazione tra il team **Delivery** ed il team **Produzione** – con la supervisione del **Responsabile Servizio di Firma**.

2.2 DESCRIZIONE DEI KIT FORNITI PER LA FIRMA DIGITALE

Vengono di seguito illustrate le caratteristiche dei kit di firma digitale che in caso di aggiudicazione saranno messe a disposizione degli Enti fruitori il servizio.
Segue dunque il dettaglio del profilo dei certificati in fornitura, delle smartcard e relativo chip crittografico, dei dispositivi token, delle scratchcard associate e dei client di firma per l'utilizzo dei certificati.

I kit di firma che verranno forniti rispettano tutti i requisiti minimi, oltre agli aspetti migliorativi, richiesti dal capitolato, tutte le normative vigenti e tutti i requisiti tecnici previsti in materia di firma digitale ed autenticazione. Aruba PEC garantisce che quanto fornito verrà mantenuto costantemente aderente all'evolversi delle norme in materia per tutta la durata del contratto, aggiornando, modificando, revisionando il sistema e le procedure tecnico/organizzative che si dovessero rendere necessarie a fronte di variazioni normative.

CERTIFICATI DI AUTENTICAZIONE E SOTTOSCRIZIONE
I certificati di autenticazione (CNS o CNS-Like) e sottoscrizione forniti da Aruba PEC e contenuti nei kit avranno durata **quinquennale** anziché triennale. Alla scadenza il certificato potrà essere

rinnovato mediante la procedura descritta nel precedente capitolo 2.1 (attraverso il sito web con procedura di self provisioning o tramite l'operator dell'Ente).

Profilo firma

Il certificato qualificato di sottoscrizione fornito avrà un profilo conforme alla vigente normativa in materia di firma digitale e in particolare a:

- D.Lgs. 7 marzo 2005, n. 82: "Codice dell'Amministrazione Digitale" (in breve: CAD) e successivi aggiornamenti e integrazioni
- Decreto del Presidente del Consiglio dei Ministri 30 Marzo 2009: "Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici"
- Deliberazione CNIPA n.45/2009: "Regole per il riconoscimento e la verifica del documento informatico"

Oltre all'indirizzo della CRL (accessibile con due diversi protocolli: HTTP ed LDAP), il certificato conterrà, all'interno dell'estensione **AuthorityInfoAccess** (OID: 1.3.6.1.5.5.7.1.1), l'indirizzo del server di validazione on-line (con protocollo OCSP), gestito da Aruba PEC.
In questo tipo di certificato potrà essere opzionalmente inserito anche il Ruolo del Titolare, inteso come il Titolo e/o Abilitazione professionale in possesso del Titolare del certificato, ovvero l'eventuale potere di rappresentare enti di diritto privato o pubblico, ovvero l'Appartenenza a detti enti nonché l'Esercizio di funzioni pubbliche.
Il ruolo, se richiesto, sarà inserito nell'attributo **title** (OID: 2.5.4.12) del campo **Subject** certificato, con la codifica specificata nelle *"Linee Guida per la certificazione delle qualifiche e dei poteri di rappresentanza dei Titolari dei certificati elettronici"* (documento emesso da AssoCertificatori e disponibile sul sito http://www.assocertificatori.org).

Profilo CNS

Il certificato di autenticazione avrà un profilo conforme alle specifiche CNIPA: "Profilo di certificato per l'autenticazione mediante Carta Nazionale dei Servizi (CNS)", v1.1, pubblicato sul sito www.agid.gov.it.
Gli attributi **CommonName** (CN, OID 2.5.4.3) e **OrganizationalUnit** (OU, OID 2.5.4.11) del campo **Issuer** del certificato saranno concordati con la Regione del Veneto e/o, dove possibile, con gli Enti Aderenti che ne faranno richiesta. Dietro richiesta di Regione del Veneto sarà inoltre possibile poter inserire all'interno del campo Subject del certificato, in aggiunta ai dati obbligatori previsti dalle specifiche AGID, anche il nome e cognome del Titolare rispettivamente degli attributi givenName (OID: 2.5.4.42) e surname (OID: 2.5.4.4)

Per consentire al titolare di usare il certificato di autenticazione anche per la protezione della posta elettronica tradizionale o certificata (cifratura e/o firma elettronica), il certificato conterrà anche i seguenti elementi informativi se richiesti o specificati in fase di registrazione:

- l'indirizzo di posta elettronica del titolare nell'attributo emailAddress del Subject
- l'indirizzo di posta elettronica del titolare nella estensione SubjectAltName
- il valore id-kp-emailProtection nell'estensione ExtendedKeyUsage
- il valore keyEncipherment nell'estensione KeyUsage

Oltre all'indirizzo della CRL (accessibile con due diversi protocolli: HTTP ed LDAP), il certificato conterrà, nell'estensione AuthorityInfoAccess, l'indirizzo del server di validazione on-line (con protocollo OCSP), gestito Aruba Pec.
Se richiesto, al fine di consentire l'utilizzo del certificato di autenticazione per il login a domini Active Directory, il certificato potrà inoltre contenere anche le seguenti informazioni se richieste in fase di registrazione:

- il valore smartCardLogon nell'estensione ExtendedKeyUsage
- il nome dell'utenza a Dominio all'interno dell'estensione SubjectAltName

In alternativa al certificato CNS gli Enti potranno richiedere la fornitura di profili CNS-like, ovvero certificati per l'autenticazione in tutto simili ai CNS ma non validi per l'autenticazione presso i portali della Pubblica Amministrazione.

Smartcard e chip crittografico

I certificati pensati per un utilizzo via smartcard e token USB verranno emessi a bordo di chip crittografico sicuro, installato su idoneo supporto plastico:

ESEMPIO DI SMARTCARD PERSONALIZZATA

ESEMPIO DI SMARTCARD PLUGIN

Si tratta del modello "**ID One Cosmo**" della **Oberthur Technologies** (o di una carta tecnicamente equivalente o superiore nelle prestazioni e caratteristiche), una smartcard performante e versatile, conforme alle specifiche tecniche della Carta Nazionale dei Servizi (CNS) e della Carta d'Identità Elettronica (CIE).
Tale smartcard è ampiamente utilizzata da Aruba PEC per le forniture ai propri Clienti, anche in versione Plug-in (formato SIM inseribile nei Token).
Il sistema operativo della carta è dotato di certificazione **Common Criteria** (ISO 15408) secondo il protection Profile CWA 14169 Type 3.

La carta soddisfa pienamente le norme vigenti relative alla firma digitale qualificata (D.Lgs. n.82 del 7 marzo 2005, DCPM del 22 febbraio 2013, Deliberazione CNIPA n.45/2009, Determinazione DigitPA n.69/2012) ed già conforme anche ai *futuri* requisiti (es. chiavi RSA a 2048 bit).
In sintesi, queste sono le principali caratteristiche della smart card:

- supporto plastico in PVC laminato con overlay di protezione sui due lati
- memoria EEPROM di **72 KB**
- almeno 500.000 cicli di scrittura dei dati in EEPROM
- sistema operativo conforme con le specifiche CNS, CIE e Netlink
- pieno supporto per le APDU conformi allo standard ISO 7816 parti 1, 2, 3, 4, 8, 9
- lunghezza PIN/PUK 8 cifre
- blocco dell'accesso al terzo inserimento PIN errato
- blocco irrevocabile del dispositivo al terzo PUK errato
- supporto per algoritmi di hashing SHA1, SHA256 e SHA512 on-chip
- pieno supporto per gli algoritmi RSA, AES, DES, 3DES on-chip
- algoritmo RSA, con chiavi di lunghezza fino a 2048 bit
- ritenzione dei dati garantita per almeno 10 anni
- pieno supporto del Secure Messaging ISO 7816
- conforme alle norme relative alla Tessera Sanitaria elettronica
- supporto dei protocolli di comunicazione T=0 e T=1

- conforme alle specifiche ICAO ed EMV 2000
- comandi per la gestione di transazioni (ad es. per applicazioni di e-ticketing)
- funzionalità certificata di generazione on-chip delle coppie di chiavi RSA (PP SSCD type 3)
- funzionalità certificata di importazione delle coppie di chiavi RSA (PP SSCD type 2)
- dimensioni conformi alla norma ISO 7810 per le carte tipo ID-1
- dispositivo sicuro per la creazione della firma (SSCD)

Microchip:
La carta Id-One Cosmo v7 si basa sulla famiglia di microprocessori P5CD080V0B, P5CN080V0B e P5CC080V0B sviluppati dalla NXP Semiconductors le cui caratteristiche e funzionalità salienti sono state riassunte nel precedente elenco.

Questi microprocessori sono dotati di certificazione di sicurezza Common Criteria (ISO 15408) a livello EAL5+ (vedere anche http://www.commoncriteriaportal.org/files/epfiles/0410a.pdf).

Sistema Operativo e Applet di Firma:
La carta Id-One Cosmo v7 si basa sul Sistema Operativo ID-One Cosmo V7.0 e sull'applet di Firma Digitale ID One CIE Java Applet sviluppati dalla Oberthur Technologies.
I due componenti, nel loro complesso, realizzano un ambiente operativo avanzato, flessibile, affidabile e pienamente conforme agli standard del settore e-ID / PKI e alle specifiche della CNS.
Sia il Sistema Operativo che l'Applet sono dotati di certificazioni Common Criteria (ISO 15408).
In particolare il Sistema Operativo è stato certificato con livello pari a EAL 5+.
L'applet ha invece ottenuto una certificazione Common Criteria con livello pari a EAL 4+ conformemente ai due Protection Profile CWA 14169 type 2 (secure signature-creation devices type 2 – con funzione certificata di importazione on-chip delle chiavi di firma) e CWA 14169 type 3 (secure signature-creation devices type 3 – con funzione certificata di generazione on-chip delle chiavi di firma).
Le carte proposte consentono di eseguire una firma digitale con chiavi RSA da **2048 bit**, in circa **1.5 secondi** (valor medio).

Le carte saranno impostate nel modo seguente:
- PIN e PUK di 8 cifre
- blocco dell'accesso dopo 3 tentativi con PIN errato

Per quanto riguarda la personalizzazione del supporto plastico, la grafica prestampata in quadricromia sarà personalizzabile su richiesta di ogni Ente Aderente.

Qualora il singolo Ente decida di attivare la funzionalità di rilascio autonoma dei kit sarà dotata di smartcard vergini che potrà personalizzare con i certificati in modo indipendente, come descritto nel par. 2.1 "**2) Produzione dei certificati effettuata dal personale incaricato dagli Enti Aderenti"**.

Nel caso in cui la Regione o l'Ente intendano attivare certificati di tipo CNS il layout grafico della smartcard, al pari del seriale ad essa associato, dovranno rispettare le regole vigenti par la "Carta Nazionale dei Servizi".

Lettore smartcard
I lettori smartcard forniti in abbinamento alle smartcard saranno di tipo Minilector EVO.

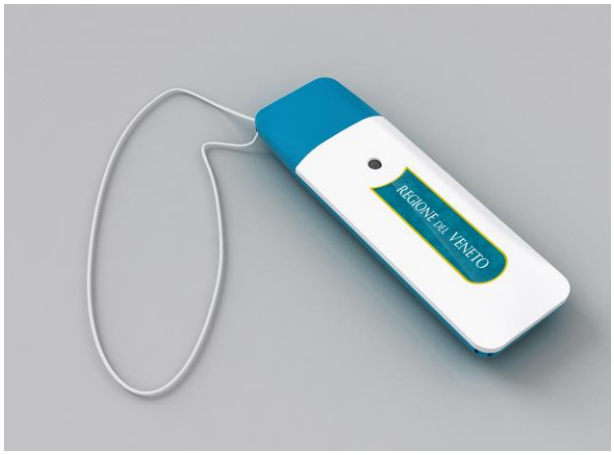
Si tratta di un dispositivo Plug&Play compatibile con gli standard ISO-7816 e EMV (livello 1) in grado di supportare smartcard Class A, B e C (5V, 3V e 1.8V) con microprocessori con protocolli T=0 e T=1.
Supporta le più comuni carte a memoria disponibili sul mercato, Supporta PPS, fornisce Protezione dal cortocircuito, è conforme con gli standard RoHS, è dotato dei seguenti certificati di compatibilità: EN 60950/IEC 60950, ISO-7816, PC/SC, CE, FCC, VCCI, CCID, Microsoft WHQL, EMV 2000 Level 1.

Essendo compatibile agli standard CCID l'installazione di driver risulta superflua.

Token usb
Il Token USB proposto da Aruba PEC è il prodotto "**Aruba Key**", prodotto di punta per i servizi di firma digitale Aruba PEC. Il dispositivo per le sue caratteristiche di affidabilità e facilità d'uso è stato infatti scelto da oltre 300.000 clienti ed è stato impiegato in importanti forniture come ad esempio:

- Le Camere di Commercio italiane
- Consiglio Nazionale Geometri
- Ordini degli Architetti
- Ordini degli Ingegneri
- Avvocati italiani

Di seguito un esempio di possibile personalizzazione del Token USB:



Il dispositivo USB comprende:

- Lettore di SIM-card conforme **CCID** e **HID** e con le seguenti specifiche:
  - Conformità ISO 7816 carte classi A, B and C (5 V, 3 V, 1.8 V)
  - Compatibilità con protocolli di comunicazione T=0, T=1
  - Supporto per PPS (Protocol and Parameters Selection)
  - Sistema di protezione dal corto circuito
- Dispositivo di memoria flash conforme alla specifica USB 2.0 Hi-Speed e con capacità pari a **8 GB**

Il token USB incorpora lo stesso chip crittografico già descritto e avrà preinstallato all'interno della flash memory tutto il software necessario al corretto utilizzo dei certificati.
L'utilizzo del dispositivo è estremamente semplice ed intuitivo per l'utente. Non è infatti necessario installare alcun software e il dispositivo funzionerà automaticamente con qualsiasi PC a cui verrà collegato, Windows, MAC o Linux.
La funzione di autoaggiornamento automatico (auto update) permetterà di installare nuove release software automaticamente all'avvio: basterà essere connessi ad Internet per rilevare eventuali aggiornamenti senza doverli scaricare sul sito di riferimento.

I dispositivi verranno inoltre forniti da Aruba PEC personalizzati graficamente (parte bianca del guscio plastico esterno), in maniera concordata con la Stazione Appaltante.
Qualora un Ente Aderente voglia personalizzare la grafica del token potrà concordare con Aruba PEC loghi e colori dell'immagine che verrà inserita nella parte bianca del guscio.

Scratchcard
Ogni dispositivo fisico sarà prodotto e consegnato in abbinamento ad una scratchcard, ovvero un supporto plastico delle dimensioni di una carta di credito, deputato alla custodia sicura dei codici di governo della carta.
Di seguito un'immagine che mostra l'aspetto di una scratchcard:

FRONTE

RETRO

Questa conterrà dunque:

- **Pin**: ovvero il codice che verrà richiesto dall'applicativo in uso per apporre la propria firma digitale;
- **Puk**: ovvero il codice che consentirà lo sblocco del dispositivo, qualora vengano inseriti consecutivamente 3 pin non corretti;
- **Codice Utente**: il codice che identifica in maniera univoca i certificati presso la Certification Authority, utile alla gestione del ciclo di vita degli stessi.

Sia il fronte che il retro del dispositivo potranno essere personalizzati con grafica e testo da concordare in sede di avvio del servizio insieme alla Stazione Appaltante.

Client di firma

Vengono di seguito illustrati i software attraverso i quali sarà possibile impiegare i certificati di firma forniti da Aruba. I software di firma forniti possono essere installati sui seguenti sistemi operativi: Windows, Linux e Mac OS.

- Software ArubaKEY

Si tratta del software contenuto all'interno dei dispositivi token usb in fornitura.
Il software verrà personalizzato con i colori e la grafica della Regione del Veneto.

Attraverso un semplice drag&drop dei files interessati sarà possibile per l'utente:

- apporre e verificare firme i formato cades, **pades** (anche in modalità grafica), **xades**;
- marcare temporalmente;
- effettuare operazioni di firma e marca contemporanee;
- **sottoporre a firma più file contemporaneamente** (anche cartelle);
- cifrare/decifrare files;

mentre le funzionalità di gestione carta consente di cambiare il pin dei propri certificati e lo sblocco.

A bordo di ogni token, oltre al software per l'apposizione e verifica di firme e marche temporali, saranno presenti:

- librerie (middleware) di interfacciamento con la smartcard
- moduli per lo switch da modalità HID a CCID
- Update Manager, modulo per la gestione degli aggiornamenti automatici in caso di rilascio di nuove versioni
- applicazioni di utilità generale tra cui:
  - web browser
  - visualizzatore PDF
  - applicazione cartella cifrata
  - sistema di autodiagnostica
- toolbar che facilita la navigazione e l'avvio delle applicazioni precaricate nel token
- software di base necessario al funzionamento delle applicazioni sopra elencate.

Il software precaricato su Aruba Key è multipiattaforma e consente di utilizzare lo stesso dispositivo su qualsiasi PC. In particolare è garantita la compatibilità con i seguenti sistemi:

- Windows XP (32 e 64 bit) e successivi;
- Macosx 10.4 e successive;
- Distribuzioni Linux maggiormente diffuse (Ubuntu, Red Hat, Suse, Debian, etc..) (32 e 64 bit);

- ArubaSign

ArubaSign è il client Aruba che consente l'apposizione di firme con smartcard. Lo stesso client viene utilizzato sia per il servizio di firma digitale con smartcard che per il servizio di firma remota, semplificando quindi l'utilizzo degli stessi da parte dei titolari che richiederanno entrambi i servizi.

L'installazione, semplice e veloce, è disponibile per sistemi operativi Windows, MAC e Linux.

Anche in questo caso l'interfaccia consente con un semplice drag&drop dei documenti interessati le stesse operazioni eseguibili tramite ArubaKEY, incluso il governo della carta (cambio pin e sblocco) e l'apposizione di marche temporali.
Lo stesso software può essere utilizzato per l'apposizione della firma remota più avanti descritta e per la verifica di documenti firmati e/o marcati temporalmente.
Le modalità di aggiornamento, come per il software a bordo del token, sono automatiche e di semplice fruizione per l'utente: trovata una nuova release all'avvio, all'utente non rimane che autorizzare o meno la procedura di aggiornamento automatico.

Insieme ai client di firma verranno consegnate le librerie per l'interfacciamento con le applicazioni già in essere presso i fruitori finali, ovvero il prodotto Ellips Capi in grado di interfacciare pienamente entrambi i client di firma sopra descritti. Tali librerie di firma permetteranno l'interfacciamento con le applicazioni di back-office degli Enti.

2.2.1 CERTIFICATI SSL (ANCHE WILDCARD)

I certificati SSL offerti da Aruba PEC sono compatibili con tutte le principali piattaforme client, web browser e web server.
La Root CA utilizzata è inclusa nell'elenco delle CA affidabili di tutte le più diffuse piattaforme e ambienti operativi: MS Windows, Apple OSX/iOS, Google Android, Linux, Oracle Java (JRE/JDK) ed altri.
In caso di aggiudicazione Aruba offrirà un'ampia gamma di certificati richiedibili:

- **SSL Server**: certifica uno specifico host su un singolo dominio (per es. www.example.it)
- **SSL Server SAN**: certifica due o più host, anche su domini o sottodomini diversi
  (es. www.example1.com + mail.aaa.example2.it + mail.bbb.example2.it);
- **SSL Server wildcard**: certifica tutti gli host appartenenti a un singolo dominio (es. *.example.com)

Per ciascun tipo di certificato potrà essere richiesta una durata variabile da 1 anno a 3 anni.

Ciascun certificato acquistato potrà essere installato su un numero qualsiasi di server (fisici o virtuali) per ragioni di alta affidabilità / load balancing.

Caratteristica	SSL Server semplice	SSL Server SAN	SSL Server wildcard
Validazione del dominio	✔	✔	✔
Validazione organizzazione	✔	✔	✔
Supporto CRL	✔	✔	✔
Supporto OCSP	✔	✔	✔
Revoca gratuita	✔	✔	✔
Supporto su tutti i browser	✔	✔	✔
Supporto per SAN multipli	–	✔	–
Licenze server incluse	illimitate	illimitate	illimitate
Tempo di emissione in condizioni normali	3 gg lavorativi	3 gg lavorativi	3 gg lavorativi

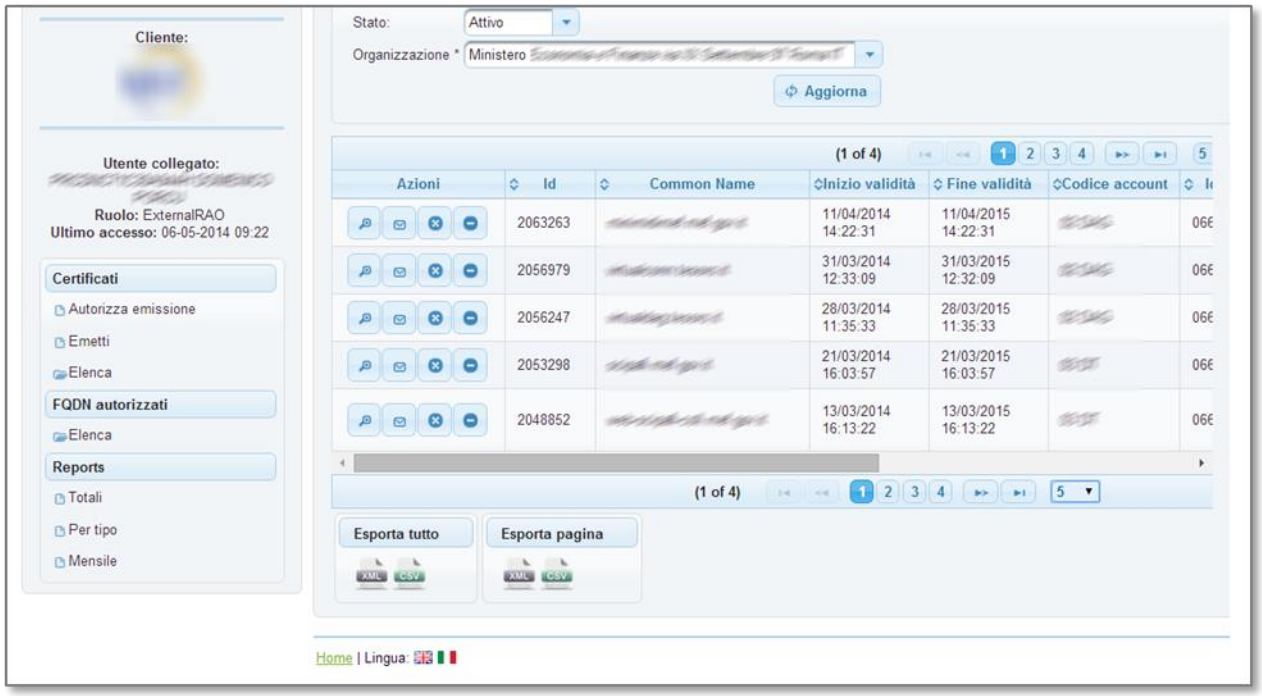
Il profilo dei certificati SSL Server forniti è conforme ai regolamenti del CAB Forum. Prima di emettere il certificato verranno svolte da parte di Aruba verifiche sulla richiesta e sul soggetto richiedente.
In particolare, si verificherà che il dominio Internet da includere nel certificato sia registrato a nome del richiedente e/o che questi abbia il pieno controllo del server da certificare.
Inoltre, verrà accertato il nome dell'organizzazione da includere nel certificato e che essa abbia effettivamente autorizzato la richiesta del certificato.

Oltre ai certificati SSL Server, potranno essere richiesti dagli Enti certificati per Code Signing, in modo da soddisfare ogni necessità di firma di codice eseguibile, compatibili con tutte le principali piattaforme client (Windows, OSX, Java, ecc), garantendo:

- l'origine del software (ovvero il soggetto produttore o distributore);
- che il software è autentico ed integro (quindi non alterato o contraffatto).

Ordine da paret degli Enti
Come per gli altri servizi, l'iter degli ordini da parte degli Enti potrà essere gestito attraverso il Pannello Unico di Gestione di cui al par. 1.2.1.b.

Richiesta ed emissione dei certificati
Per la richiesta di certificati SSL Aruba metterà a disposizione un'interfaccia web di facile uso, che consentirà agli Enti di richiedere e ottenere i certificati in tempo reale e in completa autonomia, per i domini Internet di propria competenza:



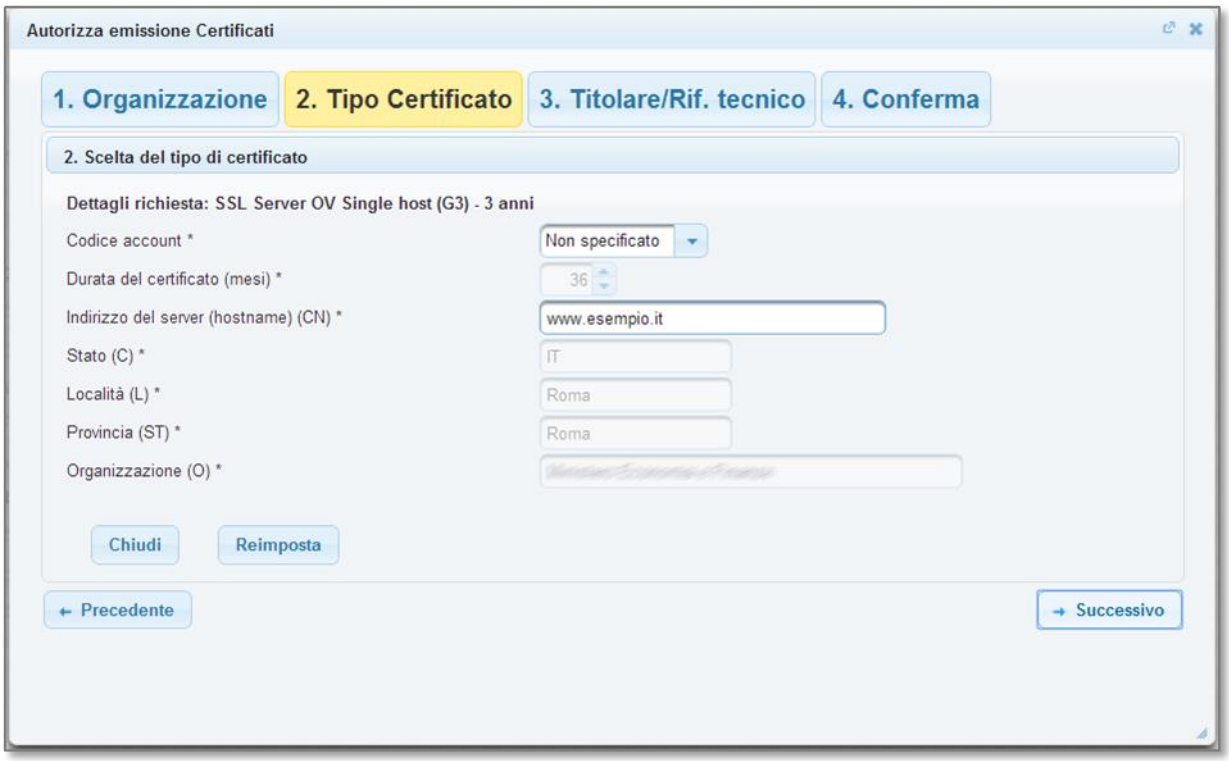
Queste le caratteristiche salienti della pannello al quale verrà fornito accesso dopo la richiesta:

- login sicuro mediante SSL client authentication
- accesso consentito a più operatori
- su richiesta, graficamente personalizzabile
- reportistica completa a video e scaricabile
- controlli automatici di correttezza delle CSR
- invio automatico e-mail al Riferimento Tecnico
- possibilità di notifica di scadenza dei certificati
- software di completa proprietà, possibilità di customizzazioni a richiesta

Il certificato sarà ottenibile in due passi da svolgersi anche separatamente:

1) autorizzazione del certificato
2) inserimento CSR e download del certificato

L'operazione di autorizzazione si basa su un semplice "wizard" che richiede l'inserimento solamente delle informazioni strettamente necessarie:



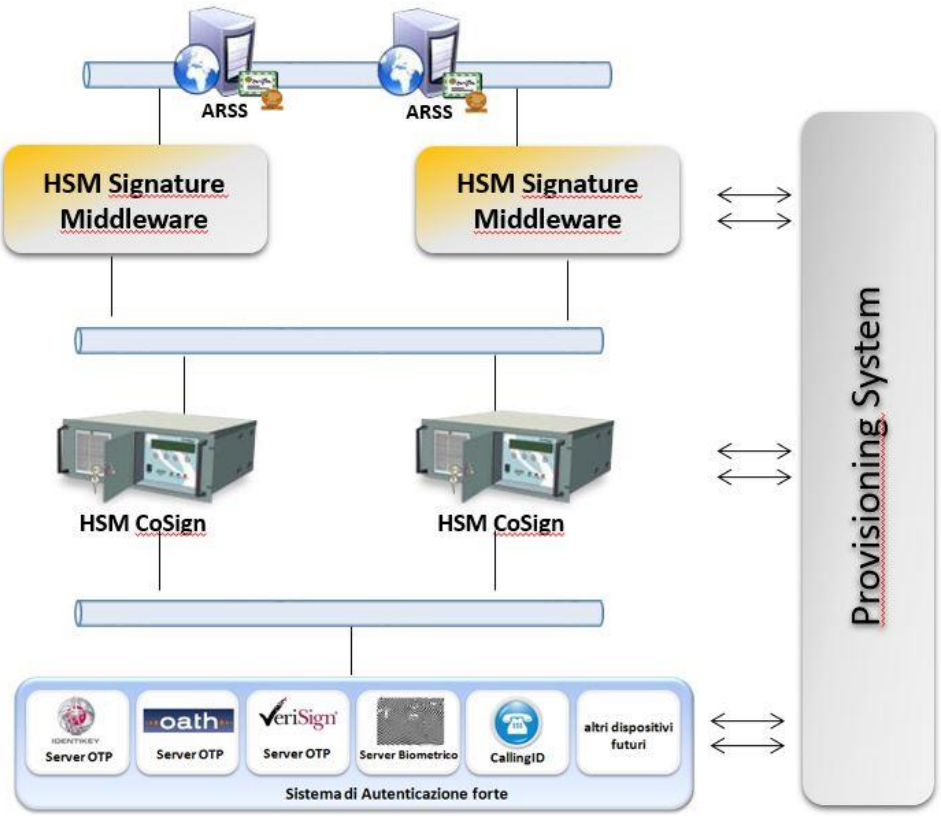
Successivamente, previa verifica dei domini indicati, Aruba genererà un profilo per l'Ente e per gli operatori da esso indicati. L'accesso al pannello richiederà un certificato client individuale che Aruba fornirà a ciascun operatore individuato.

2.3 SERVIZIO DI FIRMA REMOTA

In caso di aggiudicazione Aruba PEC fornirà una soluzione di firma remota flessibile, sicura e di semplice fruizione

La soluzione offerta garantisce funzionalità **sia di firma remota che di firma automatica massiva**. In particolare, il componente ARSS che espone le interfacce di firma potrà essere invocato per entrambe le tipologie di firma. Inoltre, come ulteriore elemento migliorativo, si fa presente che le applicazioni invocando la stessa interfaccia di firma (Web Service) potranno, semplicemente variando i parametri d'invocazione, richiedere il servizio di firma remota o automatica massiva. Questo comporta una enorme semplificazione nell'integrazione delle funzionalità di firma nelle applicazioni oltre che un risparmio sui tempi e costi d'integrazione.

La soluzione è basata sulla seguente infrastruttura:



La soluzione si compone dei seguenti componenti architetturali, ospitati presso le webfarm di proprietà:

- HSM CoSign – HSM all'interno dei quali sono generate e custodite le chiavi e i certificati digitali
- HSM Signature Middleware – componente software di gestione di tutte le richieste da e verso gli HSM
- Sistema di Autenticazione forte – il Sistema di Autenticazione forte è formato da varie componenti che possono essere interfacciate agli HSM CoSign e che consentono un'autenticazione forte del Titolare per lo sblocco delle varie operazioni di firma sull'HSM stesso
- Provisioning System - componente software che gestisce (orchestra) il dialogo con gli HSM, con il Sistema di Autenticazione forte e con la Certification Authority per la corretta attivazione del servizio di firma remota
- HA System & Monitor - componente software, trasversale all'intero sistema di firma remota, formato da vari moduli che gestiscono il monitoraggio del Sistema e che implementano tutte le funzioni necessarie a garantire l'alta disponibilità del servizio (fault-tolerance)
- Aruba Remote Signing Server (ARSS) – componente software che consente la remotizzazione delle funzionalità di firma digitale proprie dell'HSM.

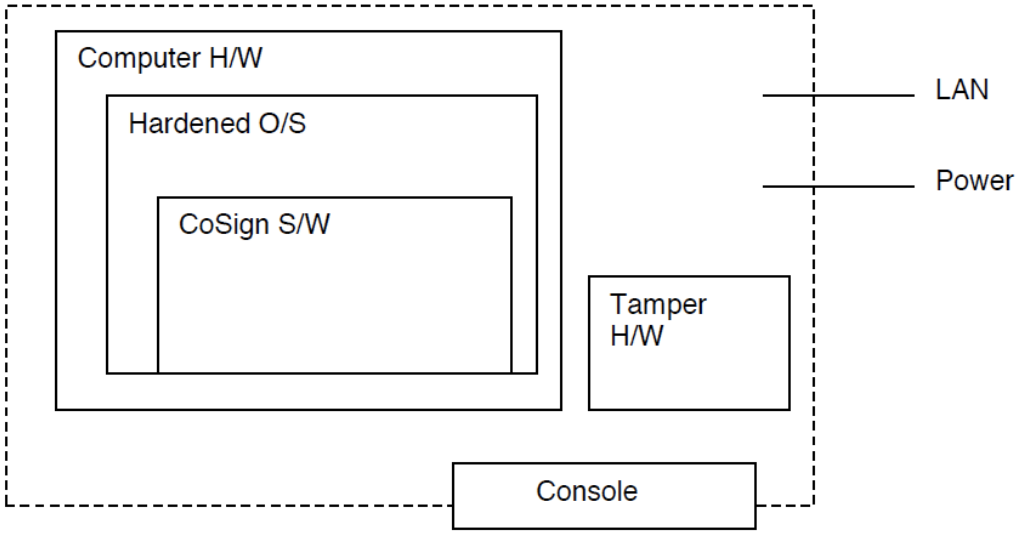
Di seguito sono riportate le caratteristiche principali delle componenti sopra citate:

HSM CoSign

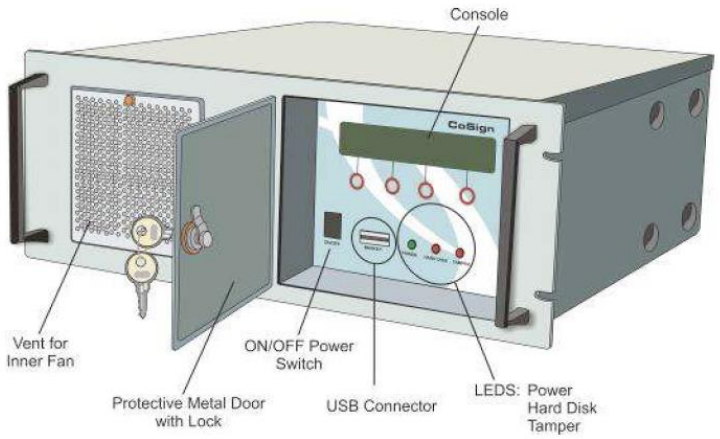
Gli HSM utilizzati dal sistema di firma remota sono il modello **CoSign 7.1** della **ARX**.

Tutte le operazioni critiche dal punto di vista della sicurezza (generazione delle chiavi, utilizzo delle chiavi private per la generazione delle firme, conservazione e confidenzialità delle chiavi private) avvengono esclusivamente all'interno degli apparati **CoSign** protette da numerose funzioni di sicurezza a livello sia hardware (es. anti-tampering) che software.

☞ **Tutte le chiavi private degli utenti ed i relativi certificati sono contenute e persistite esclusivamente all'interno degli HSM**



Il sistema, illustrato nello schema a blocchi, offre all'esterno esclusivamente interfacce certificate. Qualsiasi comunicazione con CoSign avviene esclusivamente attraverso canali sicuri (SSL, VPN). L'intero HSM è protetto da un robusto case di metallo con opportuni accorgimenti anti-intrusione.



L'apparato CoSign ha ottenuto dall'**OCSI** (Organismo di Certificazione della Sicurezza Informatica) la **certificazione CC EAL4+** richiesta dalla normativa vigente (cfr.

http://www.ocsi.isticom.it/index.php/elenchi-certificazioni/prodotti-certificati) oltre che, sempre in OCSI, ad aver **concluso con successo la Procedura di Accertamento** di Conformità di un Dispositivo per la creazione di Firme Elettroniche ai Requisiti di Sicurezza previsti dall'Allegato III della Direttiva 1999/93/CE (cfr. http://www.ocsi.isticom.it/index.php/dispositivi-di-firma/dispositivi-accertati).

In sintesi, l'HSM "Cosign" usato nell'ambito del sistema di firma remota qui descritto e proposto, è **pienamente conforme alla vigente normativa in materia di firma digitale** ed in particolare al:

- DPCM 10 Febbraio 2010, "*Fissazione del termine che autorizza l'autocertificazione circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza*";
- DPCM 14 Ottobre 2011, "*Proroga del termine che autorizza l'autocertificazione circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza di cui al decreto del Presidente del Consiglio dei Ministri 30 ottobre 2003*".
- DPCM 19 Luglio 2012 "*Definizione dei termini di validità delle autocertificazioni circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza di cui al decreto del Presidente del Consiglio dei Ministri 30 Ottobre 2003, e dei termini per la sostituzione dei dispositivi automatici di firma*"
- DPCM 22 Luglio 2013 "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b) , 35, comma 2, 36, comma 2, e 71"

Ai seguenti link (sito web dell'OCSI -Organismo di Certificazione della Sicurezza Informatica) è possibile scaricare:

- Il **Rapporto di Certificazione**

  http://www.ocsi.isticom.it/documenti/certificazioni/arx/rc_arx_cosign_v1.1.pdf

- ✓ Il **Rapporto di Accertamento**

  http://www.ocsi.isticom.it/documenti/accertamenti/arx/ac_rda_cosign_v1.1.pdf

HSM Signature Middleware

Componente software al quale viene demandata la completa gestione delle connessioni generate:

- dall'applicazione client di firma remota fornita da Aruba PEC a completamento della fornitura;
- dai server ARSS che offrono le funzionalità di firma proprie dell'HSM ad applicazioni non direttamente disponibili nell'infrastruttura di rete che ospita il sistema di firma digitale remota;
- dalle applicazioni (sia web che non), integrate con il sistema di firma remota, che richiedono la firma digitale dei documenti da queste prodotti.

Si noti che il Signature Middleware è in grado, oltre che di gestire più sessioni contemporanee, di bilanciare il carico sugli HSM in esso configurati.

Data l'architettura implementata, la soluzione è scalabile sia orizzontalmente che verticalmente.

Sistema di Autenticazione forte

Il sistema di firma digitale remota prevede che ciascun utente, per poter firmare digitalmente un documento elettronico, inserisca una Username, Password ed un codice One Time Password (OTP)

La soluzione proposta è caratterizzata dal consentire l'utilizzo di varie tipologie di sistemi di autenticazione forte, che potrebbero anche essere attivati contemporaneamente dagli Utenti (non necessità di distribuire una sola tipologia di autenticazione forte).
Di seguito si elencano i sistemi OTP forniti da Aruba PEC (basati sui protocolli del consorzio OATH):

- OTP SMS
- OTP con Display OTP
- OTP USB, basato sui protocolli del consorzio OATH
- App Mobile OTP per smartphone e tablet (iPhone, Android, Windows Phone, Blackberry)
- ArubaCall, soluzione OTP che utilizza il numero di telefono (caller ID) del chiamante come mezzo per comunicare all'Utente il codice OTP generato dal sistema in quello specifico momento e per quella specifica operazione di firma. All'atto della firma l'Utente riceverà una chiamata dall'Ente Certificatore e le ultime 4 cifre del numero visualizzato sul proprio Telefono Cellulare (qualsiasi telefono cellulare che visualizzi il caller ID) rappresentano il codice OTP da inserire per richiedere la firma dello specifico documento.

Provisioning System

Il Provisioning System è la componente software che gestisce le varie fasi necessarie all'attivazione del servizio di firma remota. Questo componente si interfaccia con i vari sistemi per la verifica delle credenziali di attivazione, gestendo il dialogo con le componenti di Autenticazione forte e con l'HSM CoSign per la creazione (laddove richiesto) degli account e con la Certification Authority per la generazione dei certificati digitali. Un possibile processo di attivazione del Servizio è descritto successivamente nel presente documento.

HA System & Monitor

Questo componente software è formato da vari moduli che interagiscono con le varie componenti del Sistema di firma digitale remota al fine di monitorare lo stato dell'intero sistema e la disponibilità del servizio erogato.

In caso di failure, l'HA monitor rileva il malfunzionamento del componente e provvede alla notifica agli amministratori del sistema tramite vari canali di comunicazione opportunamente configurati.

Aruba Remote Signing Server (ARSS)

ArubaPEC Remote Signing Server è il componente software che permette una semplice integrazione delle applicazioni e dei sistemi con il Servizio di firma digitale remota. Nel caso di applicazioni (già in uso o future) ospitate in infrastrutture IT (siti di produzione) differenti da quella dove risiede il Sistema di firma digitale remota proposto, ARSS provvederà a dialogare, su canale sicuro di comunicazione (HTTPS) con mutua autenticazione, con il Sistemi di firma remota, esponendo verso le applicazioni in questione le funzionalità di firma digitale.

In generale, il sistema di firma remota/automatica proposto garantisce, conformemente a quanto previsto dalla normativa vigente, le seguenti caratteristiche (elenco non esaustivo):

- firma di un documento in formato CADES-BES e CADES-T (secondo quanto previsto dalla Deliberazione 45/2009 e successiva Determina 69/2010)
- firma di un documento in formato PADES-Basic, PADES-BES e PADES-T (secondo quanto previsto dalla Deliberazione 45/2009 e successiva Determina 69/2010)
- firma di un documento in formato XADES-BES e XADES-T (secondo quanto previsto dalla Deliberazione 45/2009 e successiva Determina 69/2010)
- firme multiple (parallele e controfirme)

- firme multiple in modalità "matrioska"
- firma detached
- firma di un hash (impronta), nel caso in cui le applicazioni provvedano autonomamente alla creazione del documento firmato
- firma di tutti i documenti contenuti in una cartella specificata, nei formati sopraindicati
- Gestione documenti in Streaming (inteso come ottimizzazione di volumi importanti di documenti che prevedono l'invio alla CA del solo hash del documento)
- Marcatura temporale in tutte le forme previste dalla normativa vigente
- verifica firma singola/multipla
- verifica dello stato del certificato (con API separata da quella di verifica della firma).
- Documentazione utente.
- Documentazione API per lo sviluppo software.
- Adeguamenti normativi futuri

La stessa componente è in grado di gestire funzionalità di firma remota automatica.

Sicurezza della soluzione
L'architettura del sistema di firma remota/automatica di ArubaPEC è caratterizzata da meccanismi di fault tolerance e bilanciamento del carico lungo l'intera filiera elaborativa; infatti, ogni componente (HW e SW) dell'architettura è ridondata al fine di escludere "single point of failure". La stessa ridondanza si applica anche ai dispositivi HSM, su cui vengono gestiti i certificati di firma digital
La soluzione proposta prevede un sistema di Disaster Recovery ospitato presso il CED secondario di Aruba PEC che, a livello architetturale, presenta le stesse componenti di base del sito primario riducendo solamente il grado di ridondanza previsto.

Le macchine installate presso il data center secondario sono mantenute costantemente allineate a quelle di produzione con periodicità pari a 3 ore. Inoltre, i backup dei sistemi delle singole macchine coinvolte sono giornalmente trasferiti nel data center secondario per storicizzazione ed eventuale recupero relativo ai giorni precedenti.

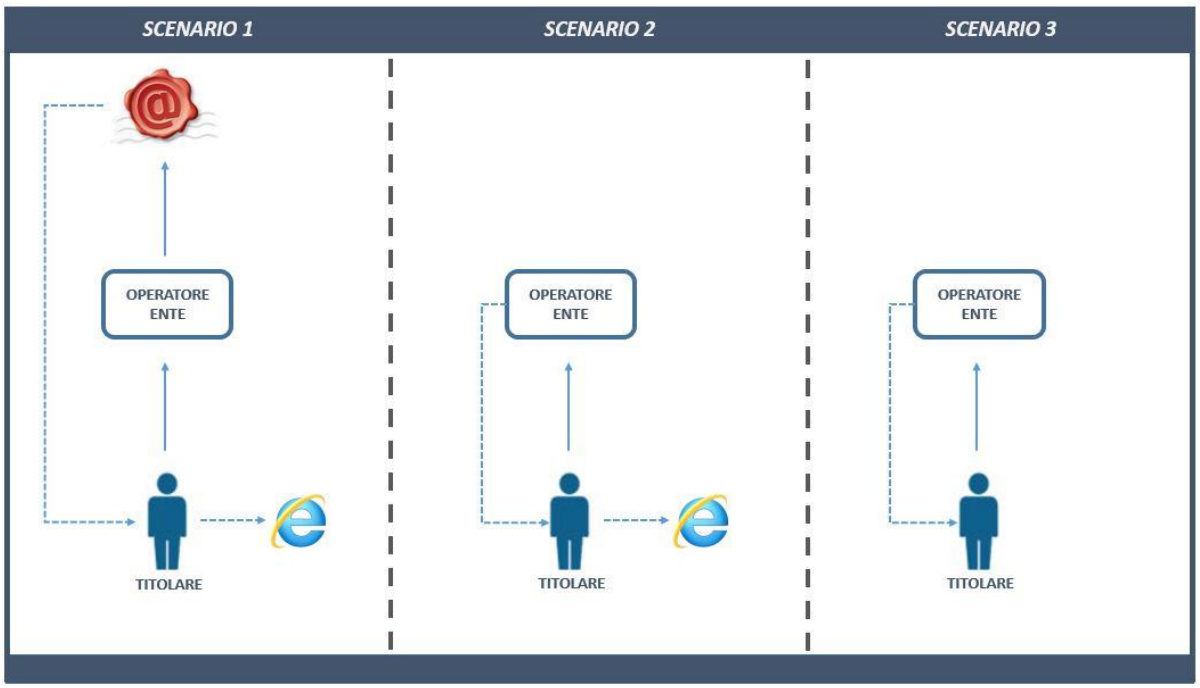
I database sono inoltre tenuti allineati con quelli di disaster recovery con gli strumenti nativi di replica asincrona da essi offerti, come per le altre componenti è previsto un riallineamento ogni 3 ore. Oltre a questo il backup giornaliero dei database coinvolti sarà giornalmente trasferito nel sito secondario per storicizzazione ed eventuale recupero relativo ai giorni precedenti.

