REGIONE DEL VENETO

Regione del Veneto
Direzione Sistemi Informativi
U.C. e-Government e Società dell'Informazione

Servizi Posta Elettronica Certificata
Firma digitale
Conservazione a norma

Descrizione dei servizi

Versione **1.0**

INDICE

1 APPROVAZIONI

Attività	Nominativo	Azienda
Redazione	Rossano Favaretto Luca Menegale Luca Boldrin	Regione del Veneto InfoCert InfoCert
Verifica	Roberto Costantin	Regione del Veneto
Approvazione	Andrea Boer	Regione del Veneto

2 STORIA DELLE MODIFICHE

Versione	Data	Descrizione

3 RIFERIMENTI

N.	Titolo	Autore	URL
1	Manuale Utente_Legalmail.pdf	Infocert	http://www.legalmail.it/upload/ManualeUtente_Legalmail.pdf
2	Manuale UtenteToken USB	Infocert	
3	RVE-Infocert-Servizi v.1.0	Regione del Veneto	

4 SCOPO DEL DOCUMENTO

I servizi descritti nel documento sono quelli offerti dalla società Infocert S.p.A. vincitrice della gara indetta con DGR n 1006 del 23/03/2010, "Fornitura dei servizi di firma digitale, marcatura temporale e conservazione sostitutiva a norma dei documenti informatici, nonché di posta elettronica certificata ed help desk a favore della Regione del Veneto e degli Enti Locali veneti", bando di gara pubblicati nel GUCE in data 25/6/2010 con numero 2010/S 121-184372.
Scopo del documento è descrivere le caratteristiche dei servizi di firma digitale, posta elettronica certificata e conservazione a norma messi a disposizione da parte della Regione del Veneto agli enti locali.
Le modalità di rilascio dei servizi agli Enti Locali Veneti sono descritte nel documento RVE-Infocert-ErogazioniServizi v.1.0 e s.m.i.
Per quanto riguarda le modalità di utilizzo sarà invece necessario fare riferimento agli specifici manuali utente che dettagliano le funzionalità e gli strumenti di lavoro.

5 FIRMA DIGITALE

5.1 Descrizione dei kit fomiti per la firma digitale

I Kit di firma forniti rispettano la normativa vigente, ed in particolare la deliberazione DigitPA 45/2009 e la determinazione commissariale 69/2010.
Il kit di firma consegnato al Titolare si compone di:

- Token USB
- il codice di attivazione (PIN/PUK), il codice di emergenza per la sospensione del certificato (ERC) e l'identificativo univoco del titolare (IUT). Tali codici verranno comunicati via e-mail in modalità sicura.
- Le condizioni generali del contratto e le prime istruzioni.

5.2 Caratteristiche dei device Token USB

Per Token USB si intende una chiavetta USB portatile che può essere utilizzata su qualsiasi PC senza necessità di installazione di software. Il software a bordo dei Token USB dispone di una funzionalità di aggiornamento automatico.
Il Token USB fornisce le funzionalità di un dispositivo di firma digitale unitamente a quelle di una memoria flash aggiuntiva. Il Token USB, include i seguenti dispositivi:

- memoria flash
- lettore/scrittore SIM Card destinato a contenere un chip crittografico in formato SIM (Plug-in).

Inoltre sono configurati per

- Max numero dei tentativi PIN: 3
- PIN e PUK: 8 digit
- Sbloccabile mediante tool all'interno del dispositivo

La memoria flash ha le seguenti caratteristiche :

- capacità disponibile pari a 4 GB;
- compatibile con driver CCID e/o HID dei sistemi operativi Windows, con driver HID per i sistemi Mac e Linux
- interfaccia USB 2.0 Full Speed;
- data Retention almeno pari a 10 anni;
- cicli di scrittura/cancellazione almeno pari a 100.000;
- *fast read* (fino a 10MB/s);
- velocità di scrittura (fino a 6MB/s).

Requisiti della stazione utente:

- Sistema operativo: Windows XP o superiori
- Sistema operativo MAC OSX 10.5 e successivi
- Sistema operativo Fedora, Ubuntu 9.0.0 e succ, RedHat
- Porta USB: 2.0
- Browser compatibile con tecnologia Applet Java; JVM versione 1.4.x o superiore

5.3 Certificati per Token USB

Il dispositivo contiene le chiavi per i seguenti certificati X509v3:

- **Un Certificato Qualificato di Sottoscrizione:** emesso da InfoCert secondo quanto previsto dal Codice dell'Amministrazione Digitale; le firme apposte con le chiavi private associate a questi certificati hanno il valore di una firma autografa.
- **Un Certificato di Autenticazione:** il cui scopo è consentire l'accesso sicuro a siti e portali web che implementino il protocollo HTTPS (SSL3.0/TLS1.0), autenticando in maniera forte l'utente che cerca di accedere. I certificati possono essere utilizzati anche per funzioni di Smart Log-on, ovvero per autenticarsi e fare log-in da un PC Windows al dominio utilizzando la propria Smart Card o il Token USB senza dover digitare user-id e password

Tutti i certificati di firma qualificata succitati vengono firmati con algoritmo sha256withRSAEncryption.
La chiave RSA ha una lunghezza minima di 1024 bit.
I certificati hanno al massimo una durata di tre anni e sono rilasciati a persone fisiche.
Tutte le estensioni e gli attributi dei certificati sono allineati alla normativa vigente sulla firma digitale.

5.4 Software

I Token USB contengono **preinstallate** tutte le funzionalità di **firma, marca e verifica** descritte **e di rinnovo**.
Il Token USB, dispone inoltre di un insieme di applicazioni "portable" precaricate che sono integrate con il dispositivo crittografico componendo così un sistema auto consistente, pur mantenendo l'usabilità da parte di applicazioni client o altri software in esecuzione sul sistema ospitante
I Token USB vengono riconosciuti automaticamente dai sistemi operativi nel momento in cui vengono inseriti nella porta USB.

E' possibile usare il Token USB come se fosse una Smart Card ovvero con i programmi installati sulla propria postazione.

Il ripristino del token è possibile a partire da un eventuale back-up eseguito con la funzione apposita.
Inoltre c'è la possibilità, attraverso il sito InfoCert dedicato ai Token USB (www.firma.InfoCert.it), di ripristinare completamente il Token a fronte di malfunzionamento o perdita accidentale del software.

Gli aggiornamenti del Software avvengono in **maniera automatica** previa autorizzazione del titolare.
Ogni aggiornamento normativo o una nuova CA accreditata vengono tempestivamente recepiti. Ed eventuali malfunzioni vengono corrette velocemente sempre attraverso l'aggiornamento automatico.

5.4.1 Applicazioni portable

Oltre all'applicazione di firma/verifica, sono presenti nel token le seguenti applicazioni e servizi:

- Browser Mozilla Firefox Portable con il quale è possibile gestire, unificandole, tutte le user-id e le password utilizzate per accedere in maniera sicura ai siti web
- Antivirus.
- Cool PDF Reader.
- Utility di back-up.
- Area cifrata per proteggere eventuali documenti contenenti informazioni sensibili e/o riservate.

5.4.2 Dike

Il software Dike nella versione Lite è già presente nella Businsess Key. Dike consente operazioni di firma e verifica nelle modalità previste dalla normativa vigente ed è compatibili con i dispositivi descritti precedentemente.
Il software proposto per la fornitura verrà distribuito con licenza d'uso perpetua a tutti i Titolari.
Il software sarà mantenuto aggiornato alle ultime regole tecniche sulla firma digitale. In particolare sui formati di firma si fa riferimento alla deliberazione DigitPA 45/2009 (nel seguito riferita come deliberazione) e successiva DigitPA Determinazione Commissariale n. 69/2010 .
Dike è inoltre disponibile nelle seguenti versioni:

- DiKe/DiKe Util per client windows
- DiKeX per MacOS 10.5 e successive
- DiKeL per Ubuntu 9.0.0 e sup , Fedora

- DiKe lite presente nel token USB
- DiKeX lite per MacOS nel token USB

Funzionalità di verifica

- Verifica file firmati, *con chiavi certificate da qualunque dei certificatori accreditati*.
- I certificati root delle Certification Authority accreditate sono memorizzate in un repository sicuro.
- Aggiornamento tempestivo e automatico della lista dei certificatori accreditati a fronte di un nuovo certificatore accreditato presso DigitPA
- Verifica file in formato DER (Distinguished Encoding Rules) o Base64 (RFC 4648)
- Verifica file firmati la cui impronta è stata generata con algoritmo di hash SHA1
- Verifica file firmati la cui impronta è stata generata con algoritmo di hash SHA256
- Verifica file firmato in formato PKCS#7 (RFC 2315) nel rispetto dei termini e delle scadenze di legge
- Verifica file firmato contenente firme parallele in formato PKCS#7 nel rispetto dei termini e delle scadenze di legge
- Verifica file firmato contenente controfirme in formato PKCS#7 nel rispetto dei termini e delle scadenze di legge
- Verifica file firmato in formato CADES-BES nelle modalità previste dalla *deliberazione*. Il formato CADES: CMS Advanced electronic signature è definito in ETSI TS 101 733
- Verifica file firmato contenente firme parallele in formato CADES-BES nelle modalità previste dalla *deliberazione*.
- Verifica file firmato contenente controfirme in formato CADES-BES nelle modalità previste dalla *deliberazione*.
- Verifica file firmato e marcato in formato CADES-T nelle modalità previste dalla *deliberazione*.
- Verifica file firmato in formato XML Signature, nelle modalità previste dalla *deliberazione*
- Verifica file firmato in formato PADES nelle modalità previste dalla *deliberazione*. Il formato PADES: PDF Advanced electronic signature è definito da ETSI TS 102 778
- Verifica file firmato e marcato formato PADES-T nelle modalità previste dalla *deliberazione*.
- Verifica marche temporali nel formato TSR, e TST come definiti in RFC 3161
- Verifica file firmati e marcati nei formati M7M (standard mime multipart), TSD (Time Stamped Data RFC5544)
- Verifica del file firmato alla data della marca temporale, del signing-time (attributo descritto in PKCS#7, CADES e PADES) o da input utente
- Estrazione del documento originale dal file firmato
- Estrazione del documento originale da file firmato e marcato
- Estrazione della marca da file firmato e marcato

Funzionalità specifiche per il dispositivo

- Attivazione dispositivo (Token USB o Smart Card)
- Cambio PIN
- Sblocco PIN
- Possibilità di scegliere tra più lettori di Smart Card/Token USB
- Verifica contenuto Smart Card/Token USB
- Visualizzazione attributi (sintetica e/o dettagliata) dei certificati contenuti nel dispositivo.

5.5 Servizio di firma remota

Il "Servizio di Firma remota Massiva" di InfoCert, reso disponibile con tecnologia Web Services in modalità ASP, permette l'apposizione di firme digitali in modo automatico, nel rispetto della normativa vigente, su un grande numero di documenti inviati da una definita procedura.
Il servizio è fruibile applicativamente mediante web services. Sono disponibili delle API java/dll per l'integrazione.
La firma digitale di un documento si realizza attraverso l'utilizzo di una chiave privata associata ad un certificato qualificato e che risiede a bordo di un dispositivo sicuro diverso dalla classica SmartCard
In questo contesto, la chiave privata del titolare viene generata in fase di attivazione all'interno di un'infrastruttura sicura presso InfoCert (HSM) a cui viene assegnato univocamente un certificato qualificato specifico per firme massive (così come stabilito dal D.Lgs n.82 del 07 marzo 2005).
La firma dei documenti avviene attraverso una procedura automatica sviluppata e gestita da InfoCert. Il titolare non è in possesso del dispositivo, ed esercita comunque il controllo esclusivo del dispositivo attraverso l'applicazione chiamante e relative credenziali, e attraverso una interfaccia web dedicata

direttamente presso il servizio di firma InfoCert che permette in qualsiasi momento di bloccare/sbloccare il proprio certificato.
L'applicazione chiamante calcola gli hash dei files oggetto di firma e, assieme alle credenziali dell'utente, li inoltra al servizio di firma remota per la firma.
Il servizio ritorna gli hash firmati, il relativo certificato qualificato ed eventualmente il riferimento temporale, l'applicazione chiamante imbusterà il tutto (firma e riferimento temporale) in tanti files p7m o PDF-embedded quanti sono i files sorgenti da firmare.
Tutta la comunicazione che coinvolge la trasmissione degli Hash e delle credenziali del titolare è rigorosamente cifrata su protocollo HTTPS per garantire la riservatezza dei dati.
Il servizio è stato realizzato in conformità al Codice dell'Amministrazione digitale (Decreto legislativo 5 marzo 2005, n. 82) che comprende anche le norme relative all'utilizzo della firma digitale per i documenti informatici, e alle specifiche regole tecniche vigenti.