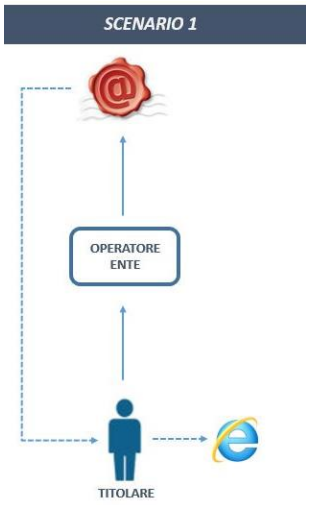
Tutte le attività di manutenzione verranno comunicate con congruo anticipo alla Stazione Appaltante, riducendo al minimo le eventuali interruzioni di servizio necessarie.

Emissione e gestione certificati
Gli account di firma richiedibili saranno costituiti da tre credenziali:
- username;
- password;
- otp.

L'impiego di questa tripletta consentirà ai titolari l'apposizione di firme in modalità remota attraverso i software più avanti descritti.
Aruba PEC offre diverse tipologie di strumenti per la generazione di OTP (One Time Password), tutte richiedibili attraverso la soluzione fornita.
Nello stesso modo, sarà facoltà degli operatori richiedere kit di firma remota per i quali il processo di attivazione finale rimarrà in carico al richiedente, oppure disporre di kit "vergini" (Scracth card ed eventuali token OTP fisici) da attivare on-demand e consegnare pronti all'uso al richiedente.

Stanti gli strumenti di gestione forniti, saranno possibili tre scenari di richiesta ed attivazione dei kit di firma remota:

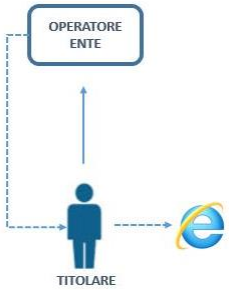




Questo flusso di richiesta prevede:

- l'utente richiede la firma all'operatore di riferimento dell'Ente;
- l'Ente preposto inoltra la richiesta ad Aruba PEC, tramite gli strumenti forniti;
- Aruba PEC produce il kit e lo spedisce all'Ente del caso;
- il titolare riceve le credenziali ad attiva il proprio account di firma remota con procedura online.

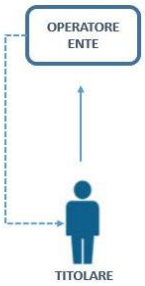
SCENARIO 2



Questo flusso di richiesta prevede:

- l'utente richiede la firma all'operatore di riferimento dell'Ente;
- L'operatore Ente produce il KIT attraverso gli strumenti forniti e i dispositivi vergini precedentement richiesti ad Aruba PEC;
- il titolare riceve le credenziali ed attiva il proprio account di firma remota con procedura online.

SCENARIO 3



Questo flusso di richiesta prevede:

- l'utente richiede la firma all'operatore di riferimento dell'Ente;
- L'operatore Ente produce il KIT attraverso gli strumenti forniti e i dispositivi vergini precedentement richiesti ad Aruba PEC;
- L'operatore attiva l'account di firma remota attraverso gli strumenti forniti;
- l'utente riceve il kit di firma remota direttamente attivo e pronto all'uso.

Ogni firma remota così rilasciata sarà abilitata all'apposizione di un numero illimitato di sottoscrizioni digitale da parte degli utenti abilitati ed un numero qualsiasi di documenti per ciascuna invocazione del servizio.

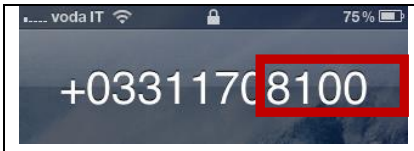
Tipologie di token OTP a disposizione

Le varie tipologie di token abbinabili al proprio kit di firma remota forniscono tutte pari garanzie di sicurezza e semplicità d'uso.
Sarà possibile scegliere in autonomia, mediante l'interfaccia fornita da Aruba PEC, la soluzione di strongh autentication legata alla firma remota che preferisce utilizzare tra le seguenti:

- Token display

	Si presenta come una chiavetta dotata di display LCD e pulsante per la generazione dei codici temporanei. Il punto di forza della soluzione hardware-display è la sua totale similarità con i dispositivi di accesso sicuro ai portali di home-banking, sempre più diffusi ed utilizzati dai cittadini.

- ArubaCall

	Utilizzando questa tipologia di token il titolare riceve, al momento dell'apposizione della firma, una chiamata al proprio dispositivo mobile: le ultime cifre del numero di telefono chiamante costituiranno l'OTP.

- Aruba SMS

	In maniera analoga all'ArubaCall, l'utente riceve un SMS contenente l'OTP necessario ad autorizzare la firma.

- OTP Mobile

	Questa soluzione prevede l'installazione dell'App Aruba mobile OTP a bordo del cellulare del titolare Una volta installata, baterà cliccare su "genera nuovo OTP" per ottenere i codici utili all'apposizione di firma remota. L'OTP Mobile potrà essere personalizzato con il logo di Regione del Veneto, come fatto con successo per altri clienti di Aruba PEC (ad es. OTP FVG Insiel, BankitOTP - Banca d'Italia, ecc.).

In ogni caso l'attivazione dei kit illustrati potrà avvenire online a cura del titolare/richiedente, presso le pagine di servizio che Aruba fornirà in caso di aggiudicazione.
Su richiesta degli Enti, potranno essere forniti kit di firma remota vergini, la cui attivazione potrà essere effettuata direttamente dagli operatori – tramite gli strumenti forniti – in modo da consegnare all'utente finale un account pronto all'uso.
I kit di firma remota forniti saranno abbinati a scratchcard, ovvero dispositivi del formato di una carta di credito utili alla custodia sicura dei codici di utilizzo e gestione dell'account.

Attivazione dell'account di firma remota
Come anticipato, i kit di firma remota potranno essere attivati direttamente "allo sportello" oppure tramite procedura online da parte del titolare.
In questo secondo caso l'utente si avvarrà delle pagine appositamente predisposte da Aruba PEC, ovvero si collegherà al portale di attivazione firma remota scegliendo il token da abbinare alla propria firma:

Si autenticherà inserendo il proprio codice fiscale ed uno dei dati contenuti nella scratchcard:

Dopodiché seguendo la procedura guidata sarà in grado di attivare autonomamente il proprio account.
Al termine della procedura riceverà un'email confermante l'avvenuta attivazione.

Gestione dell'account di firma remota

Una volta attivato il proprio account sarà possibile per il titolare gestirlo in maniera del tutto autonoma, attraverso le funzionalità online messe a disposizione dalla sezione Firma remota interna al portale di servizio fornito (par. 1.2.1.b).
Sarà infatti possibile per il titolare autenticarsi con le proprie credenziali, tipicamente nome utente e password:

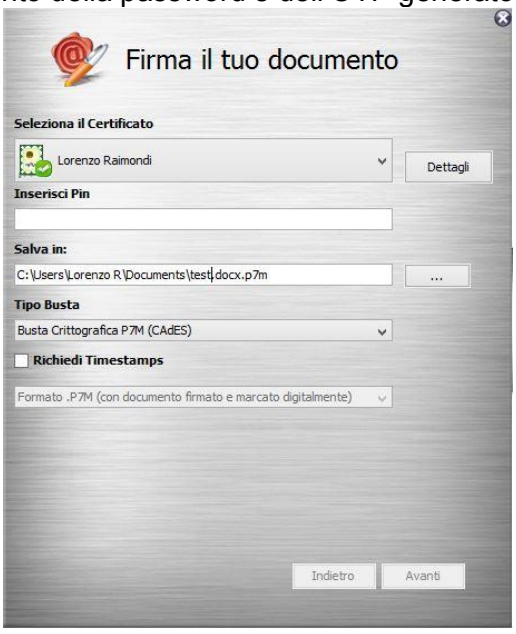
Per aver accesso alle seguenti funzionalità:
- cambio password;
- recupero password;
- recupero nome utente;
- resync token;
- cambio telefono

attraverso semplici e sicure procedure guidate, che richiederanno all'utente l'inserimento di codici di sua esclusiva conoscenza e si avvarranno di telefono cellulare (SMS) ed email per l'eventuale comunicazione dei dati richiesti.

Software per l'apposizione di firme remote
Le firme remote Aruba potranno essere utilizzate con i dispositivi di seguito illustrati.

- **ArubaSign**
Il client di firma ArubaSign, già valido per l'apposizione di firma tramite smartcard, offre la possibilità di firmare in modalità remota i propri documenti digitali.
Dopo aver inserito il proprio username all'interno del tab "Configurazione",

sarà sufficiente trascinare il file desiderato all'interno dell'area firma.
Il software richiederà l'iserimento della password e dell'OTP generato dal dipositivo in dotazione:



La scelta del formato firma desiderato, ed in pocchissimi istanti resituirà il documento sottoscritto nel formato prescelto (Cades, Pades, Xades).

- **App Mobile**
Saranno resi disponibili a tutti gli utenti anche gli applicativi di *generazione* e *verifica* firma per ambiente mobile che Aruba ha già rilasciato, in particolare per le piattaforme **Apple iPad** e **Google Android**. Si tratta di applicazioni di assai facile uso e conformi alla normativa vigente, scaricabili direttamente dagli "app store" dei relativi vendor (Apple iTunes Store, Google Play).

Entrambe le applicazioni:

- permettono la verifica completa di file firmati in standard CAdES e PAdES;

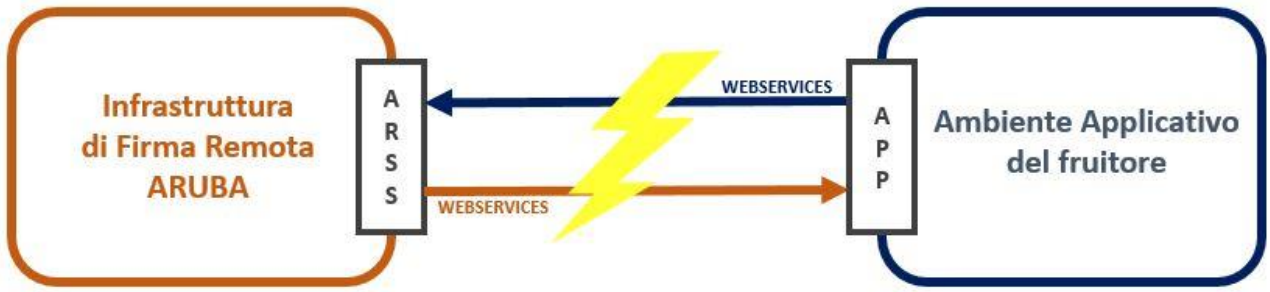
- permettono la generazione (con procedura remota) di firme CAdES e PAdES;
- supportano la marcatura temporale sia in verifica che in generazione.

Le figure seguenti mostrano alcune delle principali finestre di dialogo dell'applicazione:



- Aruba Remote Signing Server

Come sopra anticipato, l'infrastruttura di firma remota sarà della componente di remotizzazione ARSS, dedicata all'esposizione delle funzioni di firma remota.
Aruba Remote Signing Server è infatti il componente software che permette una semplice integrazione delle applicazioni e dei sistemi già in uso presso l'Organizzazione/Utente con i servizi di firma remota Aruba PEC.



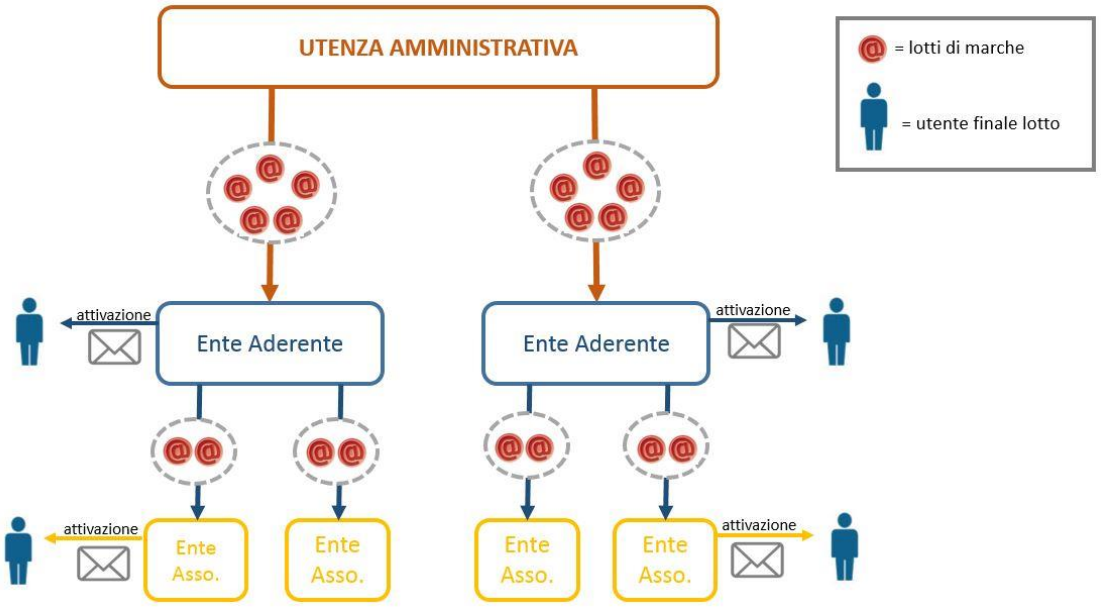
Tali funzionalità, già elencate in precedenza, sono rese disponibili tramite una semplice interfaccia Web Services (SOAP).

Il componente ARSS ha superato con successo i test di interoperabilità con tutti i certificatori accreditati DigitPA relativi alla produzione di firme in formato CAdES, PAdES e XAdES ed è funzionale anche all'appposizione di marcature temporali.

2.4 SERVIZIO DI MARCATURA TEMPORALE

Attraverso il Pannello Unico di Gestione sarà possibile, per i vari Enti coinvolti, gestire ed attivare pacchetti di marche temporali nelle quantità richieste, oltre a raccogliere gli ordini da parte degli Enti.
Sarà possibile infatti assegnare agli Enti Aderenti che ne facciano richiesta uno o più lotti da:

100, 1.000, 10.000 e 100.000 marche temporali.
L'Ente Aderente così servito potrà decidere se fruire direttamente dei lotti a disposizione, attivando gli account ed assegnandone le rispettive credenziali, oppure cederli – tutti o in parte – ai vari Enti Associati ad esso afferenti, qualora questi ne facciano richiesta.
Gli operatori abilitati potranno dunque attivare ed assegnare i pacchetti a disposizione, semplicemente inserendo l'email del destinatario/fruitore individuato:
il sistema provvederà in maniera automatica alla generazione delle credenziali (username e password), inviandole per email all'indirizzo specificato.



In questo modo sarà possibile per l'Ente Aderente mantenere visibilità costante dei lotti a propria disposizione, di quelli assegnati e di quelli residui presso gli Enti Associati del caso.
Il pannello unico di gestione darà inoltre evidenza delle marche residue per ogni lotto già attivato.

Apposizione di marche temporali
Le marche temporali fornite potranno essere utilizzate con qualunque strumento di firma sinora descritto:
- ArubaSign;
- ArubaKEY;
- App Mobile;
- Webservices;

anche in modalità detached.

Sarà sufficiente inserire le proprie credenziali, con possibilità di salvarle nel caso di utilizzo via client, e richiedere una marca per il documento selezionato, come illustrato nei paragrafi dedicati all'illustrazione dei software forniti.
Gli stessi strumenti daranno la possibilità di effettuare l'operazione "firma e marca" in unica procedura.

Caratteristiche del servizio
Il servizio di marcatura temporale offerto da Aruba è fruibile attraverso protocollo HTTPS, i formati e la codifica delle richieste accettate e delle marche temporali restituite dal servizio sono conformi alle strutture dati descritte nella RFC 3161.
La richiesta viene accettata dal web server servizi.arubapec.it, tramite l'indirizzo https://servizi.arubapec.it/tsa/ngrequest.php con le credenziali fornite da Aruba PEC S.p.A. al momento dell'attivazione dell'account TSA.

Il servizio di TSA ArubaPec accetta solo ed esclusivamente richieste di marcatura temporale contenenti impronte dell'evidenza informatica da sottoporre a validazione temporale calcolate secondo l'algoritmo hash SHA-1 (dedicated hash-function 3 definito nella norma ISO/IEC 10118-3:2004) e secondo l'algoritmo hash SHA-256 (dedicated hash-function 4 definito nella norma ISO/IEC 10118-3:2004).
Nel caso in cui il sistema TSA riceva una richiesta di marcatura temporale non conforme al requisito di cui sopra viene restituito un messaggio di errore.

Sicurezza logica e fisica del sistema di marcatura temporale
Gli elaboratori che offrono il servizio di marcatura temporale possiedono i medesimi requisiti di protezione previsti dagli elaboratori utilizzati per la generazione dei certificati di firma digitale, e sono protetti da livelli di protezione logica estremamente elevati. La medesima collocazione fisica del sistema di validazione temporale garantisce gli elaboratori dalla possibilità di compromissioni fisiche grazie agli accorgimenti tecnici atti ad impedire accessi non autorizzati da persone e danneggiamenti da eventi accidentali.

Sicurezza fisica
Il sistema di validazione temporale reso disponibile da Aruba ai propri titolari si basa su dei server web di Front-end che gestiscono le transazioni con i client, l'autenticazione, l'accounting e l'archiviazione delle marche temporali e dei server di Back-end che si occupano della creazione delle marche temporali e della gestione degli apparati di acquisizione e sincronizzazione del riferimento temporale. I server del sistema di validazione temporale sono ospitati in sale tecniche ad accesso controllato attraverso badge e/o fattore biometrico.
Solo il personale autorizzato può accedere a tali sale. Questi ambienti, inoltre, sono protetti da allagamenti ed incendi mediante appositi presidi (sensori, spruzzatori, condiziona-mento, etc) e gli elaboratori sono alimentati con linea elettrica preferenziale, sorretta da gruppo di continuità.

Sicurezza logica
I server di Front-end e di Back-end del sistema di validazione temporale dialogano tra loro attraverso protocolli di comunicazioni sicuri e possono essere attivati solo da operatori autorizzati. In particolare, i server di Back-end firmano le marche temporali mediante un dispositivo crittografico hardware (o "dispositivo di firma") di altissima qualità e sicurezza. L'algoritmo di sottoscrizione utilizzato è RSA con chiave di lunghezza 2048 bit ed usata esclusivamente a scopo di marcatura temporale. La coppia di chiavi RSA è generata all'interno del dispositivo di firma. La chiave privata della coppia è usata all'interno del dispositivo di firma. Il dispositivo di firma può essere attivato solo da un operatore appositamente autorizzato e dotato della necessaria parola-chiave.

Le marche temporali fornite in caso di aggiudicazione saranno emesse dalla Time Stamp Authority Aruba PEC. Come sancito dall'articolo 49 del Dpcm del 30/03/2009, le Marche Temporali verranno conservate in appositi archivi per un periodo non inferiore a 20 anni.

2.5 DOCUMENTAZIONE MESSA A DISPOSIZIONE

Tutti i servizi messi a disposizione saranno corredati da idonea documentazione relativa all'uso, agli aspetti tecnici e/o formali coinvolti.

Di seguito il dettaglio di quanto previsto:

FIRMA DIGITALE / CERTIFICATI DI AUTENTICAZIONE
Certificati Root CA
Manuale Operativo certificato di sottoscrizione
Manuale Operativo certificato di autenticazione
Certificate Policy CNS

Guida all'uso Token USB
Guida al ripristino del software
Guida all'uso ArubaSign
Guida alla cifratura delle email
Modulo per richiesta certificati
Modulo per richiesta revoca

FIRMA REMOTA
Guida all'uso kit di firma remota
Manuale per la gestione dell'account di firma remota
Guida all'integrazione dei servizi con web services (Manuale per lo sviluppatore)

MARCHE TEMPORALI
Manuale Operativo
Guida all'uso
Guida all'integrazione dei servizi con web services (Manuale per lo sviluppatore)

CERTIFICATI SSL
Certification Practice Statement (CPS)
Certificato della Root CA e della SubCA
Modulo di Richiesta certificato
Modulo di Richiesta Revoca

INTERFACCIA OPERATORE
Guida all'uso

In accordo con la Regione, parte della documentazione elencata potrà essere pubblicata sul portale di servizio fornito (par. 1.2.1.b).

2.6 FUNZIONALITA' AGGIUNTIVE

Seguendo la tabella proposta in sede di Capitolato Tecnico dalla Stazione appaltante, vengono di seguito riassunte le "funzioni aggiuntive" incluse nei servizi offerti e descritte nei paragrafi precedenti:

FUNZIONALITA'	DESCRIZIONE
Funzioni di firma mediante strumenti "mobile"	Tutte le tipologie di firma remota offerte, indipendentemente dal tipo di strumento OTP abbinato, potranno essere utilizzate per l'apposizione di firme attraverso l'app di firma "ArubaSignOnline..", Tale app, disponibile per IPAD ed ambiente Android, è scaricabile gratuitamente presso i web market di riferimento, e consente: - apposizione di firme

	- apposizione di marche - verifica di file firmati - gestione file firmati / da firmare mantenendo tutte le caratteristiche di affidabilità e sicurezza già garantite dal software ArubaSign illustrato nel paragrafo ad esso dedicato. Come precedentemente illustrato, i KIT di firma remota "ArubaCall" ed "ArubaOTPmobile" si avvarranno del dispositivo mobile del titolare come strumento per la generazione di codici OTP sicuri.
Memoria interna Token USB	I token USB in fornitura saranno dotati di memoria interna pari a **8Gb**.
Kit di firma personalizzati	I dispositivi smartcard, le scratchcard ed i token USB potranno essere personalizzati con la grafica concordata con l'Ente Aderente, in fase di avvio del servizio.
Rinnovo in self provisioning	All'approssimarsi della scadenza dei certificati Aruba PEC si occuperà dell'invio automatico di email di avviso a titolari, il numero e la cadenza potrà essere concordato con la Stazione Appaltante. I titolari così avvisati potranno accedere alle funzioni di rinnovo online esposte sul portale di servizio dedicato, in modalità self-provisioning, ovvero senza coinvolgimento di ulteriori attori.
Firma contemporanea di più documenti	I software di firma forniti (ArubaSign ed ArubaKEY) sono in grado di effettuare la sottoscrizione di più file contemporaneamente. E' infatti sufficiente selezionare (o trascinare) più files, anche raccolti in cartella, ed effettuare la consueta procedura di firma, come se si trattasse di un solo file (compreso l'inserimento di un solo pin/dispositivo). Analoghe funzionalità di firma multipla sono offerte dalla componente di remotizzazione dei servizi di firma ARSS.
Funzioni di firma Pades e Xades	Gli strumenti di firma offerti sono i grado di eseguire firme di tipo: - Cades; - Pades (più versioni); - Xades; conformi agli standard normativi. Per i formati che lo consentono, è possibile inoltre effettuare firme di tipo "parallelo" e "controfirme".

3 SERVIZIO DI POSTA ELETTRONICA CERTIFICATA

3.1 STRUMENTI E MODALITA' ORGANIZZATIVE PER LA GESTIONE DEL CICLO DI VITA DEL SERVIZIO

Aruba PEC gestisce, ad oggi, oltre 4 milioni di caselle PEC su domini generici (pec.it.gigapec.it, ecc) e personalizzati (ad esempio pec.nomeente.it, pec.nomeazienda.it) per pubbliche amministrazioni, aziende e privati. Il servizio è erogato in piena conformità alla normativa vigente e nel rispetto dei principali requisiti di affidabilità e sicurezza che la criticità e l'importanza del prodotto richiedono.
Il servizio prevede la migrazione delle caselle attualmente esistenti (e gestite da un altro gestore) oltre alla possibilità di creare nuove caselle sui domini attualmente assegnati all'Amministrazione Regionale (pec.regione.veneto.it, pecveneto.it) o sui domini assegnati agli enti aderenti. Se necessario sarà inoltre possibile creare dei nuovi domini PEC di secondo (ad esempio miodominiopec.it) o di terzo livello (ad esempio pec.miodominio.it).
Ogni casella sarà personalizzabile secondo il volere degli enti aderenti ed associati (ad esempio: nomecasella@pec.nomeente.it).

Oltre alle caratteristiche delle caselle che verranno fornite, di seguito si riporta una proposta di gestione delle richieste di attivazione e rilascio delle stesse. Il processo proposto, che offre come valore aggiunto la completata autonomia dell'Ente nelle fasi di attivazione e chiusura di una casella PEC, potrà comunque essere modificato in accordo con la Regione del Veneto in fase di avviamento del servizio.

In ogni caso, per ogni servizio offerto Aruba PEC consegnerà a Regione del Veneto e all'Ente Aderente, con frequenza e modalità che saranno concordate, una relazione dettagliata per singolo Ente sullo stato e la quantità dei servizi attivati ed erogati. Tali dati potranno comunque essere reperiti in autonomia anche all'interno dello strumento di monitoraggio che verrà messo a disposizione della fornitura, come descritto nel Capitolo 7.

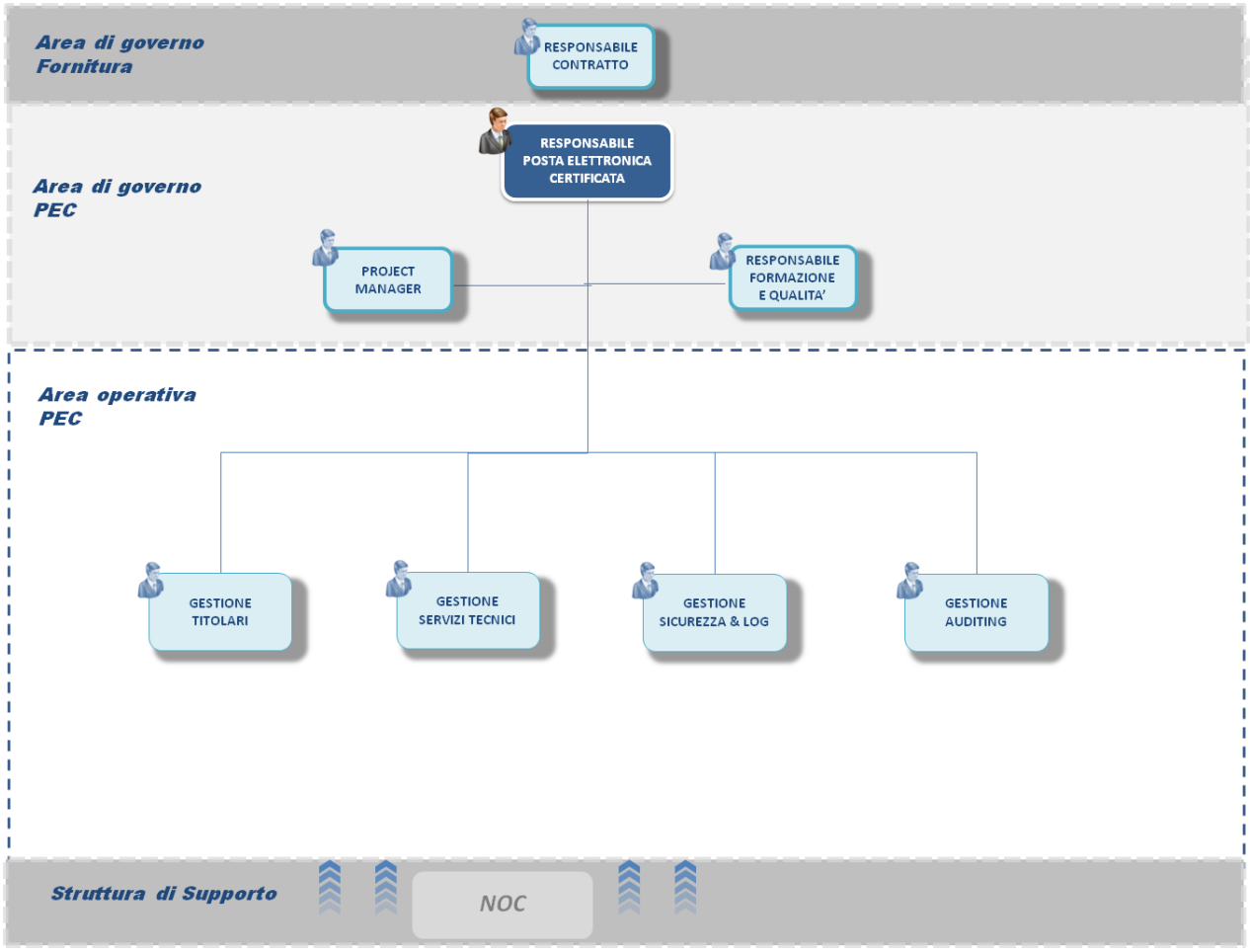
Aruba PEC garantisce il rispetto dei livelli di servizio richiesti nel par. 5.2.4 del Capitolato: i relativi dati verranno messi a disposizione all'interno dello strumento di monitoraggio che permetterà di avere una visione completa del rispetto degli SLA concordati.

I servizi offerti saranno disponibili, 24 ore al giorno e 7 giorni su 7 nel rispetto degli SLA previsti dal capitolato e monitorati attraverso lo strumento fornito da Aruba PEC e descritto nel Capitolo 7.

I fermi programmati e gli interventi di manutenzione straordinaria, ossia le interruzioni del servizio necessarie per svolgere attività di manutenzione verranno preferibilmente effettuati nella fascia oraria notturna, previa comunicazione scritta agli Enti Aderenti, da inviare con un anticipo di almeno 5 giorni lavorativi.

3.1.1 ORGANIZZAZIONE DEL SERVIZIO DI POSTA ELETTRONICA CERTIFICATA

All'interno del **modello organizzativo del Servizio di Posta Elettronica Certificata** si distinguono due aree specifiche: l'**Area di governo** e l'**Area operativa**.



Ciascun utente della Regione del Veneto può usufruire del **Servizio di Posta Elettronica Certificata** come centro di competenza identificato a gestire le richieste di attivazione dei servizi di posta elettronica certificata (**PEC**). L'organizzazione del **Servizio di PEC** prevede la sinergia tra figure professionali appartenenti a **due distinte aree funzionali**.
All'interno dell'**Area di Governo del Servizio di PEC** sono presenti le seguenti figure:

- ✓ **Responsabile PEC** – è supervisore dell'intero **Servizio di PEC**. Coordina le attività svolte dai singoli team di gestione: titolari, servizi tecnici, sicurezza & log, auditing. Ha inoltre il compito di coinvolgere la figura del **Responsabile Formazione e Qualità** qualora sia necessario un miglioramento qualitativo sugli aspetti operativi. A seguito della firma del contratto il suo nominativo e i relativi recapiti (telefono, fax, mail) verranno comunicati formalmente all'Ente Aderente in modo da mettere in piedi tutte le attività propedeutiche all'avviamento del servizio, quali ad es. attivazione e migrazione delle caselle, preparazione e consegna del manuale utente, attivazione dei canali di comunicazione, pianificazione delle eventuali attività formative ecc..

- ✓ **Responsabile Formazione e Qualità** – rappresenta il responsabile del livello di competenze e della qualità operativa svolta dai singoli team di gestione del **Servizio di PEC**. Tale figura interagisce con il **Responsabile PEC** e garantisce l'aggiornamento ed il miglioramento continuo di processi/procedure utili a perfezionare il livello di servizio.

L'**Area Operativa Posta Elettronica Certificata** ha la responsabilità di fornire operativamente il servizio agli utenti di riferimento della Regione del Veneto e degli Enti aderenti – secondo le seguenti figure:

- ✓ **Gestione Titolari** – team di supervisione della corretta attivazione del **servizio di PEC** con la corretta associazione del **titolare della casella PEC**. Verifica inoltre la correttezza degli adempimenti contrattuali e della documentazione identificativa dei titolari delle caselle PEC.

- ✓ **Gestione Servizi Tecnici** – team di monitoraggio e verifica delle performance del servizio PEC. Verifica inoltre la corretta funzionalità del servizio PEC e delle procedure tecniche e/o funzionali.
- ✓ **Gestione Sicurezza & Log** – team di controllo dei livelli di accesso ai servizi PEC e della sicurezza dei log dei messaggi di posta. Verifica inoltre i livelli di sicurezza del sistema PEC e la corretta disponibilità dei log di posta. Gestisce anomalie e/o incongruenze in relazione ai dati raccolti e/o malfunzionamenti riscontrati. Effettua inoltre test periodici in merito al mantenimento dei livelli di servizio e apposita reportistica sulle ispezioni/verifiche svolte.
- ✓ **Gestione Auditing** – team di gestione di anomalie e/o incongruenze in relazione ai dati raccolti e/o malfunzionamenti riscontrati. Effettua inoltre test periodici in merito al mantenimento dei livelli di servizio e apposita reportistica sulle ispezioni/verifiche svolte.

3.1.2 CARATTERISTICHE GENERALI DEL SERVIZIO

Verranno fornite 2 tipologie di caselle:

Tipologia Casella	Dimensione casella (inbox)	Archivio/BackUp
STANDARD	8 GB (anziché 4GB)	24 GB (anziché 20GB)
AVANZATA	14 GB (anziché 10GB)	24 GB (anziché 20GB)

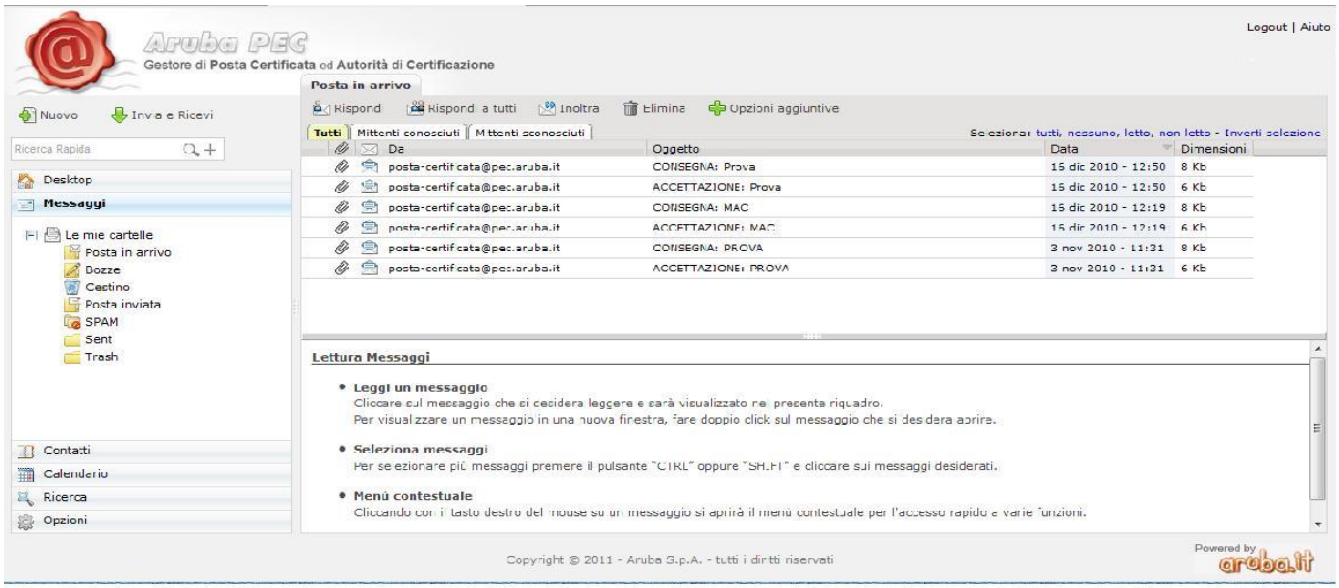
Di seguito le caratteristiche comuni di entrambe le caselle:

Caratteristica	Descrizione	
Numero di messaggi inviati/ricevuti per casella	Numero dei messaggi che possono essere inviati giornalmente	Illimitato (anziché 1.000)
Numero massimo di destinatari	Numero massimo dei destinatari in ogni messaggio inviato	1.000 (anziché 500)
Dimensione massima di un singolo messaggio compreso allegato	Dimensione calcolata in base alla dimensione del messaggio, degli allegati , moltiplicato per il numero dei destinatari	100 MB (anziché 50)
Gestione posta convenzionale	Possibilità, per ogni titolare, di specificare come trattare i messaggi non PEC: • rigettarli • inoltrarli ad un indirizzo alternativo non PEC • accettarli (come anomalia)	
Archivio	Possibilità di effettuare un backup automatico dei messaggi inviati/ricevuti e delle ricevute in base alle scelte del singolo titolare, su un archivio associato alla casella. L'archivio sarà accessibile dalla webmail o via IMAP	
Accesso da client di posta	Possibilità di accedere alla casella PEC dai più comuni client di posta (Thunderbird, Outlook, ecc)	
Webmail personalizzata	Accesso in modalità sicura (SSL - https) mediante Webmail. La webmail sarà personalizzabile con il logo della Regione del	

	Veneto e sarà accessibile attraverso i più comuni browser.
Interfaccia di gestione mail	Interfaccia web di gestione della casella PEC da parte del titolare. Attraverso l'interfaccia il titolare potrà cambiare la password, modificare i parametri di configurazione (quali le modalità di archiviazione, la gestione dei messaggi non PEC, la notifica SMS), creare filtri per i messaggi in ingresso. L'interfaccia potrà essere personalizzabile con il logo della Regione del Veneto.
Servizi POP3s, IMAPs, SMTPs	Utilizzo di protocolli sicuri (POP3s, IMAPs, SMTPs) per la ricezione e spedizione dei messaggi PEC. I suddetti servizi potranno essere personalizzati, ad esempio: • pop3s.pec.regione.veneto.it • imaps.pec.regione.veneto.it • smtps.pec.regione.veneto.it
Notifica SMS	Invio di una notifica al titolare con le informazioni salienti riguardo alla propria casella (messaggi ricevuti, messaggi non letti, ricevute non lette, ecc). Il titolare avrà la possibilità di decidere l'orario di invio della comunicazione
Inoltro automatico	Possibilità di impostare l'inoltro automatico dei messaggi in ingresso verso caselle PEC o non PEC. L'impostazione potrà essere effettuata da parte del titolare, attraverso l'interfaccia di gestione mail
Servizio antivirus	Servizio antivirus per i messaggi in ingresso ed uscita.
Servizio antispam	Servizio di antispam in conformità alla normativa (applicabile solo ai messaggi di posta convenzionale in ingresso)
Filtri (condizioni multiple sui messaggi in ingresso)	Possibilità di impostare filtri sui messaggi in ingresso. Attraverso l'interfaccia di Gestione mail sarà possibile inserire condizioni multiple (su mittente, oggetto e contenuto) che, ove soddisfatte, generino azioni sui messaggi ricevuti (ad esempio l'inoltro ad un'altra casella, la copia in una specifica cartella, la cancellazione, ecc).
API di interfacciamento	Librerie e servizi web da utilizzare per l'integrazione applicativa con servizi esterni. Attraverso i web service forniti sarà possibile comporre messaggi, inviarli, leggere la posta in ingresso, ecc).
Scaricamento archivio di backup	Il titolare avrà la possibilità di scaricare i messaggi presenti in archivio in modo da diminuire l'occupazione dell'archivio stesso. Per i dettagli si rimanda al paragrafo relativo.
Conservazione a norma dei messaggi	Possibilità di inviare i messaggi PEC nel sistema di conservazione a norma.
Spazio aggiuntivo	Possibilità di incrementare lo spazio allocato sulla casella o sull'archivio. La dimensione minima di upgrade sarà di 1 GB ed il costo sarà a carico del richiedente
APP mobile	

personalizzata	APP mobile per la consultazione e l'uso della casella PEC per i principali smartphone/tablet (IOS, Android, Microsoft). Attraverso le APP sarà possibile effettuare tutte le principali operazioni effettuabili da client di posta o da webmail. L'APP potrà essere personalizzata con il logo della Regione del Veneto e resa scaricabile dagli store ufficiali.
Notifica occupazione	Il titolare verrà avvisato via email al raggiungimento di specifiche soglie di occupazione della propria casella, in modo che possa liberare spazio o optare per l'acquisto di spazio aggiuntivo
Log transazioni	Verrà messa a disposizione del titolare la possibilità di scaricare, in autonomia, i log delle transazioni per uno specifico messaggio. Attraverso un apposito form, i titolare potrà specificare alcuni parametri (es. oggetto, mittente, ecc) e, una volta selezionato il messaggio di interesse, ottenere un documento (firmato digitalmente dal gestore) che raccoglie il log legale relativo.
Opzione multiutenza	Sarà possibile impostare ogni casella PEC in modalità multiutenza in modo da permettere a diverse persone di poterla utilizzare accedendo con le proprie credenziali. Sarà il titolare a decidere i diritti di accesso da parte di terzi alla propria casella (sola lettura, lettura invio, ecc). Le funzionalità del collaboratore saranno limitate a quelle che il titolare della casella intenderà concedere.

Riportiamo, di seguito alcune immagini dell'interfaccia grafica della webmail e del pannello di gestione mail:

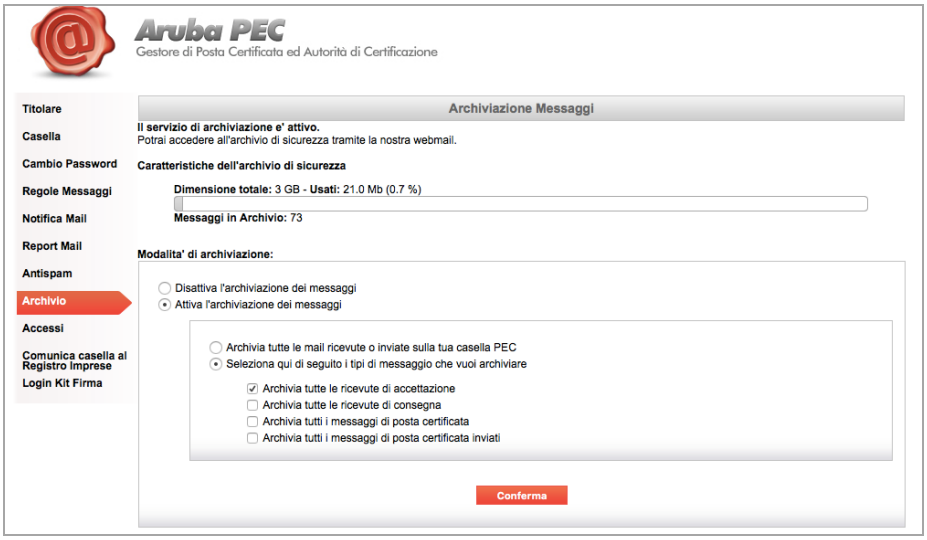


3.1.2.a. GESTIONE ARCHIVIO E CANCELLAZIONE MESSAGGI

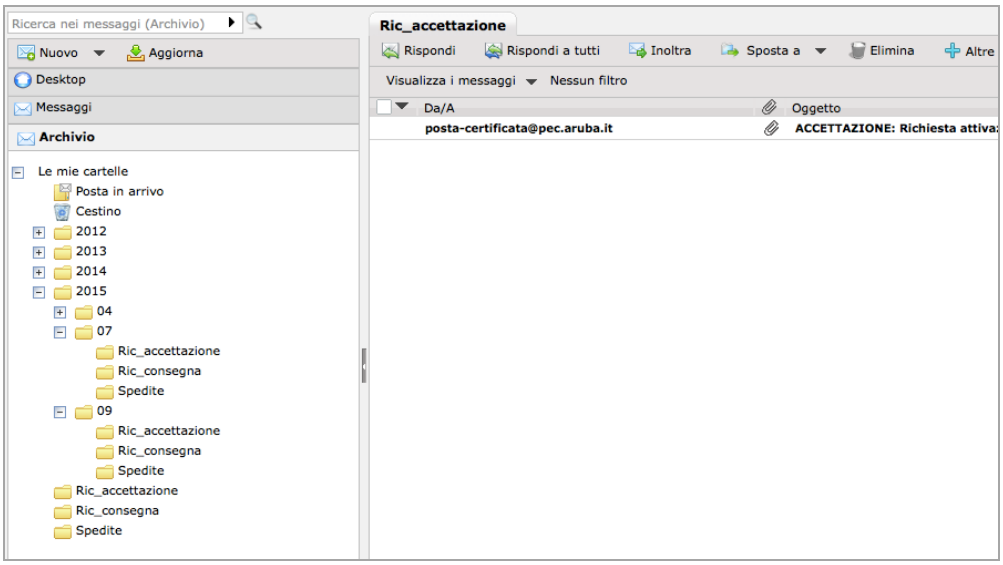
L'archivio di sicurezza può essere attivato per ogni casella ed ha lo scopo di copiare i messaggi di interesse in un'area di backup. Il titolare, attraverso l'interfaccia di gestione della propria casella, può decidere che cosa conservare:

- tutte le ricevute di accettazione
- tutte le ricevute di consegna
- tutti i messaggi di posta certificata

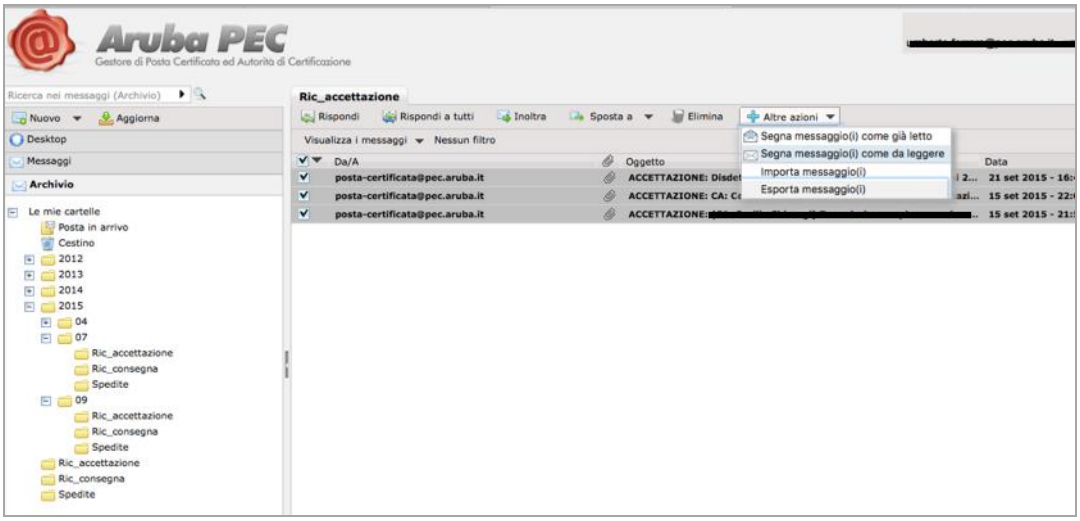
- tutti i messaggi di posta certificata inviati



L'archivio sarà visibile sia attraverso client di posta (via IMAP), che via webmail:



I messaggi verranno organizzati in cartelle (in base all'anno ed il mese di ricezione/invio), in modo da renderne più semplice il ritrovamento. Dalla stessa interfaccia web è possibile selezionare e scaricare in locale un insieme di messaggi oppure selezionare una cartella ed effettuare un download in un file "mbox" contenente tutti i messaggi in essa contenuti.



In alternativa i messaggi potranno essere scaricati in locale mediante client di posta configurato per l'accesso IMAP all'archivio.

Il titolare verrà avvisato via email al raggiungimento di una soglia di occupazione, generalmente al 70% e al 90% della quota assegnata alla casella. I suddetti valori sono personalizzabili.