5.6 Marcatura temporale

Il servizio di marcatura temporale è fruibile mediante il client Dike oppure applicativamente mediante web services. Sono disponibili delle API java/dll per l'integrazione.
Il formato e le caratteristiche di emissione delle marche temporali sono definite dalla Regole Tecniche e si basano su standard internazionali
Le marche temporali emesse da InfoCert si basano su un certificato avente validità di quattro anni, tuttavia InfoCert, in qualità di erogatore del servizio, conserva tali marche per il periodo richiesto dalle norme in vigore (attualmente 20 anni).
La marca temporale è emessa automaticamente da un sistema elettronico sicuro TSU (Time Stamping Unit); il TSU per firmare si avvale di un dispositivo HSM contente le chiavi di firma certificate dalla Time Stamping Authority o TSA dell'Ente Certificatore InfoCert.
L'Ente Certificatore appone la marca temporale nelle modalità descritte in al manuale operativo https://www.firma.InfoCert.it/documentazione/manuali.php.

6 Posta Elettronica Certificata

Lo strumento di Posta Elettronica Certificata LegalMail è fruibile mediante client di posta (Outlook, Thunderbird, etc.), tramite interfaccia Webmail oppure, applicativamente, mediante opportune librerie di integrazione. Le configurazioni necessarie all'utilizzo sono descritte in http://www.legalmail.it/configurazione/index.php

6.1 Interfacciamento delle caselle PEC con software gestionali delle Amministrazioni

Vengono rese disponibili, a richiesta, le Librerie proprietarie Java CRML API (CeRtified MaiL Application Program Interface) per velocizzare e semplificare la realizzazione di applicazioni che si interfacciano ai servizi Legalmail
Le librerie implementano le funzionalità di accesso e di invio, consentendo di:

- comporre messaggi;
- inviare messaggi;
- accedere alle caselle Legalmail
- accedere alle caratteristiche dei messaggi ricevuti nella casella

Le librerie consentono l'invio e la ricezione dei messaggi attraverso i server PEC di InfoCert, gestendo in automatico tutte le problematiche di sicurezza sottostanti ed in particolare la verifica dei certificati server. Tali librerie sono, ad esempio, già utilizzate dal protocollo di Regione Veneto e di altre amministrazioni.
I servizi di consulenza forniti all'interno della presente offerta includono il supporto all'integrazione.
Si segnala inoltre che il sistema di protocollo InfoCert, in uso presso diverse amministrazioni, integra nativamente l'invio e la ricezione di messaggi tramite caselle di posta elettronica certificata LegalMail.

6.2 Funzionalità

Le caselle di Posta Elettronica Certificata Legalmail forniscono tutte le funzionalità previste dalla normativa nonché quelle opzionali di seguito riportate:

6.2.1 Gestione messaggi non PEC

E' disponibile la funzione che permette di configurare la casella Legalmail rispetto ai messaggi provenienti da account non PEC. In particolare è possibile:

- rigettare i messaggi non PEC, avvisando il mittente.
- inoltrare i messaggi non PEC ad un diverso account (non PEC)
- accettare i messaggi non PEC (che vengono quindi gestiti come anomalie)

6.2.2 Casella multiutente

InfoCert mette a disposizioni la casella **Legalmail multiutente** che include funzionalità peculiari aggiuntive alle caratteristiche professionali già presenti nel servizio Legalmail standard:

- possibilità di avere più user/password per l'accesso alla casella Legalmail;
- definizione di una user "master": l'unica che può configurare le diverse opzioni, i filtri e i servizi aggiuntivi quali ad esempio l'Archivio di Sicurezza e la Notifica SMS;
- definizione di più user "base" che possono accedere alla casella, leggere/inviare messaggi e consultare l'Archivio di Sicurezza;
- tracciatura degli utenti che hanno utilizzato la casella Legalmail.

Ed inoltre:

- l'accesso alla casella può avvenire sia da client (Outlook, Thunderbird, …) che da webmail;
- le diverse user hanno una gestione della password separata: ogni utente definisce/modifica la propria password;
- nei log di sistema vengono registrate e mantenute separate le operazioni effettuate delle varie userid; in particolare:
- da webmail vengono registrati, per singola user, le informazioni (log) relative a:
    - login/logout,
    - invio dei messaggi,
    - prima lettura di un messaggio,
    - cancellazione di un messaggio;

- da client di posta (Outlook, Thunderbird, ecc.) vengono registrati, per singola user,
- le informazioni (log) relative a:
- login/logout
- invio dei messaggi

La configurazione della casella multiutente prevede una user “master” e una o più user “base”, sino ad un massimo di 25 user in totale.

6.2.3 Capacità casella

La capacità delle caselle standard è complessivamente di 10 GB (2 casella + 8 archivio di sicurezza). La casella gestisce l'invio di messaggi fino a 50 MB.

6.2.4 Spazio disco

Lo spazio disco della casella può essere esteso, su richiesta al Centro Servizi.

6.2.5 Filtro automatico

Le funzioni di filtro presenti in webmail consentono di preimpostare una serie di condizione multiple, a livello di mittente, oggetto e contenuto che, una volte soddisfatte, indirizzino o copino i messaggi in ingresso su diverse cartelle.
Il servizio per essere attivo deve essere configurato da parte del titolare della casella PEC vedi manuale utente (http://www.legalmail.it/documentazione/generiche.php).

6.2.6 Traffico illimitato

Le caselle standard sono fornite con traffico illimitato.