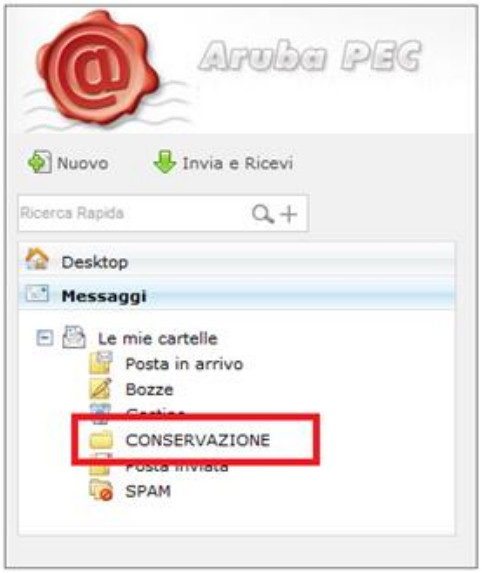
3.1.2.b. CONSERVAZIONE A NORMA DEI MESSAGGI

I meccanismi della PEC forniscono garanzie di tipo trasmissivo: garantiscono il mittente, l'integrità del messaggio ed il non ripudio mentre la conservazione sostitutiva entra nel merito del contenuto garantendo quindi il corpo del messaggio ed il contenuto degli allegati.

Dal Pannello di gestione mail ogni titolare potrà specificare la modalità con la quale vuole che i messaggi siano inviati al sistema di conservazione:

- Conservazione dei messaggi di trasporto in ingresso
- Conservazione dei messaggi di trasporto in ingresso / uscita
- Conservazione di tutto il traffico certificato in ingresso
- Conservazione di tutto il traffico certificato in ingresso / uscita

Una volta scelta la modalità, il sistema si incarica automaticamente di portare in conservazione tutti i messaggi che rispettano la regola impostata. Tramite la webmail è inoltre possibile portare in conservazione sostitutiva qualsiasi documento o mail che non dovesse rispettare tale regola: per farlo è sufficiente trascinare la mail o il documento all'interno della sottocartella Conservazione.



3.1.2.c. APP MOBILE

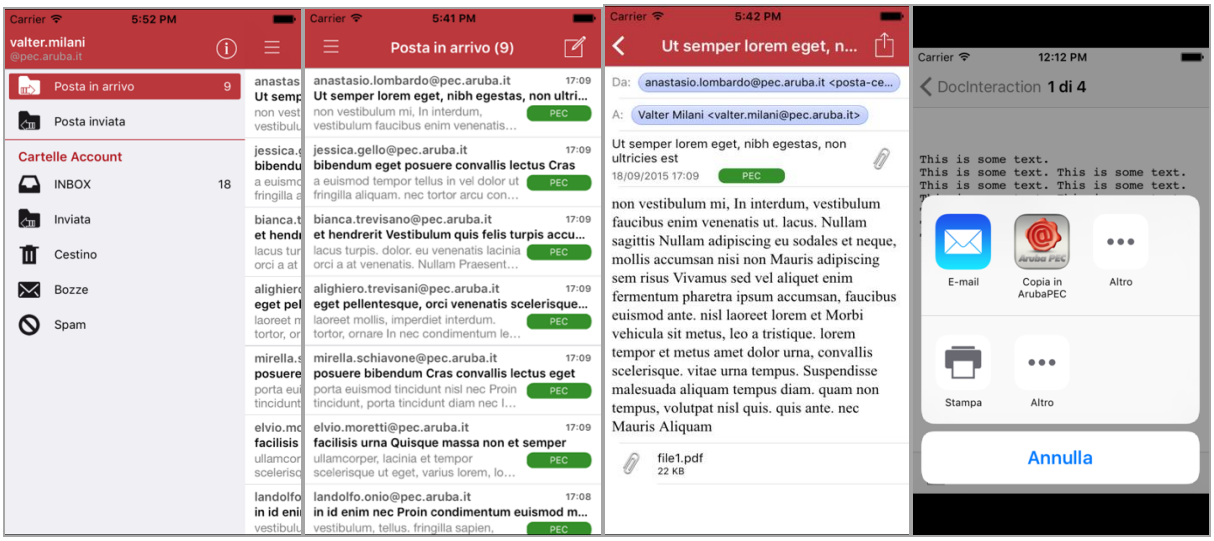
Come valore aggiunto, verrà fornita una l'applicazione **Aruba PEC Mobile** per l'utilizzo del servizio PEC dai principali dispositivi mobile (smartphone o tablet). L'applicazione, disponibile per gli ambienti IOS, Android, è scaricabile dagli "store" ufficiali.
La versione per ambiente Microsoft non è ancora presente negli store e sarà a breve rilasciata.
Aruba PEC Mobile è un'applicazione affidabile, sicura, facilmente accessibile e SEMPLICISSIMA da usare.

Le principali caratteristiche possono essere così riassunte:

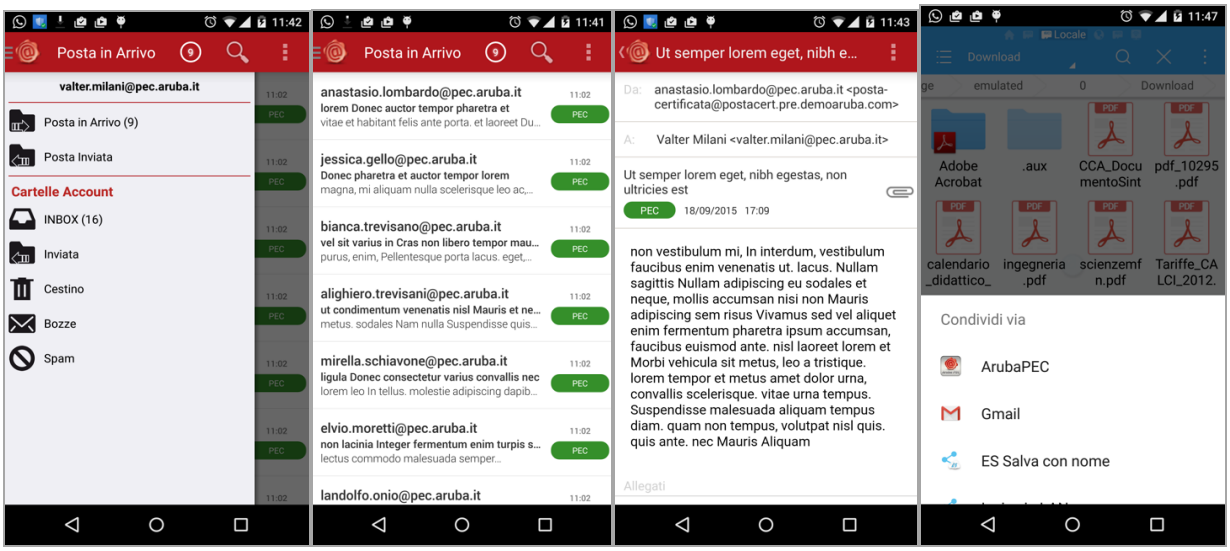
- Visualizzazione semplificata: Il contenuto del messaggio sarà disponibile con un semplice click senza necessità di estrarlo dalla busta; le ricevute e le notifiche relative all'invio/consegna saranno raggruppate nel messaggio di "Posta Inviata".
- Semplicità di utilizzo: funzioni rapide e intuitive che permettono di creare, rispondere o inoltrare una PEC in modo semplice grazie ai pulsanti facilmente raggiungibili.
- Ricerca Rapida per trovare i tuoi messaggi
- Rubrica: contatti selezionabili direttamente dalla rubrica del telefono senza necessità di doverli inserire manualmente
- Notifiche di ricezione in tempo reale per verificare velocemente la tua posta
- Possibilità di allegare ed inviare file.

Riportiamo, di seguito, alcune immagine delle applicazioni per i sistemi IOS e Android.

App mobile IOS



App mobile Android



3.1.3 PROCEDURA DI RICHIESTA ED ATTIVAZIONE

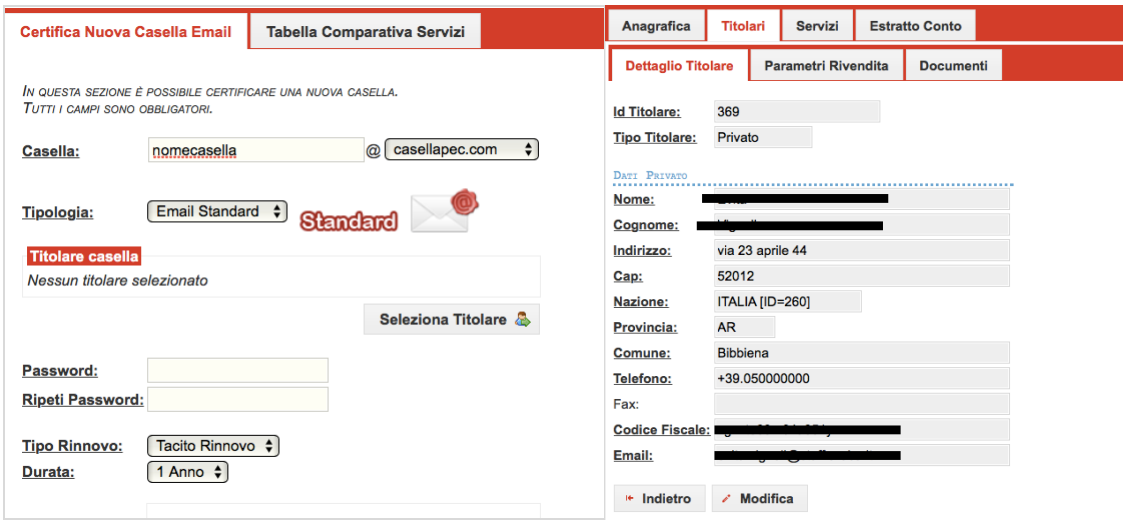
La procedura di seguito descritta è stata pensata per rendere snello e veloce il processo di attivazione delle caselle PEC ed evitare, per quanto possibile, comunicazioni asincrone che causino rallentamenti e colli di bottiglia. Per quanto possibile verranno evitate le comunicazioni via email o fax non strettamente necessarie e verrà viceversa utilizzato uno strumento online (web based) di amministrazione, detto **Pannello Partner**.

Il pannello partner è un pannello di gestione delle caselle attraverso il quale un "partner" Aruba PEC può effettuare una serie di operazione:

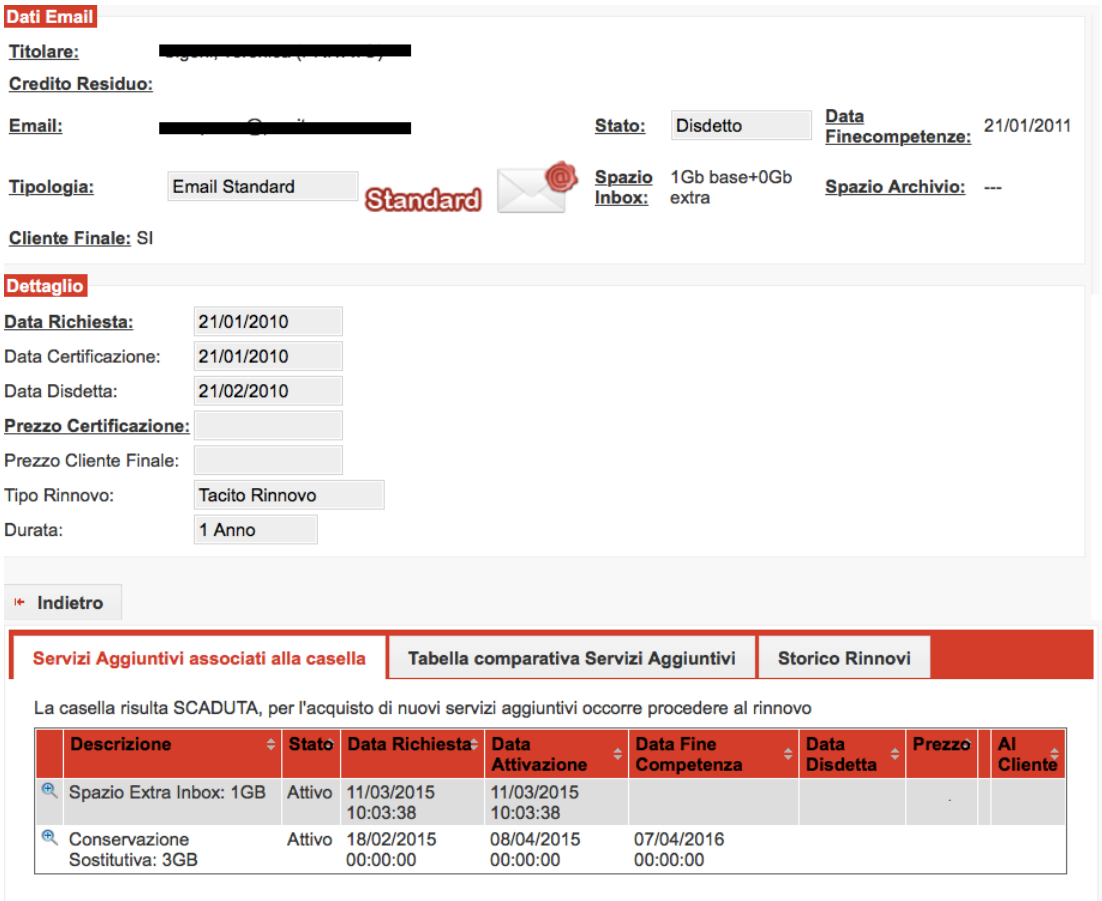
- creare una nuova casella specificandone la tipologia (AVANZATA o STANDARD)
- associare la casella ad un titolare
- chiedere il reset della password
- modificare le caratteristiche della casella impostando, ad esempio, l'opzione multiutenza o la conservazione a norma

- aggiungere spazio assegnato alla casella
- chiudere la casella

Di seguito uno screenshot delle pagine utilizzate per le creazione di una nuova casella PEC



Ogni casella può essere modificata, possono essere aggiunte opzioni come la multiutenza o la conservazione sostitutiva, ne può essere ampliata la dimensione:

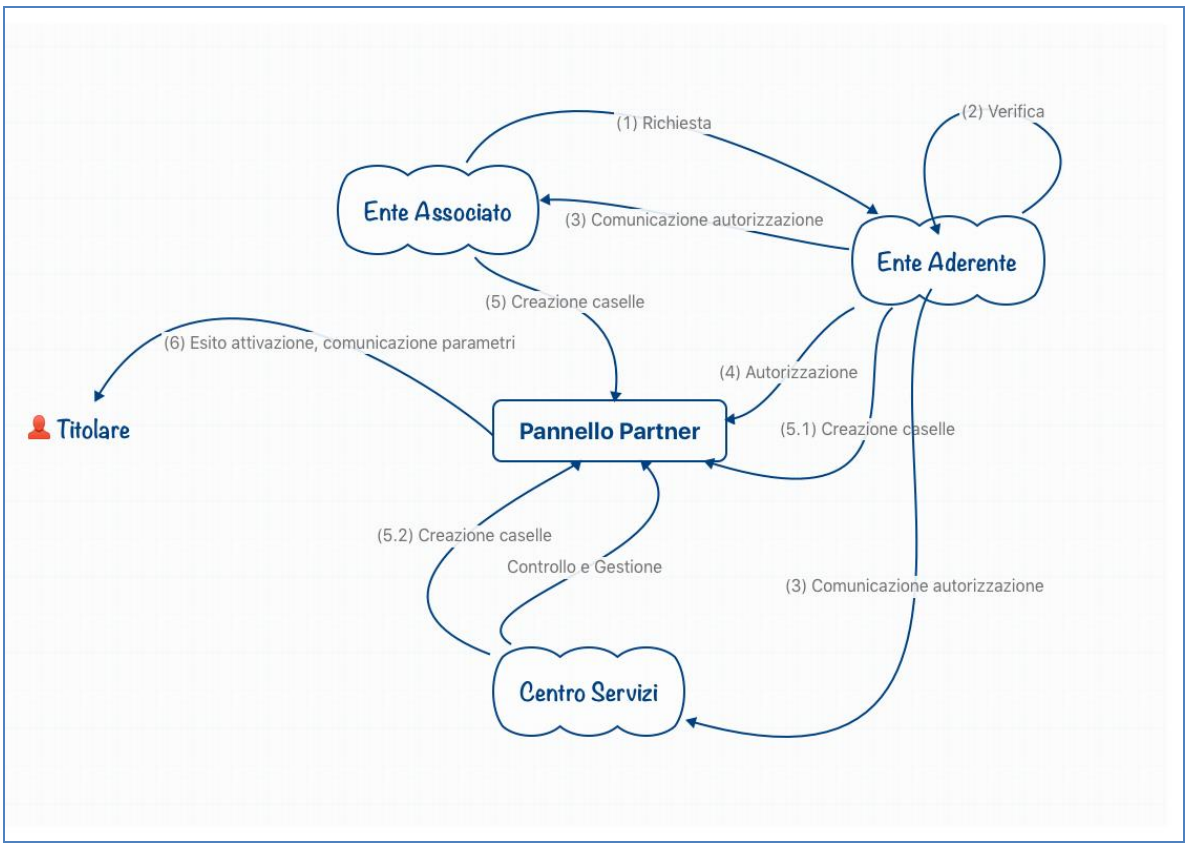


Il pannello prevede 2 profili:

- **operatore** che crea e gestisce le caselle

- **responsabile** che autorizza la creazione di nuove caselle stabilendo, a priori, quante caselle (e di quale tipologia) possono essere create.

Associando il profilo operatore al personale dell'ente associato e il profilo responsabile all'ente aderente è possibile disegnare un processo snello di attivazione delle caselle PEC.
Riportiamo di seguito una schematizzazione del processo.



1. L'ente associato richiede l'attivazione di un certo numero di caselle PEC con determinate caratteristiche
2. L'ente aderente effettua le verifiche del caso.
3. L'ente aderente comunica l'esito delle verifiche e, in caso di esito positivo, avvisa, oltre all'ente associato, anche il Centro Servizi (fornitore de servizio).
4. A questo punto l'ente aderente può accedere direttamente al pannello partner con il proprio profilo (responsabile) ed autorizzare l'ente associato alla creazione delle caselle, specificando il numero e la tipologia delle caselle che possono essere create.
5. Da questo momento, gli operatori dell'ente associato possono accedere al pannello partner ed attivare le caselle selezionando il dominio (tra quelli disponibili per l'ente), inserendo il nome della casella, scegliendo la tipologia (STANDARD o AVANZATA) ed impostando eventuali caratteristiche opzionali quali la multiutenza, la conservazione a norma dei messaggi PEC, ecc. La creazione della casella avverrà in tempo reale azzerando, di fatto, i tempi di attesa.
6. Una volta creata la nuova casella, il sistema invierà al titolare una mail contenente i parametri di accesso e le istruzioni per il suo utilizzo.

Il flusso di creazione di caselle PEC per gli enti aderenti è del tutto identico e prevede, com'è ovvio, che la funzionalità di creazione sia affidata al personale degli enti aderenti stessi (freccia 5.1 dello schema precedente).
L'utilizzo dello strumento web consente di ridurre al minimo i "tempi morti" e, conseguentemente, i tempi totali di rilascio di una nuova casella. Una volta autorizzata la creazione di un certo numero

di caselle, l'operatore dell'ente associato/aderente ha la possibilità di creare una nuova casella PEC in pochi semplici passi.

Anche la chiusura di una casella PEC potrà essere operata in completa autonomia dall'Ente.

 In questo modo i tempi di attivazione e chiusura possono ridursi dalle 48 ore richieste a pochi minuti.

Il processo appena descritto prevede la compartecipazione attiva sia degli enti aderenti che degli enti associati. Lo schema comprende però ulteriori casi nei quali è previsto un coinvolgimento del centro servizi del fornitore nel caso in cui l'ente associato/ente aderente non voglia o non abbia la possibilità di partecipare attivamente. In questi casi infatti la funzionalità di creazione delle caselle può essere demandata del tutto al centro servizi (vedi punto 5.2 dello schema precedente).
Da quanto sopra descritto è evidente che l'utilizzo dello strumento web ci consente di progettare diverse modalità in modo da adattarle alle specifiche esigenze del cliente, definendo in fase di avviamento del servizio i dettagli operativi.

3.1.4 ATTIVAZIONE CON RICHIESTA MASSIVA

Aruba PEC mette a disposizione un'ulteriore procedura nel caso in cui l'ente aderente o l'ente associato abbiano la necessità di creare un numero cospicuo di caselle.
In questo caso, gli enti potranno inviare un file CSV con un formato predefinito e concordato con la stazione appaltante nella fase di startup del progetto, contenente tutte le informazioni necessarie.

Il file verrà inviato al centro servizi che si occuperà di:

- creare le caselle con le caratteristiche specificate nel file
- comunicare l'esito della creazione all'ente richiedente
- inviare i parametri di accesso e le informazioni d'uso al titolare di ogni singola casella

Nel caso in cui venga adottata questa modalità Aruba PEC si impegna ad:

- attivare le caselle PEC desiderate
- inviare a le credenziali di accesso agli utenti finali

entro 48 (quarantotto) ore dalla richiesta, ad esclusione dei giorni festivi.

Allo stesso modo, Aruba PEC si impegna, entro 48 (quarantotto) ore, ad esclusione dei giorni festivi, a chiudere le caselle PEC dandone comunicazione agli utenti finali, come da disposizioni dell'Ente richiedente.

3.1.5 MIGRAZIONE DELLE CASELLE DAL VECCHIO AL NUOVO GESTORE PEC

Per operare la migrazione dei domini attualmente presenti e delle relative caselle è necessario avere la collaborazione tra l'Amministrazione, il vecchio gestore ed il nuovo in quanto i domini dovranno passare dalla gestione del primo a quella del secondo. E' inoltre necessario l'intervento da parte del mantainer del dominio da migrare per la modifica al DNS (record MX) ed è utile la collaborazione di AgID per le operazioni di aggiornamento dell'indice dei gestori - IGPEC e del mantainer del DNS al fine di rendere minimo il periodo di inevitabile disservizio.
Il gruppo Aruba ha maturato negli anni una grande esperienza nella migrazione delle PEC e del relativo contenuto. In particolare Aruba PEC si è occupata di:

- Migrare le caselle PEC dei titolari CEC-PAC a seguito della dismissione del servizio in convenzione fornito da Agid: le caselle che sono state ad oggi migrate sono 137.000.

- Migrare domini PEC di importanti clienti con numeri caselle di che variano da qualche centinaio a diverse migliaia. I clienti appartengono ad ogni tipologia sul mercato:
    - pubbliche amministrazioni (INPS, Infocamere, MIUR, SIAE, Università di Pisa, Università di Firenze, Regione Toscana, Ordine Psicologi Lazio)
    - banche (MPS, BNL, BCC)
    - aziende private (Giuffrè editore, RFI-Trenitalia).

Per prima cosa il **gestore sorgente** dovrà produrre un tracciato dati, opportunamente documentato, contenente le seguenti informazioni minime:

sulla casella:

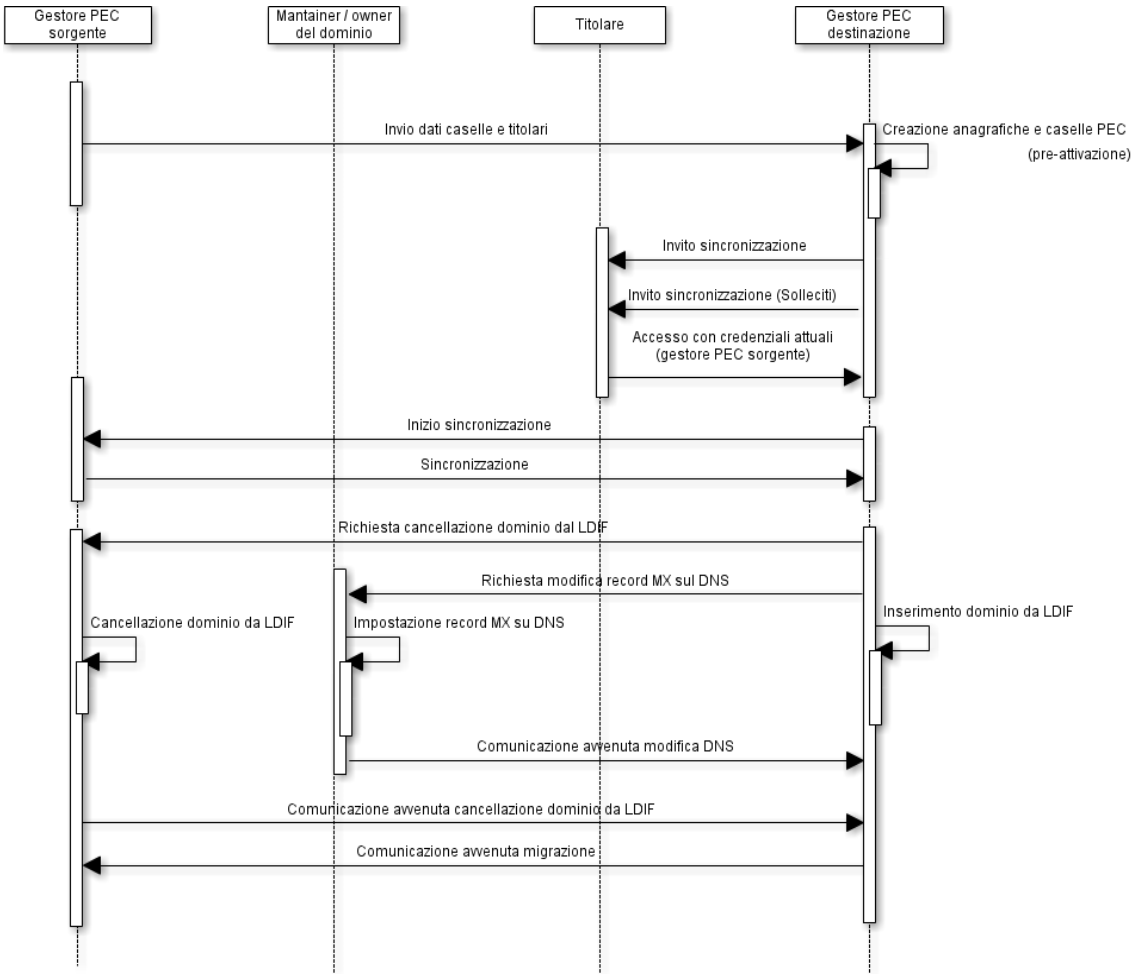
- indirizzo casella
- quota
- eventuali filtri applicati
- eventuale presenza del servizio sms con dettagli
- eventuale presenza del servizio archiviazione con dettagli
- servizio antispam con dettagli

sul titolare:

- Nome
- Cognome
- CodiceFiscale
- Indirizzo
- Località
- Provincia
- Cap
- Telefono
- E-mail convenzionale

Il formato esatto del file verrà condiviso tra i 2 gestori.
Le suddette informazioni verranno caricate sul nuovo sistema PEC e verranno create le nuove caselle mettendole in uno stato di **"pre-attivazione"** in modo che non siano utilizzabili fino alla data effettiva di passaggio.
Una volta create le caselle PEC, il titolare sarà invitato ad accedere ad una pagina sulla quale inserire le proprie credenziali del vecchio gestore al fine di far partire il **processo di sincronizzazione dei contenuti**. Le credenziali saranno conservate sul nuovo sistema in forma cifrata e verranno utilizzate solamente per la fase di migrazione del contenuto delle caselle.
Per invitare il titolare ad attivare il meccanismo di sincronizzazione, verranno inviati dei messaggi sulle caselle PEC stesse e sugli indirizzi email convenzionali, cui potranno seguire dei solleciti ad intervalli di tempo da concordare.
Per completare la migrazione sarà poi necessario aggiornare **DNS** e **IGPEC**.
La procedura standard prevede la cancellazione del dominio sul file ldif del gestore sorgente, l'aggiornamento del **record MX** e l'inserimento del dominio sul file ldif del gestore destinatario.
La fase di passaggio di dominio su IGPEC da un gestore ad un altro ha una durata minima di 6 ore a cui si deve aggiungere il tempo di propagazione del DNS.
Terminato l'aggiornamento del DNS e di IGPEC le caselle saranno attive e pienamente funzionanti sul sistema destinazione. Durante queste fasi e per un periodo approssimativo di 48 ore le caselle non saranno utilizzabili.

Per i giorni successivi al passaggio e fino a quando il gestore sorgente lo consentirà, il sistema continuerà a sincronizzare i contenuti in modo da trasferire gli eventuali messaggi che dovessero essere arrivati sulla vecchia casella durante le operazioni di migrazione.
Riportiamo di seguito il Sequence Diagram della procedura di migrazione nella quale sono evidenziate le interazioni tra gli attori e la sequenza temporale delle operazioni.



Facciamo notare che le operazioni di cancellazione dominio da LDIF da parte del gestore mittente, la modifica del record MX sul DNS da parte del mantainer e l'inserimento del dominio su LDIF da parte del gestore destinatario sono operazioni che devono essere svolte in modo sincrono e coordinato tra le parti. La buona riuscita dell'operazione e la riduzione del periodo di disservizio per gli utenti finali dipendono in larga misura proprio dal grado di collaborazione che si instaura tra le parti e dalla sincronia che si riesce a raggiungere.
Facciamo inoltre presente che, in forza dell'alto numero di domini PEC gestiti (circa 80% del totale dei domini italiani) il gruppo Aruba opera frequentemente operazioni di migrazione da e verso altri gestori PEC e per questo motivo conosce le interfacce tecniche degli altri gestori, le dinamiche che si instaurano e possiede quindi tutta l'esperienza necessaria a rendere veloce ed indolore questo necessario passaggio.

Tempistiche
Tecnicamente il processo di migrazione può essere completato in 4/5 giorni.
La fase di migrazione viene normalmente effettuata il venerdì pomeriggio al termine dell'orario di lavoro, allo scopo da ridurre al minimo il disservizio e fare in modo che il lunedì successivo le nuove caselle siano perfettamente funzionanti.

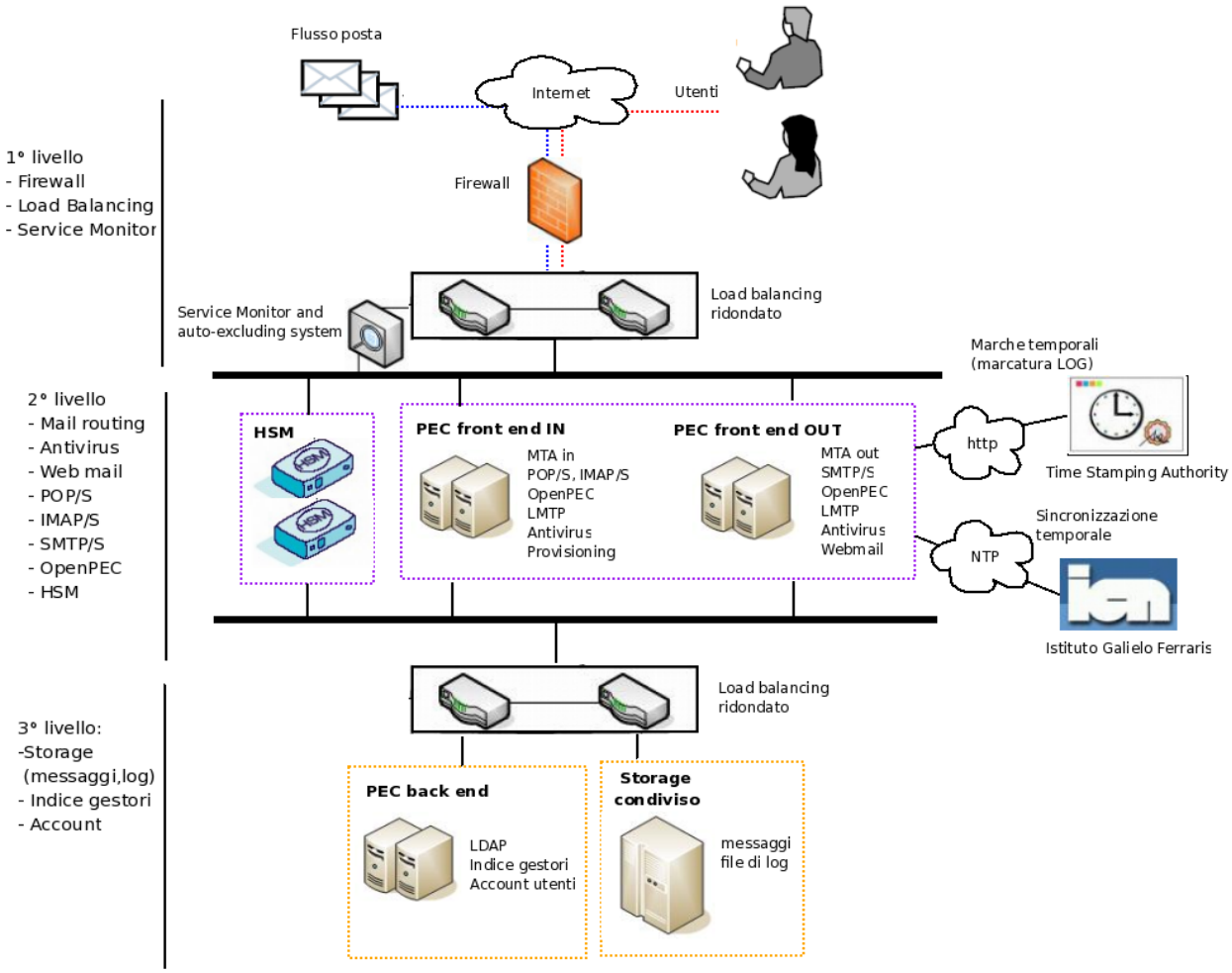
3.1.6 ARCHITETTURA DEL SISTEMA PEC DI ARUBA

L'architettura è progettata in modo da garantire una scalabilità praticamente illimitata al fine di soddisfare le esigenze di crescita di comunità di grandi dimensioni mantenendo nel contempo inalterati performance e livelli di fruibilità.
Di seguito evidenziamo alcune delle caratteristiche principali:

- Tutti i server e gli apparati di rete, inclusi gli stessi moduli HSM, sono duplicati e bilanciati per implementare un servizio non soltanto scalabile ma anche di alta affidabilità e disponibilità (high availability)
- Il front-end ed il back-end sono fisicamente separati per aumentare la sicurezza e la scalabilità
- Vengono utilizzati dei supporti di memorizzazione esterni, condivisi via NFS (tramite storage area network) e residenti su un'architettura in cluster, così da risolvere tutte le possibili problematiche di disponibilità, affidabilità e continuità del servizio.

Il sistema garantisce un elevato grado di sicurezza soprattutto riguardo alla gestione delle chiavi private e dei certificati utilizzati per la generazione delle firme delle ricevute, degli avvisi e delle buste di trasporto e per il processo di verifica delle suddette operazioni. La chiave privata del sistema di PEC nonché le operazioni crittografiche necessarie durante la firma e/o la verifica dei messaggi risiedono su un dispositivo HSM tamper proof e tamper evident certificato FIPS 140-2 level 3 (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf).

Grazie all'installazione dei principali componenti su macchine separate riusciamo ad ottenere una soluzione scalabile ed estendibile in qualsiasi momento. Tutti i componenti critici sono inoltre ridondati e bilanciati in modo da assicurare un alto livello di tolleranza ai guasti ed assicurare alte performance.
Riportiamo qui di seguito un'architettura di massima del sistema che ha il solo scopo di descrivere l'approccio utilizzato e non ha la pretesa di essere dettagliata ed esaustiva in termini di numero di macchine coinvolte e di moduli utilizzati.
Come è possibile dallo schema sotto riportato vedere il sistema è strutturato logicamente su 3 livelli.



Grazie all'installazione dei principali componenti su macchine separate riusciamo ad ottenere una soluzione scalabile ed estendibile in qualsiasi momento. Tutti i componenti critici sono ridondati e bilanciati in modo da assicurare un ottimo livello di tolleranza ai guasti ed assicurare alte performance.
Come è possibile vedere dalla figura, il sistema si interfaccia con Time Stamping Authority per la marcatura temporale dei log e con l'Istituto Galileo Ferraris di Torino per la sincronizzazione del clock delle macchine mediante protocollo NTP.
Dietro all'infrastruttura di sicurezza (firewall) sono presenti i load balancer che bilanciano i servizi delle macchine sottostanti. Il sistema è strutturato su 3 livelli.

Primo livello
Il primo livello contiene firewall, bilanciatori e service monitor ed ha il compito di proteggere le macchine sottostanti, bilanciare il carico e dirigere le richieste verso le macchine attive in caso di malfunzionamenti su alcune di esse.

Secondo livello
Il secondo livello è il **livello di front end** e contiene l'MTA che si incarica del mail routing, il modulo antivirus, il server LMTP ed il nucleo centrale del sistema **OpenPEC**, il server POP e IMAP (per l'accesso alla casella di posta tramite client), il server SMTP (per la spedizione delle mail), il sistema di provisioning (per la creazione e gestione degli account e dei domini di PEC), il modulo di web mail (per l'accesso alla casella di posta attraverso un comune browser web).
Nell'architettura sopra disegnata sono presenti 2 gruppi di macchine: uno per la ricezione dei messaggi provenienti dall'esterno ed uno per la spedizione dei messaggi verso l'esterno. In questo modo è possibile separare i compiti e dedicare ad esempio una o più macchine alla spedizione massiva di messaggi.

Il secondo livello contiene inoltre i dispositivi di firma, **HSM** (Hardware security module) utilizzati per la firma dei messaggi PEC, che nello specifico sono i modelli **netHSM 500 di Thales-NCipher**.

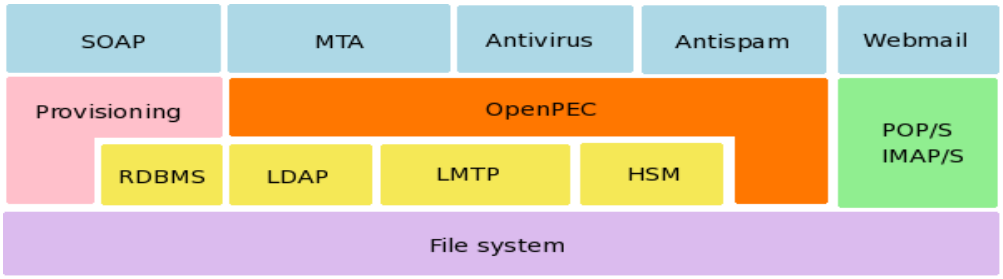
Terzo livello

Il terzo livello è il **livello di back end e data store** contiene il gruppo di macchine **PEC server back end** e lo **storage** di sistema.

Le macchine PEC server back end contengono il database degli account e l'indice dei gestori (mirror del server DigitPA) memorizzato su server LDAP.

Lo storage contiene le mailbox degli utenti ed i file di log del sistema (che devono essere conservati per almeno 30 mesi). Sullo storage vengono inoltre salvate le copie dei file di configurazione e le informazioni critiche di tutte le macchine coinvolte, in attesa che il server di backup si incarichi della loro archiviazione.

Di seguito uno schema che descrive a grandi linee i principali componenti della soluzione.



Come descritto nello schema, esiste un nucleo centrale del sistema costituito dal software open source **OpenPEC**, il quale si interfaccia con tutti gli altri moduli: il Mail Transfer Agent (MTA) che si incarica del "dispatching" delle mail, il modulo Antivirus, il server LDAP (che contiene gli account ed il mirror dell'indice dei Gestori), il server LMTP, i moduli HSM utilizzati per la firma dei messaggi, lo storage (file system), il server POP-IMAP. Nel sistema è presente un modulo di provisioning (per la creazione/modifica degli account) richiamabile attraverso interfaccia SOAP, ed una web mail.

Tutta l'infrastruttura verrà ospitata nei Data Center del Gruppo Aruba, per la cui descrizione del si rimanda al relativo paragrafo (1.2.2).

3.2 DOCUMENTAZIONE MESSA A DISPOSIZIONE

Oltre a fornire le interfacce intuitive dotate di strumenti di ausilio all'utilizzo quali help on line contestuale, Aruba PEC fornirà tutta la documentazione e manualistica necessaria a rendere l'esperienza d'uso delle applicazioni semplice e veloce.

In particolare verrà fornita la documentazione seguente:

DOCUMENTAZIONE PEC
Manuale operativo del servizio PEC
Manuale d'uso della webmail
Manuale d'uso dell'interfaccia di amministrazione (pannello partner)
Guide filmate per la configurazione dei principali client di posta (Outlook, thunderbird, ecc)

Guide all'uso della casella PEC e delle funzionalità aggiuntive
Guide per lo sviluppatore per l'integrazione applicativa con il sistema PEC attraverso web service

3.3 FUNZIONALITA' AGGIUNTIVE

Seguendo la tabella proposta in sede di Capitolato Tecnico dalla Stazione appaltante, vengono di seguito riassunte le "funzioni aggiuntive" incluse nei servizi offerti e descritte nei paragrafi precedenti:

Requisito	Richiesta del capitolato	Aspetto migliorativo
Dimensione casella STANDARD	4 GB	**8 GB**
Dimensione casella PRO	10 GB	**14 GB**
Dimensione Archivio	20 GB	**24 GB**
Funzionalità avanzate dell'archivio di backup: Scaricamento archivio per liberare spazio	Opzione aggiuntiva	✔
Funzionalità avanzate dell'archivio di backup: Conservazione a norma dei messaggi	Opzione aggiuntiva	✔
Possibilità di incrementare lo spazio allocato sulla casella o sull'archivio	Opzione aggiuntiva	✔
Traffico: Numero di messaggi ricevuti/inviati	1000	**illimitato**
Dimensione massima messaggio compresi allegati	50 MB	**100 MB**
Numero massimo destinatari	500	**1000**
Accesso alla caselle con APP mobile	Opzione aggiuntiva	✔
Personalizzazione APP mobile con il logo regionale	Non richiesto	✔
Accesso alla caselle in modalità mobile anche tramite interfaccia web	Opzione aggiuntiva	✔
Disponibilità, su richiesta, dei log delle transazioni	Opzione aggiuntiva	✔
Disponibilità di filtri e regole per i messaggi in arrivo	Opzione aggiuntiva	✔
Possibilità di l'accesso, autonomo e indipendente, alla medesima casella PEC da parte di più utenti (Multiutenza)	Opzione aggiuntiva	✔
Personalizzazione dei testi dei messaggi di notifica relativi all'occupazione dello spazio casella	Non richiesto	✔
Webmail personalizzata con logo regionale	Non richiesto	✔
Servizi POP3s, IMAPs, SMTPs personalizzati	Non richiesto	✔
Gestione mail personalizzata con logo regionale	Non richiesto	✔
Guide filmate per l'uso della PEC	Non richiesto	✔

4 SERVIZIO DI CONSERVAZIONE A NORMA

Al fine di gestire il processo di conservazione richiesto dall'Amministrazione regionale e dagli Enti Aderenti, Aruba PEC metterà a disposizione il servizio di conservazione digitale a norma DocFly, erogato in modalità *application service provider*.
La gestione del servizio non viene effettuata attraverso il Pannello Unico ma tramite un'applicazione specifica, in grado di recepire ed implementare le linee guida ed i vincoli imposti dalla normativa.
Il sistema di conservazione DocFly è infatti conforme alla normativa attualmente in vigore ed è stato sviluppato secondo gli standard e le regole tecniche previste dall'Agenzia per l'Italia Digitale (AgID) con la pubblicazione del DPCM del 3 Dicembre 2013. In particolare, il sistema assicura, dalla presa in carico da parte del produttore fino all'eventuale scarto, la conservazione dei documenti e fascicoli informatici, inclusi i metadati associati, garantendo al tempo stesso i requisiti di autenticità, integrità, affidabilità, leggibilità e reperibilità.

Aruba PEC ha inoltre conseguito il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza relativamente all'erogazione dei servizi di conservazione digitale a norma, ottenendo l'accreditamento presso AGID; ragion per cui, **è iscritta nell'elenco dei Conservatori Accreditati sul sito istituzionale dell'Ente** (link elenco conservatori http://www.agid.gov.it/agenda-digitale/pubblica-amministrazione/conservazione/elenco-conservatori-accreditati).

Con riferimento ai requisiti tecnici previsti da capitolato Aruba PEC assicura:

- lo svolgimento del processo di conservazione a norma di legge dei documenti informatici inviati in conservazione dall'Amministrazione regionale e dagli Enti Aderenti, in conformità a quanto stabilito dalle norme vigenti ed in particolare dal DPCM 03/12/2013 (per maggiori dettagli si riporta al par. 4.1.5).
- l'assunzione del ruolo di responsabile esterno del trattamento dei dati come previsto dal Codice in materia di protezione dei dati personali;
- la gestione tecnologica, sotto la propria autonomia e responsabilità, necessaria per garantire la piena efficienza del servizio oggetto della presente fornitura, continuità di erogazione dello stesso, rispetto della normativa vigente e delle sue successive evoluzioni per tutta la durata del contratto. Aruba PEC, infatti, si impegna a monitorare l'evoluzione della normativa, garantendo al tempo stesso, le attività necessarie ad installare eventuali nuove release qualora fossero individuate l'introduzione di nuove regole, requisiti, standard tecnici ecc. con impatto su quanto erogato (per maggiori dettagli si riporta al par. 4.1.8)
- un elevato livello di sicurezza fisica, logica ed organizzativa, al fine di tutelare l'integrità, la leggibilità, la disponibilità e la riservatezza dei documenti conservati. Il servizio DocFly è ospitato all'interno dei data center, di proprietà del Gruppo Aruba, che rispondono alle stringenti misure di sicurezza previste dalla normativa in materia e dotati di appositi sistemi di protezione logica e fisica al fine di impedire accessi non autorizzati. Maggiori dettagli sugli aspetti relativi alla sicurezza sono dettagliati al par. 4.3
- una soluzione modulare, scalabile e adattabile a specifiche esigenze di carico, che le consentono di sopportare picchi di lavoro ed incrementi anche cospicui dei flussi documentali, in termini di numero e dimensione dei documenti, di numero di invii in conservazione e di richieste di esibizione.
- la conservazione nel tempo dei documenti e dei relativi metadati nei formati previsti dal presente capitolato e dagli allegati, in archivi logicamente separati per ciascun Ente produttore che usufruisce del servizio, offrendo funzioni di invio in conservazione, ricerca, esibizione, cancellazione logica, scarto e gestendo un archivio dei software per la visualizzazione dei documenti conservati;
- un sistema di autenticazione e profilatura degli accessi che consente solo agli utenti autorizzati da ciascun Ente (sia per l'accesso dell'operatore umano che mediante

meccanismi di interoperabilità con i sistemi degli Enti), di accedere esclusivamente ai documenti di propria competenza

- l'utilizzo di una semplice ed intuitiva interfaccia web che consente agli utenti abilitati delle Pubbliche Amministrazioni aderenti al servizio: l'invio in conservazione, la ricerca, l'esibizione ed ogni altra funzione presente sul pannello (per maggiori dettagli si rimanda al 4.1.7)
- l'esposizione dei servizi web su protocolli standard che, in linea con quanto previsto nel capitolato, garantiscono l' interoperabilità con le applicazioni del sistema informativo degli Enti aderenti, i quali potranno invocare le diverse funzionalità limitatamente ai documenti di propria pertinenza.
- la gestione ed il mantenimento di un apposito archivio dei programmi di visualizzazione per tutti i formati dei documenti conservati, al fine di soddisfare le richieste di esibizione dei documenti nel tempo.
- l'integrazione del sistema DocFly con il costituendo Polo Archivistico Regionale secondo le specifiche tecniche che saranno rese disponibili dalla stazione appaltante
- la totale rispondenza ai requisiti minimi obbligatori e opzionali previsti da capitolato. In particolare, viene assicurata la gestione delle notifiche tramite (mail) in caso di raggiungimento di soglie relative allo spazio a disposizione, nonché la possibilità di inviare in conservazione documenti con caratteristiche, in termini di dimensionamento, superiori a quelle minime indicate (per maggiori dettagli si rimanda al 4.6).
- un servizio di disaster recovery atto ad evitare qualunque perdita di dati/documenti gestiti all'interno dei datacenter del Gruppo Aruba, al fine di consentire il loro ripristino in tempi e modalità in linea con la normativa in materia (per maggiori dettagli sul piano di DR e sulle modalità tecniche che caratterizzano tale servizio si rimanda ai paragrafi 4.3.8)

In caso di aggiudicazione della gara, Aruba PEC assicura la realizzazione e la gestione delle seguenti attività:

- fornitura della documentazione amministrativa, contrattuale e operativa per l'utilizzo del servizio di conservazione a norma (per maggiori dettagli si rimanda al 4.4.1)
- servizio di formazione mirato a fornire ai Responsabili della Conservazione e agli operatori, il know-how necessario per garantire rispettivamente: presidio dell'organizzazione e corretto utilizzo del sistema di conservazione DocFly (per maggiori dettagli si rimanda al Cap. 6)
- servizio di help desk (per maggiori dettagli sul servizio si rimanda al Cap. 5)
- servizio di monitoraggio, costante e dettagliato, dei volumi di archiviazione conseguiti per ciascun Ente rispetto alla quantità totale di archiviazione richiesta e messa a disposizione da Aruba PEC (per maggiori dettagli sul servizio si rimanda al Cap. 7)

Aruba PEC garantisce la disponibilità di personale esperto sia dal punto di vista tecnico che normativo. I servizi di conservazione e le forniture richieste, oltre quelle direttamente connesse al dominio tecnico-specialistico del fornitore dei servizi/sistema, saranno realizzate in stretta sinergia/coordinamento con la Stazione appaltante e rese agli enti territoriali senza costi aggiuntivi e senza ulteriori interventi tecnici, se non quelli strettamente previsti/ricompresi nel presente capitolato e necessari per la loro attivazione.