6.2.7 Antispam e antivirus

InfoCert mette a disposizione delle caselle Legalmail un servizio antispamming ad alte prestazioni, configurabile da webmail. E' possibile scegliere che tutti i messaggi ritenuti spam dal sistema Legalmail vengano direttamente eliminati o automaticamente spostati un una cartella di posta indesiderata. Le caselle Legalmail dispongono di antivirus aggiornato più volte al giorno.
Ogni casella è già configurata con le impostazioni di base ma è possibile, per il titolare, intervenire mediante webmail per personalizzare le regole di antispam.

6.2.8 Inoltro automatico

La funzione di Inoltro Automatico consente di reinviare automaticamente i messaggi in entrata nella casella Legalmail verso un'altra casella, standard o certificata.
Questa funzione è molto importante in quanto la casella PEC è usualmente una casella utilizzata per attività specifiche e probabilmente meno consultata rispetto alle caselle standard.

6.2.9 Firma e crittografia da webmail

L'indirizzo Legalmail dell'utente può essere associato al certificato di autenticazione e può essere utilizzato per firmare il messaggio PEC in partenza, attraverso la specifica funzione presente su webmail; in tal modo il destinatario ha la possibilità di riconoscere con certezza il mittente con tutte le informazioni certificate.
Inoltre, i messaggi in partenza possono essere crittografati da webmail, utilizzando la chiave pubblica del certificato di autenticazione del destinatario, garantendo in tal modo l'assoluta riservatezza della trasmissione.

6.2.10 Archivio di sicurezza

L'archivio di Sicurezza messo a disposizione all'interno del servizio dispone di molte funzionalità. Il cliente attraverso webmail può configurare le diverse opzioni di salvataggio, che permettono di coprire tutte le esigenze.
Il cliente può decidere autonomamente di archiviare:

- tutti i messaggi in entrata
- tutti i messaggi in uscita
- oppure alcune tipologie specifiche degli stessi, quali:
  - i messaggi certificati in entrata;
  - i messaggi non certificati in entrata;
  - tutte le ricevute;

- le ricevute di accettazione;
- le ricevute di consegna;
- i messaggi inviati ad un destinatario certificato;
- i messaggi inviati a destinatari non certificati.

E' possibile scegliere una combinazione fra le diverse tipologie.
Il cliente può modificare nel tempo e a suo piacimento la combinazione scelta dei nuovi messaggi da salvare.
Tramite specifiche funzioni, l'utente può effettuare una ricerca dei messaggi archiviati utilizzando un'ampia serie di parametri: dalla ricerca nei singoli campi (o una combinazione degli stessi) alla ricerca testuale sull'intero messaggio.
I messaggi archiviati possono eventualmente anche essere cancellati dall'utente.
Il cliente può accrescere la dimensione dell'Archivio di Sicurezza della sua casella acquisendo ulteriori blocchi da un Gigabyte.
L'archivio di sicurezza non svolge funzioni di conservazione a norma dei documenti. Costituisce solo un supplemento di spazio a disposizione della casella e copia di sicurezza delle mail.
Il servizio per essere attivo deve essere configurato da parte del titolare della casella PEC vedi manuale utente (http://www.legalmail.it/documentazione/generiche.php).

6.2.11 Servizio SMS

I messaggi di Posta Elettronica Certificata hanno valenza legale e si intendono ricevuti al momento del deposito nella propria casella certificata: quindi è importante verificare frequentemente il contenuto della propria casella.
Legalmail mette a disposizione il servizio di notifica SMS per informare l'utente della presenza di nuovi messaggi in arrivo nella sua casella.
Il servizio controlla quotidianamente, ad un'ora prestabilita dal cliente, la presenza di nuovi messaggi di posta certificata non letti e, in caso positivo, invia un messaggio SMS di notifica della ricezione al numero di cellulare indicato dal Cliente.
Si fa presente che il servizio non controlla le ricevute e i messaggi di posta non certificata.
Il servizio prevede non più un messaggio di notifica al giorno, per un massimo di 365 messaggi annui.
Il servizio per essere attivo deve essere configurato da parte del titolare della casella PEC vedi manuale utente (http://www.legalmail.it/documentazione/generiche.php).

6.2.12 Firma e crittazione tramite smart card

Il servizio permette l'utilizzo di firma e crittografia con smart card e token InfoCert. In particolare l'interfaccia webmail permette la firma e crittazione dei messaggi in invio e le relative verifiche e decrittazione in fase di ricezione.

6.3 Riepilogo caratteristiche casella PEC

CARATTERISTICHE	
Spazio Casella	10 GB (2 di posta + 8 di archivio sicurezza)
Dimensione max messaggio	50 MB
Numero Max Destinatari per mail inviata	500 totali
Archivio di sicurezza	8 GB
Antivirus	Presente come da normativa
Antispam	Attivo e configurabile dall'utente
Ricezione mail non certificate	A scelta dell'utente
Accesso Webmail	SI