Aruba PEC garantisce il rispetto dei livelli di servizio richiesti nel par. 5.3.4 del Capitolato: i relativi dati verranno messi a disposizione all'interno dello strumento di monitoraggio che permetterà di avere una visione completa del rispetto degli SLA concordati.

I servizi offerti saranno disponibili, 24 ore al giorno e 7 giorni su 7 nel rispetto degli SLA relativi alle fasce orarie previste dal capitolato e monitorati attraverso lo strumento, fornito da Aruba PEC e descritto nel Capitolo 7.

I fermi programmati e gli interventi di manutenzione straordinaria, ossia le interruzioni del servizio necessarie per svolgere attività di manutenzione verranno preferibilmente effettuati nella fascia oraria notturna, previa comunicazione scritta agli Enti Aderenti, da inviare con un anticipo di almeno 5 giorni lavorativi.

4.1 TECNOLOGIE E STRUMENTI UTILIZZATI NELL'EROGAZIONE DEL SERVIZIO

Il sistema di conservazione DocFly, è stato sviluppato interamente attraverso personale qualificato interno e secondo standard qualitativi ben definiti che lo rendono affidabile, sicuro e, al tempo stesso, altamente personalizzabile essendo totalmente indipendente da terze parti.
La soluzione presentata prevede un sistema di conservazione centralizzato, dotato di un insieme di strumenti e tecnologie, in grado di garantire l'intero processo di conservazione a norma di qualsiasi tipo di documento rispondendo, quindi, con un'unica soluzione a tutte le diverse esigenze di conservazione legale che ogni Ente può riscontrare.
Il processo di conservazione viene alimentato attraverso il sistema di versamento; quest'ultimo è rappresentato dalle diverse modalità tecniche mediante le quali il sistema DocFly consente di interfacciarsi con i sistemi documentali, alimentando di fatto il processo di conservazione.

Nei successivi paragrafi, oltre ad essere riportati alcuni concetti chiave che sono alla base del processo di conservazione, sono dettagliati tutti gli strumenti e le funzionalità messe a disposizione degli utenti autorizzati dagli Enti per il versamento, ricerca, recupero ed esibizione dei documenti conservati.

4.1.1 QUADRO NORMATIVO DI RIFERIMENTO

Il servizio di conservazione digitale DocFly è conforme ai seguenti standard/ specifiche tecniche relative alla formazione, gestione e conservazione di documenti informatici e documenti amministrativi informatici come di seguito riportati:

Relativamente alla formazione, gestione di documenti informatici:

- UNI ISO 15489-1: 2006 Informazione e documentazione - Gestione dei documenti di archivio – Principi generali sul record management;
- UNI ISO 15489-2: 2007 Informazione e documentazione - Gestione dei documenti di archivio – Linee Guida sul record management;
- ISO/TS 23081-1:2006 Information and documentation - Records management processes – Metadata for records – Part 1 – Principles, Quadro di riferimento per lo sviluppo di un sistema di metadati per la gestione documentale;
- ISO/TS 23081-2:2007 Information and documentation - Records management processes – Metadata for records – Part 2 – Conceptual and implementation issues, Guida pratica per l'implementazione;
- ISO 15836:2003 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core;
- PDF/A, XML, TIFF, JPEG 2000, RFC 2821, 2822,ISO 216;

Relativamente alla conservazione digitale di documenti informatici

- ISO 14721:2012 OAIS (Open Archival Information System - OAIS), Sistema informativo aperto per l'archiviazione.
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System).
- ETSI TS 101 533-1 V1.1.1 (2011-05) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.

- ETSI TR 101 533-2 V1.1.1 (2011-05) Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare Sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.
- UNI/TS 11465/1 – (UNI/TS 11465/2) - UNI/TS 11465/3;
- UNI 11386:2010 S-Recupero degli Oggetti digitali.
- ISO 15836:2003 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.
- MoReq2 - per la gestione di record elettronici, requisiti funzionali relativi alla gestione di record Elettronici da parte di un sistema di gestione di record elettronici (Electronic Records Management System - ERMS).

Inoltre il sistema di conservazione risponde alle seguenti normative:

- Nuove Regole tecniche in materia di sistema di conservazione DPCM del 3 dicembre del 2013 ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44 –bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n.82 del 2005;
- Decreto legislativo 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali;
- Decreto legislativo del 7 marzo 2005, n. 82 e s.m.i.i., pubblicato sulla Gazzetta ufficiale n. 112 del 16 maggio 2005, a seguito della delega al Governo contenuta all'articolo 10 della legge 29 luglio 2003, n. 229 (Legge di semplificazione 2001).
- DPR 28 dicembre 2000, n. 445. Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
- D.M. 17 giugno 2014 Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005
- Circolare Ministeriale n. 36/E del 6 dicembre 2006 sulla conservazione sostitutiva dei documenti informatici e analogici rilevanti fiscalmente.

Per quanto riguarda la firma digitale facciamo riferimento al D.P.C.M. 22 febbraio 2013 che stabilisce le regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici che le firme digitali e le marche temporali utilizzate dal processo di conservazione dovranno rispettare.

4.1.2 I PACCHETTI INFORMATIVI

In linea con la normativa vigente (DPCM del 3/12/2013), i documenti informatici oggetto di conservazione digitale sono trattati dal sistema di conservazione in pacchetti informativi. Ogni invio di informazione ad un sistema di conservazione da parte di un sistema produttore (documentale) e ogni diffusione di informazioni ad un utente necessita di una o più trasmissioni, nella forma di pacchetti informativi.

Un Pacchetto informativo è un contenitore astratto di due tipi di informazioni: contenuto informativo (ovvero il documento) e le informazioni sulla conservazione (ovvero i metadati).

I pacchetti informativi sono suddivisi in tre tipologie, come descritto di seguito:

- Pacchetto di Versamento (PdV): Si tratta del pacchetto informativo inviato dal soggetto produttore dell'alimentazione del processo al sistema di conservazione DocFly e oggetto del Contratto di servizio, ovvero del documento finalizzato alla definizione di tutte le componenti informative che il sistema di conservazione necessita per creare degli PdA (Pacchetti di Archiviazione) coerenti e ben strutturati.
- Pacchetto di archiviazione (PdA): E' quello conservato dall'OAIS e possiede un insieme completo di metadati necessari per la conservazione a lungo termine e l'accesso ai documenti di archivio. E' generato a partire dal pacchetto di versamento. Il PdA è composto

dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del DPCM del 3 Dic. 2013 e secondo le modalità riportate nel manuale di conservazione.

- Pacchetto di distribuzione (PdD): In risposta ad un ordinativo, l'OAIS fornisce all'utente tutto o parte di un pacchetto di archiviazione (PdA) sotto forma di pacchetto di distribuzione (PdD); il pacchetto di distribuzione è definito in base alle esigenze dell'utente e può contenere anche un set parziale di metadati. E' generato a partire dai pacchetti di archiviazione.

4.1.3 OVERVIEW DELLE FASI E DELLE ATTIVITÀ DEL PROCESSO DI CONSERVAZIONE

La conservazione non viene svolta all'interno della struttura organizzativa dell'Ente (soggetto titolare dei documenti informatici da conservare), ma è affidata ad Aruba PEC, che dovrà espletare le attività per le quali ha ricevuto formale delega, nei limiti della stessa e per le quali opera in modo autonomo e ne è responsabile.
In linea di massima, la sequenza di attività che vanno dalla fase propedeutica alla formazione dei documenti informatici alla fase di conservazione degli stessi è di seguito schematicamente rappresentata:

Sistemi	Fase	Descrizione e MACRO FASI del processo di conservazione	Attività a carico di:	
			Ente	Aruba PEC
Sistema di gestione del Polo Archivistico Regionale	1	Produzione/formazione/emissione a norma dei documenti informatici e contestuale generazione dei relativi metadati	X	
	2	Produzione del pacchetto di versamento	X	
	3	Deposito in conservazione del pacchetto di versamento e dei relativi documenti informatici completi di metadati	X	
Sistema di Firma Digitale	4	Servizio di Firma Automatica e di apposizione marca temporale, da effettuare sui documenti prima dell'invio al sistema di conservazione.	X	X
Sistema di conservazione digitale dei documenti informatici	5	Acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico		X
	6	Verifica che il pacchetto di versamento ed i documenti informatici in esso descritti siano coerenti e conformi alle prescrizioni stabilite dal Contratto di servizio		X
	7	Eventuale rifiuto del pacchetto di versamento o dei documenti informatici, nel caso in cui le verifiche di cui alla fase 5 abbiano evidenziato delle anomalie		X
	8	Generazione, anche in modo automatico, e sottoscrizione del rapporto di versamento relativo a ciascun pacchetto di versamento		X

	9	Invio all'Ente del rapporto di versamento		X
	10	Preparazione e gestione del pacchetto di archiviazione		X
	11	"Chiusura" del pacchetto di archiviazione mediante sottoscrizione con firma digitale di ARUBA PEC e apposizione di marca temporale		X
	12	Richieste di esibizione dei documenti informatici conservati	X	
	13	Preparazione e sottoscrizione del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'utente con tutti gli elementi necessari a garantire l'integrità e l'autenticità degli stessi		X
	14	Richiesta dell'Ente di duplicati informatici	X	
	15	Produzione di duplicati informatici su richiesta dell'Ente, al fine di adeguare il formato di cui all'art. 11 del citato DPCM 03/12/2013, in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico;		X
	16	lo scarto del pacchetto di archiviazione dal sistema di conservazione su specifica richiesta dell'Ente produttore.	X	X

Dal prospetto di cui sopra emerge chiaramente come ogni singola fase del processo è propedeutica alle altre.

4.1.4 SISTEMA DI VERSAMENTO - INTEGRAZIONE DEL SISTEMA DOCFLY NEL CICLO DI VITA DOCUMENTALE

La soluzione DocFly può dialogare con diverse sorgenti documentali e, in linea con le richieste di capitolato, garantisce l'interoperabilità con le applicazioni del sistema informativo degli Enti aderenti.
DocFly potrà interfacciarsi con sistemi esterni mediante web services con canali sicuri di trasmissione che saranno concordati con la stazione appaltante nella fase di analisi. Il trasferimento dei documenti informatici nel sistema di conservazione avviene generando un pacchetto di versamento.
Si tratta del pacchetto informativo contenente il documento digitale o l'insieme dei documenti digitali, corredati da tutti i metadati descrittivi, nonché dalle informazioni di contesto, stabilite dal Contratto di servizio stipulato tra gli enti aderenti al servizio e il Conservatore Aruba PEC (per maggiori dettagli si rimanda al paragrafo 4.2 dedicato alle procedure organizzative) .
Il pacchetto di versamento contiene tutte le componenti informative che il sistema di conservazione DocFly necessita per creare dei Pacchetti di Archiviazione coerenti e ben strutturati.

Struttura del Pacchetto di Versamento
Il pacchetto di versamento e' composto, oltre che dai documenti, da un file xml chiamato indice del pacchetto di versamento; quest'ultimo contiene informazioni caratterizzanti il pacchetto stesso: nome file del pacchetto, ID univoco del PdV; ID univoco di ogni documento comprensivo della sua impronta e dei metadati che lo descrivono.
Tale indice del pacchetto di versamento rappresenta lo standard di DocFly da utilizzare per il versamento dei documenti digitali a prescindere dalla modalità adottata per l'invio dei documenti stessi.

Modalità di invio dei documenti
La documentazione soggetta a conservazione digitale a norma può pervenire tramite:

- FTPS L'utente, mediante un client ftp, ossia trasferimento dei file mediante protocollo FTP trasferisce i documenti in un'apposita area messa a disposizione da Aruba PEC. Questa modalità consente upload di un unico file compresso (zip) contenente tutti i file del lotto di conservazione ed è particolarmente indicata per l'inoltro di grosse moli di documenti.

- PEC Tra i canali di versamento il più immediato risulta quello dell'invio dei documenti da conservare tramite in una mail. Docfly prevede questa possibilità mettendo a disposizione un indirizzo PEC, concordato con il cliente, per la ricezione di documenti da mettere in conservazione
- Https E' prevista la possibilità da parte dell'utente di effettuare l'upload dei singoli documenti o dell'intero pacchetto di versamento tramite un'intuitiva interfaccia web accessibile tramite qualsiasi browser.
- Web Services: Aruba PEC fornirà tutti gli strumenti affinché il sistema documentale sorgente possa essere integrato via web services con DocFly, e permettere la corretta alimentazione del processo di conservazione a norma. Aruba PEC fornirà adeguata documentazione che descriva i requisiti funzionali e tecnici per l'integrazione di ulteriori altri sistemi informatici aziendali.

I metadati

La soluzione DocFly garantisce l'indicizzazione dei documenti inviati in conservazione, secondo i campi che saranno definiti insieme alla stazione appaltante e/o all'Ente Aderente nelle fasi di analisi. In particolare, Aruba PEC si impegna a definire e condividere con la stazione appaltante eventuali metadati ulteriori (extra-info), rispetto a quelli minimi (obbligatori) previsti dalla normativa.

Con il termine "metadati" si indicano tutte le informazioni significative associate al documento informatico, escluse quelle che costituiscono il contenuto del documento stesso.

Più nello specifico, i metadati devono riferirsi:

- alla provenienza: descrive la fonte del documento, chi lo ha formato e conservato dall'origine, la sua storia in generale (incluse le vicende legate al suo trattamento, cioè la sua creazione, le trasformazioni subite, i passaggi di possesso, ecc.). Metadati sono anche le informazioni riguardanti gli autori, gli eventuali sottoscrittori e le modalità di sottoscrizione e la classificazione del documento;
- al contesto: descrive come il documento si lega alle altre informazioni esterne al pacchetto informativo, quali, ad esempio, il motivo della sua creazione o le relazioni con altri contenuti informativi (vincolo archivistico);
- all'identificazione: definisce uno o più identificatori (univoci e persistenti) attraverso i quali il documento è identificato univocamente nel sistema;
- all'integrità: contiene gli elementi che proteggono il documento da alterazioni non documentate, ad esempio, la firma digitale, hash, ecc. Documentano quindi i meccanismi per verificare che le informazioni non siano state alterate.

I Formati

In linea con le regole tecniche (DPCM 3 Dic. 2013) il sistema considera standard i seguenti formati:

- PDF/ PDF-A
- TIFF
- JPG
- Office Open XML (OOXML)
- ODF (Open Document Format)
- XML
- TXT

Riguardo i formati menzionati sopra, Aruba PEC garantisce nel tempo: i requisiti di immodificabilità e staticità, nonché l'adozione di applicazioni software in grado di esibire i documenti nei formati ammessi. Al fine di garantire la conservazione e l'accesso ai documenti informatici nel lungo periodo, Aruba PEC adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati.

Per assicurare la leggibilità dei documenti informatici nel lungo periodo, Aruba PEC mantiene le specifiche del formato del documento informatico, assicurando che esisteranno applicazioni software in grado di esibire tutti i formati dei documenti conservati.

4.1.5 PROCESSO DI CONSERVAZIONE E CONTROLLI

Aruba PEC garantisce la piena conformità del processo di conservazione dei documenti prodotti dagli Enti aderenti al servizio, rispetto alle norme sancite dal CAD (Codice dell'Amministrazione Digitale) ed, in particolar modo ai requisiti di cui al DPCM 3.12.2013 in tema di conservazione di documenti informatici.

In linea con le richieste del Capitolato Aruba PEC metterà a disposizione un sistema di conservazione che, rispondendo ai requisiti, permetterà di:

- inviare in conservazione un singolo documento informatico, composto da uno o più file, o un insieme di documenti e dei relativi metadati che descrivono le proprietà di quella specifica tipologia documentale
- associare a ciascun singolo documento di un codice univoco che ne consenta l'identificazione certa all'interno del sistema di conservazione
- applicare il processo di conservazione dei documenti ricevuti, così come definito dalla normativa, dal capitolato tecnico e dagli allegati
- ricercare all'interno dell'archivio di conservazione per mezzo di chiavi diverse (codice identificativo del documento, codice pacchetto, data e qualunque altra informazione compresa nei metadati) ed estrarre le informazioni relative ai pacchetti/documenti che soddisfano i criteri di ricerca
- ottenere l'esibizione a norma dei documenti conservati, eventualmente attivata a partire dai risultati della ricerca di cui al punto precedente
- rettificare, sostituire le informazioni comprese nei metadati, operazioni che per la loro delicata natura verranno opportunamente tracciate nel sistema di conservazione
- scartare i documenti ai sensi dell' Art. 21 lettera d Dlgs 22 gennaio 2004 n. 42.

In questo capitolo sono descritte le fasi, i controlli, la gestione degli scarti e le notifiche che caratterizzano il processo di conservazione dei documenti informatici.

4.1.5.a. FUNZIONE DI ACQUISIZIONE

La fase di alimentazione del sistema di conservazione è quella che dà vita al processo e si attiva con la ricezione di un pacchetto di versamento. Nel sistema di conservazione DocFly, verranno accettati pacchetti di versamento che rispondono alle caratteristiche tecnologiche e informative previste all'interno del contratto di servizio, che rappresenta l'insieme di documenti che regolano i rapporti tra l'ente e il conservatore (Aruba PEC).

La ricezione e presa in carico di un pacchetto di versamento segue uno schema logico di funzionamento che si articola in due fasi distinte:

- la prima fase consiste nella ricezione dell'indice del pacchetto di versamento (xml);
- la seconda fase consiste nella ricezione dei documenti informatici descritti nel suddetto pacchetto di versamento.

<u>Prima Fase - Ricezione dell'indice del pacchetto di versamento (PdV)</u>

La funzione di ricezione dei pacchetti di versamento nel sistema di conservazione effettua una serie di controlli circa la regolarità di formazione del pacchetto stesso nonché dei dati relativi ai documenti che formeranno oggetto di deposito. Fondamentale è la funzione "controllo di qualità" che convalida l'esito positivo del trasferimento del PdV nell'area di lavorazione. Alla ricezione dell'indice del PdV, il sistema produce dei log indipendentemente dai canali di versamento. In linea con quanto previsto da normativa, saranno conservate e mantenute l' evidenze (log) atte a

dimostrare l'invio del Pacchetto di Versamento al Sistema di Conservazione. I controlli effettuati da sistema sull'indice del PdV sono riportati nella successiva tabella.

Il Sistema fornisce al Produttore una conferma della ricezione dell'indice del PdV che può includere una richiesta di ripetizione del versamento, qualora siano occorsi degli errori durante la fase di acquisizione. In entrambi i casi viene restituito al mittente (Produttore) un rapporto di conferma che riporta un riepilogo dei dati elaborati e l'indicazione di eventuali errori.

Seconda Fase - Ricezione dei documenti associati ad un pacchetto di versamento e controlli
A seguito della corretta ricezione dell'indice del pacchetto di versamento, il sistema di conservazione è pronto per la ricezione dei documenti informatici descritti nel pacchetto stesso. Qualora i documenti versati dovessero superare le verifiche di qualità previste, il sistema provvede all'invio del rapporto di versamento che formalizza la presa in carico del pacchetto.

Controlli di Sistema e Gestione degli scarti
Le funzionalità attivate nel processo di versamento/acquisizione del pacchetto di versamento prevedono dei controlli sia nella fase di ricezione dell'indice del PdV che sui singoli documenti inviati e corrispondenti a quanto previsto nell'indice stesso. La tabella riportata in basso elenca le diverse tipologie di controlli effettuati e per ognuna di esse indica l'azione prevista da sistema. Quest'ultima può tradursi in una operazione di scarto o notifica di un warning.

Controlli dell'indice del Pacchetto di versamento
Il deposito di un pacchetto di versamento e' distinto per ciascun lotto di documenti informatici omogenei (documenti omogenei, ossia aventi la stessa classe documentale). Pertanto, a classi documentali diverse corrispondono diversi PdV e versamenti, uno per ogni classe.

Controlli nella fase di ricezione dell'indice del PdV

ID	Oggetto del controllo	Azione in caso di check negativo
Verifica Autorizzazioni		
1.01	viene verificato che l'utente che effettua il versamento sia abilitato all'invio dei Pdv	Il sistema scarta l'intero pacchetto
Verifica formale indice del PdV		
2.01	viene verificato che l'oggetto ricevuto sia formalmente un indice xml in linea con lo standard DocFly	Il sistema scarta l'intero pacchetto
2.02	Viene verificato che il PdV è versato nei termini contrattuali e di servizio stabiliti col produttore	WARNING: Il sistema accetta il PdV ma non garantisce la conservazione nei termini concordati
Verifica presenza dati-documenti nell'indice del PdV		
3.01	viene verificato che l'indicazione del sistema di conservazione sia corretta	Il sistema scarta il PdV poiché il metadato contenuto nell'indice indica un sistema di conservazione diverso da DocFly
3.02	viene verificato che l'identificativo specificato nel Pdv non sia già presente nel sistema di conservazione	Il sistema verifica se il PdV (che contiene lo stesso ID) non sia già stato conservato. In questo caso il sistema considera il nuove indice in sostituzione del precedente. Viene invece scartato qualora il PdV risulta essere in stato 'conservato'.

3.04	Viene effettuato un controllo semantico sui metadati presenti nell'indice del PdV	Il sistema scarta il PdV poiché uno o piu' metadati non rispettano il formato condiviso nel contratti di servizio
3.05	viene controllato che per ciascun documento dichiarato e descritto all'interno dell'indice del Pdv: a. tutti i metadati minimi obbligatori siano presenti e nel formato corretto; b. il formato del documento è un formato ammesso c. l'estensione del documento sia tra quelle ammesse per il tipo documento; d. il formato dichiarato sia corrispondente all'estensione del nome file	Il sistema scarta il PdV perché le verifiche formali sui documenti dichiarati nell'indice del PdV hanno avuto esito negativo
Verifiche Paternità		
4.01	viene verificato che il Pdv, nel caso abbia estensione P7M, sia firmato con certificato valido	Il sistema scarta il PdV perché le verifiche formali sui certificati di firma hanno avuto esito negativo
4.02	viene verificato che tutte le firme apposte al Pdv siano valide	Il sistema scarta il PdV perché le verifiche formali sui certificati di firma hanno avuto esito negativo

Controlli nella fase di ricezione dei documenti

A seguito della corretta ricezione dell'indice del PdV, il sistema di conservazione è pronto per la ricezione dei relativi documenti informatici (files) descritti nel pacchetto stesso.

Controlli nella fase di ricezione dei documenti (files)

Controllo ricezione documenti		
1.01	viene verificato che l'hash del documento informatico inviato sia corrispondente all'hash dichiarato all'interno del medesimo indice del pacchetto al fine di avere garanzia che la trasmissione del pacchetto sia avvenuta correttamente e che l'integrità del documento informatico ricevuto sia assicurata	Il sistema scarta il documento se non atteso
1.02	in caso di file P7M viene verificata la validità della firma apposta su ogni singolo documento: o Controllo di conformità. o Controllo Crittografico. o Controllo Catena Trusted. o Controllo Certificato. o Controllo CRL	Il sistema scarta il documento qualora il certificato di firma non sia valido WARNING: in caso di documenti firmati e il certificato di firma utilizzato è prossimo alla scadenza, il sistema evidenzia un warning.
1.03	viene verificato che il documento sia leggibile	Il sistema scarta il documento nel caso questo non sia leggibile

1.04	viene verificato che il formato del documento informatico sia effettivamente valido e corrispondente a quanto dichiarato nel pacchetto di versamento. In tal caso i controlli eseguiti variano in funzione del formato atteso per ciascuno specifico documento.	Il sistema scarta il documento poiché il formato non è quello atteso
1.05	viene verificato che i documenti ricevuti non siano già presenti nel sistema di conservazione;	WARNING: il documento viene accettato e il sistema invia una notifica
1.06	Viene verificato che la ricezione dei documenti si sia correttamente conclusa entro la data limite di ricezione stabilita col produttore nel contratto di servizio	WARNING: il documento viene accettato ma il sistema non garantisce la conservazione nei termini concordati

Predisposizione del rapporto di versamento

Il sistema di conservazione predispone, per ciascun pacchetto di versamento, un rapporto di versamento che viene firmato dal responsabile del servizio di conservazione di Aruba PEC. Tale rapporto di versamento, viene identificato univocamente e contiene un riepilogo dei documenti e dei dati ricevuti e l'indicazione degli identificativi che il sistema di conservazione assegna a ciascun documento (impronte). I medesimi identificativi sono contenuti anche nel rapporto di conferma e sono indispensabili per procedere all'invio dei documenti stessi al sistema di conservazione a seguito dell'accettazione di un pacchetto di versamento.
E' bene notare che il rapporto di versamento viene reso disponibile solamente a seguito della completa e corretta ricezione di tutti i documenti descritti nel pacchetto di versamento.
Il rapporto di versamento viene sottoscritto con firma digitale del Responsabile del sistema di conservazione, il quale appone la marca temporale in luogo del riferimento temporale. Tale rapporto viene anche inviato via PEC (o altro canale certificato) all'indirizzo specificato nella configurazione di sistema.

4.1.5.b. FUNZIONE DI ARCHIVIAZIONE

La funzione "creazione dei pacchetti di archiviazione" trasforma uno o più pacchetti di versamento (PdV) in uno o più pacchetti di archiviazione (PdA) conformi agli standard dell'archivio.
La funzione di archiviazione fornisce, all'interno del sistema di conservazione, i servizi e le funzioni per l'archiviazione, la tenuta e il recupero dei Pacchetti di Archiviazione (PdA). In concreto, una volta che i PdV sono stati accettati nel sistema, essi sono pronti ad essere trasformati in pacchetti di archiviazione e quindi diventare l'oggetto della conservazione a lungo termine.

Pacchetto di archiviazione (PdA)

Il p*acchetto di archiviazione* (PdA) viene conservato nel sistema di conservazione ed è costituito da un indice in formato xml che contiene i contenuti minimi previsti dalla normativa e quelli specifici derivanti dalla particolare classe documentale cui l'indice si riferisce, utili alla conservazione a lungo termine.
Tale **pacchetto è realizzato secondo l'Allegato 4 al DPCM 3.12.2013.** Si tenga presente che ciò che nell'Allegato 4 è denominato IPdA (Indice del Pacchetto di Archiviazione) nello standard SInCRO è indicato come IdC (Indice di Conservazione).

L'IPdA è l'evidenza informatica associata ad ogni PdA, contenente un insieme di informazioni articolate.
Entrando nel dettaglio, all'interno dell'elemento IPdA si trovano le seguenti strutture:

- informazioni generali relative all'indice del pacchetto di archiviazione: un identificatore dell'IPdA, il riferimento all'applicazione che l'ha creato, eventuali riferimenti ad altri IPdA da cui deriva il presente, e un eventuale elemento "ExtraInfo" che consente di introdurre

metadati soggettivi relativi all'IPdA liberamente definiti dall'utilizzatore con un proprio schema;

- informazioni inerenti il Pacchetto di Archiviazione, in particolare: un identificatore del PdA, eventuali riferimenti ad altri PdA da cui deriva il presente, informazioni relative a una eventuale tipologia/aggregazione (di natura logica o fisica) cui il PdA appartiene e infine un eventuale elemento "ExtraInfo" che consente di introdurre metadati soggettivi relativi al PdA;
- indicazione di uno o più raggruppamenti di uno o più file che sono contenuti nel PdA. È possibile raggruppare file sulla base di criteri di ordine logico o tipologico ed assegnare ad ogni raggruppamento / singolo file le informazioni di base e un eventuale elemento "ExtraInfo" che consente di introdurre metadati definiti dall'utilizzatore. Ogni elemento file contiene l'impronta attuale dello stesso, ottenuta con l'applicazione di un algoritmo di hash e un'eventuale impronta precedentemente associata ad esso: in questo modo è possibile ad esempio gestire il passaggio da un algoritmo di hash diventato non più sicuro ad uno più robusto.
- Informazioni relative al processo di produzione del PdA, come: l'indicazione del nome e del ruolo dei soggetti che intervengono nel processo di produzione del PdA (es. responsabile della conservazione, delegato, pubblico ufficiale ecc.), il riferimento temporale adottato (generico riferimento temporale o marca temporale), l'indicazione delle norme tecniche e giuridiche applicate per l'implementazione del processo di produzione del PdA ed, infine, anche per il processo, un elemento "ExtraInfo" che consente di aggiungere dati soggettivi relativi al processo.

Chiusura del pacchetto di Archiviazione e File di Chiusura

Il soddisfacimento dei requisiti della conservazione digitale implica che l'indice dei pacchetti di archiviazione vengano firmati digitalmente, attraverso uno standard ETSI ammesso dalla normativa, dal responsabile del sistema di conservazione (Aruba PEC) o da un suo delegato e marcati temporalmente per assicurarne la validità nel corso del tempo.
Il File di Chiusura è un insieme di metadati in grado di fornire prova dell'integrità dell'insieme dei documenti, ad esso correlati la cui conservazione decorre da una data determinata, la cui prova di integrità è fornita tramite una firma elettronica qualificata, corroborata da una marca temporale.
La struttura del file di chiusura è costruita sulla base delle specifiche della struttura dati (UNI 11386:2010) contenute nell'allegato 4 alle regole tecniche e secondo le modalità riportate nel manuale della conservazione. Con la firma apposta in calce al file di chiusura, il Responsabile della conservazione di Aruba PEC dichiara, che il processo di conservazione è stato correttamente eseguito, in osservanza delle disposizioni legali vigenti.
In sostanza, con la suddetta firma apposta in calce al file di chiusura, l'apposizione della marca temporale e la suddetta dichiarazione il conservatore non sottoscrive il contenuto e la semantica dei documenti conservati ma asserisce solamente che il processo di conservazione è stato eseguito correttamente, nel rispetto delle norme giuridiche e delle indicazioni contrattuali di servizio.

Prolungamento della validità del documento conservato

La normativa vigente conferisce alla firma digitale il ruolo di strumento in grado di garantire l'autenticità nel tempo dei documenti. La firma deve risultare valida nel momento in cui il documento entra nel sistema di conservazione.
Il sistema di conservazione espone un servizio che raccoglie i documenti firmati. Questo servizio attiva un processo che, producendo una serie di "registrazioni" di dati gestite da un sottosistema apposito, si occupa di mantenere nel tempo la prova di autenticità del documento per mezzo di apposite marche (temporali) di controllo e di mantenimento della validità temporale del documento.
Il sistema di conservazione assicura inoltre che le firme emesse per suo conto (per esempio sui File di Chiusura – Pacchetto di Archiviazione) siano mantenute come specificato nei seguenti punti, così che la loro validità possa essere verificata in ogni istante durante il periodo di conservazione:

- al fine di permettere la verifica affidabile di un'AdES, anche se il relativo certificato è stato

revocato oppure è scaduto dopo il momento della firma, viene applicata una marca temporale il più vicino possibile al momento della firma, per fornire prova che l'AdES esisteva prima della scadenza o della possibile revoca del certificato;

- nel sistema di conservazione DocFly vigono procedure (sottoponibili ad audit) per assicurare il mantenimento delle firme che, dove del caso, prevedano la raccolta di prove a sostegno della validità della firma.

Sostanzialmente, il sistema di conservazione DocFly assicura che l'autenticità, l'integrità e la leggibilità del File di Chiusura siano assicurate nel tempo.

Dimensione dei documenti

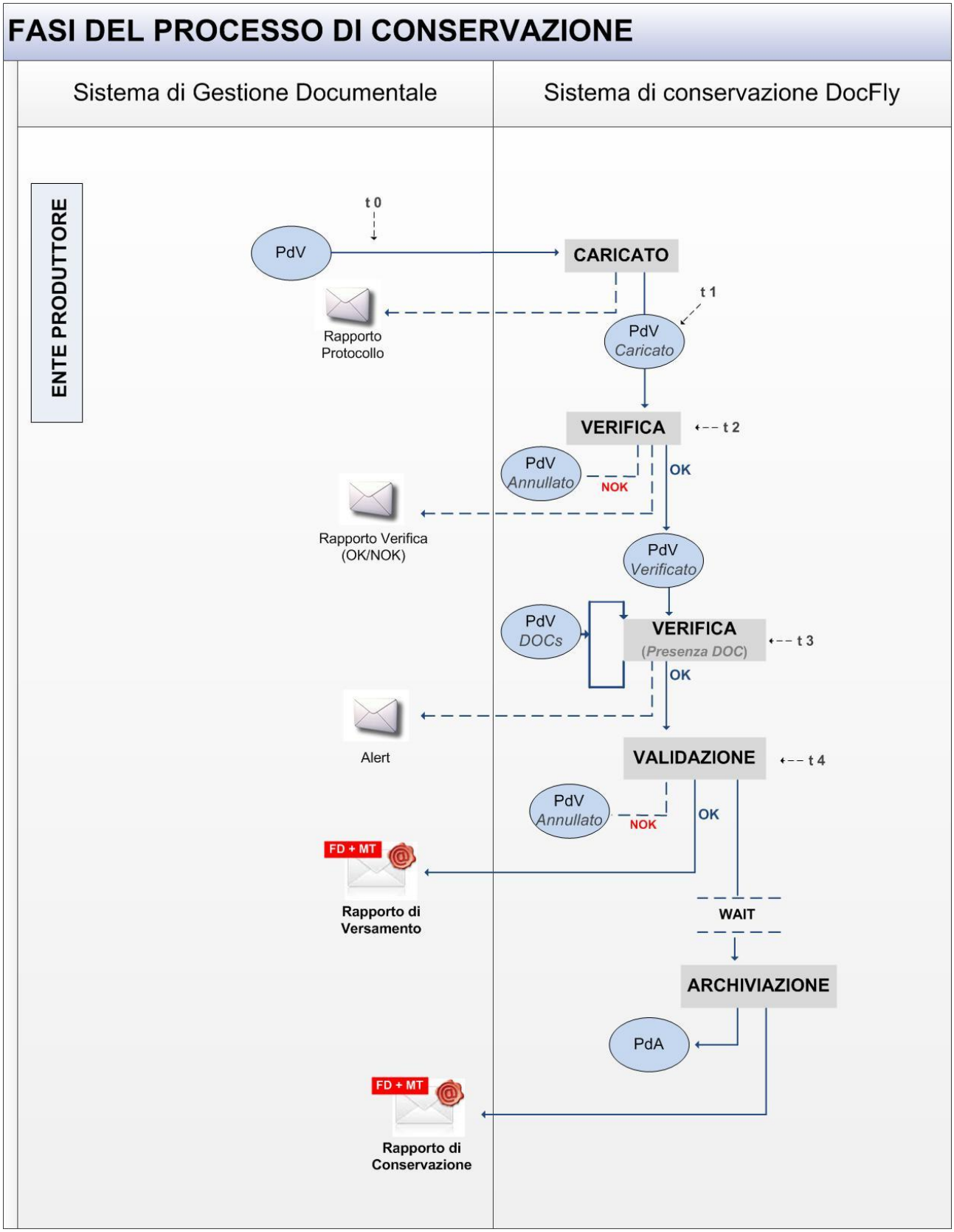
Relativamente ai documenti conservati, il sistema DocFly assicura le specifiche minime previste da capitolato:

- dimensione massima del singolo documento: 100 MByte
- dimensione massima di un file: 100 Mbyte
- numero massimo di file per documento: 100
- lunghezza massima dei nomi dei file: 80 caratteri

La soluzione proposta è in grado, inoltre, di gestire file di dimensioni maggiori rispetto a quelli minimi sopra indicati, attraverso opportuni canali descritti al par. 4.6.2.

4.1.6 SCHEMA DI PROCESSO E INVIO DELLE NOTIFICHE

Le diverse operazioni, che si succedono lungo il processo di conservazione, sono riportate nello schema sottostante.



Schema: Notifiche processo di conservazione

Come si evince dallo schema, il sistema di conservazione prevede la produzione di rapporti di notifica che 'scandiscono' le principali fasi del processo di conservazione del documento digitale:

- **T1 - Rapporto di Protocollo (PdV Caricato):** indica l'avvenuta ricezione nel sistema di un

oggetto Digitale

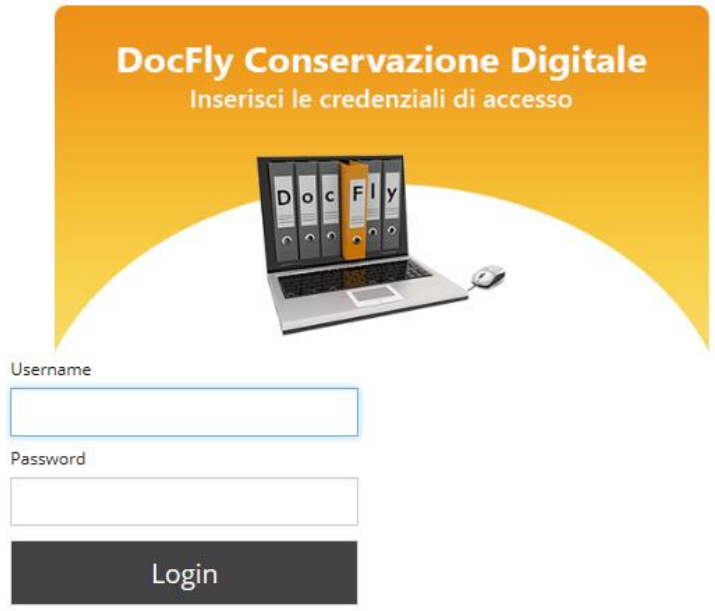
- **T2 - Rapporto di Verifica (PdV Verificato):** Indica che l'indice del PdV ha superato correttamente i controlli qualitativi
- **T4 - Rapporto di Versamento (PdV Validato):** Il PdV, e documenti contenuti, sono stati accettati dal sistema di conservazione
- **T5 - Rapporto di Conservazione (PdV Conservato)**: Indica la chiusura e passaggio in conservazione del PdA

I rapporti di notifica, secondo lo standard DocFly, sono inviati via PEC agli indirizzi dei destinatari scelti dall'Ente. Tuttavia, sono contemplati eventuali canali alternativi, i quali saranno eventualmente analizzati con la stazione appaltante.

4.1.7 PORTALE DI CONSERVAZIONE DOCFLY

Nella progettazione del servizio DocFly va certamente evidenziata la grande importanza del ruolo ricoperto dal tema dell'usabilità, intesa come la facilità con cui un utente svolge un compito per mezzo dello stesso. A tal proposito, grazie all'esperienza maturata fino ad oggi e ai *feedback* ricevuti dagli utenti finali, la soluzione DocFLy può vantare una interfaccia intuitiva e semplice da usare.
Il pannello di gestione è accessibile tramite interfaccia web, protocollo sicuro https; attraverso il quale, l'utente che accede, dispone di tutti gli strumenti utili per la gestione delle sue attività, in linea quanto richiesto da capitolato.
Attraverso il portale di conservazione, l'utente, in linea con i privilegi previsti per la specifica utenza, può effettuare le seguenti operazioni: versamento manuale, ricerca ed esibizione dei documenti conservati.

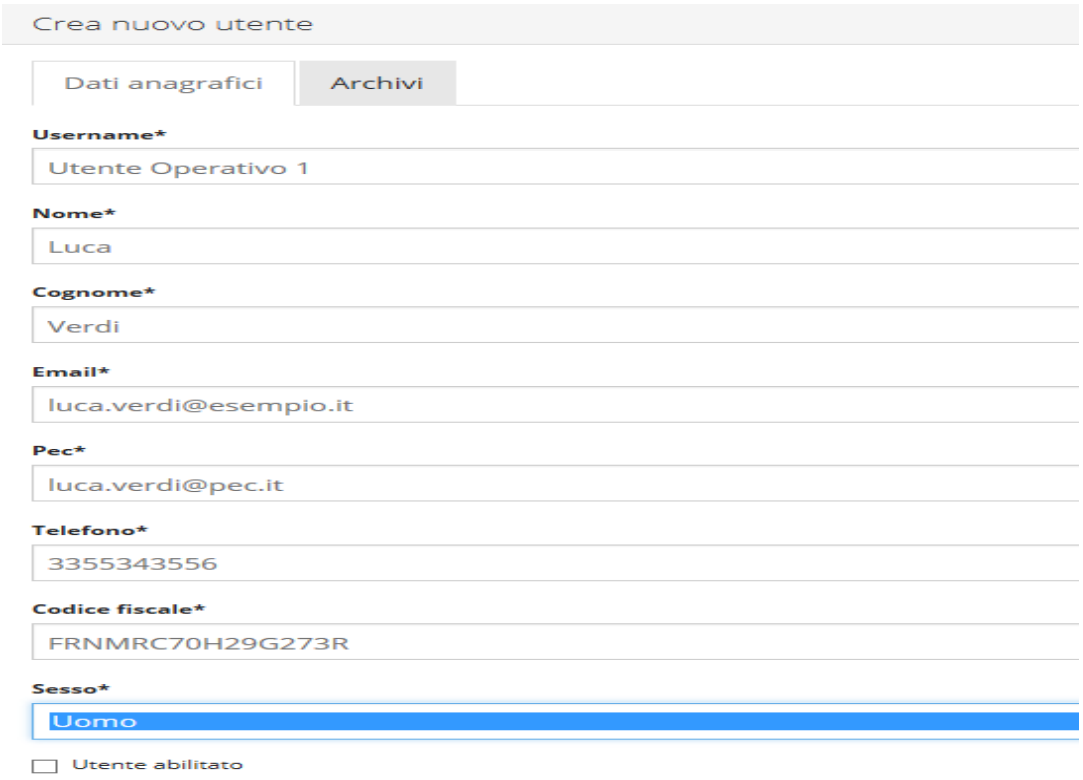
In basso nella figura viene mostrata la pagina di accesso al pannello di sistema



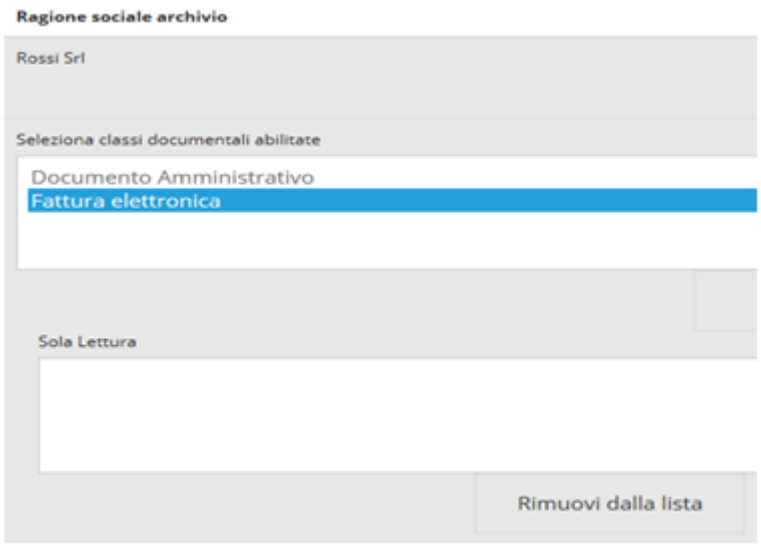
4.1.7.a. GESTIONE DELLE UTENZE E ACCESSO AL SISTEMA

Tutti gli utenti che hanno accesso a DocFly sono sottoposti alle regole di autenticazione e sicurezza previste dalla legge come descritto dettagliatamente nel paragrafo relativo alla sicurezza al par. 4.3. Tutte le pagine web che richiedono l'uso di credenziali utilizzano il protocollo SSL (Secure Sockets Layer) per tutelare sicurezza e privacy.
DocFly garantisce la registrazione degli accessi; la sessione utente ha un timeout configurabile da sistema. La password non è memorizzata in chiaro nel database, ed è modificabile dall'utente in

qualsiasi momento tramite un pannello apposito. Nel database viene memorizzato l'HASH (SHA256) criptato della password. Le credenziali di accesso sono personali, univoche e non riutilizzabili.
L'utente "*Master*", entro i limiti delle risorse assegnate, può creare e gestire in completa autonomia, uno o più profili, sulla base delle utenze in suo possesso; soddisfacendo in questo modo la richiesta di capitolato che prevede la possibilità da parte dell' Ente di permettere l'accesso ai documenti inviati in conservazione solo agli utenti autorizzati da quest'ultimo.



Come mostrato nella figura in alto, le operazioni necessarie per la creazione di un nuovo Utente sono facilmente intuibili. Tramite semplici configurazioni e' inoltre possibile assegnare all'utente i permessi di "lettura" e/o "scrittura" su una o più specifiche tipologie documentarie, in modo da abilitare l'utente operativo sia alle operazioni di ricerca e visualizzazione che di versamento (conservazione) dei documenti.



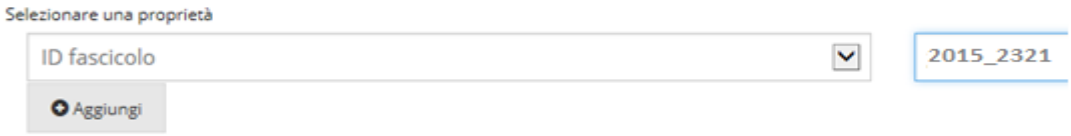
4.1.7.b. PROCEDURA DI VERSAMENTO E CONSERVAZIONE TRAMITE PANNELLO WEB

In linea con quanto previsto da capitolato, il portale di conservazione consente di versare dei documenti da conservare e i metadati che li specializzano. La procedura segue uno schema logico di funzionamento che si articola in due fasi distinte: ricezione dell'Indice del Pacchetto di Versamento (IPdV) e ricezione dei documenti che fanno parte del Pacchetto di Versamento (PdV).
La procedura di acquisizione tramite pannello web, permette di caricare da pannello uno o più documenti appartenenti alla stessa classe documentale che saranno oggetto di conservazione. L'operazione di acquisizione richiede che i documenti siano sempre associati all'indice del pacchetto di versamento; quest'ultimo, descritto in precedenza, è un file in formato xml che riporta i metadati previsti per l'indicizzazione e ricerca dei documenti conservati.
Il sistema prevede la possibilità per l'utente di creare, in completa autonomia, l'indice del pacchetto di versamento attraverso due modalità: procedura guidata (wizard) e procedura manuale.
L'utente grazie ad un *form* semplice e intuitivo, compila i campi necessari per generare l'Indice del Pacchetto di Versamento e caricare i documenti oggetto di conservazione. In alternativa, l'utente può effettuare l'upload del/i file/s da sottoporre a conservazione tramite la medesima maschera.
Entrambe le procedure sono riportate nella figura in basso:

Nel caso di errori durante l'elaborazione del/i files, i dati interessati verranno opportunamente evidenziati dal sistema.

4.1.7.c. FUNZIONALITÀ DI RICERCA E DOWNLOAD

Le operazioni di visualizzazione/ricerca dei documenti conservati, sono gestite tramite un'apposita 'maschera', la quale permette di effettuare la ricerca del documento di cui è richiesta l'esibizione sulla base della classe documentale, del nome del documento, del periodo di appartenenza inteso come anno, della data del documento e del valore di tutti i metadati che sono stati definiti per la classe documentale specifica.
Il sistema espone un *form* attraverso il quale l'utente può ricercare il documento editando uno dei campi (metadati) previsti dalla classe documentale (nell'esempio viene utilizzato il campo "ID fascicolo" come chiave di ricerca).



L'operazione di ricerca restituisce il documento/i ricercato/i, indicando la data di trasferimento nel sistema e lo stato di conservazione, come mostrato in figura

	Titolo	Creato da	Data versamento	Conservato
☐	Modulo_registrazione_2321.pdf	IBP	22/09/2015	Conservato
☐	ID_devisu_2321.mp4	IBP	15/06/2015	Conservato

4.1.7.d. FUNZIONALITÀ DI CREAZIONE DELLA CLASSE DOCUMENTALE

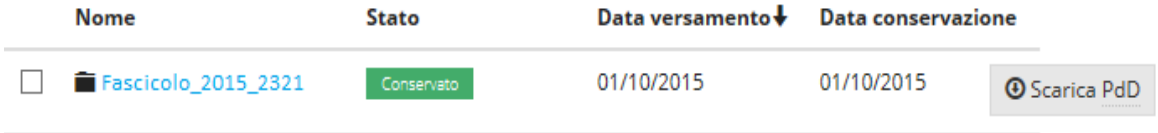
La soluzione DocFly garantisce l'indicizzazione dei documenti inviati in conservazione, secondo i campi che saranno definiti insieme alla stazione appaltante nelle fasi di analisi. Un set di indici consente di creare e identificare una precisa tipologia di documento (classe documentale). In particolare, una classe documentale è formata da un insieme di indici minimi, ovvero, quelli previsti dalla normativa vigente, e un altro che possiamo individuare come insieme dei metadati cosiddetti "extra-info"; quest'ultimi saranno definiti e condivisi con la stazione appaltante tenendo conto delle specificità legate al contesto di ognuno degli Enti coinvolti nel processo di conservazione. E' bene ricordare che occorre prestare particolare attenzione al complesso sistema di metadati agganciati ai documenti, poiché solo da questi emerge il significato del documento ed è sui metadati che il sistema effettua i controlli.

Il motore delle classi documentali è stato realizzato sfruttando il principio dell'ereditarietà. Ovvero ogni classe è vista sempre come sottoclasse di una meno specifica ereditando, di fatto, l'insieme dei metadati e delle extrainfo della classe padre, ma con la possibilità di essere estesa con nuovi metadati ed extrainfo e definendone le regole in termini di obbligatorietà.
Questa soluzione permette una migliore gestione delle informazioni, in quanto definisce delle regole ben fondate per la catalogazione dei documenti e consente l'estensibilità futura di classi documentali in maniera più compatta e con minore rischio di errori.
L'albero delle classi ha come vertice delle classi base che garantiscono l'aderenza di qualsiasi altra classe alle norme vigenti: Documento Informatico, Documento Amministrativo e Documento Tributario.

4.1.7.e. ESIBIZIONE CON VALENZA LEGALE – IL PACCHETTO DI DISTRIBUZIONE

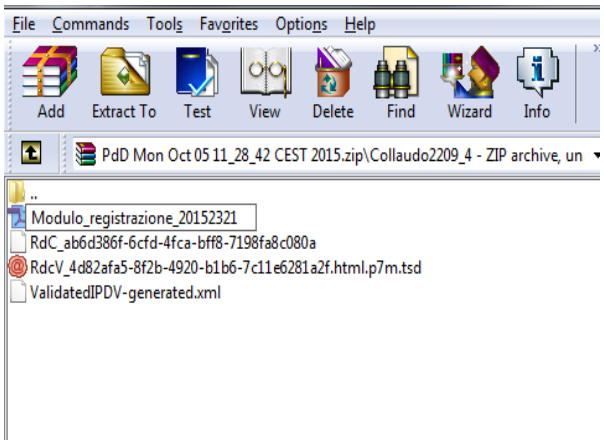
La soluzione DocFly mette a disposizione degli utenti la funzionalità di creazione del pacchetto di distribuzione; quest'ultimo assicura l'esibizione con valenza legale e può essere utilizzato nei confronti degli organi di vigilanza e le loro attività di accertamento.

L'utente può richiedere la creazione di un pacchetto di distribuzione contenente il documento digitale o l'insieme dei documenti digitali, corredati da tutti o parte dei metadati previsti nel pacchetto di archiviazione. Attraverso alcune semplici operazioni, l'utente potrà selezionare uno o più documenti appartenenti anche a diverse tipologie documentarie e ottenerne una replica esatta secondo i fini previsti dalla norma.



	Nome	Stato	Data versamento	Data conservazione	
☐	Fascicolo_2015_2321	Conservato	01/10/2015	01/10/2015	Scarica PdD

In corrispondenza del file di proprio interesse è possibile salvare in locale, in formato *zip*, il relativo pacchetto di distribuzione, nella struttura prevista dalla normativa vigente



In risposta alla richiesta iniziale di esibizione, da parte dell'utente, il sistema di conservazione DocFly risponderà restituendo un pacchetto di distribuzione che nel caso più completo conterrà:

- Nome (ID) dei files/ documenti richiesti nel formato previsto per la loro visualizzazione e contenuti nel pacchetto.
- Un'estrazione dei metadati associati ai documenti.
- L'indice di conservazione firmato e marcato dal Responsabile del Servizio di Conservazione o delegato.
- Indice del Pacchetto di Archiviazione di appartenenza
- I viewer necessari alla visualizzazione dei documenti del pacchetto: Aruba PEC infatti provvederà a gestire e mantenere un apposito archivio dei programmi di visualizzazione per tutti i formati dei documenti conservati.

A fronte di una richiesta di produzione del pacchetto di distribuzione, il sistema effettua delle verifiche di coerenza e correttezza del pacchetto e dei documenti in esso contenuti. A tal proposito, la soluzione DocFly verifica che le impronte dei documenti restituiti nel PdD corrispondano a quelle presenti nel relativo indice del pacchetto di archiviazione; in modo da garantire che i documenti stessi non abbiano subito alterazioni o modifiche nei contenuti.

4.1.7.f. WEB SERVICE

La soluzione DocFly può dialogare con diverse sorgenti documentali e tool di gestione in uso presso Regione del Veneto e gli Enti Aderenti e, in linea con le richieste del capitolato, potrà interfacciarsi con sistemi esterni mediante web services che permettono di effettuare chiamate real time al sistema DocFly, mediante canali sicuri di trasmissione che saranno concordati nella fase di analisi.
L'interfaccia web service fornisce tutti i metodi utili sia per il processo di versamento dei documenti che per le operazioni di interrogazione al sistema. L'interfaccia è stata realizzata secondo il protocollo REST, dando così maggiore flessibilità al client nel costruire le proprie politiche di integrazione.
Aruba PEC metterà a disposizione di Regione del Veneto e degli Enti aderenti il Manuale per lo sviluppatore, con ovvero una guida all'integrazione dei servizi con web services messi a disposizione per il servizio di conservazione.

4.1.7.g. FUNZIONALITÀ DI MONITORAGGIO

Il sistema di reportistica di base del sistema DocFly, prevede l'analisi dell'uso delle risorse da parte dei vari utenti ed è disponibile all'interno del pannello web messo a disposizione. DocFly considera, come elemento granulare, l'archivio di ogni singolo Ente in maniera da avere un migliore controllo delle informazioni a corredo.
Di ogni archivio di tale tipo, una utenza, potrà effettuare delle verifiche globali sui principali dati di sintesi del servizio in erogazione, onde verificarne l'andamento nel periodo di fornitura. In particolare, il sistema permette di reperire le seguenti informazioni:

- numero di utenti che possono accedere all'archivio in qualità di Titolare, ovvero in modalità di ricerca e lettura dei pacchetti e dei documenti
- spazio disco utilizzato dall'archivio.

Oltre a questi dati, disponibili direttamente sul pannello di gestione DocFly, Aruba PEC metterà a disposizione tutte le informazioni richieste dal capitolato tecnico all'interno dello strumento di monitoraggio complessivo del progetto, descritto nel Capitolo 7.

4.1.8 MANUTENZIONE EVOLUTIVA

In linea con le richieste di capitolato, Aruba PEC si impegna a monitorare l'evoluzione normativa e garantirà, per tutta la durata del contratto, le attività necessarie ad installare eventuali nuove release del prodotto al software applicativo.

Il servizio di manutenzione evolutiva è generalmente di tipo preventivo, in quanto, i processi di installazione degli aggiornamenti si muovono su base pianificata. Il servizio proposto si farà carico delle attività di sviluppo ed evoluzione di tutte le procedure realizzate e/o modificate nell'attuale fornitura. Aruba PEC infatti si impegna a monitorare l'evoluzione della normativa applicabile al servizio di conservazione a norma, per individuare tempestivamente l'introduzione di nuove regole, requisiti, standard tecnici ecc. con impatto su quanto erogato.

In particolare, Aruba PEC garantirà di:

- comunicare la necessità di adeguamento e il piano di adeguamento;
- procedere alla realizzazione necessaria previa autorizzazione dei referenti della Regione del Veneto e comunicare l'avvenuto rilascio della soluzione;
- provvedere all'aggiornamento della documentazione.

Per maggiori dettagli sulle modalità di manutenzione si rimanda al par. 1.2.3.

4.2 PROCEDURE ORGANIZZATIVE ADOTTATE

I successivi paragrafi si pongono come obiettivo principale l'identificazione di tutti gli aspetti riguardanti le convenzioni tra i soggetti coinvolti nel processo di conservazione dei documenti informatici, nonché la descrizione di dettaglio delle metodologie adottate da Aruba PEC per l'erogazione del servizio di conservazione a norma, tenuto conto del contesto organizzativo degli enti coinvolti nel processo.

Il paragrafo anticipa alcuni di questi contenuti e mette in risalto le principali novità che il processo di conservazione apporterà nel contesto Regione del Veneto e degli Enti Aderenti.

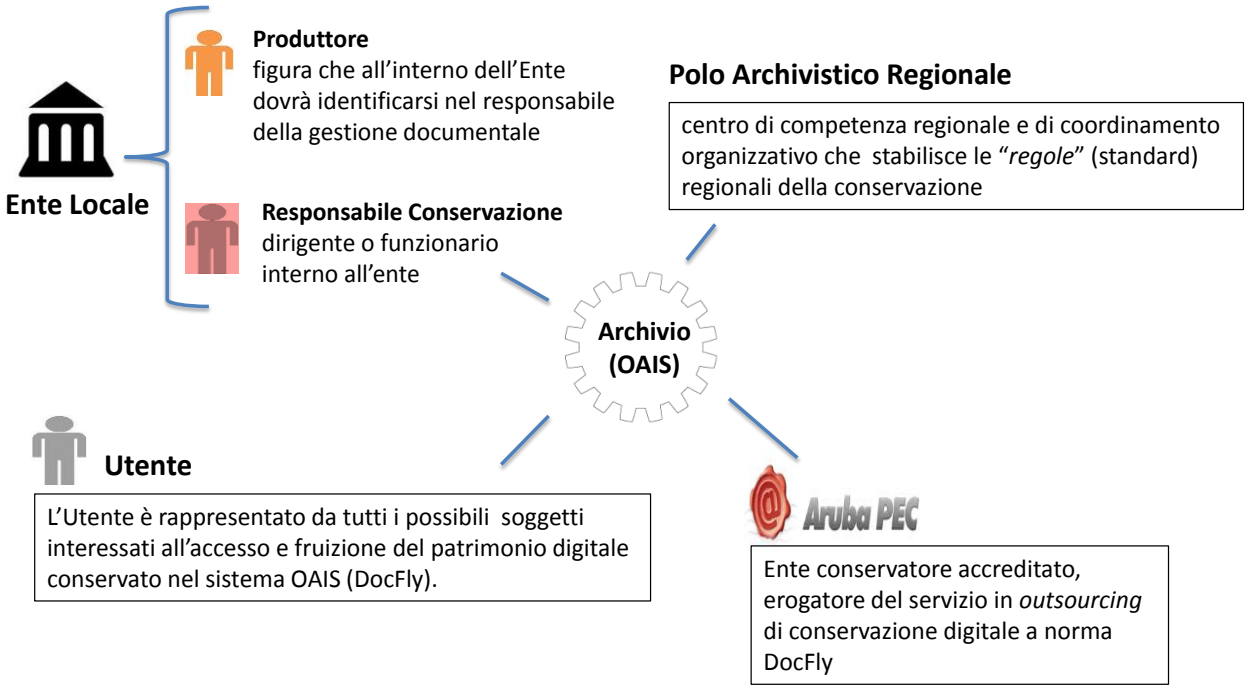
4.2.1 IL MODELLO DI RIFERIMENTO OAIS - IL CONTESTO REGIONE DEL VENETO

Con la pubblicazione del DPCM 3 Dicembre 2013, che sostituisce la Delibera CNIPA/2004 in tema di regole tecniche sui sistemi di conservazione elettronica dei documenti (fiscali e non), vengono introdotte importanti novità sia a livello tecnico che di processo. In particolare, le nuove

regole tecniche sono state stilate dal legislatore in conformità allo standard internazionale ISO 14721 (OAIS) che, oltre a introdurre i concetti di Sistema OAIS e pacchetto informativo, esplicitano una netta separazione tra i ruoli che interagiscono con un archivio OAIS.

Ruoli Funzionali

I soggetti coinvolti nel contesto Regione Veneto



In aderenza con il modello concettuale OAIS, è possibile individuare nel contesto della Regione del Veneto i seguenti ruoli:

- **Ente Locale**: all'interno di ognuno degli Enti della Regione aderenti al servizio, sono individuate le figure di Responsabile Produttore e Responsabile della Conservazione.

  Responsabile Produttore tale figura si identifica con il responsabile della gestione documentale, il quale diviene responsabile a tutti gli effetti del contenuto del pacchetto di versamento e trasmissione di tale pacchetto al sistema di conservazione secondo i modi, nei termini ed in conformità a quanto stabilito in un contratto di servizio, dal Manuale del sistema di conservazione e dai rispettivi allegati.

  Responsabile della Conservazione nelle pubbliche amministrazioni il ruolo del Responsabile della Conservazione è svolto da un dirigente, da un funzionario formalmente designato o dallo stesso responsabile della gestione documentale ovvero dal coordinatore della gestione documentale, ove nominato. In linea con quanto indicato nelle nuove regole tecniche art. 6 (Ruoli e responsabilità) co. 6, *"..il responsabile sotto la propria responsabilità, può delegare lo svolgimento del processo di conservazione o di parte di esso ad uno o più soggetti di specifica competenza ed esperienza in relazione alle attività ad essi delegate. Tale delega è formalizzata, esplicitando chiaramente il contenuto della stessa, ed in particolare le specifiche funzioni e competenze affidate al delegato*". Nel nostro ordinamento, la responsabilità della conservazione non può essere trasferita e quindi rimane in capo agli Enti.

- **Polo Archivistico Regionale**: in linea con quanto previsto da capitolato, costituisce il centro di competenza regionale di coordinamento organizzativo e stabilisce le 'regole' regionali della conservazione. Il Polo, una volta costituito, assumerà un ruolo strategico volto a garantire un approccio alla conservazione omogeneo, organizzato e interoperabile. In particolare, tale organo gestirà sia il rapporto con i fornitori dei sistemi di gestione documentale degli Enti che si dovranno integrare verso li sistema di conservazione nel rispetto delle regole stabilite dallo stesso, che la raccolta delle deleghe necessarie ai fini dell'attivazione del servizio di conservazione DocFly (come dettagliato ai par. 4.2.3 Integrazione tra Sistemi e 4.4 Avvio del Servizio).
- **Utente:** nel contesto Regione del Veneto l'utente può essere rappresentato da qualsiasi soggetto (organo vigilanza, ente terzo, etc..) che richiede al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge.
- **Archivio** (OAIS)**:** struttura responsabile della trattazione quotidiana degli oggetti informativi archiviati, con procedure e metodi che ne assicurano la conservazione e fruizione a lungo termine. DocFly rappresenta il sistema OAIS messo a disposizione da Aruba PEC.
- **Aruba PEC** (Ente Conservatore Accreditato): Il DPCM all'art 6 co. 7 contempla la possibilità di affidare la conservazione ad un soggetto esterno, mediante contratto o convenzione di servizio che preveda l'obbligo del rispetto del manuale di conservazione predisposto dal responsabile della stessa. Nella fattispecie, il responsabile della conservazione dell'Ente, sotto la propria responsabilità, affida ad ARUBA PEC, quale prestatore del servizio di conservazione digitale dei documenti informatici, il servizio di conservazione digitale dei documenti informatici dell'ufficio, delegando le attività previste dal relativo Contratto di servizio (per maggiori dettagli si riporta al par. 4.4).

Gli Enti coinvolti nel processo, titolari dei documenti informatici posti in conservazione e giuridicamente responsabili della conservazione, sotto la propria responsabilità affideranno ad Aruba PEC, quale prestatore del servizio di conservazione digitale dei documenti informatici, il processo di conservazione digitale dei documenti informatici oggetto di capitolato.

Ai fini dell'erogazione del servizio di conservazione digitale a norma, Aruba PEC svolgerà le attività ad essa delegate dagli Enti come riportato nel documento di Nomina del responsabile del servizio di conservazione digitale dei documenti informatici del Cliente che sarà allegato al Contratto di servizio. Nel contempo, Aruba PEC sarà nominata Responsabile esterno del trattamento dei dati come previsto dal Codice in materia di protezione dei dati personali (D.Lgs. 196/2003 e s.m.i.).

In questo modo, la responsabilità della conservazione digitale dei documenti informatici è interamente delegata ad Aruba PEC. Gli Enti coinvolti nel procedimento saranno, di conseguenza, sollevati da tutti i complessi adempimenti e oneri conseguenti agli obblighi imposti dalla normativa regolante la conservazione digitale di documenti informatici, come il rispetto dei termini temporali di conservazione, la salvaguardia dell'integrità e leggibilità dei documenti, la gestione della sicurezza fisica ed informatica del sistema di conservazione, l'aggiornamento tecnologico e normativo.

Aruba PEC si impegna a conservare tutti i documenti ricevuti in conservazione con la diligenza richiesta dalle attività oggetto del presente capitolato e sarà tenuta a risarcire gli Enti Aderenti fruitori del servizio dei danni diretti ed indiretti che dovessero derivare a questi o a terzi, in caso di mancata osservanza ad essa imputabile delle tempistiche, delle tecnologie o del processo di conservazione dei documenti trasmessi, stabilite dalla normativa, dal presente capitolato, e in caso di perdita o danneggiamento dei dati sottoposti a conservazione.

In linea con quanto previsto da capitolato, Aruba PEC assicura inoltre la redazione e predisposizione di un idoneo manuale delle procedure di conservazione in conformità con quanto prescritto dall'art. 8 del citato DPCM, che verrà adottato da ciascun Ente come riferimento documentale in materia di conservazione dei documenti informatici.

4.2.2 SISTEMA DI GESTIONE DOCUMENTALE E OAIS - IL CONFINE DELINEATO DALLA NORMATIVA

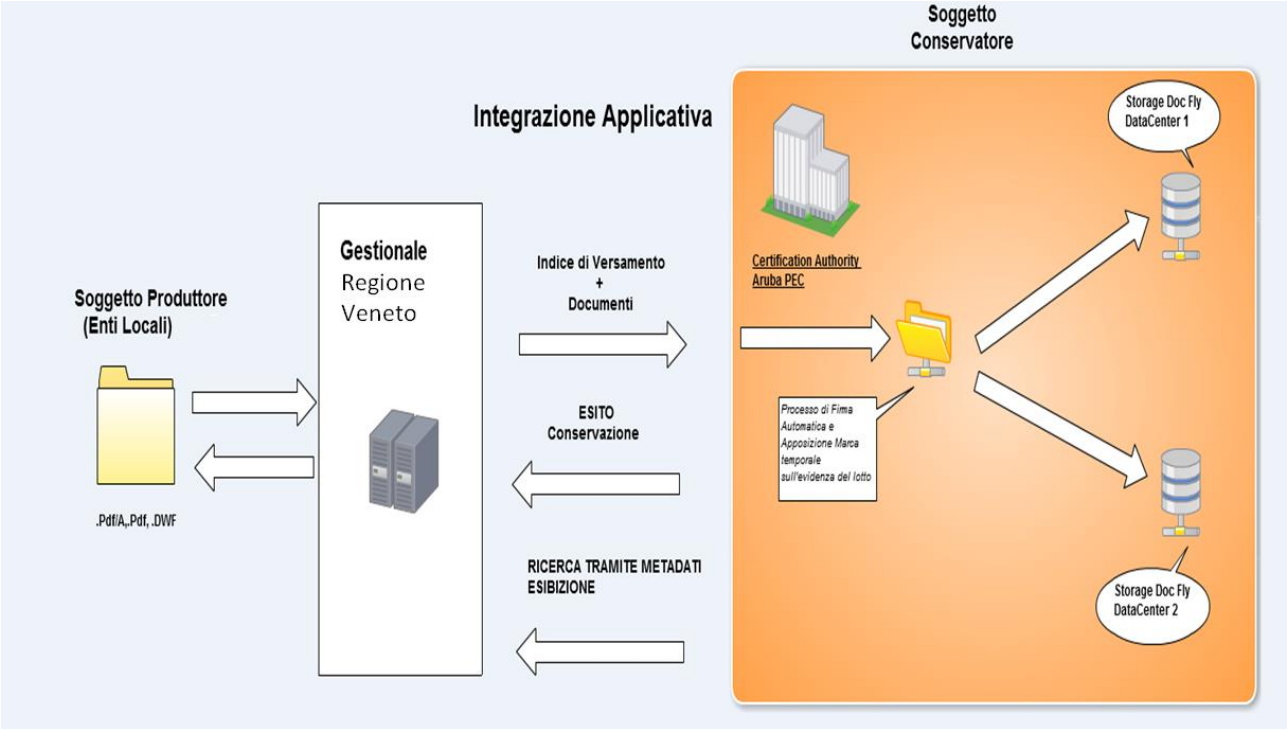
Il sistema di conservazione digitale a norma DocFly opera secondo modelli organizzativi che garantiscono la sua distinzione logica e fisica dal sistema di gestione documentale, che resta sotto la completa responsabilità dell'ente comunale Produttore; quest'ultimo, in assoluta autonomia, provvede, anche attraverso propri incaricati, alla produzione/formazione/emissione e sottoscrizione dei documenti informatici propri e dei metadati ad essi associati, che saranno versati in conservazione.

L'ente comunale Produttore coinvolto nel procedimento, dovrà attenersi alle disposizioni del Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 (in vigore dallo scorso 11 aprile 2014) che riporta le regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

In particolare, con la redazione del manuale di gestione (art 5 del suddetto decreto), il Produttore descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni generali per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

4.2.3 INTEGRAZIONE TRA SISTEMI

Sulla base delle informazioni contenute nel capitolato, è possibile riportare una descrizione ad alto livello riguardante l'integrazione dei sistemi coinvolti nel processo di conservazione digitale dei documenti informatici di proprietà degli Enti Regione del Veneto.



Come mostrato in figura, appare evidente il ruolo strategico che sarà conferito al Polo Archivistico Regionale Veneto che , attraverso la definizione di regole ben precise sulla conservazione, gestirà lo snodo tecnologico per isolare la complessità operativa e facilitare e supportare gli Enti in tutte le fasi della conservazione: conferimento, ricerca, esibizione, scarto ecc.

In linea con quanto previsto da capitolato e le risposte ai chiarimenti riportate nel documento "TEC1-009-R-Varie.pdf", Il Polo Archivistico Regionale sarà costituito da un unico nodo centralizzato (Hub regionale) che si occuperà di ricevere i documenti dai relativi produttori (Enti) e di metterli a disposizione del conservatore.

In caso di aggiudicazione della gara, Aruba PEC in qualità di fornitore del servizio di conservazione assicura:

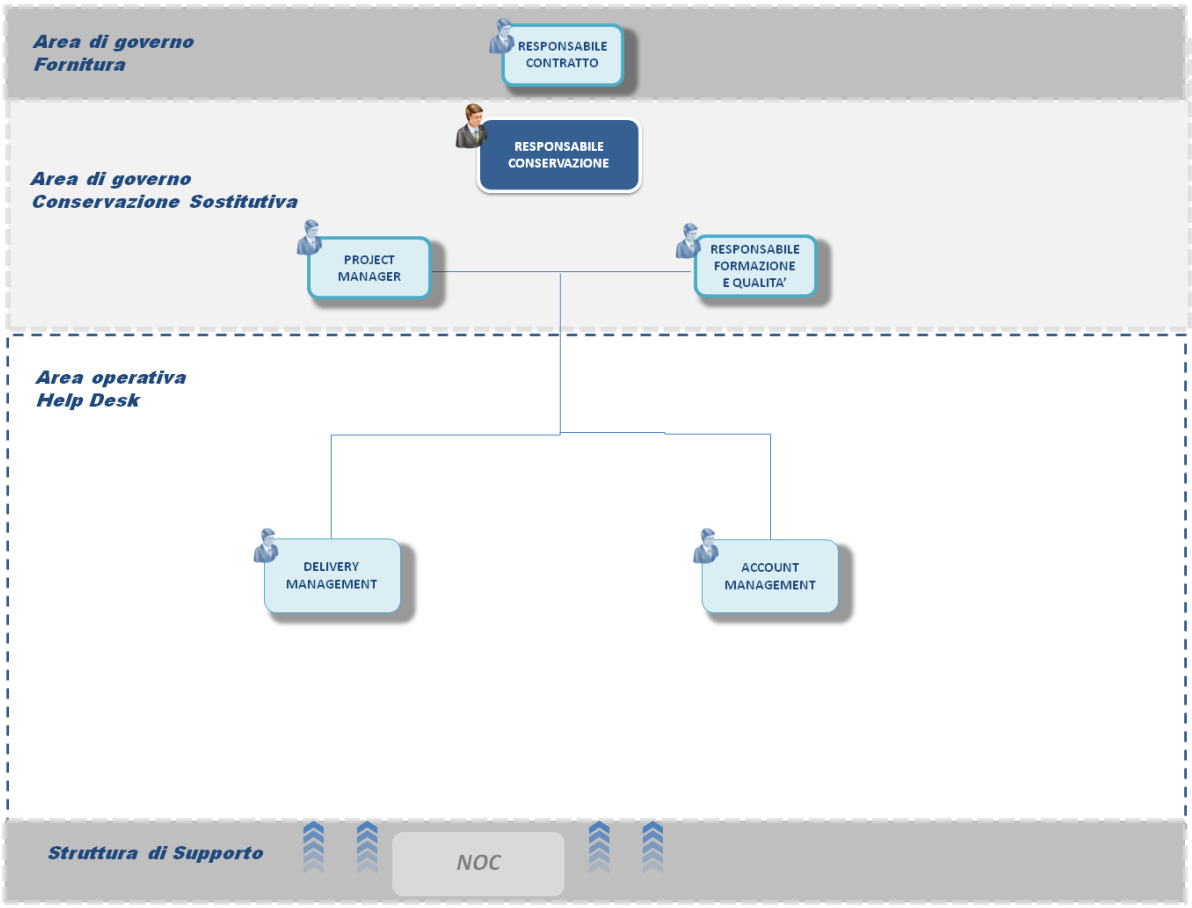
- la realizzazione dei servizi di colloquio con il Polo Archivistico Regionale attraverso standard SPC/SPCoop, secondo le specifiche che sono state messe a disposizione della stazione appaltante
- l'integrazione degli stessi con il proprio sistema di conservazione DocFly
- l'erogazione dei servizi mediante il Polo

Il flusso operativo che descrive l'integrazione dei sistemi prevede le seguenti fasi:

1. L'Ente della Regione del Veneto invia i documenti al Polo Archivistico in base alle regole e standard definiti
2. Il Polo Archivistico Regionale invia in conservazione i documenti degli Enti al sistema di conservazione DocFly – tramite l'integrazione dei sistemi e secondo le specifiche condivise con Aruba PEC
3. Aruba notifica l'esito della conservazione all'Ente richiedente – con la possibilità di poter ricercare tali documenti attraverso i metadati al fine della loro esibizione.

4.2.4 ORGANIZZAZIONE DEL SERVIZIO

All'interno del modello organizzativo del Servizio di Conservazione si distinguono due aree specifiche: l'Area di governo e l'Area operativa.



Ciascun utente della Regione del Veneto può usufruire del **Servizio di Conservazione** come centro di competenza identificato a gestire le richieste di conservazione a norma dei documenti. L'organizzazione della **Conservazione Sostitutiva** prevede la sinergia tra figure professionali appartenenti a **due distinte aree funzionali**.

All'interno dell'**Area di Governo della Conservazione** sono presenti le seguenti figure:

- ✓ **Responsabile Conservazione** – è supervisore dell'intero **Servizio di Conservazione**. Coordina le attività svolte dal team Delivery e dal team Account - a garanzia del massimo livello di qualità di servizio. Ha inoltre il compito di coinvolgere la figura del **Responsabile Formazione e Qualità** qualora sia necessario un miglioramento qualitativo sugli aspetti operativi. A seguito della firma del contratto il suo nominativo e i relativi recapiti (telefono, fax, mail) verranno comunicati formalmente all'Ente Aderente in modo da mettere in piedi tutte le attività propedeutiche all'avviamento del servizio, descritte nel par. 4.4.

- ✓ **Responsabile Formazione e Qualità** – rappresenta il responsabile del livello di competenze e della qualità operativa svolta dal team Delivery e dal team Account. Tale figura interagisce con il **Responsabile Conservazione** e garantisce l'aggiornamento ed il miglioramento continuo di processi/procedure utili a perfezionare il livello di servizio.

L'**Area Operativa Conservazione** ha la responsabilità di fornire operativamente il servizio agli utenti di riferimento della Regione del Veneto e degli Enti aderenti – secondo le seguenti figure:

- ✓ **Delivery Management** – è supervisore dell'erogazione del **Servizio di Conservazione**. Coordina le attività svolte dal team **Delivery** – finalizzate ad evadere le richieste di conservazione dei documenti da parte degli utenti della Regione del Veneto – interfacciandosi con il **Polo Archivistico**.
- ✓ **Account Management** – è supervisore della gestione delle richieste di conservazione dei documenti da parte degli utenti della Regione del Veneto. Rappresenta l'interfaccia tra

l'utente richiedente della Regione del Veneto ed il team **Delivery** – a garanzia della corretta gestione di richieste di conservazione specifiche e/o fuori standard.

4.3 SICUREZZA DEL SISTEMA

In linea con gli standard previsti dalla vigente normativa in materia di sicurezza, Aruba PEC adotta idonee e preventive misure sia nella fase di realizzazione che nell'erogazione dei propri servizi.
Il sistema di conservazione di Aruba PEC è ospitato presso i data center proprietari del Gruppo Aruba. I data center, descritti nei par. 1.2.2 e ss., sono caratterizzati per il rispetto dei massimi standard di sicurezza e affidabilità. In particolare verrà garantita la riservatezza, l'integrità e la disponibilità delle informazioni, la sicurezza logica e fisica del sistema, degli strumenti hardware e software e dei locali, attraverso sistemi antincendio, antintrusione, di sicurezza perimetrale e sorveglianza, descritti nel Capitolo 1. Sono inoltre previste opportune politiche di back-up descritte nel par. 4.3.6.

Aruba PEC si impegna a:

- verificare periodicamente l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti (come descritto successivamente al par. 4.3.9);
- mantenere in corso di validità tutti i documenti ricevuti in conservazione per tutta la durata del contratto mediante l'apposizione di ulteriori marcature temporali ovvero l'estensione del periodo di validità dei certificati , come descritto nel dettaglio al par. 4.1.5.b (Prolungamento della validità del documento conservato).

La soluzione si caratterizza per la sua modularità che le consente di essere scalabile, e al tempo stesso affidabile. La sua architettura flessibile, garantisce elevate performance e la rende adattabile a specifiche esigenze di carico. Il sistema di conservazione DocFly e' ridondato e resiliente ai guasti, grazie alla funzionalità di HA e Fault Tollerance.

Nei paragrafi successivi sono descritti i principali aspetti relativi ai livelli e procedure atte a garantire la sicurezza del sistema di conservazione.

4.3.1 ARCHITETTURA LOGICA DELLA SOLUZIONE

Il Sistema di Conservazione DocFly è sviluppato nell'ottica di fornire una soluzione Enterprise, ed è un insieme di applicazioni clusterizzabili che permettono una facile scalabilità e una gestione automatica dei processi.
Vista l'esperienza del Gruppo Aruba nell'ambito della gestione di grandi volumi di dati è sempre stato un obiettivo per il Gruppo creare un'architettura elastica: "espandibile" in caso di aumento del carico di lavoro oppure "limitabile" nel caso di una riduzione delle necessità.
L'intera soluzione è stata progettata per essere in grado di gestire l'elaborazione di grandi volumi di dati. Per questa ragione, DocFly può essere scalato sia verticalmente che orizzontalmente e, le singole componenti, possono essere distribuite su più server.

L'architettura del sistema DocFly e' modulare, implementata al 100% su infrastruttura di virtualizzazione con hypervisor Vmware e garantisce i seguenti vantaggi:

Affidabilità - Totale ridondanza ai guasti HW

- Funzionalità di HA e Fault Tollerance
- Controllo completo delle prestazioni
- Adattabile a specifiche esigenze di carico

Architettura scalabile orizzontalmente

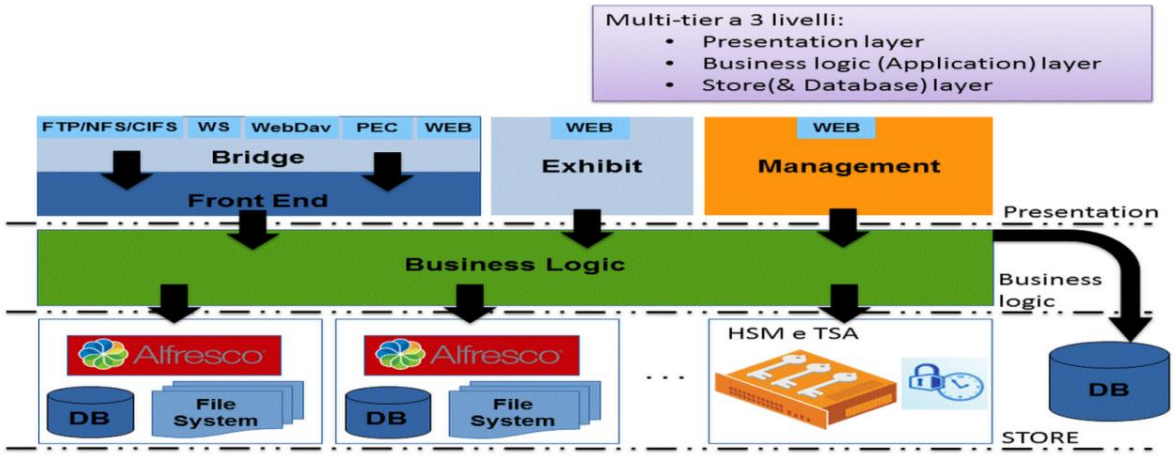
- Nodi di Front-End ed Application contemporaneamente attivi

- DBMS in configurazione Master-Master

Storage di livello Enterprise

- Alte prestazioni
- Funzionalità di replica
- Esposizione diretta di FS avanzati

Di seguito riportiamo l'immagine rappresentativa delle componenti logiche del sistema di conservazione:

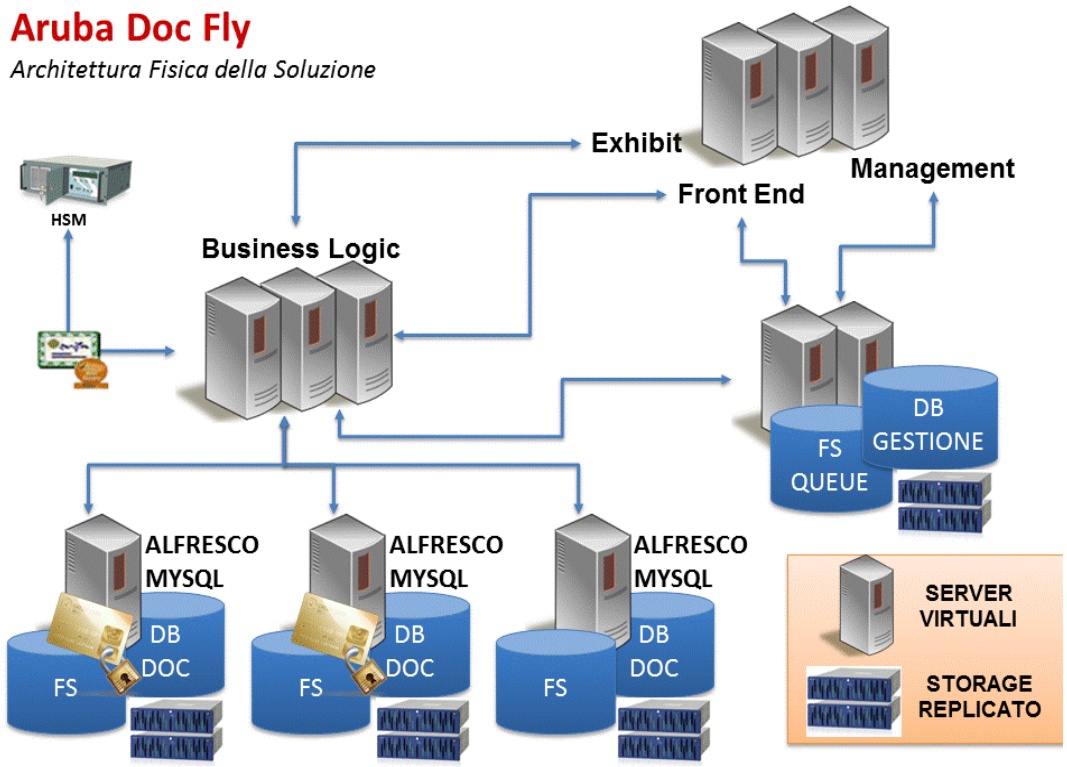


Come si evince dalla figura l'architettura è basata su una soluzione multi-tier a 3 livelli:

- **Presentation layer**: L'applicazione è pensata per essere scalabile, aumentando il numero dei Web container attraverso una logica di server clustering, gestita automaticamente dal sistema, che, a seconda del livello di carico di ciascun server, distribuirà al meglio le richieste dei client.
- **Business logic (o application) layer**: La Business Logic ha l'intelligenza di scrivere sull'istanza Alfresco disponibile. Tutte le istanze Alfresco sono sempre disponibili almeno in lettura
- **Store (& Database) layer**: La parte di back end e' composta da diverse coppie di istanze di Alfresco. Ogni istanza e' costituita dal DB e dal file system. Il DB risiede sul cloud privato e contiene i metadati conservati; il FS contiene l'archivio (dati conservati). Ognuna delle istanze e' replicata a livello applicativo. Tale replica garantisce continuità in termini di consultazione, qualora uno dei due nodi non dovesse essere disponibile.

4.3.2 ARCHITETTURA FISICA DELLA SOLUZIONE

L'intera infrastruttura di DocFly è basata su una completa ridondanza del dato grazie alla distribuzione geografica delle macchine e degli storage necessari all'erogazione del servizio.



Al fine di garantire ridondanza e bilanciamento del traffico vengono utilizzati dispositivi di load balancing in grado di distribuire il carico di lavoro su un numero di macchine virtualmente illimitato. Questo meccanismo permette di risolvere oltre a problemi prestazionali con la semplice aggiunta a caldo di nuove macchine, anche problemi relativi ad eventuali guasti delle componenti bilanciate.
Lo storage, di livello enterprise, per la conservazione dei dati prodotti dalla stazione appaltante rispondono ai più avanzati criteri di sicurezza e di aggiornamento tecnologico, con configurazione in RAID, ed offrono opportune soluzioni tecniche in grado di garantire la massima robustezza intrinseca del sistema di memorizzazione e la possibilità di recupero automatico del fault di una singola unità disco.

Aruba PEC ha implementato un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) conforme alla norma ISO 27001. Nell'ambito del Sistema di Conservazione proposto sono adottate misure di sicurezza fisica, logica e organizzativa coerenti con tale SGSI e con la normativa vigente in tema di protezione dei dati personali (D.lgs. 196/2003), potendo essere inviati in conservazione documenti contenenti dati personali, sensibili e giudiziari.
In questo capitolo sono descritti i principali aspetti relativi ai livelli e procedure atte a garantire la sicurezza del sistema di conservazione.

4.3.3 AUTENTICAZIONE E MISURE DI CONTROLLO SUGLI ACCESSI

Gli utenti possono accedere – previa identificazione ed autenticazione – solamente alle risorse (es. sistemi, funzionalità, informazioni) per cui sono stati esplicitamente autorizzati in base al ruolo ricoperto. I permessi sono attribuiti alle utenze secondo il principio del "least privilege" e rivisti periodicamente per mitigare il rischio di abuso di privilegi. Ad ogni persona (interna od esterna) viene assegnata un'utenza personale ed univoca. Le utenze di gruppo sono usate solo per esigenze particolari ed espressamente autorizzate.
Tutte le pagine web che richiedono l'uso di credenziali utilizzano il protocollo SSL (Secure Sockets Layer) per tutelare sicurezza e privacy.
Inoltre, per garantire la massima sicurezza, DocFly supporta varie forme di Strong Authentication. In particolare, per la soluzione proposta a Regione del Veneto, Aruba PEC fornirà un sistema di accesso allo strumento di conservazione con Autenticazione forte, tramite smartcard/token per gli

utenti con particolari profili autorizzativi (ad es. utenti abilitati a mandare in conservazione i documenti, utenti amministratori ecc.).
Per l'autenticazione potrà essere usata sia la smartcard operatore, assegnata a tutti gli ODR del servizio di firma digitale come descritto nel par. 2.1, sia una smartcard/Token USB contenente i certificati di autenticazione CNS o CNS Like.
Per gli utenti che, invece, avranno profili limitati di sola ricerca e consultazione potrà essere usato un sistema di autenticazione basato su Username e Password.

La soluzione proposta presenta quindi le seguenti caratteristiche:

- l'utilizzo di sistemi di autenticazione forte tramite smartcard/token
- l'integrazione di altre soluzioni di autenticazione forte che la stazione appaltante volesse adottare in futuro.

DocFly garantisce la registrazione degli accessi; la sessione utente ha un timeout configurabile da sistema. La password non è memorizzata in chiaro nel database, ed è modificabile dall'utente in qualsiasi momento tramite un pannello apposito. Nel database viene memorizzato l'HASH (SHA256) criptato della password. Le credenziali di accesso sono personali, univoche e non riutilizzabili.
In linea con quanto previsto nel capitolato, il sistema DocFly garantisce la tracciabilità delle attività eseguite, sia da parte dell'utente esterno (invio in conservazione, modifica, esibizione) sia dalle procedure interne di Aruba PEC (esempio: apposizione firma digitale sui documenti presi in carico, marcatura temporale, riversamento, ecc.). L'accesso alle informazioni tracciate sarà garantito al Responsabile della conservazione dell'Ente aderente per i dati di propria competenza.

4.3.4 MONITORAGGIO EVENTI E VULNERABILITÀ DI SICUREZZA

Nell'ambito del Servizio di Conservazione, viene conservata e periodicamente esaminata una traccia (**audit log**) delle operazioni svolte dagli utenti e dai processi, in modo che tali azioni possano essere documentate ed attribuite a chi le ha eseguite o causate (accountability), anche allo scopo di rilevare eventi di sicurezza, incidenti e vulnerabilità associati ai sistemi coinvolti nel processo di conservazione. Tali log vengono archiviati su supporto permanente e non è permesso agli utenti non autorizzati di accedervi.

4.3.5 CIFRATURA

Come previsto dal Piano della Sicurezza del Servizio di Conservazione di Aruba PEC, tutte le comunicazioni tra il Sistema e gli utenti (interattivi o applicativi) sono protette col protocollo sicuro SSL/TLS e pertanto sono cifrate. Per la cifratura del canale, si utilizzano algoritmi di cifratura con chiavi di lunghezza ≥ 128 bit.

4.3.6 BACKUP

Nell'ambito della gestione operativa del Servizio di Conservazione, sono definite ed applicate procedure di backup finalizzate alla creazione e conservazione di copie di sicurezza dei dati, dei software applicativi, delle loro configurazioni e di ogni altra informazione necessaria per ripristinare il servizio in caso di necessità (per es. a fronte di guasti hardware o incidenti più severi).

Nello specifico Aruba PEC realizzerà il servizio di Backup geografico **nel sito di Disaster Recovery**: un server dedicato ad alte prestazioni gestirà in automatico i backup in uno spazio riservato, offrendo servizio di retention 8-4-3, ovvero 8 backup giornalieri, 4 settimanali e 3 mensili su tutti i dati di produzione.
Il backup geografico su macchina dedicata è una soluzione che permette di garantire un recovery dei dati ottimale per il fatto che esso è connesso con link dedicato a 1Gbps su una diversa sede. Anche in caso di disastro quindi è possibile accedere ai dati di backup di settimane e mesi precedenti.

I dati vengono scritti e salvati sempre in duplice copia sincrona sui sistemi di storage distribuiti geograficamente con la garanzia dell'effettiva scrittura su entrambi i siti. Su i due storage utilizzati inoltre vengono effettuate copie di sicurezza attraverso meccanismi di snapshot e backup per garantire la massima salvaguardia del dato.
I metadati e i dati utenti sono salvati su istanze dedicate distribuite su due siti geografici distinti e configurate in mirror transazionale in modo da avere una duplicazione non solo del dato ma anche di tutti i metadati necessari alla propria reperibilità e ricerca.

Per quanto riguarda i **documenti**, si fa presente che essi sono sempre conservati in **doppia copia**, ciascuna presso un data center separato (per i documenti, dunque, non vi è una reale distinzione tra copia di produzione e copia di backup).