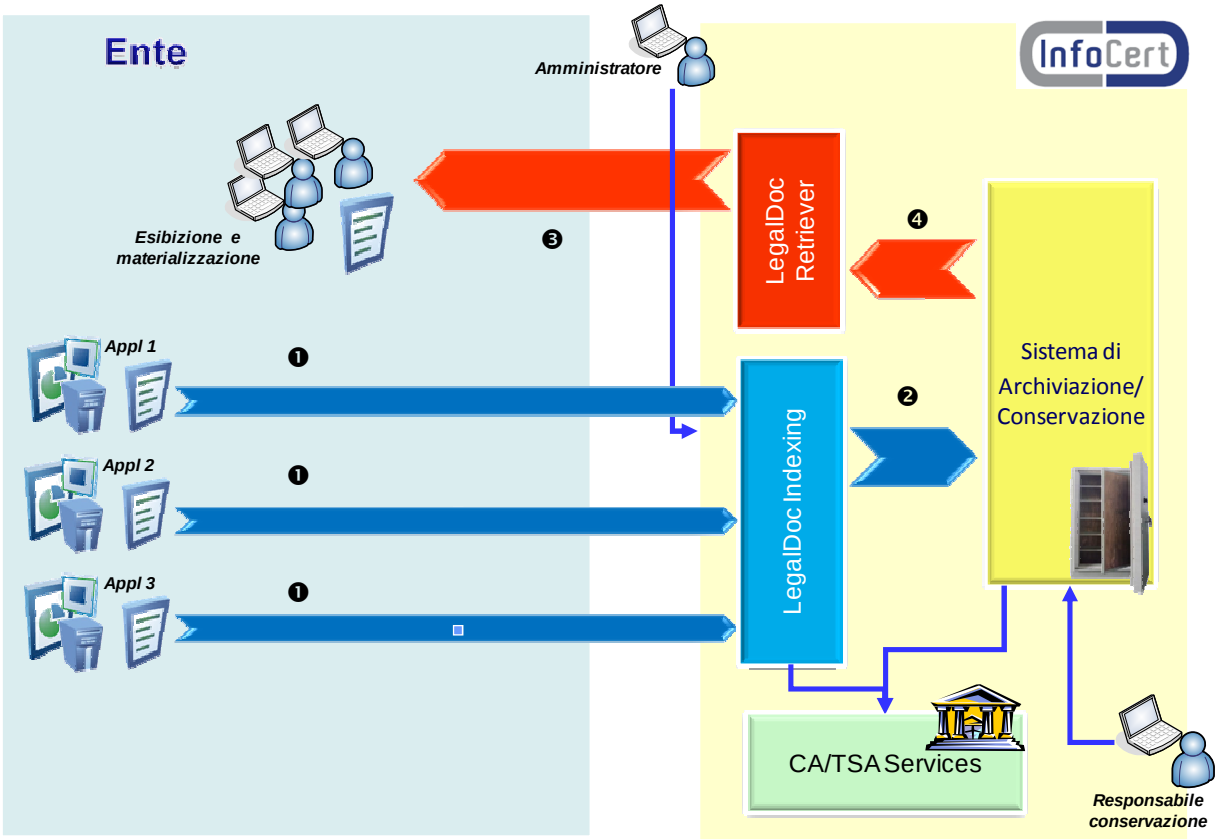
Filtri e regole per i messaggi in arrivo	SI e configurabile dall'utente
Accesso tramite client di posta	SI
Servizio SMS	SI
Traffico illimitato	SI
Casella Multiutente	SI
Ricezione mail non certificate	SI e configurabile dall'utente
Inoltro automatico messaggi ad altra casella	Attivabile da Webmail
Utilizzo da client di posta	SI
Firma digitale del messaggio	SI
Crittografia del messaggio	SI

7 Servizio di Conservazione a norma

Il servizio di conservazione a norma LegalDoc garantisce la conservazione sostitutiva dei documenti nel pieno rispetto della normativa vigente. LegalDoc permette di conservare un documento in maniera sostitutiva anche a partire da un originale cartaceo.
La firma digitale del Responsabile della Conservazione e la marca temporale conferiscono ai documenti pieno valore legale.
I file sono archiviati sui sistemi di InfoCert che, in qualità di Responsabile della Conservazione, ne garantisce la piena integrità, leggibilità ed accessibilità per tutto il tempo previsto dalla normativa di riferimento. I documenti conservati con LegalDoc sono sempre disponibili e la loro esibizione è opponibile a terzi.

7.1 Tecnologie e strumenti utilizzati nell' erogazione del servizio

Il servizio, consente la gestione del flusso di conservazione con relativi metadati in ASP. In questo modo il Cliente è svincolato dalle problematiche di gestione sicura dei documenti e metadati, controllo dei processi di creazione lotti, indicizzazione, marcatura, etc., poiché tali processi vengono svolti dal servizio ASP, sotto il presidio del fornitore.
Il sistema si propone in due diverse modalità. La prima modalità prevede l'invio diretto al sistema di conservazione da parte dei sistemi del cliente, tramite interfacce applicative.



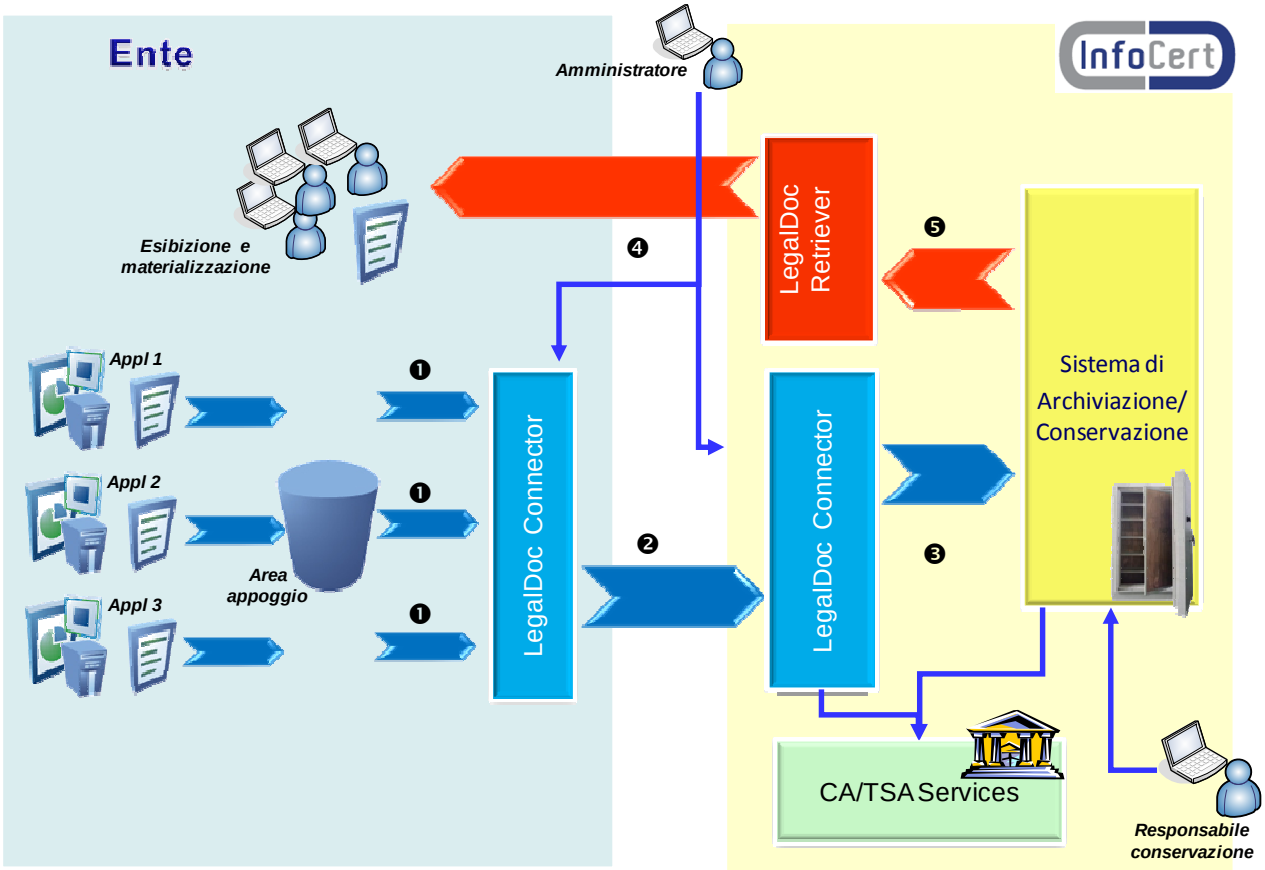
Architettura di conservazione con invio diretto