4.3.7 ISOLAMENTO DELLE COMPONENTI CRITICHE

I sistemi e le risorse tecnologiche alla base del Servizio di Conservazione sono isolate dagli altri ambienti di elaborazione a livello fisico e logico (in quanto risiedono su hardware dedicato a tale Servizio), nonché parzialmente a livello organizzativo, in coerenza coi requisiti indicati nel Piano della Sicurezza e nel Manuale della Conservazione.

4.3.8 BUSINESS CONTINUITY

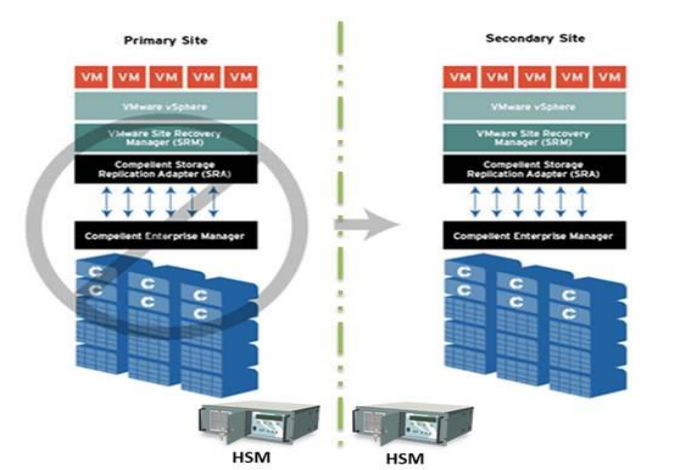
Grazie ad un'architettura ridondata e all'housing del Sistema presso un Data Center tra i più evoluti a livello nazionale (DC di proprietà del gruppo Aruba sito in Arezzo, caratterizzato da un'ampia gamma di misure di sicurezza e di ridondanza a tutti i livelli: alimentazione, networking, ecc. si veda nel seguito per ulteriori dettagli), Aruba PEC può garantire un'elevatissima affidabilità del servizio di conservazione.
Le misure adottate ai fini del Disaster Recovery e della Business Continuity sono documentate nel piano di Continuità Operativa.

Il data center che costituisce il sito primario è situato in un'area classificata come di "basso rischio idrogeologico", inoltre l'edificio è completamente antisismico ed è posto ad un piano rialzato dal livello stradale, in modo da risultare maggiormente protetto alle calamità naturali.
L'intero Data center è continuamente monitorato sia in sede locale che in più sedi remote ed è dotato delle soluzioni di sicurezza più avanzate descritte in seguito. La struttura è inoltre collegata con un secondo Datacenter, sempre di proprietà di Aruba, che rappresenta la sede di Disaster recovery.

4.3.8.a. CARATTERISTICHE TECNICHE DEL SERVIZIO DI DISASTER RECOVERY

I servizi legati alla conservazione e oggetto di fornitura del presente capitolato, risiederanno su server collocati presso i Data Center del Gruppo Aruba. Al fine di garantire il servizio di Disaster Recovery, l'ambiente di DR sarà composto da una macchina di Frontend (per l'interfaccia utente) e un macchina di Backend su cui risiedono i dati (Database e dati conservati).
La sincronizzazione dei DB e' prevista in modalità sincrona. I dati conservati saranno salvati contemporaneamente sul sistema di produzione e su quello di DR; solo a processo finito viene restituito da sistema una notifica di confermando relativamente alla messa in conservazione a norma di legge. In caso di switch del sistema verrà seguita una procedura manuale che prevede il cambio dei puntamenti dei servizi dalla produzione verso l'ambiente di DR.

<u>Schema e descrizione tecnica del servizio di Disaster Recovery</u>
La figura che segue riporta lo schema logico del servizio di DR adottato per il progetto Terna



Come si evince dallo schema, il servizio di DR consta presenta le seguenti caratteristiche:

Replica Storage Base

- Macchine Virtuali
- Data Base – sia sincrono che tramite dump (golden copy)
- File System

HSM Replicato

- Immediata riattivazione delle VM alla dichiarazione di Disastro
- Raggiungibilità tramite altri collegamenti di rete
- Verifica consistenza dei Data Base replica sincrona (RPO=0)
- RTO pari alla diffusione del nuovo indirizzamento DNS

Procedura di ripristino del Servizio

La procedura di ripristino del servizio nella soluzione proposta da Aruba PEC alla stazione appaltante offre valori misurabili di reliability in termini di RTO e RPO e pari a:

- **RTO pari a 1 ore**
- **RPO pari a 0 ore**

L'indice RTO esprime l'arco temporale massimo entro cui il ripristino delle risorse minime deve essere garantito, al fine di contenere gli impatti, legati all'indisponibilità, a livelli sopportabili per il cliente, mentre l'RPO rappresenta l'intervallo temporale massimo a cui far riferimento per individuare il punto di ripristino dei dati e/o del sistema.
Il tempo di RTO offerto e' pari ad un'ora è necessario per lo switch dei nomi DNS registrati per la conservazione e per l'esibizione documentale in quanto l'infrastruttura sul datacenter secondario è già pronta per l'erogazione.
L'RPO pari a 0 è giustificato dal fatto che l'applicazione di conservazione effettua la registrazione documentale su entrambi i siti contemporaneamente in maniera sincrona garantendo la massima affidabilità.

4.3.8.b. LIVELLI DI PROTEZIONE DEI DATI.

Aruba PEC in caso di aggiudicazione, contestualmente alla sottoscrizione del Contratto verrà nominata responsabile esterno del trattamento dei dati personali ai sensi dell'art 29 D. Lgs n. 196/03 e si impegna ad seguire le istruzioni che saranno impartite dalla stazione appaltante, nonché a consentire alla stazione medesima di eseguire verifiche periodiche circa la puntuale osservanza delle disposizioni normative e delle proprie istruzioni.

Aruba PEC, quale responsabile esterno del trattamento dovrà, in via meramente esemplificativa:

1. designare per iscritto, le persone fisiche, incaricate del trattamento
2. individuare i diversi livelli di accesso di ciascun incaricato, in corrispondenza delle specifiche mansioni ad esso attribuite
3. adottare le misure minime di sicurezza che possano ridurre al minimo i rischi di distruzione, perdita, anche accidentale di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta (artt. 31 e ss. del Codice e Allegato B al medesimo Codice). In particolare dovrà attenersi alle prescrizioni del Garante per la protezione dei dati personali del 27 novembre 2008, "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle funzioni di amministratore di sistema" e successive modifiche e integrazioni
4. comunicare senza indebito ritardo alla stazione appaltante e comunque entro i termini previsti nel provvedimento del Garante per la protezione dei dati personali del 04 aprile 2012 in tema di "attuazione della disciplina sulla comunicazione delle violazioni dei dati personali (data breach)" gli eventi e le informazioni necessarie a consentire alla stazione appaltante di adempiere agli obblighi di notifica al Garante e al contraente della violazione dei dati personali, come previsto dall'art. 32-bis co. 1 e 2 D. Lgs n. 196/03
5. adeguare le risorse tecnologiche messe a disposizione del fornitore
6. allineare costantemente il sistema alle evoluzioni della normativa.

4.3.9 VERIFICA INTEGRITÀ E LEGGIBILITÀ DEI DOCUMENTI CONSERVATI

In linea con quanto previsto dalla normativa vigente, il sistema DocFly dispone di funzionalità che permettono di verificare, con cadenza non superiore ai cinque anni, l'integrità del documento dal momento della sua conservazione, confrontando l'impronta attuale con quella contenuta nell'Indice di Conservazione. Tale funzionalità risulta utile nell'assolvimento dei requisiti di verifica periodica della leggibilità dei documenti, come richiesto dalla normativa. A questa funzione viene aggiunta la verifica dell'integrità della firma digitale apposta al relativo Indice di Conservazione. In qualsiasi momento a seguito di una ricerca, è possibile effettuare una verifica sul singolo file o insieme di file.

Al fine di garantire la conservazione e l'accesso ai documenti informatici, Aruba PEC adotta, inoltre, misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità adotta analoghe misure con riguardo all'obsolescenza dei formati. Gli strumenti a disposizione permettono di individuare se il contenuto del file di partenza e di arrivo è rimasto inalterato. In altre parole è necessario capire se le significant properties si sono conservate.

Aruba PEC ha impostato dei test automatici di controllo, che prevedono la migrazione dei formati, operazione, questa, che potrà essere necessaria sulla base dello specifico formato divenuto obsoleto e sulla base del nuovo formato di destinazione scelto per l'operazione di migrazione.
In tale ottica, l'obiettivo di garantire, nel tempo, l'integrità dei documenti è perseguito anche attraverso il loro riversamento, diretto o sostitutivo su supporti di nuova generazione.

4.4 AVVIO DEL SERVIZIO

Aruba PEC ha maturato numerose esperienze in progetti analoghi a quello oggetto della presente fornitura, che ci hanno permesso di approfondire e conoscere il contesto delle PA ed in particolare i soggetti e le entità coinvolte nel processo di conservazione. In virtù di questa esperienza è stato possibile consolidare le procedure e documentazione contrattuale, necessarie ai fini dell'efficiente avvio del servizio.

A seguito della firma del contratto sarà comunicato formalmente all'Ente aderente il nominativo e relativi recapiti (telefono, fax, mail) del referente aziendale responsabile del servizio di conservazione a norma, in modo da mettere in piedi tutte le attività propedeutiche all'avviamento del servizio, che si concluderà entro i 30 giorni richiesti dal Capitolato.

Durante la fase di avviamento verranno predisposte tutte le procedure, attività, ruoli, funzioni propedeutiche per la fruizione del servizio da parte degli Enti aderenti.
Aruba PEC si occuperà inoltre di eseguire tutti i test di integrazione con il sistema informatico degli Enti aderenti e di acquisire tutti i documenti conservati dal precedente fornitore del servizio, verificando e quindi certificando la validità, l'integrità, la leggibilità dei documenti e la loro corretta conservazione.
La conclusione delle attività di avviamento sarà certificata da un verbale di collaudo controfirmato dalle parti. Il sistema sarà considerato attivo solo al termine di quest'attività e, da questo momento, i nuovi documenti potranno essere inviati in conservazione.

Il conservatore accreditato Aruba PEC, in linea con la normativa vigente, si avvale di contratti o accordi scritti necessari ai fini dell'avvio del servizio e che specificano i seguenti aspetti: diritti e responsabilità, versamento e acquisizione, mantenimento, accesso, ritiro, deposito, diritti e responsabilità di conservazione sui documenti che tratta, natura economica e di servizio.
L'inserimento del processo di conservazione all'interno del ciclo documentale dei documenti prodotti dagli Enti della Regione del Veneto, implica l'integrazione alle attuali convenzioni che disciplinano e regolano i rapporti tra i soggetti e le istituzioni coinvolte nel procedimento. In particolare, come descritto successivamente all'interno del paragrafo, si viene ad instaurare un rapporto diretto (contratto di servizio) tra il conservatore (Aruba PEC) e il soggetto Produttore; quest'ultimo coincide con l'Ente (titolare del proprio archivio).

Ai fini dell'attivazione e l'erogazione del servizio di conservazione, il soggetto Produttore (Ente) sottoscrive il contratto di servizio e suoi allegati:

- Contratto di Conservazione a Norma
  Il presente documento disciplina le condizioni di fornitura generali della soluzione di conservazione DocFly, in linea con quanto definito dalle Regole Tecniche in materia di conservazione del DPCM 3 dicembre 2013 e ss.mm.ii.

- Atto di Delega
  Ai fini dell'erogazione del servizio di conservazione digitale a norma, Aruba PEC svolge le attività ad essa delegate dal Responsabile della Conservazione dell'Ente comunale, come riportate nel documento di Nomina del responsabile del servizio di conservazione digitale dei documenti informatici, allegato al Contratto di servizio. Nel contempo, l'Ente comunale coinvolto nel procedimento nomina Aruba PEC quale Responsabile esterno del trattamento dei dati come previsto dal Codice in materia di protezione dei dati personali (D.Lgs. 196/2003 e s.m.i.) e indicato all'art 6 co. 8 delle nuove regole tecniche (DPCM del 3 Dic 2013).Pertanto, i ruoli di Responsabile della conservazione e di Titolare del trattamento sono ricoperti dall'Ente comunale, mentre i ruoli di Responsabile del servizio di conservazione e di Responsabile esterno del trattamento dei dati saranno ricoperti da Aruba PEC.

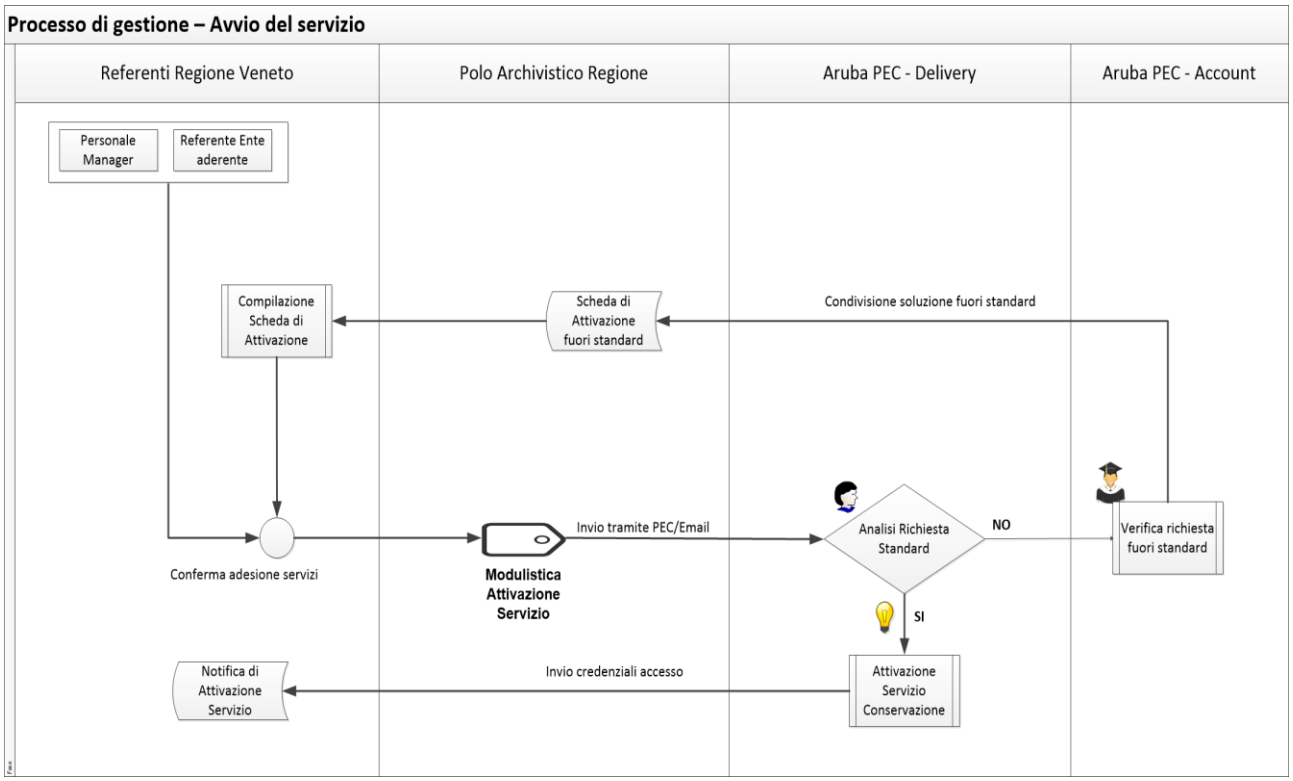
- Elenco Persone

Ai fini dell'affidamento del servizio di conservazione digitale di documenti informatici, il soggetto Produttore (Ente comunale) comunica l'identità delle persone fisiche titolate ad operare in nome e per conto del soggetto Produttore medesimo, precisandone funzione e ruolo.

- Scheda di Conservazione
  La scheda di conservazione è un documento costituente parte integrante e sostanziale del contratto per l'affidamento del servizio di conservazione digitale di documenti informatici.
  Il soggetto Produttore (Ente) condivide con il conservatore Aruba PEC le caratteristiche, le modalità ed i termini di versamento dei documenti informatici da sottoporre a conservazione digitale, approvando espressamente quanto indicato nelle scheda conservazione.
  Fra i diversi aspetti da concordare attraverso la scheda di conservazione, i principali sono:

  - le tipologie di documenti da conservare;
  - i metadati minimi riferiti ad ogni classe/tipo documento
  - eventuali (metadati) extrainfo riferiti ad ogni classe/tipo documento sui quali effettuare specifici controlli;
  - formati da adottare per ogni classe/tipo documento;
  - eventuali software in grado di interpretare e rendere leggibili per l'uomo i formati prescelti in caso di formati fuori standard;
  - modalità e termini di comunicazione tra conservatore e produttore.

In caso di aggiudicazione definitiva, Aruba PEC ritiene necessario sottoscrivere con il Polo Archivistico Regionale un separato accordo che regoli le peculiari condizioni operative di fornitura del Servizio di conservazione digitale a norma dei documenti informatici. Sulla base di tale accordo, il contratto di servizio e suoi allegati, dovranno essere trasmessi agli Enti finali a cura del Polo Archivistico Regionale e da questi (Enti finali) ri-consegnati e/o trasmessi ad Aruba PEC ai fini dell'attivazione del Servizio. Tale approccio mira a semplificare e uniformare le procedure di attivazione nonché a diminuire i tempi di messa in funzione del servizio.



Di seguito sono descritti i principali step che caratterizzano il processo di gestione del servizio di conservazione digitale a norma:

1. la procedura di avvio del servizio prende inizio tramite richiesta formale di adesione da parte dell'Ente, che contatta il Polo Archivistico Regionale tramite un suo referente comunale o regionale. L'adesione al servizio prevede la sottoscrizione da parte dell'Ente della modulistica di attivazione.
2. il Polo Archivistico trasmette via PEC o Email la documentazione contrattuale sottoscritta dall'Ente direttamente al dipartimento di delivery di Aruba PEC
3. la richiesta di attivazione viene analizzata dal dipartimento di delivery di Aruba PEC, il quale provvede all'attivazione del servizio in caso di richiesta standard, ovvero, in linea con le convenzioni e accordi stabiliti tra Polo e conservatore Aruba PEC.
4. in caso di richiesta fuori standard, viene ingaggiato l'account il quale interagisce con il dipartimento di delivery per la realizzazione di una scheda di attivazione fuori standard. Tale scheda viene condivisa con il Polo Archivistico Regionale e in caso di esito positivo viene prodotta la documentazione di attivazione del servizio. La documentazione definitiva viene inviata sia all'Ente che al Polo e contribuisce a formare un nuova soluzione standard.
5. La conclusione del processo di gestione prevede la notifica di avvenuta attivazione del servizio sia all'Ente che al Polo Archivistico Regionale e l'invio delle credenziali di accesso al referente indicato dall'Ente all'interno dei moduli di attivazione

Presa in carico dei documenti da precedente Fornitore

Una richiesta di attivazione inoltrata dall'Ente può prevedere la presa in carico di documenti depositati presso l'attuale Fornitore del servizio di conservazione. In tal caso, la richiesta viene gestita come standard ma può richiedere un approfondimento da parte del dipartimento di delivery circa le modalità e strumenti da adottare ai fini del trasferimento dei documenti.

Grazie all'esperienza maturata in tale ambito, Aruba PEC garantisce l'acquisizione dei documenti digitali pregressi, già conservati a norma su fornitori esterni, attraverso procedure informatiche idonee per l'importazione massiva dei documenti, le quali si sviluppano nelle seguenti fasi:

- acquisizione del pregresso;
- trasferimento in conservazione;
- indicizzazione dei documenti;
- associazione dei relativi metadati.

Riguardo la fase di acquisizione del pregresso, Aruba PEC è in grado di garantire la massima flessibilità, assicurando la presa in carico dei documenti attraverso le modalità e gli strumenti che meglio si adattano alle esigenze dell'Ente richiedente: web services, FTP su canali sicuri, caricamento dei documenti tramite DVD consegnati dal precedente fornitore, etc…

4.4.1 DOCUMENTAZIONE SISTEMA DI CONSERVAZIONE A NORMA DOCFLY

Aruba PEC si impegna a fornire tutta la documentazione e manualistica necessaria ai fini del corretto utilizzo della piattaforma DocFly.

In particolare verrà fornita la documentazione seguente:

DOCUMENTAZIONE CONSERVAZIONE A NORMA
Manuale operativo del servizio DocFly (Utente "Master")
Manuale operativo del servizio DocFly (Utente "Operativo")
Specifiche Tecniche (componenti web services, interfaccia PEC, FTP)

4.5 CONCLUSIONE DEL SERVIZIO

Il servizio proposto da Aruba PEC, essendo basato sul modello OAIS, garantire la completa compatibilità e riversabilità del dato verso altri sistemi a norma al termine del contratto, in conformità con quanto previsto dallo allo standard UNI 11386:2010 "Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali" in modo da garantire all'Ente la piena libertà di rivolgersi ad altri fornitori senza alcun rischio di interpretazione delle informazioni conservate dall'operatore.
Le operazioni di chiusura del servizio avranno inizio con congruo anticipo prima della scadenza del contratto con la pianificazione di tutte le attività necessarie per transitare tutti i documenti al nuovo fornitore del servizio di conservazione.
Aruba PEC, a conclusione del contratto, supporterà l'Ente e/o altro fornitore da questo indicato, relativamente alle attività necessarie per il porting verso una eventuale diversa piattaforma, inclusa la migrazione dei dati conservati.
A sostegno della migrazione richiesta, entro due mesi dalla scadenza contrattuale, Aruba PEC si impegna ad eseguire le seguenti attività:

- supporto alle attività di migrazione
- consegna dei dati oggetto di conservazione su supporto ottico fino alla data di porting

Durante tale fase di chiusura l'utenza non subirà alcun peggioramento del servizio erogato, e Aruba PEC garantisce che sarà messo a disposizione tutto il personale necessario per supportare questa fase, senza distogliere le figure normalmente impiegate nell'erogazione del servizio dalle proprie attività.

4.6 FUNZIONALITA' AGGIUNTIVE

4.6.1 GESTIONE DEGLI ALERT E NOTIFICHE

Ognuno degli Enti coinvolti nel processo verrà configurato nel sistema DocFly associando un Archivio logico a cui vengono assegnate delle risorse in termini di spazio allocato, sulla base delle esigenze espresse dall'Ente direttamente o tramite il Polo Archivistico Regionale, una volta istituito.
L'assegnazione della quota (spazio disco) e' virtuale; pertanto, in caso di sforamento della stessa, il sistema garantisce la continuità dei versamenti dei documenti informatici.
La soluzione DocFly prevede la possibilità di configurare degli alert che, all'avvicinarsi di determinate soglie prestabilite, notificano via mail ai referenti indicati dall'Ente/Polo Archivistico Regionale la necessità di ridefinire le risorse.
L'impostazione dei parametri di soglia può essere effettuata direttamente dall'Utente 'Master' tramite interfaccia web.

L'attuale configurazione standard del sistema di notifiche, prevede:

- invio mail di alert al Responsabile della Conservazione dell'Ente (opzionalmente possono essere aggiunti il Resp. Amministrativo e il Ref tecnico se presente) al raggiungimento della **soglia del 70%**

- invio mail di alert al Responsabile della Conservazione dell'Ente (opzionalmente possono essere aggiunti il Resp. Amministrativo e il Ref tecnico se presente) al raggiungimento della **soglia del 90%.** Raggiunta tale soglia, il sistema effettua un upgrade di spazio pari ad una quota di incremento precedentemente concordata con l'Ente e il Polo Archivistico Regionale.

4.6.2 GESTIONE DI DOCUMENTI DI GRANDI DIMENSIONI

Come descritto nei paragrafi precedenti, il sistema consente versamenti da varie tipologie di canali. Per versamenti 'occasionali' o comunque di piccole entità può essere sufficiente l'utilizzo del pannello web. In tale ottica, l'utente può utilizzare un comune browser, inserire i metadati che qualificano i documenti da versare e infine effettuare l'upload dei documenti stessi.

Riguardo il versamento di file contenenti documenti di grandi dimensioni, il sistema espone altri canali da cui è possibile effettuare versamenti anche in maniera automatizzata. E' questo il caso di caricamenti massivi o di documenti particolarmente onerosi in termine di peso. Principalmente possono essere usati, insieme o in alternativa, i canali web service e FTP (per maggiori dettagli si rimanda al par. 4.1.4).

Il canale FTP consente il caricamento di file di grandi dimensioni in maniera sicura e controllata, fornendo, al tempo stesso, un riscontro immediato circa il corretto *upload* dei documenti, anche se di grandi dimensioni, e comunque il *resume* dell'upload in caso di improvvisa disconnessione.

Alla luce di quanto riportato, sia il canale FTP che web service, non presentano vincoli in termini di dimensione massima e tantomeno sul numero di file caricabili.

5 SERVIZIO DI HELP DESK

5.1 STRUTTURA DI HELP DESK PROPOSTA

Il **Servizio di Help Desk** messo a disposizione rappresenterà il punto di contatto per fornire assistenza agli utenti (personale autorizzato, utenti del servizio e specifici referenti) della Regione del Veneto e degli Enti aderenti ai servizi offerti in gara:

- **firma digitale**
- **marcatura temporale**
- **certificato SSL**
- **posta elettronica certificata**
- **conservazione sostitutiva a norma**

Tale servizio costituisce un'interfaccia unica (**SPOC – Single Point Of Contact**), competente e precisamente identificata per affrontare e risolvere tutte le richieste di assistenza rivolte alla soluzione sia di problemi tecnologici e sia di supporto all'utilizzo dei servizi sottoscritti.
Ciascun utente della Regione del Veneto verrà adeguatamente informato – in modo chiaro e completo – sulle modalità di utilizzo del servizio di assistenza: indirizzi, numeri di telefono e fax, orari, sito web, ecc. A seguito dell'attivazione dei servizi verrà infatti divulgato - a tutti gli utenti della Regione del Veneto – un apposito manuale di assistenza.
Le attività di risoluzione delle richieste sono eseguite dall'**Operatore del Servizio di Help Desk** insieme all'utente richiedente della Regione del Veneto. L'operatore fornisce supporto all'utente su questioni tecnologiche e modalità di utilizzo dei servizi. Nel caso in cui il problema rilevato non possa essere risolto dagli **operatori** presenti nel canale di assistenza – l'operatore verrà coadiuvato da **tecnici esperti**.
Tutte le richieste vengono gestite attraverso una piattaforma software, in grado di monitorare ciascuna richiesta tramite un codice univoco di identificazione.

☞ L'assistenza del **Servizio di Help Desk** viene fornita in conformità allo **standard ITIL v3** ed è tuttora dimensionato a soddisfare costante supporto ad oltre migliaia di persone.

5.1.1 METODOLOGIA DEL SERVIZIO HELP DESK

Il **Servizio di Help Desk** si attiva tramite la ricezione della richiesta di **assistenza** da parte degli utenti della Regione del Veneto e degli Enti aderenti.
Il servizio sarà disponibile – come da capitolato di gara - nella seguente fascia oraria:

- **dal Lunedì al Venerdì - dalle ore 8,00 alle ore 18,00**
- **il Sabato - dalle ore 8,00 alle ore 14,00**

per 365 giorni all'anno per tutta la durata del contratto (4 anni) - escluse le festività del calendario italiano ed eventuali fermi servizio programmati.

Canali di Contatto
I **canali di contatto** messi a disposizione tra gli utenti della Regione del Veneto e gli **Operatori del Servizio di Help Desk** saranno i seguenti:

- ✓ **Numero Verde gratuito** in lingua italiana - accessibile sia da rete fissa che da rete mobile - attivo nella seguente fascia oraria:
  - da Lunedì a Venerdì - dalle ore 8:00 alle ore 18,00
  - Sabato (festivi esclusi) – dalle ore 8:00 alle ore 14:00

☞ Tale **canale di contatto** è dotato di un **Centralino IVR**, in grado di instradare automaticamente la chiamata al centro di competenza che risiede all'interno dello stesso

Team operatori Help Desk di 1° Livello. La strategia di instradamento prevede l'indirizzamento in base alla **Tipologia Servizio** (Firma Remota, Marcatura Temporale, PEC, Conservazione sostitutiva). In tal modo per l'utente è possibile entrare immediatamente in contatto con gli operatori specializzati sulla tematica di interesse – e in grado di distinguere le richieste in base alla **Tipologia Richiesta** (Assistenza Tecnologica o Funzionalità Servizio).

☞ In caso di necessità e/o interventi pianificati (es. per fermi servizio) – come elemento migliorativo - il **routing su IVR** può essere configurato al fine di comunicare in prima battuta dei messaggi informativi automatici di preavviso in merito ad **aggiornamenti e/o eventi pianificati sui sistemi** (che potrebbero avere impatti sulla normale operatività). In tal modo – a scopo preventivo – può essere garantita una sensibile riduzione della ricaduta delle chiamate dirette sugli operatori ed una conseguente garanzia del tempo di attesa anche in momenti di picco sul volume delle chiamate.

A seguito di richieste pervenute tramite canale telefonico – è prassi dell'operatore **Help Desk** procedere all'apertura del **Ticket** sulla piattaforma – a conferma della presa in carico. L'operatore **Help Desk** effettua l'apertura del **Ticket** in base alla **Tipologia Servizio** (Firma Remota, Marcatura Temporale, PEC, Conservazione sostitutiva) ed in funzione dell'ambito specifico della **Tipologia Richiesta** (Assistenza Tecnologica o Funzionalità Servizio). Ciò rappresenta un elemento migliorativo, in quanto consente la completa tracciabilità delle richieste di assistenza e la conseguente attendibilità della valutazione delle performance e livelli di servizio.

- ✓ **Numero di Fax dedicato** - adibito a fornire supporto a seguito della ricezione di una nuova richiesta. Successivamente alla ricezione via fax – la richiesta genera automaticamente l'apertura di un **Ticket** nel **Portale Web** – che consente la presa in carico da parte dell'operatore **Help Desk**.

- ✓ **Casella di Posta Elettronica dedicata** - adibita a fornire supporto agli utenti della Regione del Veneto tramite:
  - ricezione di una nuova richiesta - con successiva apertura automatica del **Ticket** sulla piattaforma **Portale Web**
  - ricezione di una risposta ad una richiesta aperta - con successiva sincronizzazione ed accodamento automatico del **Ticket** anche sulla piattaforma dedicata.

- ✓ **Portale Web** - utilizzato dagli utenti della Regione del Veneto per ricevere assistenza tramite:
  - apertura nuovo **Ticket** – identificato da un codice univoco - all'interno della **piattaforma di Trouble Ticketing dedicata** (in caso di nuova richiesta) e/o aggiornamento di Ticket esistente (in caso di approfondimenti sulla richiesta attiva)
  - visione delle **FAQ** utili per operare in **self-assistance.**
  - ☞ richiesta di **contatto outbound** da parte di un operatore tramite il servizio **Call me back** (predisposto all'interno delle varie sezioni delle **FAQ**) – con un tempo di richiamata entro 10 minuti dalla richiesta di contatto.

☞ Le richieste di assistenza - pervenute entro la fascia oraria lavorativa indicata – vengono prese in carico da un operatore del **Servizio di Help Desk** con i livelli di servizio previsti dal capitolato di gara. Al di fuori di tale fascia oraria – come ulteriore elemento migliorativo – **Aruba PEC** continua comunque a garantire:

- la ricezione delle richieste tramite i canali di **Posta Elettronica** e **Portale Web e Fax**
- la ricezione di segnalazioni per malfunzionamenti e/o problemi di sicurezza attraverso i sistemi di monitoraggio interni

- la comunicazione di interventi e/o fermi servizio pianificati

La continuità del servizio è infatti garantita dai centri **NOC** (**Network Operations Center**) presenti all'interno di ciascun **Data Center** - attivi 24hx7gg - che monitorano costantemente i servizi erogati ed interagiscono proattivamente sia con il servizio di **Help Desk** e sia con l'organizzazione generale al fine di poter garantire la risoluzione di eventuali malfunzionamenti e/o problemi di sicurezza.

Metodologia di Assistenza

La metodologia adottata da **Aruba PEC** per l'erogazione del **Servizio di Help Desk** è modellata sullo **standard ITIL** che costituisce una **best practice** di forte valore aggiunto per garantire l'operatività in contesti delicati in cui è fondamentale garantire qualità ed efficacia.
Il **Servizio di Help Desk** dedicato rappresenta un sistema **User Centric** (in cui l'utente richiedente e al centro) e **Ticket Driven** (basato su un meccanismo di richieste), in grado di rispondere a tutte le esigenze di gestione e verifica dei **Livelli di Servizio** (**SLA**), di monitoraggio e di controllo del tracciamento dei singoli **Trouble Ticket**.

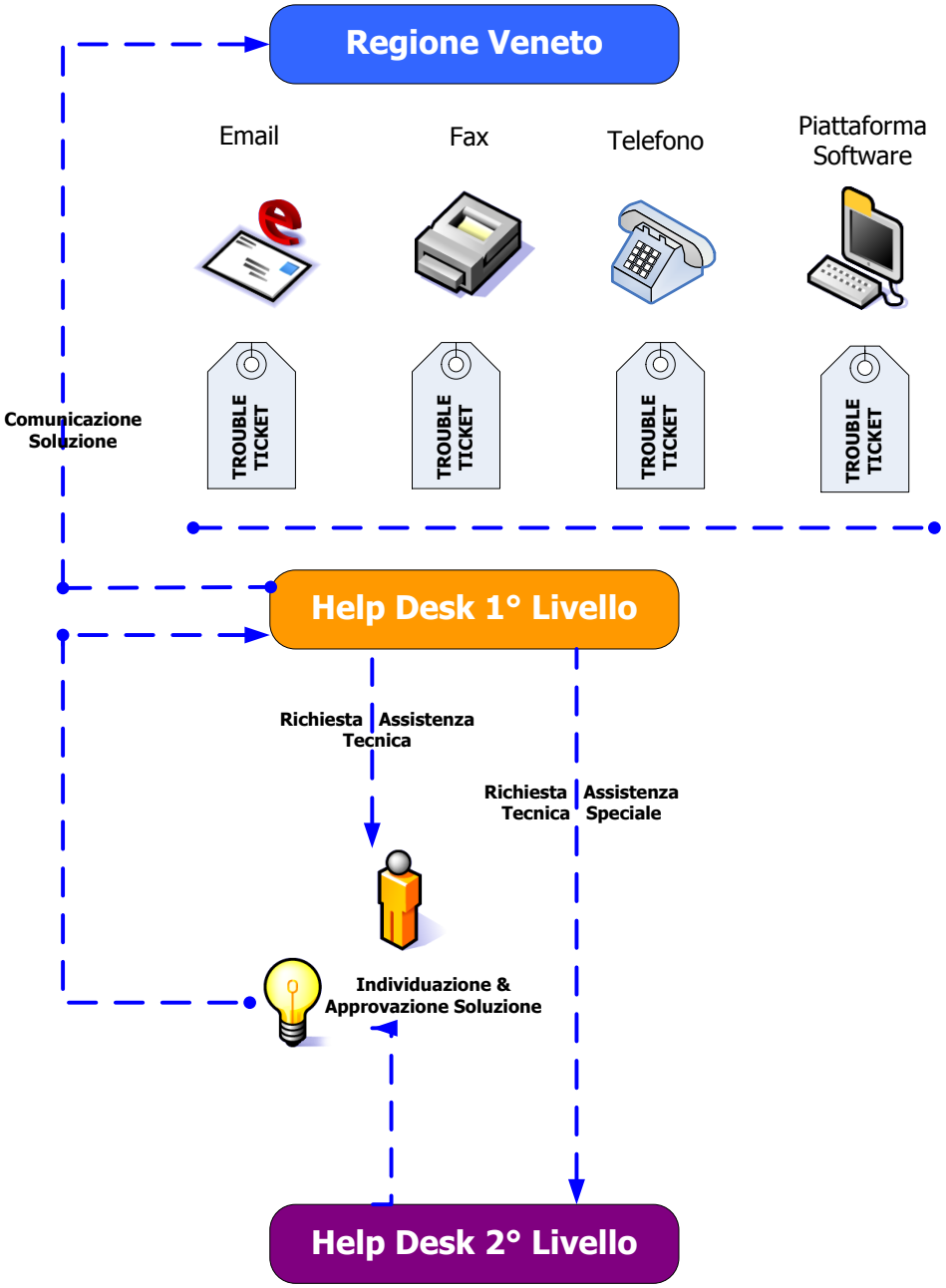
Il **Service Desk** sarà quindi strutturato in 2 Livelli:

- Help Desk di 1° Livello;
- Help desk di 2° Livello.

Il **gruppo Aruba** avrà il compito di designare un **Responsabile del Servizio Help Desk** dedicato alle fasi di attivazione del servizio, il cui riferimento potrà comunque essere utilizzato anche nelle fasi di erogazione del servizio. Tale figura di responsabile si occuperà inoltre di organizzare, coordinare e controllare l'attività svolta dal personale di **1° Livello** e **2° Livello** (che si occuperà dell'assistenza agli utenti della Regione del Veneto).

Il **Servizio di Help Desk** manterrà – come elemento migliorativo - per tutta la durata contrattuale (4 anni) la banca dati relativa alla registrazione di tutte le segnalazioni ricevute (**Trouble Ticket**). Il **Sistema di Trouble Ticketing** messo a disposizione consentirà infatti di fare estrazioni parziali e/o operazioni di natura statistica sulle segnalazioni, sugli interventi effettuati, il loro stato e le tempistiche di gestione.

Lo schema sotto riportato rappresenta il flusso operativo attraverso il quale verranno gestite e risolte le problematiche segnalate dagli utenti della Regione del Veneto.



Il **Servizio di Help Desk** rappresenta il primo punto di contatto per gli utenti della Regione del Veneto e degli Enti Aderenti in merito a segnalazioni di problematiche tecnologiche e/o inerenti all'utilizzo dei servizi in fornitura.
Gli **Operatori del Help Desk di 1° Livello** sono gli incaricati di tutte le richieste di assistenza (tramite Telefono, Fax, E-mail o Portale Web) provenienti dagli utenti.
Il personale dell'**Help Desk di 1° Livello** svolgerà le seguenti funzioni:

- risposta a richieste di supporto per problemi tecnologici ed assistenza per l'utilizzo servizi;
- gestione delle chiamate ed apertura dei **Trouble Ticket** – a conferma della presa in carico;
- prima analisi delle problematiche e supporto agli utenti;
- risoluzione delle problematiche più semplici e comunicazione agli utenti;
- chiusura dei **Trouble Ticket** e comunicazione della strategia risolutiva agli utenti
- controllo dello stato di avanzamento **Trouble Ticket**;
- eventuale inoltro delle segnalazioni agli **Operatori del Help Desk di 2° Livello** (qualora non possa intervenire direttamente).

Il **Servizio di Help Desk di 1° Livello** sarà raggiungibile tramite i canali di contatto previsti nella fornitura di gara. Tutte le richieste di contatto pervenute al **1° Livello**, attraverso uno qualunque dei canali messi a disposizione, genereranno l'apertura di una richiesta - da parte dell'**operatore di 1° Livello** - all'interno del sistema di **Trouble Ticketing**.
L'apertura del **Trouble Ticket** innesca l'invio automatico di una notifica all'Indirizzo Email comunicato dall'utente, contenente l'identificativo della segnalazione aperta. La richiesta di assistenza sarà immediatamente disponibile agli utenti che - tramite il **Portale Web** oppure direttamente dalla Casella di Posta elettronica - potranno consultare in qualsiasi momento.
Successivamente all'apertura automatica della segnalazione, l'**Operatore del Servizio di Help Desk** potrà contraddistinguere la natura del **Trouble Ticket** in base all'assegnazione della **Tipologia Servizio** (Firma Remota, Marcatura Temporale, PEC, Conservazione sostitutiva) e della **Tipologia Richiesta** (Assistenza Tecnologica o Funzionalità Servizio).

Il **Servizio di Help Desk di 2° Livello** costituisce il supporto specializzato per gli operatori del **Help Desk di 1° Livello**, in quanto possiede le competenze utili a risolvere le problematiche e richieste più complesse.
Il personale specializzato del **Help Desk di 2° Livello** avrà il compito di:

- prendere in carico le segnalazioni inoltrate dagli **Operatori del 1° Livello** tramite l'assegnazione di appositi **Trouble Ticket**;
- fornire il supporto tecnico agli **Operatori del 1° Livello** per consentire il corretto utilizzo dei servizi tecnologici;
- gestire le anomalie evidenziate dagli strumenti di monitoraggio predisposti, effettuando gli interventi risolutivi e/o preventivi necessari per il funzionamento dei servizi forniti nel rispetto degli **SLA** richiesti;
- monitorare le prestazioni dei servizi forniti ed effettuare adeguata **reportistica** (utile a garantire l'adeguato stato di avanzamento delle attività di manutenzione).

Processo di Gestione Inbound

Ciascuna **richiesta di assistenza** può essere effettuata dalla Regione del Veneto e dagli Enti Aderenti – utilizzando i canali di contatto offerti in gara - attraverso gli utenti autorizzati: personale della Regione del Veneto, utenti del servizio della Regione del Veneto e referenti degli Enti aderenti.

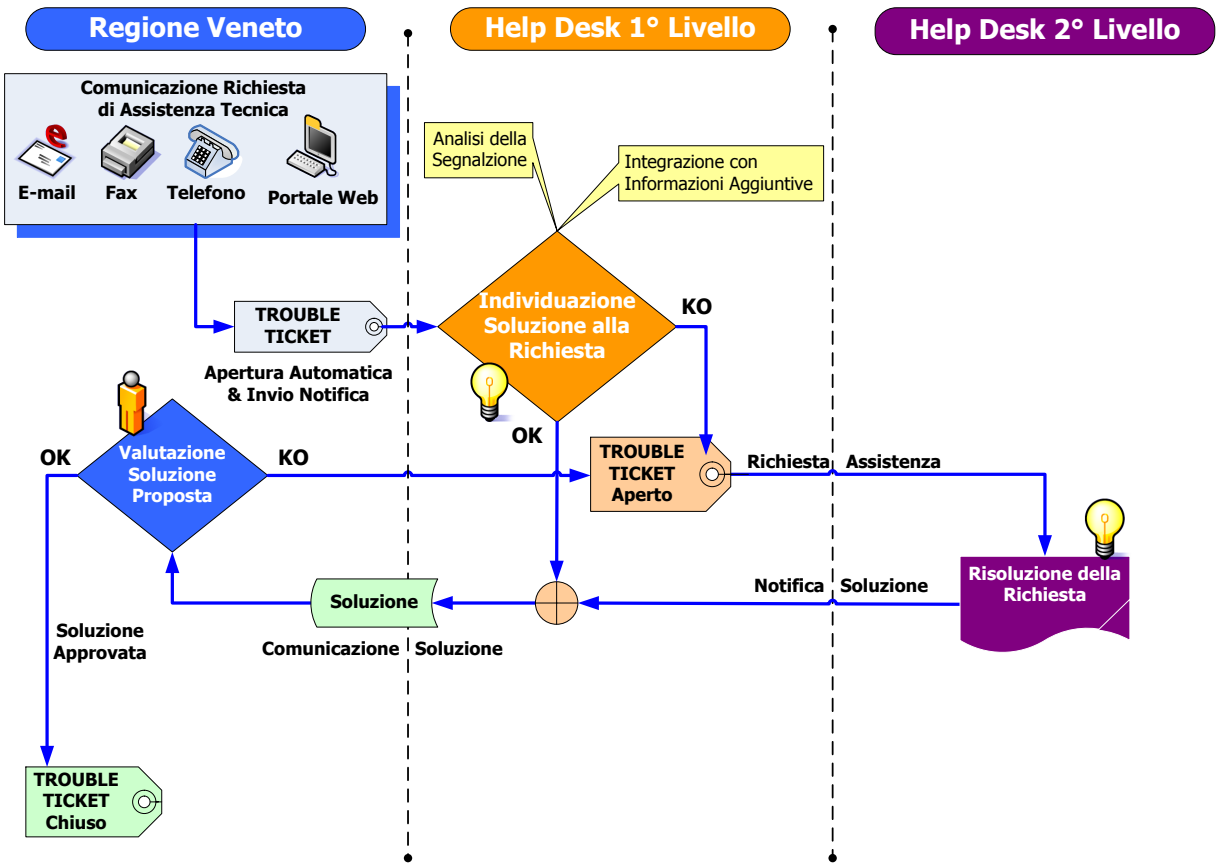
A seguito di ciascuna richiesta - il **processo Inbound** si attiva da parte del **Help Desk** con l'apertura (o conferma) via **Ticket** per la presa in carico della problematica.

A prescindere dai canali utilizzati, ogni richiesta di assistenza implica la creazione di un **Trouble Ticket**. L'apertura del **Ticket** innesca l'invio automatico di una notifica all'Indirizzo Email comunicato dal referente della Regione del Veneto, contenente l'identificativo della segnalazione. La richiesta di assistenza sarà immediatamente disponibile ai referenti della Regione del Veneto che - tramite il **Portale Web** - potranno consultare in qualsiasi momento. Il **Ticket** sarà classificato in funzione della tipologia del problema e sarà corredato da tutte le informazioni previste da capitolato - e necessarie a tracciare il ciclo di vita della richiesta.
Di seguito viene descritto il ciclo di vita di un **Trouble Ticket**:

a) ricezione delle richieste provenienti dagli utenti (tramite **E-mail**, **Telefono**, **Fax**, **Portale Web**), con la conseguente apertura di un **Trouble Ticket** e l'invio della notifica all'utente;
b) presa in carico della segnalazione (**Trouble Ticket**) da parte dell'**Operatore di 1° Livello**, con successiva analisi della problematica ed eventuale integrazione del **Trouble Ticket** con informazioni aggiuntive;
c) individuazione della soluzione e comunicazione della strategia risolutiva all'utente che ha inviato la segnalazione;
d) chiusura del **Trouble Ticket** - da parte dell'**operatore tecnico di 1° Livello** – contenente la soluzione individuata, con successivo invio della notifica all'utente;
e) richiesta dell'intervento di un **Operatore di 2° Livello** ed assegnazione del **Trouble Ticket**, qualora non fosse possibile risolvere il problema tramite l'**Help Desk di 1° Livello**;

f) eventuale presa in carico del **Trouble Ticket** da parte dell' **Operatore di 2° Livello**, con successiva risoluzione del problema
g) chiusura del **Trouble Ticket** da parte dell'**operatore tecnico di 2° Livello** ed invio della notifica all'utente

Il **processo di gestione delle richieste** prevede diversi livelli logici in linea con l'organizzazione:



- ✓ **Help Desk 1° Livello** - gli operatori forniscono assistenza - nei tempi previsti da capitolato - effettuando l'analisi della soluzione ed eventuale integrazione del **Ticket** con informazioni aggiuntive in base agli aspetti:
  - **Tecnologici e/o Funzionali**. La formazione trasversale su tutti i servizi oggetto della fornitura e gli strumenti di supporto alla conoscenza (pannelli di **FAQ** e **Knowledge Base**), in generale consentono agli operatori di poter garantire la risoluzione del problema. Qualora i contenuti tecnici e/o la formazione trasversale impartita agli operatori non consenta di raggiungere una soluzione, l'operatore incaricato indirizzerà la richiesta al **2° Livello**. Se non risultasse comunque possibile raggiungere una soluzione, viene effettuata ulteriore escalation verso gli esperti dei **Centri di Supporto** e l'operatore del **2° Livello** incaricato ricopre temporaneamente il ruolo di **Case Manager**.
- ✓ **Help Desk 2° Livello** - gli operatori possiedono le competenze per risolvere le problematiche più complesse e forniscono assistenza specializzata sugli aspetti **tecnologici e funzionali**. A seguito della risoluzione del problema gli operatori provvedendo alla **chiusura del Ticket**, alla comunicazione della risposta all'utente e (qualora la procedura possa essere tradotta in routine operativa) alimentare gli strumenti della conoscenza (**FAQ**, **Knowledge Base**). Qualora non sia invece possibile raggiungere una soluzione, viene effettuata opportuna escalation verso gli esperti dei **Centri di Supporto** e l'operatore incaricato ricopre temporaneamente il ruolo di **Case Manager**.