L'architettura è suddivisa in 3 sottosistemi:

- **LegalDoc Indexing**, che realizza la gestione dei metadati di indicizzazione del documento
- **LegalDoc Core.** E' il cuore del sistema, che gestisce la creazione dei lotti di conservazione, la loro firma da parte del Responsabile della Conservazione e la marcatura temporale. Mette a disposizione strumenti per la validazione nel tempo dei documenti conservati
- **LegalDoc Retriever**, che consente la ricerca del documento per indici e il reperimento dell'oggetto dal sistema ASP. Il documento viene quindi validato rispetto alle evidenze di conservazione. Alla fine

del processo di validazione, il documento completo e le evidenze di conservazione associate sono resi disponibili

La seconda modalità prevede l'invio in conservazione mediato da un tool fornito da InfoCert che semplifica l'interfacciamento applicativo. In questo caso le applicazioni del cliente si preoccuperanno soltanto di depositare i documenti da conservare e i relativi indici (all'interno di files xml con un opportuno tracciato) in un'area di appoggio. L'applicazione LegalDoc Connector si preoccuperà dell'acquisizione e dell'invio in conservazione dei documenti, gestendo tutte le opportune segnalazioni (completamento, errore, …) verso il cliente.



Architettura di conservazione con invio mediato

Il questa seconda modalità il normale flusso di conservazione e esibizione, secondo la numerazione in figura, prevede:

1. recepimento di documenti/indici depositati in un'opportuna area di lavoro
2. il trasporto dei documenti/indici presso il sistema ASP.
3. presso il servizio ASP: l'attivazione degli indici e il deposito dei documenti presso il servizio di conservazione
4. in fase di esibizione, la ricerca dei documenti tramite gli associati indici di ricerca. L'utilizzo degli indici di ricerca remoti offre garanzia di alta affidabilità e di mantenimento nel tempo degli stessi.
5. l'estrazione del documento con le rispettive evidenze di conservazione, dal sistema di conservazione

Questa seconda soluzione può essere estesa con opportuni connettori ad hoc verso specifiche applicazioni.

7.2 LegalDoc Core e Preservation Services

LegalDoc Core gestisce la fase relativa allo "stoccaggio digitale" e alla memorizzazione del documento ai fini della sostituzione e mantenimento della validità legale nel tempo.
LegalDoc, consente la conservazione sostitutiva di documenti informatici, costituiti da uno o più file che possono essere o meno firmati digitalmente, e l'esibizione a norma dei documenti conservati.

In LegalDoc un documento è un insieme di uno o più file digitali, anche di diverse tipologie, con dati di indicizzazione facoltativi. Ad ogni documento è associato un identificativo univoco generato da LegalDoc. In LegalDoc un documento rappresenta l'unità minima di elaborazione nel senso che viene memorizzato ed erogato come un tutt'uno. Non è possibile consultare parti di un documento
Nello specifico, il servizio di conservazione prevede le seguenti funzionalità:

- la conservazione sostitutiva, tramite invio telematico, di un documento informatico o di un documento analogico opportunamente digitalizzato;
- la ricerca e l'esibizione di un documento già conservato in modalità sostitutiva;
- il rispetto degli adempimenti previsti dalla normativa relativi alla sicurezza fisica e logica dell'archivio dei documenti conservati costitutivamente e dell'intero procedimento di conservazione sostitutiva in maniera automatizzata (compresa la firma e marca).
- la gestione automatica degli adempiti previsti per il responsabile della conservazione (ad. Es. controllo automatico con cadenza inferiore ai 5 anni sulla leggibilità dei documenti)
- gestione multisocietà e anagrafica organizzativa e documentale che permette raggruppamenti omogenei su cui definire diversi responsabili della conservazione
- gestione dei termini di conservazione imposti dall'applicazione chiamante

La componente Legaldoc supporta le funzionalità di riversamento sostituivo. Tuttavia, data la complessità dell'argomento, l'operazione di riversamento sostitutivo si configura come un'attività progettuale.
Ogni documento inviato in conservazione viene accompagnato da un file di indici: è previsto un sottosistema di indicizzazione basato sulla tecnologia open-source Lucene.

7.3 LegalDoc Retriever

L'esibizione a norma dei documenti conservati avviene normalmente mediante l'interfaccia web nativa del sistema in ASP. Tale modalità è completa di tutti gli strumenti a supporto della verifica di validità dei documenti conservati.
L'esibizione può anche essere effettuata mediante un'invocazione applicativa ai web services del servizio,

Il documento richiesto viene richiamato direttamente dal servizio di conservazione sostitutiva LegalDoc ed esibito con garanzia della sua opponibilità a terzi. Tale modalità deve essere necessariamente utilizzata nel caso in cui si voglia far valere il valore legale del documento.
Nell'esibizione a norma di un documento sono resi disponibili anche i file di corredo che attestano la corretta conservazione. Essi sono:

- *il file di controllo del documento* firmato digitalmente dal responsabile della conservazione ed eventualmente marcato temporalmente. Viene fornito in esibizione per poter, in combinazione con il file di chiusura del lotto, qualificare il processo stesso.
- il *file delle direttive di conservazione* inviato con la richiesta di conservazione del documento. Viene fornito in esibizione per poter verificarne la coerenza con quanto inviato dal Cliente
- *il file di ricevuta* di presa in carico della conservazione fornito in risposta alla richiesta di conservazione
- *il file di responso*. Contiene le informazioni di servizio sull'operazione
- *il file di chiusura del lotto*.

7.3.1 Verificatore per copie notarili

Il sistema dispone di uno strumento di esibizione dei documenti dall'archivio di conservazione che consente la verifica della correttezza della conservazione (Verificatore LegalDoc).
Questa particolare procedura di esibizione che è parte integrante della componente LegalDoc, è integrata nativamente nel sistema di retrieval e permette di rendere disponibili tutti gli strumenti di controllo necessari ad attestare l'autenticità del documento conservato .
Questa particolare esibizione del documento rappresenta un'esibizione completa, che permette di verificare automaticamente online:

- *La validità della firma digitale apposta sul documento oggetto di conservazione*
- *L'integrità del documento nel tempo*
- *La validità della firma digitale del responsabile della conservazione*
- *La validità della marca temporale apposta a chiusura del processo di conservazione*

Lo strumento permette inoltre di scaricare i documenti "sbustati" (nel caso di documento con firma P7M o marcato temporalmente): non è quindi necessario disporre di un software di verifica firma/marca sul client.

7.3.2 Interfaccia applicativa di esibizione

In alternativa all'interfaccia utente, il sistema dispone di un'interfaccia applicativa (SOAP) per l'esibizione, che può essere richiamata dalle applicazioni del cliente. L'esibizione può essere richiesta inviando il token o un altro identificativo univoco specificato al momento della richiesta di conservazione. La gestione del token è, in questo caso, a carico dell'applicazione chiamante.

7.4 Reportistica

I clienti del sistema di conservazione InfoCert dispongono di un cruscotto per il monitoraggio dell'utilizzo del servizio. Il cruscotto fornisce funzioni di interrogazione sulle quantità e i volumi, che consente di specificare il periodo e il livello di aggregazione delle rilevazioni.
Il report, esportabile su foglio elettronico, contiene le informazioni relative a tutti i parametri significativi della conservazione.

7.5 Procedure organizzative adottate

Il presidio applicativo del servizio ASP è realizzato da personale del fornitore utilizzando la console di controllo, che permette di monitorare il flusso dei documenti e dei lotti conservati in termini di numerosità e di spazio.
In virtù del contratto stipulato con il Cliente, al fornitore possono essere delegate alcune delle attività necessarie alla conservazione. Il fornitore svolge tali attività nel pieno rispetto delle norme di legge, delle Condizioni Generali di Contratto e dei relativi Allegati.
Il sistema di conservazione documentale del fornitore e il processo da questi implementato rispondono interamente alle norme di legge poste che regolano la materia.

7.5.1 Durata della conservazione, controlli e riversamenti

La conservazione è garantita per tutto il periodo contrattuale ed eventuali estensioni, secondo le retention richieste dal cliente. Alla cessazione del rapporto contrattuale è prevista la restituzione dei documenti oggetto di conservazione in ASP attivi alla data, secondo le modalità che saranno concordate.
Il servizio di conservazione prevede le verifiche di leggibilità periodiche, il riversamento diretto e sostitutivo, a norma di legge.

7.5.2 Il manuale della conservazione

L'utilizzo del sistema viene normalmente documentato all'interno del "Manuale di gestione del protocollo informatico, dei documenti e dell'archivio", predisposto dalle PA ai sensi dell'art. 3 , comma c) del decreto del Presidente del Consiglio dei Ministri del 31 ottobre 2000 concernente le "Regole tecniche" per il protocollo informatico.

7.5.3 Aderenza agli standard

InfoCert presta particolare attenzione alle problematiche di standardizzazione, e si adopera per la loro adozione.
La soluzione di conservazione di InfoCert adotta come riferimento:

- le specifiche prodotte dal gruppo di lavoro UNI sulla conservazione sostitutiva
- le specifiche per la produzione dei files di chiusura lotto prodotte dal gruppo di lavoro DIAM di UNI
- le specifiche per la conservazione dei documenti amministrativi prodotte da ETSI – TS 102 573 "

InfoCert dichiara, più in generale, una sostanziale aderenza allo standard ISO 27001.

7.6 Avvio del servizio

Il servizio di Conservazione LegalDoc prevede la predisposizione di un piano di avvio dove vengono considerati i seguenti aspetti:

- requisiti formali
- verifica dei prerequisiti tecnologici
- integrazione applicativa
- eventuale migrazione da altro sistema

7.6.1 Requisiti formali

Dal punto di vista formale, l'attivazione del servizio di conservazione LegalDoc ha bisogno dei seguenti

requisiti:

- avere conferito la delega per lo svolgimento delle attività del procedimento di conservazione ad InfoCert a norma dell'Art. 5, Comma 3 della citata Delibera CNIPA n. 11/2004
- fornire ad InfoCert tutte le informazioni richieste, necessarie alla configurazione del sistema (previste nel modulo di attivazione)
- verificare la congruità dei viewer standard proposti da InfoCert per la lettura dei documenti conservati, o depositare, presso InfoCert, appositi visualizzatori

7.6.2 Requisiti tecnologici

In prima istanza, devono essere soddisfatti i requisiti di connettività: è possibile effettuare la connessione tramite collegamento ad Internet di qualsiasi tipo.
Dal punto di vista tecnologico, I requisiti tecnologici sono diversi nel caso di accesso diretto (web services) e mediato (LegalDocConnector):

- nel primo caso non ci sono vincoli particolari, assunto che la piattaforma del cliente sia in grado di interrogare web services (SOAP with attachments).
- nel secondo caso, è necessaria l'installazione di un apposito client, disponibile sia in ambiente Linux che in ambiente Windows. I requisiti dell'ambiente sono standard.