- ✓ **Centri di Supporto** - gli operatori vantano di competenze su tematiche specifiche - calate anche sul singolo Ente della Regione del Veneto - pertanto provvedono a fornire la soluzione della problematica e fornire comunicazione alla figura del **Case Manager**, che a seguito ha il compito di **chiudere il Ticket** (rimasto in precedenza in stato "pending") completo della notifica all'utente.

Processo di Gestione Outbound

Il **processo Inbound** dell'**Help Desk** si attiva con l'apertura di un **Ticket** che identifica la presa in carico di una richiesta. A seguito della richiesta di assistenza tramite la **piattaforma di Trouble Ticketing** – la richiesta viene classificata in funzione della tipologia e del servizio di appartenenza. Qualora la problematica non sia risolvibile dai primi **2 livelli dell'Help Desk**, la richiesta viene instradata al **3° livello** (costituito da operatori specializzati per tematica). Durante questa fase il **Ticket** rimane in sospeso ed il **Case Manager** di riferimento avrà il compito di monitorare l'evasione della richiesta fino alla notifica all'utente.

☞ Nell'organizzazione del **Help Desk** è possibile l'insorgere della richiesta di **contatto Outbound**. L'intervento in assistenza scaturisce da un primo contatto telefonico da parte dell'operatore verso l'utente. L'utente– durante la navigazione delle **FAQ** per la ricerca di una soluzione in **self-assistance** – potrebbe avere necessità di approfondimenti per la risoluzione della questione di interesse. A tale proposito per l'utente è disponibile la funzione di **Call me Back** – attivabile tramite popup direttamente da ciascuna pagina web delle **FAQ** di interesse – avente la finalità di richiedere un **contatto Outbound** da parte dell'operatore **Help Desk**. La finalizzazione della richiesta di contatto tramite **Call me Back** avviene appena l'utente ha inserito e confermato i parametri minimi necessari a stabilire un **contatto outbound**: nome utente, canale di contatto desiderato e recapito telefonico.
A seguito del contatto telefonico – qualora la consulenza telefonica non venga ritenuta risolutiva dall'utente - è prassi che le attività di assistenza vengano tracciate tramite l'apertura del **Ticket** e successivo aggiornamento con lo stato di avanzamento.

Gestione delle Code tramite Canale Telefonico

Il **canale telefonico con Numero Verde** prevede l'implementazione di un **sistema IVR (Interactive Voice Response)** in grado di instradare in modo opportuno le chiamate in virtù della tipologia di richiesta di assistenza e del servizio di interesse.
In particolare l'IVR richiederà all'utente l'immissione di 3 informazioni chiave:

- **Tipologia Servizio**
- **Tipologia Richiesta (di tipo tecnologica o funzionale)**

tramite digitazione su tastiera telefonica. Tali informazioni permetteranno:

- di instradare la richiesta in modo opportuno ai **due cluster di operatori di 1° livello** - di tipo **Assistenza Tecnologica** o di tipo **Funzionalità Servizio**;
- di instradare la richiesta - nel caso in cui non sia soddisfatta al 1° livello - all'**operatore di 2°** livello specializzato sui servizi di competenza.

La **gestione delle code** sarà ottimizzata sulla base di alcuni criteri - di seguito indicati a scopo esemplificativo:

- ✓ instradamento **auto-adattativo** delle richieste. Le richieste di assistenza più frequenti verranno indicizzate e perciò potranno essere instradate già dall'**operatore del 1° Livello** all'**operatore del 2° Livello** specializzato sulla specifica problematica richiesta.
- ✓ ☞ proposta di **"messaggi di intro"** da parte dell'**IVR** durante la fase di risposta all'utente. Tali messaggi comunicano le **news o le contingenze** relative ai servizi erogati (es. indisponibilità dei sistemi dovute a eventi pianificati sui sistemi, nuovi servizi disponibili, ecc.). La loro finalità è quella di fornire informazioni esaustive su tali eventi,

con la finalità di esaurire il contatto a livello di **IVR** ed evitare un sovraccarico di chiamate sugli operatori di **Help Desk**.

Il servizio di help-desk che verrà fornito da Aruba PEC è in gradi di garantire agli utenti la risposta telefonica di un operatore entro 1 (uno) minuto di attesa.

Gestione di Fermi Servizio programmati

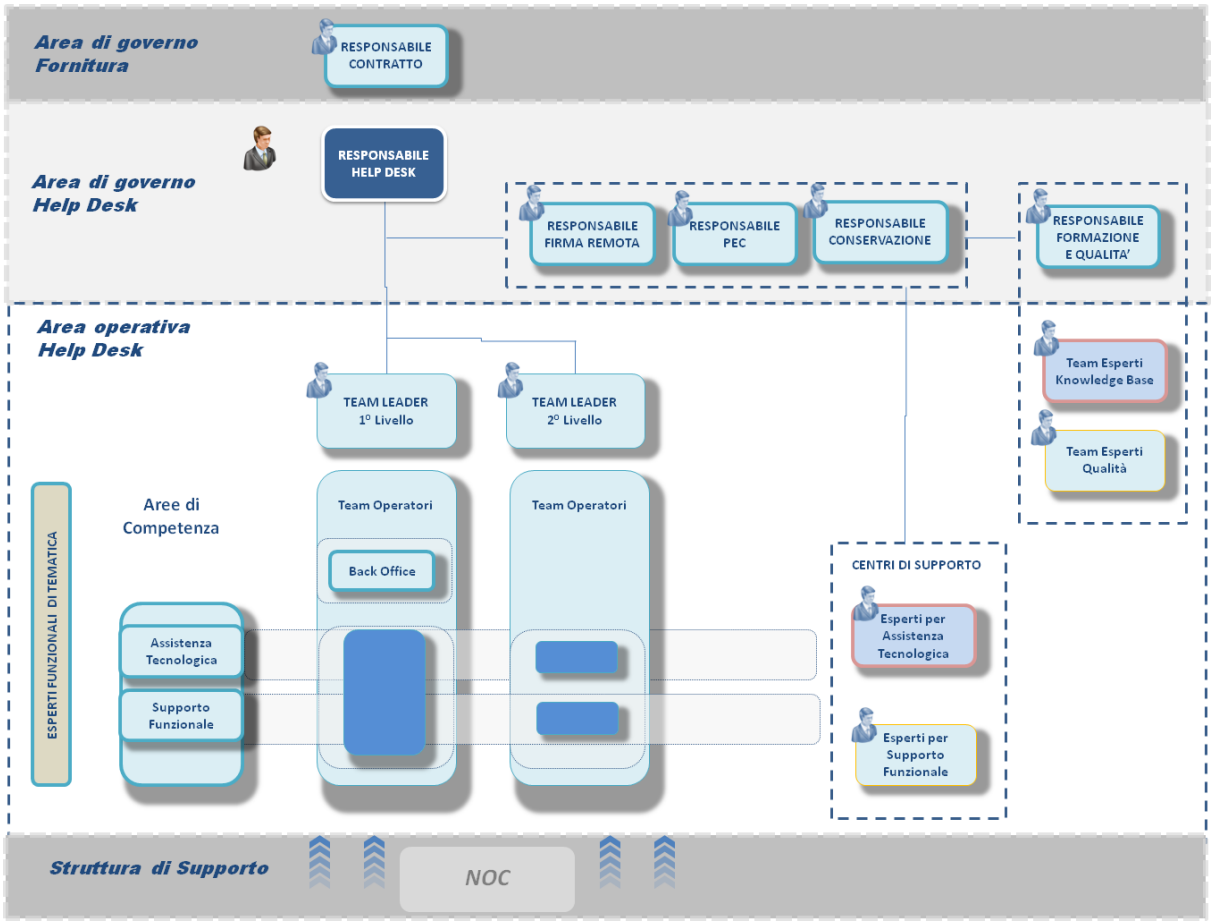
Eventuali **fermi servizio programmati** – onde evitare che influiscano nel livello e qualità del servizio offerto – verranno comunicati in forma scritta (tramite Email) all'Amministrazione Regionale e all'utenza - con un preavviso di almeno 5 giorni. Tali eventi verranno effettuati esclusivamente nella fascia oraria giornaliera compresa tra le ore 00.00 e le ore 07.00.
Ad elemento migliorativo tali comunicazioni verranno inserite come **messaggio di intro** sul **canale IVR** del **Numero Verde**, al fine di replicare informazioni esaustive e poter disporre di un maggiore numero di operatori per richieste di assistenza più specifiche e/o di altro genere.

5.1.2 ORGANIZZAZIONE DEL SERVIZIO DI HELP DESK

Il **modello organizzativo del Servizio di Help Desk** è stato progettato sulla base di criteri atti a garantire:

- **la formazione** degli operatori, svolta periodicamente tramite sessioni dedicate e attraverso sistemi condivisi - per consentire specializzazioni molteplici su tematiche oggetto delle richieste di assistenza
- **la flessibilità** delle risorse garantita dalla struttura a matrice dell'organizzazione che consente - in base al livello di complessità del supporto richiesto (1° Livello o 2° Livello) - di strutturarsi in più linee di erogazione
- **la sinergia** tra gli operatori del 1° livello e 2° livello di assistenza - garantita dalla semplicità del processo messo in atto per la gestione dei ticket d'intervento
- **la chiarezza nei ruoli di responsabilità** - le responsabilità e i compiti sono chiaramente definiti e rapportati alle fasi che scandiscono la gestione della risoluzione di una problematica
- **presenza di organismi di verifica e controllo** - la struttura della **Formazione & Qualità** garantisce attività di verifica sulla qualità dei servizi erogati.

All'interno del **modello organizzativo del Servizio di Help Desk** si distinguono due aree specifiche: l'**Area di governo** e l'**Area operativa**.



Ciascun utente della Regione del Veneto può usufruire del **Servizio di Help Desk** come un'interfaccia unica, competente e precisamente identificata a gestire le richieste di assistenza su tutti gli aspetti tecnologici e funzionali sui servizi oggetto della fornitura. L'organizzazione del **Help Desk** prevede la sinergia tra figure professionali appartenenti a **due distinte aree funzionali**.

All'interno dell'**Area di Governo del Help Desk** sono presenti le seguenti figure:

- ✓ **Responsabile Help Desk** – è supervisore dell'intero **Servizio di Help Desk**. Coordina le attività svolte da ciascun team di operatori tramite l'interazione con le figure di **Team Leader** - a garanzia del massimo livello di qualità di assistenza sui servizi di fornitura. Ha inoltre il compito di coinvolgere la figura del **Responsabile Formazione e Qualità** qualora sia necessario un miglioramento qualitativo sugli aspetti operativi dello staff e/o un intervento di formazione sugli operatori stessi in funzione di nuova fornitura di servizi e/o Enti aderenti della Regione del Veneto.
- ✓ **Responsabile Formazione e Qualità** – rappresenta il responsabile del livello di competenze e della qualità operativa dello staff operatori sui servizi della Regione del Veneto. Coordina ed organizza le attività di formazione sugli operatori e di aggiornamento dei **portali della conoscenza** (**FAQ e KB**). Tale figura interagisce con il **Responsabile Help Desk** e garantisce l'aggiornamento ed il miglioramento continuo di processi/procedure utili a perfezionare il livello di servizio di assistenza.

  Qualora si verifichino richieste massive e/o transitori picchi di attività:
  - si adopera con ad attingere risorse dal **Team Esperti Qualità** al fine di organizzare **Focus Group** - in forma di seminari e workshop - dedicati agli utenti della Regione del Veneto.
  - si adopera ad attingere risorse dal **Team Esperti KB** al fine di verificare l'efficienza delle procedure operative ed assicurare la qualità del servizio agli utenti della Regione del Veneto.

L'**Area Operativa Help Desk** ha la responsabilità di fornire operativamente l'assistenza agli utenti di riferimento della Regione del Veneto e degli Enti aderenti. La dimensione organizzativa è basata sul seguente schema:

- La dimensione verticale è costituita da ciascun **Team Leader** per gli operatori di **1° e 2° Livello**. L'operatività del **Team Leader** consiste nell'organizzare le attività degli operatori e supervisionare la risoluzione delle richieste di assistenza pervenute al **1° Livello** ed eventualmente trasferite al **2° Livello**
  - Una volta raggiunto il **Team Operatori di 2° Livello** - qualora il **servizio di assistenza** non sia in grado di risolvere la problematica - il **Team di Operatori** effettua opportuna escalation verso gli esperti funzionali di tematica presenti all'interno dei **Centri di Supporto**. In tale occasione la richiesta viene impostata in stato "pending" e viene incaricata una risorsa del **Team di Operatori di 2° Livello** a ricoprire temporaneamente il ruolo di **Case Manager**. La figura del **Case Manager** funge da interfaccia verso i **Centri di Supporto**, con lo scopo di seguire a livello procedurale la risoluzione del problema ed a seguito assicurare a livello operativo l'evasione della richiesta (temporaneamente in stato "pending").
- La dimensione orizzontale è organizzata in base alle aree funzionali e di competenza: **Assistenza Tecnologica** e **Supporto Funzionale**.
  - Le attività di assistenza su tali ambiti vengono organizzate dagli appositi **Team Leader** e coordinate all'interno dei **Team Operatori di 1° Livello e 2° Livello**. Entrambi i **Team di Operatori** – istruiti con adeguata formazione - si occupano di gestire e risolvere le richieste di assistenza in funzione della specifica area di competenza e livello di supporto necessario.

A garantire ulteriore tempestività nella corretta risoluzione delle richieste di assistenza – qualora la problematica sia stata impostata in stato "pending" dal **Team Operatori di 2° Livello** – è previsto il ricorso all'intervento da parte dei **Centri di Supporto**. Si tratta di un gruppo di risorse costituito dai massimi esperti di conoscenza per tipologia di tematica, che ha diretta dipendenza gerarchica e funzionale dal **Responsabile di Servizio** di competenza (**Firma digitale, Posta elettronica certificata, Conservazione sostitutiva**).

Dal punto di vista della **gestione operativa dei Data Center** – la **Struttura di Supporto** al modello organizzativo – è rappresentata dal **NOC** (**Network Operation Center**) che fornisce **assistenza 24 ore al giorno, 365 giorni all'anno**. Tale struttura organizzativa è composta da personale altamente qualificato che controlla costantemente gli aspetti inerenti la sicurezza su tutti gli asset (end-to-end) e sui servizi erogati. In tempo reale viene verificata ogni possibile minaccia o evento anomalo che possa minare la sicurezza in termini di disponibilità e continuità del servizio, riservatezza, integrità ed affidabilità delle informazioni. Il personale che costituisce il **NOC** ha ampia conoscenza ed adeguata esperienza in merito ai servizi erogati dalla presente fornitura.

5.2 PROCEDURE E STRUMENTI PROPOSTI

La gestione del **Servizio Help Desk** prevede che ciascuna richiesta derivante da qualsiasi canale di contatto previsto dal capitolato (Telefono, Fax, Email e Ticket) preveda la trasformazione e tracciamento della richiesta tramite **Ticket sul Portale Web** - da parte dell'**Operatore Help Desk**.
Tale requisito operativo – sebbene possa sembrare un approccio schematico – comporta notevoli vantaggi - quali un puntuale monitoraggio e tracciabilità di ciascuna richiesta di assistenza di carattere tecnologico e/o funzionale.

5.2.1 LIVELLI DI SERVIZIO

Gli **operatori del Servizio Help Desk** saranno istruiti con interventi formativi – soprattutto nella prima fase di progetto – sulle peculiarità dei servizi e dell'infrastruttura in uso dalla Regione del Veneto e dagli Enti aderenti.
Le prestazioni del **Servizio di Help Desk** vengono espletate nel rispetto dei **Livelli di Servizio** (**SLA**) previsti nella fornitura di gara. I **Livelli di Servizio** (**SLA**) vengono garantiti – senza oneri aggiuntivi per la Regione del Veneto – con alcuni miglioramenti come dalla seguente tabella:

Attività del Servizio Help Desk	Descrizione	SLA Offerto in Gara	SLA Richiesto da Capitolato	KPI di riferimento in Gara
Risposta Help Desk tramite Canale Telefonico	Dal momento in cui l'utente contatta il servizio Help Desk – tramite canale telefonico - al momento in cui l'Operatore Help Desk risponde alla chiamata	**1 minuto**	Almeno 95% delle chiamate ricevute con risposta entro 1 minuto	**QSHD >= 95%**
Presa in carico della richiesta /con trasformazione in Ticket	Dal momento in cui l'Operatore 1° Livello riceve la richiesta di assistenza – tramite canale Telefonico, Email o Portale Web o Fax – al momento in cui l'operatore formula la prima risposta all'utente	**15 minuti**	N/D	**N/D**
Tempo di richiamata a seguito richiesta di contatto Outbound	Dal momento in cui l'utente richiede una richiesta di contatto telefonico in Outbound al momento in cui l'Operatore 1° Livello provvede a contattare l'utente	**10 minuti**	N/D	**N/D**
Tempo Risoluzione del problema / Chiusura del Ticket	Dal momento in cui l'Operatore 1° Livello riceve la richiesta di assistenza – tramite canale Telefonico – e formula la risoluzione del problema all'utente della Regione del Veneto Tempo Risoluzione per Fascia a) – più del 40% delle richieste risolte nel corso della telefonata b) – più del 90% delle richieste risolte entro le 24 ore c) – più del 98% delle richieste risolte entro le 48 ore d) – 100% delle richieste risolte oltre le 48 ore	**Tempo Risoluzione per Fascia come da Capitolato di Gara**	Tempo di risoluzione del problema entro i limiti previsti per fascia	**TRHD per fascia**
Disponibilità	Il servizio sarà disponibile	**98%**	Disponibiltà per	**DSHD >=**

del Servizio	nella fascia oraria prevista dal capitolato di gara: • **dal Lunedì al Venerdì - dalle ore 8,00 alle ore 18,00** • **il Sabato - dalle ore 8,00 alle ore 14,00** per 365 giorni all'anno per tutta la durata del contratto (4 anni) - escluse le festività del calendario italiano ed eventuali fermi servizio programmati.		almeno il 98% del tempo di servizio	**98%**

Gli utenti della Regione del Veneto – autorizzati al ruolo - possono monitorare le prestazioni e la qualità del **Servizio di Help Desk** tramite l'accesso diretto al **Portale Web**, che contengono misurazioni delle tempistiche di evasione e chiusura dei **Trouble Ticket** (in forma di tabella e/o di grafico).

5.2.2 CLASSIFICAZIONE DELLE RICHIESTE

L'adeguata qualità del servizio viene garantita da un processo di gestione fondato su una corretta classificazione delle richieste e su un dettagliato tracciamento del loro stato di avanzamento tramite **Trouble Ticket**. La classificazione delle richieste avviene in base alla **Tipologia Servizio** (Firma Remota, Marcatura Temporale, PEC, Conservazione sostitutiva) e **Tipologia Richiesta** (Assistenza Tecnologica o Funzionalità Servizio).

5.2.3 REPORTISTICA E STATISTICHE

Il **Servizio di Help Desk** avrà il compito di mantenere - per tutta la durata del contratto - la banca dati relativa alla registrazione di tutte le segnalazioni (**Trouble Ticket**).
Sulla base dello storico delle segnalazioni (**Trouble Ticket**) si potranno effettuare estrazioni parziali e/o operazioni di natura statistica, in relazione alle richieste ricevute e agli interventi effettuati (con l'evidenza dell'esito e della tempistica di evasione).
La **piattaforma software** individuata per la gestione del **Sistema di Trouble Ticketing** del **Servizio di Help Desk** è in grado di rispondere a tutti i requisiti del capitolato di gara.
Il **gruppo Aruba** garantisce la fornitura di **report trimestrali** alla Regione del Veneto – comunicandoli ad un indirizzo e-mail definito. La **reportistica** – contenente informazioni relative alle performance del servizio di assistenza - consentirà alla Regione del Veneto valutare i **livelli di servizio** ed in caso verificare direttamente la reportistica tramite l'accesso al **Portale Web**.
L'applicazione fornita da **Aruba PEC** tiene traccia di tutte le informazioni necessarie per la gestione del processo di assistenza:

- dettaglio tramite ticket delle richieste di assistenza pervenute su tutti i canali offerti in gara;
- informazioni sui ticket con suddivisione per tipologia e stato delle richieste;
- disponibilità dei tempi di risposta per ciascuna richiesta.

5.2.4 STRUMENTI COMPLEMENTARI DI CONTATTO

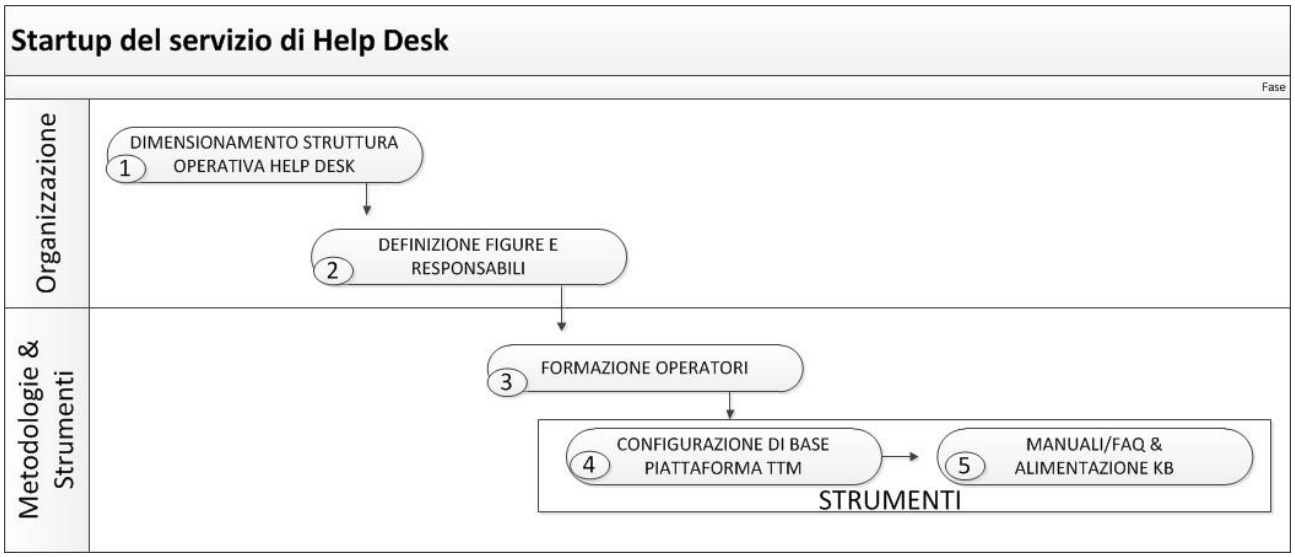
Oltre ai canali di contatto previsti in gara – come elemento migliorativo – vengono messi a disposizione ulteriori strumenti complementari, utili a fornire un'assistenza più efficiente ed efficace agli utenti della Regione del Veneto:

- ***Knowledge Base esterna*** – repository web della conoscenza completo di processi funzionali e linee guida operative utili a supportare l'utente nella risoluzione dei principali problemi in maniera autonoma.
- **FAQ esterne** – sezione web rivolta agli utenti della Regione del Veneto, contenente le istruzioni e linee guida risolutive per le tematiche più frequenti.
- **Call me Back** - canale di immediato contatto rivolto a mettere in comunicazione gli utenti della Regione del Veneto con il **Team Operatori di 1° Livello**.

5.2.5 STARTUP DEL SERVIZIO

La **fase di startup** del **Servizio di Help Desk** – come rappresentato dal seguente flusso di processo – è suddivisa in sequenza nelle seguenti sotto-fasi:

- **Organizzazione** – costituita dalle attività di dimensionamento degli operatori e definizione dei figure/ruoli nell'organizzazione
- **Metodologie & Strumenti** - costituita dalle attività di formazione rivolte agli operatori e agli utenti richiedenti della Regione del Veneto, configurazione iniziale delle piattaforme di lavoro ed alimentazione degli strumenti della conoscenza (**KB** e **FAQ**) con i contenuti base



La **sessione formativa** prevista in **fase di startup** per il servizio **Help Desk** prevede di istruire li operatori in merito alle principali peculiarità dei sistemi e servizi presenti all'interno della Regione del Veneto e degli Enti aderenti. Il personale impiegato frequenta periodicamente corsi di aggiornamento e specializzazione per aumentare il livello di competenze e le capacita, in modo da espletare tutte le attività e le mansioni legate ai servizi erogati
In merito alle piattaforme di lavoro e strumenti della conoscenza – a completamento della **fase di startup** – è prevista la configurazione di base per:

- la piattaforma di ticketing
- il censimento dell'anagrafiche degli Enti aderenti e dei servizi erogati
- la profilazione di utenti ed asset
- i contenuti della **KB esterna** e le evidenze delle **FAQ**

In caso di nessuna richiesta formativa in **fase di startup** - viene comunque garantita la disponibilità ad organizzare in seguito delle attività di affiancamento (in forma di seminari, workshop e consulenze) agli utenti della Regione e degli Enti che ne faranno successiva richiesta.

6 SERVIZI DI SUPPORTO E FORMAZIONE

Aruba PEC garantisce il servizio di supporto e formazione al personale di tutte le Amministrazioni che usufruiranno dei servizi in convenzione.
Il servizio mira a rendere disponibili, al personale della Regione del Veneto e degli Enti locali che usufruiranno dei servizi erogati, alcuni strumenti formativi di carattere normativo, tecnologico e di utilizzo degli strumenti/applicazioni in materia di firma digitale e marcatura temporale, posta elettronica certificata e conservazione sostitutiva a norma.
Le giornate formative potranno essere utilizzate anche per seminari e workshop organizzate dalla Regione.

☞ Quale elemento migliorativo, al fine di incentivare l'adesione degli Enti e la diffusione dei servizi oggetto del presente bando, Aruba PEC organizzerà, senza oneri aggiuntivi, **7 workshop dedicati al progetto**, 1 per Provincia.

I workshop, organizzati da personale esperto in eventi a stretto contatto con il responsabile formativo e con i referenti aziendali della fornitura, avranno lo scopo di presentare le novità introdotte con la convezione, gli strumenti messi a disposizione, le novità normative e le opportunità che l'utilizzo di tali servizi potranno offrire agli Enti.
Un'apposita segreteria provvederà a contattare i potenziali Enti interessati e ad organizzare gli eventi, secondo un calendario concordato con Regione del Veneto.
Agli eventi parteciperanno gli *specialist* di Aruba PEC sui servizi offerti che, oltre a proiettare il materiale fornendo un'anteprima delle interfacce e dei prodotti, rilasceranno della documentazione formativa/informativa a tutti i partecipanti.

Verrà nominato un **Responsabile del servizio di supporto e formazione** i cui riferimenti e relativi recapiti (telefono, fax, mail) saranno forniti in seguito alla firma del contratto.

☞ Oltre al Responsabile della formazione, quale elemento migliorativo, Aruba PEC metterà a disposizione una ***segreteria didattica***, raggiungibile tramite mail, per pianificare l'attività formativa. Tale struttura si occuperà di:

- concordare le date di formazione con i referenti degli Enti interessati gestire eventuali variazioni;
- organizzare le classi anche sulla base delle conoscenze normative, tecnologiche e informatiche dei dipendenti;
- comunicare il nominativo del docente che si occuperà della formazione;
- predisporre il registro delle presenze;
- predisporre gli attestati di partecipazione.

Tale struttura permetterà di realizzare dei corsi strutturati e ben organizzati in modo che possano essere soddisfatte tutte le esigenze conoscitive del personale degli Enti.

Aruba PEC farà inoltre seguire a ciascun corso un periodo di tutoraggio e supporto via email per ciascuno dei partecipanti. I partecipanti al corso potranno chiedere chiarimenti sugli argomenti trattati. Ovviamente questo tipo di supporto non vuole e non può sostituirsi all'assistenza tecnica, ma servirà per sciogliere eventuali dubbi emersi nei giorni successivi al corso sui contenuti mostrati.

Si precisa inoltre che, limitatamente al servizio di firma digitale, per svolgere le attività di riconoscimento de visu e rilascio in autonomia dei certificati, gli operatori degli Enti dovranno essere appositamente formati, in modo che operino nel pieno rispetto delle vigenti normative in materia.
In particolare i CDRL (Centri di Registrazione Locale o Registration Authority - RA), parte integrante dell'Ente Certificatore, lo rappresentano di fronte al titolare, che si presenta presso di loro per richiedere un certificato. I CDRL operano grazie ad un Accordo sottoscritto con l'Ente Certificatore stesso, ovvero un documento che regola i rapporti tra le parti, indicando i reciproci impegni nell'esecuzione delle attività. Nell'ambito di un Centro di Registrazione operano gli addetti al rilascio (o Registration Authority Officer - RAO) che possono, laddove se ne presenti la necessità, essere affiancati da un'altra figura, gli incaricati al riconoscimento (Incaricato della Registrazione - IR).
Sia i RAO che gli IR devono essere identificati ed autorizzati ai sensi della legge 196/2003 (viene loro conferita una lettera di nomina quali incaricati al trattamento dei dati personali da parte dell'Ente Certificatore).
Sia i RAO che gli IR svolgono le loro attività previa partecipazione ad opportuni corsi di formazione somministrati da personale dell'Ente Certificatore ed il superamento del test valutativo finale.

☞ Per adempiere a tale formalità e formare gli operatori all'utilizzo degli strumenti messi a disposizione, Aruba PEC fornirà un corso gratuito di ***formazione a distanza***.

☞ L'utilizzo del corso e-learning per la formazione obbligatoria prevista dalla normativa per gli IR e gli ODR permetterà di soddisfare queste formalità senza ulteriori costi per gli Enti, che non dovranno attingere alle giornate formative in aula. Qualora invece l'Ente preferisca utilizzare un metodo tradizionale di formazione, Aruba PEC s'impegna ad organizzare ed espletare i relativi corsi nelle modalità di seguito descritte.

Tale corso rappresenta uno strumento valido ed alternativo alla formazione in aula per i momenti didattici ovvero per trasmettere aggiornamenti normativi o sul sistema di emissione oppure per formare nuovi addetti ed incaricati senza richiedere giornate di formazione in aula aggiuntive.

L'*e-learning* è un metodo online di formazione a distanza che, attraverso l'utilizzo di apposite piattaforme informatiche, permette di condividere materiali didattici (file audio, video, esercitazioni pratiche).
Negli ultimi anni questo metodo formativo si è diffuso molto rapidamente tanto nelle più importanti realtà aziendali quanto in quelle accademiche. In generale si è rivelato efficace sia per superare le difficoltà legate alla presenza fisica, sia per favorire una maggiore condivisione di contenuti e opinioni in modo immediato.
Aruba PEC ha sperimentato con successo tale modalità formativa in altre esperienze: ad esempio attraverso questo strumento sono stati formati oltre 500 operatori delle Camere di Commercio italiane.

Gli aspetti positivi del corso e-learning:

- Supera i limiti posti dall'assenza di un luogo fisico come l'aula tradizionale;
- Riduce i costi complessivi dell'intervento didattico a regime;
- È svincolata dal tempo, dallo spazio e dai luoghi di fruizione dell'apprendimento.

Aruba PEC si impegna a mettere a disposizione all'interno della propria piattaforma di e-learning un corso dedicato sia agli addetti sia per gli **incaricati al riconoscimento** che operano all'interno della Regione del Veneto e degli Enti aderenti:

- **Corso di formazione Incaricati al Riconoscimento** per il rilascio di Carte Nazionali dei Servizi (CNS) e firma digitale. Il corso fornisce le informazioni e la descrizione degli strumenti necessari ad effettuare le operazioni di riconoscimento "de-visu" di chi richiede il rilascio di un dispositivo di firma digitale.

- **Corso di formazione per addetti di registrazione** che si occuperanno del rilascio di Carte Nazionali dei Servizi (CNS) e firma digitale. Il corso fornisce le informazioni e gli strumenti necessari ad effettuare le operazioni di riconoscimento "de-visu" e rilascio di un dispositivo di firma digitale.

Il corso e-learning fornirà le seguenti informazioni e competenze:

- sapere cos'è un certificato di firma digitale,
- sapere cos'è una firma remota,
- conoscere il sistema di gestione dei certificati e le caratteristiche degli strumenti messi a disposizione,
- sapere come si registra e si rilascia un dispositivo con certificato di Firma Digitale e di autenticazione utilizzando gli strumenti software messi a disposizione da Aruba PEC.

I temi trattati sono:

- CNS, Certificati di autenticazione e Firma digitale e normativa di riferimento
- Dispositivi e lettori
- Card Management System
- Registrazione di un Utente(IR e RAO)
- Rilascio di un dispositivo (RAO)

Al termine del corso, sarà effettuato un test di valutazione, che ha lo scopo di verificare la conoscenza dei contenuti del corso e l'apprendimento delle normative di firma digitale.
Il corso messo a disposizione sarà disponibile per le piattaforme Browser più comuni (Internet Explorer, Mozilla Firefox, Chrome, Opera).
Il corso di e-Learning sarà inoltre dotato di immagini animate ed audio supporto per il sostegno dell'operatore in fase di autoapprendimento.
Per la sua visualizzazione non sono necessarie installazioni di componenti aggiuntive da parte dell'utente finale.

L'Ente che desidera usufruire della modalità e-learning si collegherà ad un apposito sito all'interno del quale sarà richiesta la compilazione di un Form, necessario all'utente per la creazione della propria Username e Password dedicata, in modo che la piattaforma possa creare per ogni utente registrato un proprio report con l'esito finale del corso.

Aruba PEC sarà comunque disponibile, secondo il modello di remunerazione previsto, a realizzare ulteriori sessioni di formazione/addestramento in aula, a richiesta di Regione del Veneto e degli Enti aderenti, per gli addetti ed incaricati.

Oltre a questi corsi specifici per gli addetti, relativi al servizio di firma digitale e remota, Aruba PEC potrà strutturare giornate formative in aula per presentare la convenzione e fornire informazioni di carattere normativo, tecnologico e di utilizzo degli strumenti/applicazioni in materia di firma digitale e marcatura temporale, posta elettronica certificata e conservazione sostitutiva a norma.

In tali casi, Regione del Veneto e gli Enti aderenti contatteranno il Responsabile della formazione comunicando il tipo di supporto richiesto, le quantità previste e le possibili date. Con l'ausilio della Segreteria didattica verrà strutturato il corso di formazione o l'attività di supporto, una proposta di piano d'intervento che verrà condivisa ed eventualmente modificata.

Per la formazione in aula il docente sarà completamente autonomo per quanto riguarda l'attrezzatura necessaria (computer, lettori di smart card, carte di test, proiettore, documentazione cartacea ecc.).

Per i contenuti trattati nei corsi sarà sviluppato **materiale specifico** sia in formato cartaceo che in formato elettronico che i destinatari della formazione potranno utilizzare come materiale didattico.
In generale i corsi potranno essere corredati di:

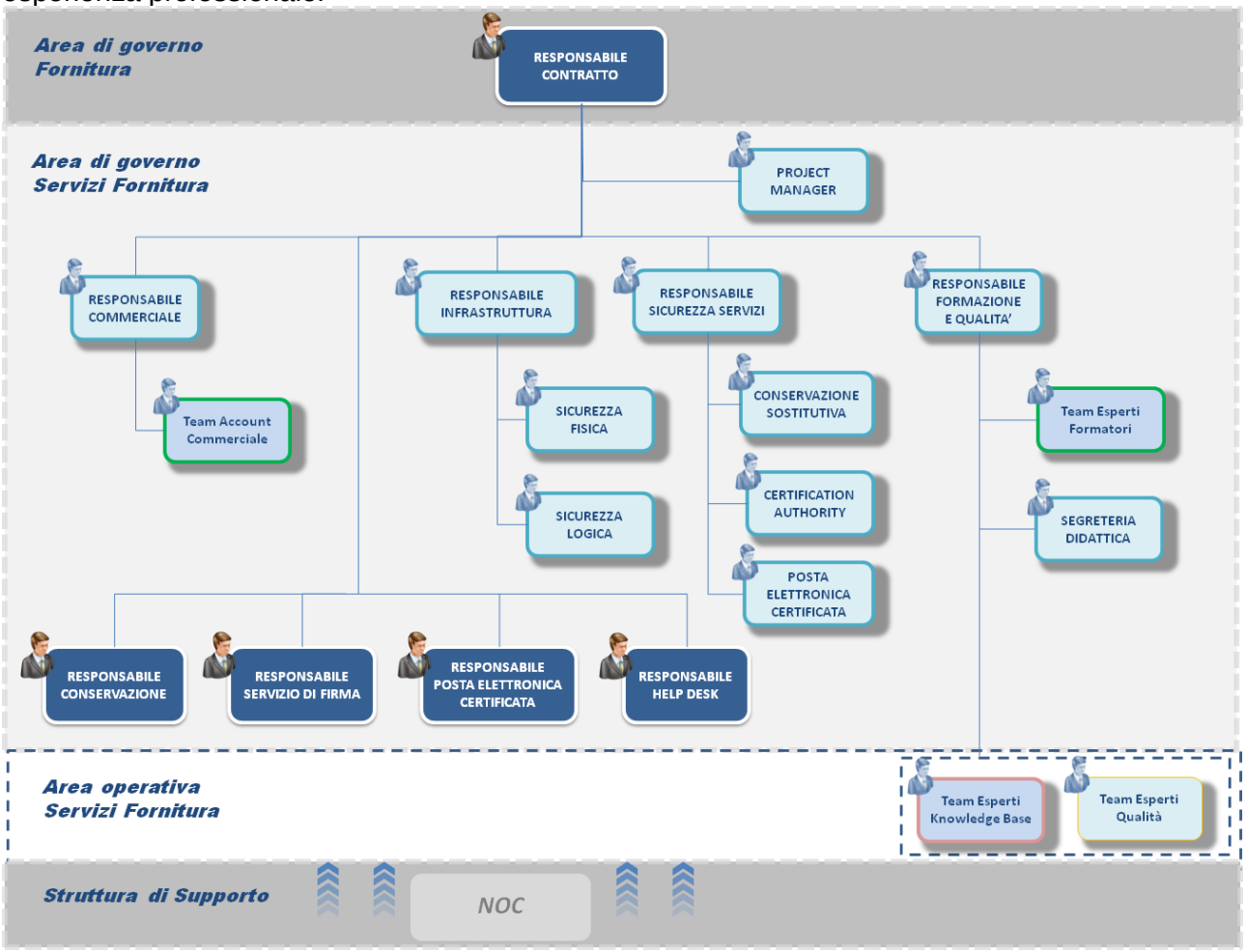
- **Guida Istruttore**: è il documento che supporta il docente nell'attività d'aula, sia teorica che pratica; il documento "consolida" la conoscenza, esplicita i contenuti e la struttura del corso, contiene suggerimenti e commenti su come condurre la didattica, indica i messaggi "chiave" da lanciare, descrive nei particolari le esercitazioni e le regole per la loro conduzione;
- **Guida Partecipante**: è il documento di riferimento per il partecipante; coincide con il manuale d'uso per l'utente.

Grazie al proiettore verranno rappresentati in aula degli schemi e slide che permetteranno ai partecipanti di seguire più agevolmente quanto spiegato dal docente.
A tutti gli utenti sarà consegnato il manuale d'uso relativo ad ogni sistema/sottosistema illustrato e un **attestato di partecipazione** al corso, firmato dal docente, a seguito del superamento con successo dei test valutativi previsti a fine giornata formativa.

6.1 COMPETENZE FIGURE PROFESSIONALI

Come descritto nel par. 1.2 del presente documento, Aruba PEC predisporrà un modello organizzativo volto alla gestione del progetto, impiegando nell'esecuzione del servizio un team di professionisti, costituito da risorse con precedenti esperienze in progetti analoghi realizzati caratterizzati da problematiche applicative e tecnologiche similari.
Tale pluriennale e specifica esperienza acquisita dai professionisti costituisce un capitale di conoscenze (contesti, metodologie, strumenti, tematiche applicative, ambienti tecnologici) di immediata riusabilità e di alta affidabilità, maturata non solo attraverso l'attività svolta nei relativi progetti, ma anche attraverso la continua formazione sulle tematiche di specifica competenza.

Di seguito si riporta lo schema organizzativo proposto e un riepilogo delle principali competenze delle figure professionali coinvolte. Quello che viene di seguito fornito è un profilo "minimo" dei membri del team: le persone specifiche saranno indicate a seguito della aggiudicazione della gara. Alla stessa persona potranno eventualmente essere assegnati più ruoli a seconda della specifica esperienza professionale.



6.1.1 RESPONSABILE DEL CONTRATTO

Il Responsabile di Contratto rappresenta una figura di riferimento tanto esterna quanto interna. Risulta essere, infatti il primo punto di contatto per il cliente e la figura di coordinamento delle risorse impiegate per lo svolgimento e l'erogazione dei servizi oggetto del contratto.

Profilo professionale	Responsabile del Contratto – Direttore Commerciale
Esperienza	7 anni
Titolo di studio	Laurea Breve in Scienze dell'Informazione
Certificazioni	Certificazione Sales Cisco Channel
Competenze	Direttore commerciale del gruppo Aruba. Da oltre 15 anni opera nel mondo ICT nel settore commerciale. Ottime capacità relazionali, di trattativa e problem solving. Capacità di guidare team di persone su progetti complessi.
Compiti	È il responsabile dell'attuazione delle politiche commerciali dell'azienda. Il direttore commerciale ha il compito di raggiungere gli obiettivi strategici dell'impresa con le risorse finanziarie, umane e strumentali di cui dispone. A tale scopo: - elabora i piani d'azione, con cui stabilisce come impiegare le risorse a sua disposizione; – dà indicazioni operative a ciascun componente della rete commerciale

6.1.2 PROJECT MANAGER

Il Project Manager è garante della fornitura dei servizi sottoscritti dagli Enti della Regione del Veneto, s'interfaccerà con questi e rappresenterà il punto di contatto diretto per i **Responsabili di area** ed il punto di riferimento trasversale per i **Responsabili di servizio**.
Il PM che verrà incaricato di seguire il progetto sarà una figura di alto spessore e consolidata esperienza in progetti complessi. In particolare questa figura si è occupata con successo di portare avanti importanti progetti, con team eterogenei, quali ad es. la fornitura del servizio di C.A. per tutte le CCIAA italiane e la gestione della Carta Sanitaria Elettronica per Regione Toscana.

Profilo professionale	Project Manager
Esperienza	Superiore a 10 anni
Titolo di studio	Laurea in Scienze dell'Informazione
Certificazioni	Prince 2 Practitioner (project management)
Competenze	• Ottima conoscenza della normativa in ambito PEC e firma digitale • Ottima conoscenza dei sistemi di posta elettronica certificata; • Ottima conoscenza dei principali utilizzi dei certificati digitali e del loro utilizzo nei processi di dematerializzazione dei documenti; • Gestione di progetti) di rilascio certificati CNS e di firma digitale (come PM principale all'interno di RTI • Gestione di progetti di gestione e rilascio di TS-CNS (come PM principale all'interno di RTI) • Consulenza tecnico/normativa per le aziende/enti interessate a diventare Gestore PEC • Progettazione architetture di sistemi PEC complessi (infrastrutture di erogazione per gestori PEC, piattaforme di invio massivo di messaggi, soluzioni PEC personalizzate)

	• Conduzione ed armonizzazione team di sviluppo e gruppi di lavoro eterogenei • Database design

Compiti	• Project manager
	  ○ Interfaccia principale verso li cliente (verso il responsabile di progetto per l'Ente)
	  ○ Pianificazione attività
	  ○ Supervisione dei gruppi di lavoro
	  ○ Invio reportistica riassuntiva dell'andamento del progetto
	  ○ Organizzazione e partecipazione a riunioni di avanzamento interne e con il cliente
	  ○ Gestione eventuali criticità o emergenze
	• Coordinamento con i responsabili di tutti i servizi erogati,
	• Coordinamento con il responsabile del servizio di assistenza

6.1.3 RESPONSABILE INFRASTRUTTURE

Tutti i servizi offerti saranno erogati attraverso i data center del Gruppo Aruba, dotati dei maggiori standard di sicurezza ed affidabilità. Tutta l'infrastruttura sarà monitorata H24 da personale altamente specializzato, da anni operante nel settore ICT.
In particolare è presente un Responsabile dell'infrastruttura che avrà il ruolo di escalation in caso di problemi sul funzionamento dei sistemi coinvolti nell'erogazione dei servizi di gara.

Profilo professionale	Responsabile Infrastruttura - Architetto di sistema Hardware
Esperienza	12 anni
Titolo di studio	Laurea magistrale in Ingegneria Informatica
Certificazioni	Corso Microsoft SQL 2005; Corso Cisco MDSCT (Fiber channel e SAN). Corso Microsoft Clustering su Windows 2000/2003 Corso MOF (Microsoft Operation Framework). Corso EMC Networker. Corso su Storage Area Network basata su apparati EMC Corso ITIL v3 Foundation
Competenze	Progettazione e realizzazione di datacenter e infrastrutture. Analisi e dimensionamento di sistemi server, storage e networking. Conoscenza approfondita di tutti i brand enterprise e dei relativi prodotti: HP, IBM, DELL, EMC, Netapp, etc. Gestione di team di progettazione.
Compiti	Il Responsabile dell'Infrastruttura è il supervisore del corretto funzionamento, della sicurezza e dell'operatività delle infrastrutture di sistema collocate nei data center Aruba. Garantisce la conduzione e l'adeguata manutenzione degli apparati e sistemi infrastrutturali nel rispetto degli standard di Sicurezza Fisica e di Sicurezza Logica.

Il **Responsabile dell'infrastruttura** sarà coadiuvato da un team di esperti sistemisti con profili professionali analoghi a quello sotto riportato:

Profilo professionale	Sistemista
Esperienza	6 anni
Titolo di studio	Diploma di Perito Elettronico-Informatico
Certificazioni	Certificazione Cisco CCNA - Certificazione Evault Server Protection - Frequentato corso di formazione Red Hat System Administration
Competenze	Competenze specifiche al mondo IT: • Amministrazione Microsoft Windows/Windows Server, Failover clustering, Active Directory • Amministrazione Linux/Unix • Conoscenza dei linguaggio Python, C#, Powershell • Scripting e automazione di sistemi Windows attraverso Powershell • Implementazione sistemi avanzati PXE (Preboot Execution Environment) • Amministrazione servizi IIS, apache, ftp, postfix, qmail, dovecot, • Conoscenza avanzata di VMware Vsphere e Microsoft Hyper-V, Cloud Computing • Amministrazione database SQL server, MySQL, postgreSQL • Gestione e configurazione di apparati di rete quali Firewall (Zyxel, Fortinet) e switch (Dell • Powerconnect, Force10, Cisco Nexus) • Gestione sistemi storage quali Equallogic, Netapp, Compellent, con protocolli iscsi, nfs, cifs • Conoscenze avanzate su sistemi di bilanciamento software ipvs, haproxy, nginx • Sviluppo sistemi di monitoring complessi su piattaforma Nagios o simili • Gestione server VPN
Compiti	• Sviluppo di sistemi automatici di deploy e configurazione per i maggiori sistemi operativi esistenti, Windows, Linux, Unix, su piattaforme virtualizzate quali VMware Vsphere o Microsoft Hyper-V e su macchine fisiche, creazione di template specifici per il Cloud Computing e sistemi avanzati PXE. • Gestione dell'infrastruttura IT del gruppo aruba • Cloud Computing, inclusa la manutenzione, il monitoraggio delle performance/uptime e l'integrazione di nuove risorse. • Attività di supporto sistemistico di 2° livello relativo ai servizi Cloud Computing e Virtual Private Server

Il responsabile dell'infrastruttura sarà coadiuvato da esperti progettisti e sistemisti con le caratteristiche esplicitate di seguito

Profilo professionale	Progettista
Esperienza	6 anni
Titolo di studio	Laurea breve in BS Computer Science

Certificazioni	VMWare Certified Professional on vSphere 5.5 - VCP 550 - #142193 VMware Certified Professional on vSphere 5.1 - VCP 510 - #142193 Palo Alto Configuration Engineer
Competenze	Server Consolidation hardware e applicativa. VMware ESX, Infrastructure e Vsphere 2, 3, 4, 5. Progettazione, dimensionamento e implementazione. Microsoft HyperV. Progettazione, dimensionamento e implementazione. Networking, progettazione, realizzazione, configurazione di reti nei datacenter. Storage Area Network, progettazione, realizzazione, dimensionamento e configurazione. Linguaggi di programmazione: Framework .NET, Java, C, C++, C#, PHP, Python, Assembly x86. Sistemi Operativi: Windows, Linux. Configurazione e implementazione di Webservers, Apache e IIS. Configurazione e implementazioni di architetture basate su J2EE, Jboss e Tomcat. Database Microsoft SQL Server, Mysql, Postgres, Oracle sia in configurazione standalone che RAC. Progettazione e modellazione di Domini Microsoft Active Directory
Compiti	- Sviluppo di sistemi automatici di deploy e configurazione per i maggiori sistemi operativi esistenti, Windows, Linux, Unix, su piattaforme virtualizzate quali VMware Vsphere o Microsoft Hyper-V e su macchine fisiche, creazione di template specifici per il Cloud Computing e sistemi avanzati PXE. - Gestione dell'infrastruttura IT legata ad uno dei principali business aziendali di Aruba, il Cloud Computing, inclusa la manutenzione, il monitoraggio delle performance/uptime e l'integrazione di nuove risorse. - Attività di supporto sistemistico di 2° livello

Profilo professionale	Progettista
Esperienza	6 anni
Titolo di studio	Laurea specialistica
Certificazioni	• **Executive Master in Project Management**, presso Quality Evolution Consulting S.r.l. – Anno 2014/2015. • **ITIL Foundation Cert. n° 02398050-01-MDVY rilasciata da APMG-Int. – Anno 2014.** • **Cisco Certified Network Associate** Cert. n° 413454170421JPBI rilasciata da Cisco – Anno 2013. • **Dell Networking Technical Specialty** Cert. n° 66552441 rilasciata da Dell – Anno 2012. • **Certified Sonicwall Security Administrator** CertID: 5218-40EC-B089-4E61 rilasciata da Dell Sonicwall – Anno 2012. • **Dell KACE - Systems Management** Cert. n° 13208210 rilasciata da Dell – Anno 2012. • **Dell EqualLogic Sales v2**, **EqualLogic Technical v2, Compellent Top Gun Storage Architect Technical** e **Compellent Top Gun Storage Sales** rilasciati da Dell – Anno 2011/2012. • **Paloalto Networks ACE** rilasciata da Paloalto Network – Anno 2011. • **DWDM Theory and MHL3000** corso presso la Ericsson Academy di Genova – Anno 2010 • **Operating Juniper Router Enterprise (OJRE)** corso presso l'Università di Pisa – Anno 2007-2008
Competenze	Buona conoscenza dei **sistemi operativi e applicativi**:

	- Windows Server 2003/2008R2/2012R2, Ubuntu Server Edition 14.04, Debian 7.x, Slackware 14.x, CentOS 6.x/7.0, suite Office, Microsoft Active Directory, Samba, OpenLDAP, FreeRadius, Matlab, Network Simulator 2, Wireshark, Dell System Management Kace K1000 e K2000. Buona conoscenza dei **protocolli** e **architetture** di: - *Internetworking*: ATM, TCP/IP, STP/RSTP, MSTP, VSTP, PVST+/RPVST+, VRRP, OSPF, RIPv2, xDSL, Frame Relay, PPP, SDH, DWDM, MPLS, GMPLS, WSON - *QoS*: IntServ, RSVP-TE, DiffServ, DiffServ over MPLS - *Telefonia*: SIP, 3GPP IMS (IP-Multimedia Subsystem), INAP CS1, H.323 Buona conoscenza dei **dispositivi**: - *Switch*: Juniper Switch EX-Series (JunOS), Cisco Multilayer switches (Cisco IOS), Dell Force10 Multilayer switches (FTOS), Dell PowerConnect - *Firewall*: Sonicwall TZ-Series, NSA-Series, SuperMassive-Series, Paloalto Networks: PA-500, PA-2050, PA-5060 (PAN-OS 4.1, PAN-OS 5.0), Fortinet Fortigate Series - *Storage*: Dell Compellent, Dell Equallogic, Dell PowerVault - *Server*: Dell PowerEdge Series 12 e 13, Dell Blades - *IN Application Server:* Piattaforme di telefonia intelligente Alcatel-Lucent *MAS* e *eVPN* - *Apparati Fotonici:* Marconi Ericsson DWDM *MHL3000* - *Virtualizzazione: VMware (ESXi 5.5, vCenter, vCloud, vSphere Replication, Site Recovery Manager), Microsoft (Hyper-V, SCVMM 2012R2, Windows Azure Pack)*
Compiti	Progettazione di infrastrutture di virtualizzazione dedicate e personalizzate sulle richieste dei clienti che desiderano esternalizzare i propri servizi o creare ambienti di Disaster Recovery. Sviluppo e gestione dei progetti interni ed esterni

6.1.4 PERSONALE IMPIEGATO NELL'ATTIVITÀ FORMATIVA E CONTROLLO QUALITA'

Aruba PEC metterà a disposizione, per lo svolgimento dei corsi, docenti adeguatamente qualificati e dotati di consolidata esperienza nella realizzazione di analoghi corsi. Il Gruppo Aruba ha infatti organizzato numerose sessioni formative per progetti in ambito sicurezza informatica e digitalizzazione, quali ad es.:

- Regione Toscana: formazione di oltre 400 operatori CSE (Carta Sanitaria Elettronica)
- Regione Sardegna: formazione di oltre 200 operatori delle aziende sanitarie locali
- Regione Basilicata: formazione degli addetti al rilascio alle CNS ai cittadini
- Infocamere ScpA: formazione di oltre 500 operatori addetti presso le CCIAA italiane.

Di seguito, il profilo-tipo del docente che sarà impiegato per la formazione:

Profilo professionale	Specialista / Consulente
Esperienza	Superiore a 3 anni
Titolo di studio	Laurea o Diploma
Competenze	• Ottima conoscenza delle norme, in particolare: ▪ Linee Guida CAD ▪ Determina AgID n. 63/2014 – Firma digitale verificata ▪ Legge 15/03/1997 n. 59, art. 15 comma 2

	▪ D.P.R. 08/12/2000 n. 445 ▪ D. Lgs. 07/03/2005 n. 82 e successive modifiche e integrazioni (Codice dell'Amministrazione Digitale) ▪ D.P.C.M. 05/02/15 – dispositivi certificati per apposizione di firme elettroniche ▪ D.P.C.M. 22/02/13 (Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali.) ▪ D.P.C.M. 19/07/12 – Decreto sui dispositivi automatici di firma – HSM ▪ D.P.C.M. 30/03/09 - Regole tecniche firma digitale ▪ Deliberazione CNIPA 45/2009 (Regole per il riconoscimento e la verifica del documento informatico) e 69/2010 ▪ Normativa europea: Direttiva 99/93/CE relativa ad un quadro comunitario per le firme elettroniche ▪ Nuove Regole tecniche in materia di sistema di conservazione DPCM del 3 dicembre del 2013 ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44 –bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n.82 del 2005 ▪ Decreto legislativo 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali • Ottima conoscenza di Internet Explorer e dei browser in generale, dei principali sistemi di posta elettronica; • Conoscenza e utilizzo del Sistema Operativo Windows; padronanza nelle procedure di installazione hardware (lettori smart card, Token USB, stampanti ecc…). • ottima conoscenza dei principali utilizzi dei certificati digitali e del loro utilizzo nei processi di dematerializzazione dei documenti; • progettazione degli interventi didattici; attività di docenza con l'utilizzo di tecniche didattiche rivolte a platee eterogenee. • Conduzione di gruppi di lavoro tematici volti alla ricerca di soluzioni organizzative ed applicative. • Ricerca e sperimentazione di metodologie didattiche innovative. • Competenze nelle tematiche specifiche della materia insegnata.
Compiti	• presenza in aula durante le ore previste dal calendario didattico; • svolgimento del programma didattico, utilizzando metodologie appropriate che garantiscano in ogni caso il raggiungimento dell'obiettivo didattico indicato; • fornitura del materiale didattico relativo al modulo svolto; • verifica il livello di partecipazione dei destinatari; • verifica dei contenuti formativi sviluppati; • verifica dei risultati emersi dai questionari valutativi dei corsi;

	• relazione sugli obiettivi didattici raggiunti e sul rendimento dell'aula in termini di apprendimento, atteggiamenti e motivazione (sia individuale che complessiva).

L'adozione di una check-list di riferimento da parte dei docenti per il controllo delle attività, riportata di seguito, permetterà di garantire un notevole livello di standardizzazione nell'organizzazione del corso e nel completamento delle attività previste.

Check-list corso: del __/__/____ a _____	
GIORNI PRECEDENTI	
effettuare fotocopie materiale didattico (manuale etc.)	
stampare Attestati partecipazione	
stampare Test di valutazione	
stampare Foglio Presenze con lista partecipanti	
stampare Questionari di valutazione corso	
preparare materiale (lettori, dispositivi, documenti cartacei, etc.)	
preparare proiettore	
GIORNO DEL CORSO	
far firmare Foglio Presenze	
sottoporre Test di valutazione ai partecipanti	
consegnare Attestato partecipazione al corso	
far compilare ai partecipanti il Questionario di valutazione corso	
GIORNI SUCCESSIVI	
archiviare la modulistica prodotta durante il corso	

Oltre ai formatori, Aruba PEC metterà a disposizione un **Responsabile della formazione** che coordinerà le attività formative e si occuperà anche della verifica della qualità dei servizi erogati, avendo competenze specifiche in ambito ISO.

Profilo professionale	**Responsabile Formazione e Qualità**
Esperienza	Superiore a 10 anni
Titolo di studio	Laurea o Diploma
Certificazioni	• Certificazione PRINCE2 • Certificazione ITIL Foundation • Certificazione ISO 9001 & ISO 19011 • Specializzazione in Supply Chain Management • Specializzazione in Sicurezza D. Lgs. 81/08
Competenze	• Conoscenza delle principali piattaforme ERP e CRM • Conoscenze dei principali RDBMS • Conoscenza dei principali Sistemi Operativi Windows

	• Conoscenza dei principali strumenti Web • Conoscenza in ambito tecnologie di firma digitale/remota, conservazione e PEC • Conoscenza in ambito infrastrutture fisiche e virtuali per DataCenter • Conoscenza in ambito Supply Chain • Conoscenza in ambito Project Management • Conoscenza in ambito di processi e procedure IT • Conoscenza in ambito Sicurezza ISO 27001 • Conoscenza in ambito Qualità ISO 9001 • Conoscenza dei principali metodi e strumenti di formazione • Conoscenza degli strumenti MS Office • Conoscenza della lingua inglese (tecnica)
Compiti	• **Responsabile** del livello di competenze e della qualità operativa durante l'erogazione e manutenzione dei singoli servizi • Interazione con ciascun **Responsabile di servizio** a garanzia del miglioramento continuo di processi/procedure per la fornitura • Gestione del **Team Esperti Formatori** finalizzati all'erogazione di contributi formativi su aspetti funzionali/utilizzo in occasione di seminari e/o workshop • Gestione del **Team Esperti Qualità e del Team Esperti KB** finalizzati all'erogazione di aggiornamenti formativi su processi/procedure operative in occasione di seminari e/o workshop • Supervisione della **Segreteria Didattica** finalizzata ad organizzare e pianificare percorsi formativi dedicati • Coordinamento ed organizzazione di attività formativa sugli **operatori Help Desk** • Supervisione degli aggiornamenti formativi sui **portali della conoscenza** (**FAQ e KB**)

6.1.5 RESPONSABILE DELLA SICUREZZA DEI SERVIZI

Aruba PEC è azienda certificata ISO 27001:2013 per la sicurezza delle informazioni sui servizi oggetto di gara.

Tutti i servizi offerti saranno erogati attraverso i data center del Gruppo Aruba, dotati dei maggiori standard di sicurezza ed affidabilità, che opera secondo gli standard ISO 27001.
In particolare è presente un Responsabile della sicurezza incaricato di garantire la sicurezza dei sistemi coinvolti nell'erogazione dei servizi di gara e il rispetto della normativa di riferimento.
Come riportato nel paragrafo 1.2 il Responsabile Sicurezza Servizi sarà supervisore degli standard e policy di sicurezza necessarie a garantire la corretta erogazione dei servizi. Nello specifico garantisce l'adeguato mantenimento dei livelli di sicurezza per il **servizio di Conservazione, Certification Authority e PEC** oggetto della fornitura in gara.

Profilo professionale	Responsabile Sicurezza Servizi
Esperienza	8 anni
Titolo di studio	Laurea
Certificazioni	CISSP – Certified Information Systems Security Professional
• **Competenze**	Capacità e competenze organizzative e tecniche - capacità di guidare efficacemente team di progetto, capacità di coordinamento e supervisione gestione progetti complessi, analisi tecnica /funzionale con varie metodologie (tra cui UML); capacità e competenze informatiche • conoscenza degli standard tecnici alla base delle PKI (emissione e gestione dei • certificati, buste crittografiche, marcatura temporale, protocolli sicuri, ecc) • ottima conoscenza della normativa italiana ed europea sulla firma digitale e temi correlati • ottima conoscenza del linguaggio di programmazione Java • conoscenza di base dei linguaggi di programmazione C, C#, Visual Basic • conoscenza di base degli standard relativi al "mondo" XML e Web Services • conoscenza di base delle principali architetture e framework • familiarità coi sistemi operativi Windows, MacOS X, Linux ed altri Unix • ottima conoscenza delle smartcards (tecnologia, standard di riferimento, ecc) • buona conoscenza degli HSM (Hardware Security Modules) • ottima conoscenza della CNS (Carta Nazionale dei Servizi) • conoscenza della piattaforma JavaCard + GlobalPlatform • familiarità con il software open source
Compiti	Attività di pre-vendita e Project Management, in particolare nei campi della CNS/CRS e dei servizi di CA e di firma remota e/o automatica • Redazione delle offerte tecniche in risposta ad RFP/RFQ e bandi di gara • Consulenza ai clienti sugli standard tecnici, la normativa, le smartcard, ecc. • Responsabile della Sicurezza nell'ambito dei servizi PKI erogati • Principale referente del gruppo ARUBA nei confronti del DigitPA/AgID è supervisore degli standard e policy di sicurezza necessarie a garantire la corretta erogazione dei servizi. Nello specifico garantisce l'adeguato mantenimento dei livelli di sicurezza per il servizio di Conservazione, Certification Authority e PEC oggetto della fornitura in gara.

6.1.6 PERSONALE IMPIEGATO NEI SERVIZI DI C.A.

Il team di firma digitale è organizzato nel pieno rispetto della normativa di settore e formato da personale di alto livello con competenze specifiche nel servizio.

Direttore C.A.

Profilo professionale	Direttore dei Servizi di Certification Authority
Esperienza	6 anni
Titolo di studio	Laurea
Certificazioni	Key Manager Verisign - Il Key Manager è il responsabile della definizione e configurazione dei parametri specifici della Certification Authority e della sua corretta generazione, secondo le Policy e procedure imposte da Verisign stessa.
Competenze	Direttore dei servizi di Certificazione del gruppo Aruba, da oltre 13 anni opera nel mondo della firma digitale, posta certificata, CNS e più in generale nei progetti legati all'identità digitale. Membro del Consiglio Direttivo di Assocertificatori e Socio sostenitore di AIFAG (Associazione Italiana Firma Elettronica Avanzata, Biometrica e Grafometrica), partecipa attivamente ai tavoli di lavoro sulla compliance normativa ed interoperabilità delle soluzioni proposte.
Compiti	Attività di Direttore dei Servizi di Certification Authority: • consolidamento dei processi CA del gruppo (Actalis e ArubaPec) • supporto all'attività commerciale (pre-sales, post-sales) • supporto all'attività di Delivery • Attività di PM su progetti interni ed esterni • supporto all'attività dell'ufficio Gare, Redazione relazioni tecniche, verifica con stazione appaltante pre-requisiti, kick off, ... • sviluppo nuovi prodotti e servizi • coordinamento "trasversale" con le varie strutture aziendali per la corretta gestione ed esercizio dei servizi di CA ed e-security • Gestione dei rapporti con AgID, Assocertificatori, AIFAG ed Enti Istituzionali • Partecipazione a Convegni, Fiere, Eventi con Speech/Workshop

Responsabile servizi C.A.

Profilo professionale	Specialista
Esperienza	Superiore a 3 anni
Titolo di studio	Laurea
Certificazioni	**PRINCE2 foudation** **ISECOM-OPST** (OSSTMM Professional Security Tester). **CCSA NGX** (Check Point Certified Security Administrator NGX). **Cisco Information Security Specialist** **Cisco Firewall Specialist** che comprende: **SND** (Securing Cisco Network Devices) . **SNRS** (Securing Networks with Cisco Routers and Switches). **SNPA** (Securing Networks with PIX and ASA). **CCNA** (Cisco Certified Network Associate).

Competenze	**CRITTOGRAFIA** Competenza nelle seguenti aree: Sistemi di crittografia simmetrica e asimmetrica, Algoritmi di hash, Infrastrutture PKI, Sistemi di Certification Authority basati su X509, Sistemi di firma digitale basati su specifica PKCS7, CMS, CADES, XML, XADES, PDF e PADES, Sistemi di Marcatura Temporale, Sistemi OCSP, Sistemi di interfacciamento di dispositivi crittografici basati su specifica PKCS#11 e MS Crypto API (CSP). **SISTEMI OPERATIVI** Buona conoscenza di Windows (98, ME, NT, 2000, XP, Vista, Seven, 2008), Linux (Suse, Mandrake, Debian), OS X (Panther, Tiger), Cisco IOS, Cisco IOS Firewall. **WEB SERVER** IIS, Apache. **LINGUAGGI DI PROGRAMMAZIONE ED AMBIENTI DI SVILUPPO** Conoscenza dei linguaggi C, Java, Perl, C++, MatLab **OFFICE AUTOMATION** Buona conoscenza del pacchetto Microsoft Office 2003 (Word, PowerPoint, Excel, FrontPage, Exchange).
Compiti	Project-Manager e Coordinatore Tecnico presso la Certification Authority di Aruba Pec S.p.A., Ente Certificatore Accreditato DitiPA (ex CNIPA) per l'emissione di certificati di firma Digitale e Carta Nazionale dei Servizi. * Coordinamento tecnico e normativo per il mantenimento della Certification Authority ai livelli di servizio previsti dalla normativa Nazionale ed Europea; * Coordinamento tecnico e normativo per la realizzazione di circuiti di emissione per Carta Nazionale dei Servizi; * Coordinamento tecnico e normativo per l'implementazione di soluzioni di Firma Remota e Firma Automatica; * Key Manager, Responsabile della configurazione e generazione delle Certification Authority Aruba Pec; * Responsabile della qualificazione di prodotti hardware e software per Firma Digitale (SSCD, HSM, software di firma e verifica); * Responsabile della realizzazione di dispositivi portable per la Firma Digitale; * Responsabile del servizio di Marcatura Temporale; * Coordinamento tecnico e normativo nell'accreditamento della Certification Authority di Aruba Pec S.p.A. presso DigitPA; * Project Manager in progetti legati a tematiche sulla Firma Digitale/PKI ed attività di Pre-Sales e supporto all'azione commerciale presso il Cliente.

CMS Specialist

Profilo professionale	Specialista Card Management System
Esperienza	Superiore a 5 anni, maturata in ambito analogo a quello del servizio offerto
Titolo di studio	Laurea
Certificazioni	Prince2 (Project Management)
Competenze e conoscenze	• Ottima conoscenza della normativa in ambito firma digitale • Ottima conoscenza dei sistemi di Card Management • Ottima conoscenza dell'ambito di utilizzo dei certificati digitali • Project management di progetti in ambito firma e certificati digitali • Esperienza nel tutoring e nella formazione relativi ai servizi di firma
Compiti	• Responsabile dell'area del servizio dedicata ai certificati • Coordinamento interno con gli altri responsabili (PEC, Conservazione), con l'interfaccia unica verso la Stazione Appaltante e con il delivery • Interfacciamento con il cliente finale in caso di avvio dei servizi ed escalation

6.1.7 PERSONALE IMPIEGATO NEL SERVIZIO DI CONSERVAZIONE

Anche il team che si occuperà della conservazione sarà organizzato nel pieno rispetto della normativa di settore e formato da personale di alto livello con competenze specifiche nel servizio.

Responsabile del servizio di conservazione

Profilo professionale	Project Manager
Esperienza	15 anni
Titolo di studio	Laurea in Economia e Commercio
Certificazioni	Project Management Professional, Prince 2 Foundation, ITIL V3 Foundation
Competenze	Project/Client Manager con esperienza pluriennale su più tecnologie e progetti complessi in ambito Telco e IT. Esperienza significativa in contesti muti-culturali in diverse Aziende e Paesi. Gestione del progetto e degli stakeholder con una comprovata esperienza dei principi di project management più diffusi (PMI, Prince2, e SCRUM) Competenze consolidate in ambito Datacenter; in particolare su: • Conservazione Digitale a Norma • Firma Elettronica • Housing Colocation, Server Dedicati • Disaster Recovery e Business Continuity • Soluzioni Cloud basate su piattaforma tecnologia VMWARE • Microsoft Exchange Server

Compiti	• Attività di presales su portafoglio prodotti e servizi • Gestione di risorse umane nell'ambito dei progetti ICT in carico • Attività di project and delivery management • Conduzione e coordinamento di studi di fattibilità, incluso stima del budget, in accordo con le attività richieste • Partecipazione ai tavoli tecnici in materia di dematerializzazione e conservazione digitale a norma • Partecipazione alla redazione di Tender pubblici e privati • Relatore eventi formative, presentazioni, workshops, seminari

Responsabile della funzione archivistica di conservazione

Profilo professionale	*Responsabile della funzione archivistica di conservazione*
Esperienza	4 anni
Titolo di studio	Laurea Magistrale in letteratura Archivistica
Certificazioni	Partecipazione a corsi di formazione tecnologica e normativa sulle Nuove Regole in materia di Conservazione a norma dei documenti e sugli standard OAIS e Dublin Core
Competenze	Buone capacità di coordimento, gestione e motivazione delle risorse umane, Buone capacità di problem solving e di gestione dello stress.
Compiti	Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte del Cliente, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; definizione del set di metadati di conservazione dei documenti e dei fascicoli in-formatici; monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; collaborazione col Cliente ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.

Responsabile dello sviluppo e della manutenzione del sistema di conservazione

Profilo professionale	Responsabile dello sviluppo e della manutenzione del sistema di conservazione
Esperienza	10 anni
Titolo di studio	Laurea
Competenze	Sistemi operativi Windows, Linux, Unix Linguaggi di programmazione e di markup: Object Pascal, SQL, PL/SQL, PHP, Java, HTML, Javascript Strumenti di sviluppo Borland Delphi, Oracle JDeveloper, Eclipse.
Compiti	Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione; pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; monitoraggio degli SLA relativi alla manutenzione del sistema di

	conservazione; interfaccia col Cliente relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni ver-so nuove piattaforme tecnologiche; gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.

6.1.8 PERSONALE IMPIEGATO NEL SERVIZIO PEC

Responsabile del servizio PEC

Profilo professionale	Responsabile servizio Posta Elettronica Certificata
Esperienza	15 anni
Titolo di studio	Laurea
Certificazioni	Prince 2
Competenze	Ingegneria dei sistemi Progettazione software Progettazione database TecnologieOpen Source e loro integrazione Change management Servizi Web Sviluppo di software Recruitment
Compiti	Sviluppo di sistemi di posta elettronica e Posta Elettronica Certificata, studio e analisi delle tecnologie e delle regole tecniche. Il Responsabile del servizio di Posta Elettronica Certificata è supervisore dell'intero **Servizio di PEC**. Coordina le attività svolte dai singoli team di gestione: titolari, servizi tecnici, sicurezza & log, auditing.

Responsabile dello sviluppo e della manutenzione del sistema PEC

Profilo professionale	Responsabile sviluppo PEC
Esperienza	15 anni
Titolo di studio	Laureando in informatica
Competenze	Sistemi Operativi: Linux, *BSD, UNIX Linguaggi di programmazione: C, shell scripting, Perl Posta Elettronica: Postfix, Dovecot, Courier IMAP, PLL LMTP, SpamAssassin, Amavis, ClamAV Database e Directory Server: MySQL, Redis, MongoDB, OpenLDAP Virtualizzazione: KVM, LXC, Amazon Web Services Web: Apache HTTP, nginx, Squid Monitoraggio/Reportistica/Management: Ganglia, Nagios, collectd, sysstat
Compiti	Sviluppo ed implementazione di sistemi di posta elettronica e Posta Elettronica Certificata. Studio e analisi delle tecnologie e delle regole tecniche volte all'aggiornamento ed evoluzione dei prodotti di posta elettronica certificata.

7 MONITORAGGIO DELLA FORNITURA E DEI SERVIZI

Per mantenere sotto controllo il processo di erogazione dei servizi distribuiti agli Enti del territorio, Aruba PEC metterà a disposizione un'apposita consolle di monitoraggio ad uso e consumo degli amministratori ed operatori regionali e degli enti aderenti.
La consolle sarà costituita da un'interfaccia web based e sarà accessibile via internet.
Gli utenti saranno profilati ed avranno visibilità solamente alle informazioni di propria pertinenza/interesse:

Tipologia operatore	Visibilità
Amministratore di sistema	Configura e gestisce la consolle di monitoraggio, inserisce alcune informazioni quali le giornate di formazione e di supporto erogate
Operatore ente aderente standard	informazioni sugli ordini, consumi, livelli di servizio del proprio ente
Operatore ente aderente full	informazioni sugli ordini, consumi, livelli di servizio del proprio ente e degli enti associati collegati
Operatore regionale standard	informazioni sugli ordini, consumi, livelli di servizio dell'amministrazione regionale
Operatore regionale full	informazioni sugli ordini, consumi, livelli di servizio dell'amministrazione regionale e di tutti gli enti aderenti ed associati

La consolle verrà messa a disposizione per tutto il periodo di copertura della gara ed esporrà una serie di funzionalità, attraverso le quali sarà possibile:

- gestire l'anagrafe degli Enti Aderenti/Associati;
- controllare l'attivazione e cessazione dei servizi da parte di Regione del Veneto e degli Enti aderenti;
- verificare le quantità richieste in termini di numeri, giorni, Gb, ecc, utilizzate e residue;
- confrontare le esigenze dichiarate dai singoli Enti con i reali consumi degli Enti stessi;
- supervisionare e monitorare la contabilità della fornitura
- verificare ed analizzare i livelli di servizio, compresa la possibilità di recuperare tutte le informazioni necessarie al loro calcolo;
- generare report e statistiche con possibilità di export in vari formati (csv, pdf. ecc.).

Le informazioni riportate all'interno della consolle verranno prelevate dai vari servizi e raccolte all'interno di un database specifico, dove verranno aggregate al fine di creare report e statistiche di semplice e veloce consultazione. La raccolta delle informazioni avverrà con cadenza giornaliera in modo che le informazioni si riferiscano al giorno precedente. Qualora l'Ente appaltante ritenga necessaria una maggiore "freschezza" delle informazioni presentate, sarà possibile aumentare la frequenza di aggiornamento dei dati.

7.1 STRUMENTI E MODALITA' ORGANIZZATIVE DELLA CONSOLLE DI MONITORAGGIO

La consolle di monitoraggio è parte integrante del Pannello Unico di gestione, descritto nel par. 1.2.1.a e sarà accessibile da web dietro inserimento di credenziali di accesso.
Una volta effettuato l'accesso, l'utente verrà indirizzato sulla pagina principale (home page) contenente:

- alcuni dati relativi all'utente collegato (nome, cognome, ente di appartenenza, ecc)
- una serie di informazioni di riepilogo dei servizi erogati;
- una serie di tasti che consentono di visualizzare le informazioni di dettaglio dei servizi e di accedere alle funzionalità di gestione degli enti:
    - Anagrafe Enti aderenti

- Servizio firma digitale
- Servizio certificati SSL
- Servizio marche temporali
- Servizio PEC
- Servizio di conservazione
- Servizio di assistenza
- Servizio di formazione
- Misure di andamento del servizio

I paragrafi che seguono descrivono le singole sezioni, in conformità con quanto descritto dal Capitolato di Gara. Si tratta di una proposta che potrà essere comunque modificata in fase di startup del progetto qualora il cliente lo ritenga opportuno.
Le informazioni aggregate di seguito elencate potranno essere esportate in formato csv e pdf, mediante appositi tasti presenti all'interno delle singole pagine.

7.1.1 SEZIONE ENTI ADERENTI

La sezione consente di gestire l'anagrafica degli Enti. In particolare sarà possibile:

- inserire un nuovo Ente
- modificarne i dati
- associare ad un Ente aderente un elenco di Enti Associati

Le informazioni che verranno inserite per ogni Ente sono le seguenti:

Anagrafe degli Enti Aderenti

• Ente:
  ○ Nome ente
  ○ Provincia ente
  ○ Località
  ○ Indirizzo
• Referente dell'ente:
  ○ Nome
  ○ Cognome
  ○ Codice fiscale
  ○ Email
  ○ Telefono
• Elenco Enti Associati

Inoltre per ciascun servizio erogato e per ciascun ente associato (legate all'Ente) verranno raccolte informazioni relative all'attivazione, ai quantitativi totali ordinati, ai fabbisogni dichiarati, alle quantità residue. La pagina metterà a disposizione una serie di filtri che permetteranno all'operatore di selezionare il singolo ente ed il singolo servizio in modo da poter visualizzare i dati specifici:

- Ricerca per Ente: nome dell'Ente
- Ricerca per Servizio: firma digitale, PEC, ecc.

Di seguito i dati relativi al servizio che verranno visualizzati:

Dati relativi al servizio
• Nome Ente • Stato della pratica • Durata del contratto (Dal – al) • Data richiesta attivazione • Data di erogazione del servizio

- Quantità fornite in ogni trimestre
- Quantità residua per ogni singolo ente rispetto ai fabbisogni dichiarati
- Quantità residua complessiva rispetto ai fabbisogni complessivi indicati nel capitolato

Sempre per ogni servizio e per ogni singolo ente (aderente o associato) verranno fornite le seguenti informazioni economiche:

Dati economico contabili relativi al servizio

- Costo unitario servizio
- Costo complessivo dei servizi attivi/attivati alla data della visura
- Importo fatturato complessivo per servizio
- Valore residuo di spesa disponibile

7.1.2 MONITORAGGIO SERVIZIO FIRMA DIGITALE

La sezione firma digitale visualizzerà una serie di informazioni di dettaglio sui certificati totali ordinati ed emessi dall'Ente di afferenza o, nel caso di utenti con profilo full, dagli Enti collegati. Ad esempio un operatore regionale full potrà visualizzare l'elenco dei certificati ordinati dalla Regione, degli Enti Aderenti e dei relativi Enti Associati.

Verranno visualizzate le informazioni aggregate a livello di ente. Per ogni ente (associato al profilo con cui l'utente si è collegato) verranno riportate le seguenti informazioni, in forma tabellare:

Dati Aggregati per Ente

- Ente
- Numero certificati richiesti
- Numero certificati emessi

L'utente, avrà a disposizione un form attraverso il quale impostare i criteri di ricerca, ad esempio:

- ente
- titolare (codice fiscale, cognome)
- data di emissione del certificato
- stato della pratica (richiesta, evasa, ecc)
- stato del certificato (valido, sospeso, revocato)
- tipologia (token, smart card, firma remota)

Dopo aver applicato un filtro, l'operatore potrà visualizzare, in forma tabellare, l'elenco dei risultati che potrà anche ordinare per ente, data della richiesta e stato della richiesta. Cliccando su una singola riga sarà poi possibile visualizzare le informazioni di dettaglio:

Dati di dettaglio di ogni singolo certificato

- Nome ente
- Titolare certificato
  - Nome
  - Cognome
  - Codice fiscale
- Data rilascio certificato
- Data scadenza certificato
- Stato del certificato (valido, sospeso, revocato)
- Tipologia (smart card, token, firma remota)

Nella sezione sarà infine possibile visualizzare alcuni indicatori dell'andamento del servizio:

Indicatori sul servizio	
Indicatore **DSFR**	Misura la percentuale di disponibilità del servizio di firma remota nel periodo di riferimento (come da Capitolato) Periodo di riferimento: trimestre
Indicatore **TRKF**	Misura la percentuale di rilascio di kit di firma che rispettano il limite di attivazione richiesto (come da Capitolato) Periodo di riferimento: trimestre

7.1.3 MONITORAGGIO SERVIZIO MARCHE TEMPORALI

La sezione visualizzerà una serie di informazioni di dettaglio sulle marche temporali acquistate ed utilizzate dall'Ente di afferenza o, nel caso di utenti con profilo full, dagli Enti collegati.
L'utente, avrà a disposizione un form attraverso il quale filtrare (se richiesto) l'ente di interesse, dopodiché, cliccando su una delle righe contenenti i risultati ottenuti, potrà visualizzare le seguenti informazioni:

Dati di dettaglio per Ente
• Nome Ente • Quantità lotto • Data di attivazione del lotto • Marche usate • Marche residue

La sezione riporterà i valori degli indicatori dell'andamento del servizio:

Indicatori sul servizio	
Indicatore **DSMT**	Misura la percentuale di disponibilità del servizio di apposizione e di verifica della marcatura temporale nel periodo di riferimento (come da Capitolato). Periodo di riferimento: trimestre

7.1.4 MONITORAGGIO CERTIFICATI SSL

La sezione visualizzerà una serie di informazioni di dettaglio sui certificati SSL acquistati ed dall'Ente di afferenza o, nel caso di utenti con profilo full, dagli Enti collegati.
L'utente, avrà a disposizione un form attraverso il quale filtrare (se richiesto) l'ente di interesse, dopodiché, ciccando su una delle righe ritrovate, potrà visualizzare i seguenti dati:

Dati di dettaglio di ogni singolo certificato
• Nome Ente • Data di rilascio certificato

- Data di scadenza certificato

7.1.5 MONITORAGGIO SERVIZIO PEC

La sezione visualizzerà una serie di informazioni di dettaglio sulle caselle PEC attivate dall'Ente di afferenza o, nel caso di utenti con profilo full, dagli Enti collegati.

In prima battuta verranno visualizzati, in forma tabellare, i dati complessivi per tutti gli enti "visibili" dal profilo:

Dati riassuntivi
• Elenco caselle PEC attive • Elenco caselle PEC revocate

Cliccando su una riga verranno visualizzati i dati specifici dell'ente selezionato:

Dati riassuntivi del singolo Ente
• Nome Ente. • Elenco caselle PEC attive • Elenco caselle PEC revocate

L'utente avrà poi la possibilità, attraverso apposito form, di impostare una serie di filtri:

- ente
- titolare (codice fiscale, cognome)
- data di attivazione
- data di (eventuale) cessazione
- stato della casella

Dopo aver applicato un filtro e selezionata una singola casella, l'operatore avrà modo di accedere alle informazioni di dettaglio della singola casella:

Dati di dettaglio di ogni singola casella

• Nome Ente
• Titolare
  ○ Nome
  ○ Cognome
  ○ Codice fiscale
• Nome casella PEC
• Stato della casella
• Data attivazione
• Data cessazione
• Tipologia (standard o avanzata)
• Casella multiutente (si/no)
  ○ Collaboratori (eventuali) abilitati alla multiutenza:
  ▪ Nome collaboratore
  ▪ Cognome collaboratore

La sezione riporterà i valori degli indicatori dell'andamento del servizio:

Indicatori sul servizio	
Indicatore **DSPC**	Misura la percentuale di disponibilità del PEC nel periodo di riferimento (come da Capitolato).

	Periodo di riferimento: trimestre.
Indicatore **QSPC**	Misura la percentuale di attivazione di nuove caselle che rispettano il limite di attivazione richiesto. Periodo di riferimento: trimestre.

7.1.6 MONITORAGGIO SERVIZIO DI CONSERVAZIONE

La sezione visualizzerà una serie di informazioni di dettaglio sul servizio di conservazione relativo all'Ente di afferenza o, nel caso di utenti con profilo full, agli Enti collegati.
La pagina visualizzerà, in forma tabellare, le seguenti informazioni riassuntive

Dati riassuntivi
• Nome Ente • Quantità documenti conservati • Dimensione totale (Gb) documenti conservati

L'utente, avrà a disposizione un form attraverso il quale filtrare l'ente di interesse (ricerca per "sottostringa"), dopodiché, cliccando su una delle righe contenenti i risultati ottenuti, potrà visualizzare le seguenti informazioni:

Dati di dettaglio per Ente
• Nome Ente • Data attivazione servizio • Quantità documenti conservati • Dimensione totale (Gb) documenti conservati

La sezione riporterà i valori degli indicatori dell'andamento del servizio:

Indicatori sul servizio	
Indicatore **DSCO**	Misura la percentuale di disponibilità del servizio di conservazione nel periodo di riferimento (come da Capitolato). Periodo di riferimento: trimestre.
Indicatore **QSCO**	Qualità del servizio di conservazione la percentuale di attivazione di nuove caselle che rispettano il limite di attivazione richiesto. Periodo di riferimento: trimestre.

7.1.7 MONITORAGGIO SERVIZIO HELP DESK

La sezione visualizzerà una serie di informazioni di dettaglio sul servizio di assistenza erogato relativo all'Ente di afferenza o, nel caso di utenti con profilo full, agli Enti collegati.
La pagina visualizzerà, in forma tabellare, le seguenti informazioni riassuntive

Dati riassuntivi
• Nome Ente • Numero complessivo di richieste di assistenza. • Elenco complessivo dell'esito delle richieste di assistenza.

Cliccando sul singolo Ente, verranno visualizzate, in forma tabellare, le seguenti informazioni:

Dati riassuntivi
• Tipologia ticket • Stato del ticket • Data e ora apertura ticket • Data e ora chiusura ticket • Descrizione richiesta di assistenza

La sezione riporterà, inoltre, i valori degli indicatori dell'andamento del servizio:

Indicatori sul servizio	
Indicatore **DSHD**	Misura il tempo di indisponibilità del servizio considerando la finestra di servizio nel periodo di riferimento. Periodo di riferimento: trimestre.
Indicatore **QSHD**	Misura il tempo medio di risposta telefonica da parte dell'operatore del call center Periodo di riferimento: trimestre.
Indicatore **TRHD**	Misura il tempo di attesa tra la formulazione di una richiesta e la sua completa evasione Periodo di riferimento: trimestre.

7.1.8 MONITORAGGIO SERVIZIO DI SUPPORTO E FORMAZIONE

La sezione visualizzerà una serie di informazioni di dettaglio sul servizio di supporto e formazione assistenza erogato relativo all'Ente di afferenza o, nel caso di utenti con profilo full, agli Enti collegati. Il sistema consentirà la verifica delle richieste di formazione e supporto pervenute consentendo ad esempio l'utilizzo di filtri e ordinamenti per ente data di attivazione ecc..

La pagina visualizzerà, in forma tabellare, le seguenti informazioni riassuntive

Dati riassuntivi
• Nome Ente • Giorni di formazione • Giorni di supporto

Gli amministratori di sistema avranno la possibilità di aggiornare i suddetti dati mediante apposite pagine web.

7.1.9 MISURE DI ANDAMENTO DEL SERVIZIO

Le pagine di monitoraggio hanno lo scopo di tenere sotto controllo il reale andamento di tutti i servizi erogati. A questo scopo riteniamo molto utile raccogliere tutti gli indicatori descritti nei precedenti paragrafi, all'interno di un'unica pagina, in modo da avere una vista immediata e sintetica della situazione generale dei sistemi coinvolti, rimandando alle specifiche sezioni dei singoli servizi per gli eventuali approfondimenti.

7.2 DOCUMENTAZIONE MESSA A DISPOSIZIONE

Aruba PEC fornirà un manuale d'uso della consolle di monitoraggio che descriverà tutte le funzionalità messe a disposizione, profilate per tipologia di utente e per i relativi Enti di afferenza.

L'interfaccia verrà inoltre corredata di help contestuale per un aiuto immediato e sintetico durante l'utilizzo dello strumento.

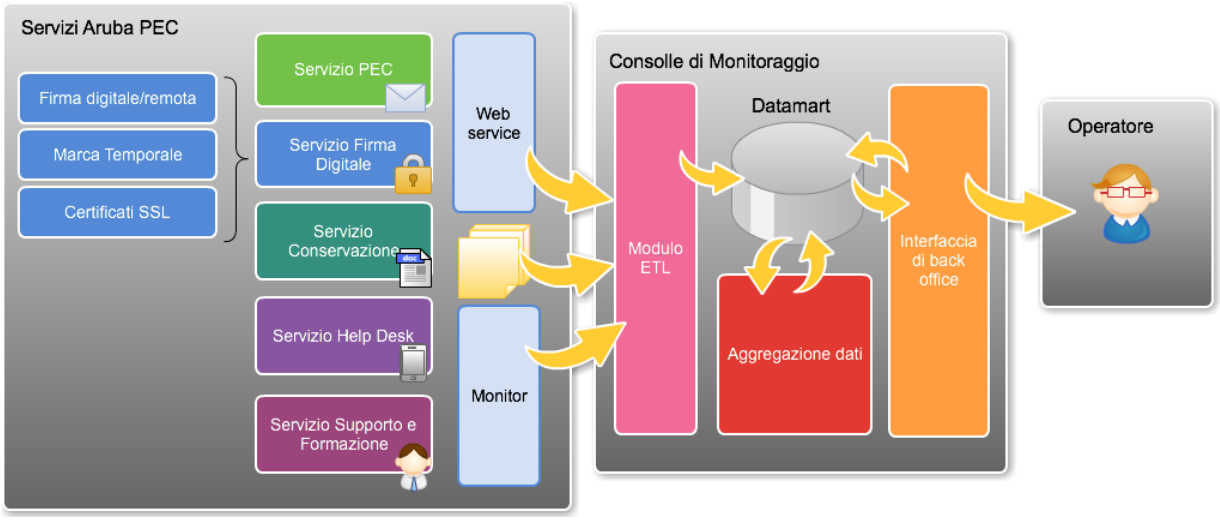
7.3 FUNZIONALITA' AGGIUNTIVE

Aruba PEC metterà a disposizione per gli utenti della Regione Veneto – oltre alla fornitura di manualistica tecnica – ulteriore elemento migliorativo caratterizzato dalla possibilità di richiedere **contatto outbound** da parte di un operatore Help Desk tramite la funzione **Call me Back**, che verrà estesa anche al **Pannello Unico di Gestione** (oltre che alla sezione **FAQ** del **Sito Web dedicato**). In tal modo ciascun utente potrà interagire direttamente con un operatore al fine di poter approfondire modalità d'uso ed informazioni riscontrate nella sezione di help contestuale e nella manulaistica tecnica.

Il sistema di rilevazione dei livelli di servizio - incluso all'interno della Consolle di Monitoraggio – fornisce un monitoraggio giornaliero dello stato dei servizi previsti nella fornitura di gara.
La Consolle di Monitoraggio sarà costituita da:

- un modulo di ETL per il recupero delle informazioni dai vari servizi
- un database di supporto (datamart) contenente le informazioni da visualizzare
- un modulo di post elaborazione per l'aggregazione dei dati
- un'interfaccia utente (di back office)

Viene di seguito riportato un diagramma riassuntivo del sistema proposto:



I singoli servizi metteranno a disposizione le informazioni attraverso appositi web service e/o file piatti. Le informazioni necessarie a calcolare i valori di performance dei livelli di servizio (SLA) vengono infatti recuperate nelle due seguenti modalità - tramite un modulo ETL che funge da interfaccia con la base dati Datamart:

1. lettura dei dati direttamente da Web Service o sistema di monitoring del singolo servizio
2. elaborazione di script per il recupero dei dati da file in sola lettura

Il modulo ETL preleva con frequenza automatica – tramite protocolli di sicurezza (HTTPS, ACL, LDAP, etc.) - le informazioni dai vari servizi tramite le precedenti modalità, in seguito provvede all'elaborazione dei dati ed aggregazione nella base dati Datamart.
Il Datamart rappresenta la base storica delle informazioni monitorate e conterrà le informazioni necessarie alla fase di post-elaborazione che alimenterà i dati visibili attraverso l'interfaccia utente della Consolle di Monitoraggio.
Gli indicatori previsti dal capitolato - e descritti nei paragrafi precedenti - verranno calcolati in fase di post-elaborazione e visualizzati nella Consolle di Monitoraggio.
La frequenza di recupero delle informazioni tramite modulo ETL e la successiva aggregazione nella base dati Datamart – verrà concordata tra le parti in sede di startup di progetto. Se ritenuta sufficiente, la frequenza può essere giornaliera e le operazioni di recupero ed aggregazione dei

dati potrebbero essere effettuate in orario notturno. In alternativa sarà possibile incrementare la frequenza in modo da avere un aggiornamento dei dati più volte al giorno.
L'interfaccia utente della Consolle di Monitoraggio prevede un adeguato livello di qualità e completezza delle informazioni messe a disposizione, in quanto tutti gli indicatori del livello di servizio saranno accessibili tramite un'unica pagina web.
L'interfaccia utente prevede un facile utilizzo (user-friendly) ed immediata visualizzazione dei valori aggiornati dei livelli di servizio in fornitura. La semplicità d'uso da parte dell'utente è garantita tramite le seguenti caratteristiche della consolle:

- rapido accesso alle sezioni di interesse per singolo servizio attraverso appositi link ipertestuali
- visualizzazione dei dettagli sul singolo Ente aderente attraverso filtri di selezione
- immediata analisi delle informazioni per periodo storico attraverso possibilità di drill-down (e drill-up)

La robustezza della Consolle di Monitoraggio proposta è infine garantita dal fatto che le informazioni necessarie al monitoraggio – reperite tramite Web Services oppure file dati – risiedono all'interno dell'infrastruttura fisica dei singoli servizi.