InfoCert si riserva di apportare i cambiamenti che si renderanno eventualmente necessari dandone tempestiva comunicazione alla Regione Veneto.

7.6.3 Integrazione applicativa

L'integrazione avviene in modo diverso nel caso di accesso diretto (web services) e mediato (LegalDocConnector, o connettore specifico):

- nel primo caso le applicazioni del cliente devono integrare i servizi di conservazione, invocando i relativi web services secondo quanto specificato nel documento "Specifiche tecniche di integrazione" che verrà consegnato all'Ente. Per l'accesso verranno fornite apposite credenziali e un certificato (p12) per l'autenticazione al servizio.
- nel secondo caso le applicazioni del cliente si limiteranno ad esportare i documenti oggetto di conservazione in un'apposita area di appoggio che sarà predisposta. Il client Ldoc Connector, appositamente configurato, si preoccuperà dell'invio di tali documenti al servizio di conservazione seguendo un'opportuna schedulazione.
- è altresì possibile la realizzazione di un connettore diretto verso i sistemi del cliente.

InfoCert si riserva di apportare i cambiamenti che si renderanno eventualmente necessari dandone tempestiva comunicazione alla Regione Veneto.

7.6.4 Eventualie migrazione

Qual'ora il cliente disponga già di documenti conservati, che intenda riversare sul servizio di conservazione LegalDoc, sarà necessario predisporre una specifica attività. La normativa richiede, in questo caso, una precisa analisi del flusso di riversamento, in modo da poter garantire che il processo di conservazione è stato svolto senza soluzione di continuità. InfoCert si rende disponibile a tale attività nei modi che saranno concordati con l'Ente interessato.

7.7 Conclusione del servizio

A conclusione del servizio, InfoCert prevede la possibilità di esportare l'intero patrimonio documentale del cliente, oggetto di conservazione attiva, ai fini del suo trasferimento sotto la responsabilità di un diverso soggetto, nell'ottica di garantire la continuità del processo di conservazione.
InfoCert proporrà a tale fine una modalità standard di formattazione dei documenti e dei relativi metadati di conservazione, coerenti con gli standard definiti (e in corso di definizione) a livello italiano (UNI) ed europeo (ETSI – Standard Task Force 401). Formati diversi possono essere concordati con il cliente.

8 Formazione e supporto

8.1 Formazione

Viene reso disponibile all'interno del Sito di Governo della Fornitura un **kit di avviamento alla dematerializzazione**, al fine di fornire ai destinatari tutte le nozioni di carattere normativo, tecnico e di uso dei servizi oggetto della gara.
Il kit è realizzato secondo un approccio modulare per temi e per servizio. Ogni modulo conterrà uno più documenti, oltre ad una presentazione di sintesi degli elementi contenuti.
All'interno del sito di e-learning di Regione del Veneto vengono inoltre resi disponibili 4 moduli di autoapprendimento sui temi:

- DEMATERIALIZZAZIONE
- FIRMA DIGITALE
- CONSERVAZIONE A NORMA
- POSTA ELETTRONICA CERTIFICATA

8.2 Consulenza

InfoCert dispone di servizi di consulenza per l'affiancamento agli Enti che ne faranno richiesta per la fornitura di consulenza specifica, seminari o workshop.
La formazione e la consulenza di InfoCert copre diversi ambiti, sia tecnici sia legati alla conformità alla normativa vigente in termini di dematerializzazione (compliance): ad esempio l'implementazione dei processi con l'uso di nuove tecnologie (firma digitale, posta elettronica certificata, gestione documentale, workflow, fatturazione elettronica, e così via), la conservazione sostitutiva, il protocollo informatico, la privacy,
Le giornate possono inoltre essere utilizzate in attività di certificazione di processi, ovvero la verifica che una procedura di dematerializzazione sia correttamente implementata rispetto alle previsioni di legge, che un flusso di conservazione sia coerente con la normativa di riferimento, che l'adozione degli strumenti di firma digitale all'interno di una procedura sia eseguita in modo da diminuire al minimo il rischio di contenzioso.
La consulenza offerta può inoltre essere utilizzata per supportare gli Enti nella presentazione di interpelli all'Agenzia delle Entrate, per risolvere casi specifici, ovvero nella presentazione di istanze con richieste di chiarimenti alle autorità di controllo (es: DigitPA, Garante Privacy, Ministero Funzione Pubblica, Ministero Industria,…).
Le attività di consulenza offerte si basano sulla costante attività di analisi della normativa, della tecnologia e delle applicazioni di dematerializzazione svolta da InfoCert.
Nel corso delle attività di consulenza e formazione, InfoCert metterà a disposizione le seguenti figure professionali:

1. **Specialisti informatici sulle tematiche della dematerializzazione** con pluriennale esperienza sugli argomenti della firma digitale e marcatura temporale, conservazione sostitutiva e posta elettronica certificata e la loro integrazione in procedure del cliente.
2. **Specialisti informatici sulle tematiche della gestione documentale** per effettuare **l**'analisi dei flussi ed analisi dei processi documentali, interfacciandosi direttamente con le interfacce disegnate nelle attività di raccolta di informazioni e approfondimenti sui flussi documentali;
3. **consulenti esperti in archivistica e gestione documentale,** qualora le richieste impattino sulla corretta gestione dei flussi di documenti ai fini
    - addestramento e formazione del personale dei Clienti all'utilizzo delle diverse funzionalità dei Prodotti e Servizi in ambito Gestione Documentale;
    - analisi dei flussi e delle modalità operative dei Clienti in ambito Gestione Documentale e loro ottimizzazione/reingegnerizzazione (in accordo con il singolo Cliente) sulla base delle funzionalità garantite dai Prodotti e Servizi;
    - erogazione di sessioni di consulenza archivistica

- **consulenti esperti in informatica giuridica sui temi della dematerializzazione**, con il compito di gestire direttamente il progetto con le interfacce designate, coordinare le attività delle diverse figure eventualmente coinvolte, provvede direttamente alle attività di analisi e approfondimento;erogare interventi di addestramento e formazione sulle componenti dell'Offerta InfoCert "utilizzate" dai prodotti/servizi di Gestione Documentale (PEC, Firma Digitale, Conservazione a Norma LegalDoc, ecc.).