Ministro per l'Innovazione e le Tecnologie

Piano Nazionale di e-Government

REGIONE DEL VENETO

e-goVernment Veneto

Direzione Sistema Informatico

SIRV

INFRASTRUTTURA DI COOPERAZIONE APPLICATIVA

Versione 1.0.0

13 giugno 2003

Insiel

GRUPPO TELECOM ITALIA-FINSIEL

Approvazioni

Il presente documento è stato approvato da:

Storia delle Modifiche

Versione	Data	Descrizione

Riferimenti

Numero	Titolo	Prodotto da	Versione	Data

Sommario

1. Premessa

Scopo del presente documento è di illustrare i principi e i modelli di Cooperazione applicativa di riferimento per il piano di e-Government e di presentare la soluzione offerta.

La prima parte richiama le linee guida dettate dal Ministero per l'Innovazione e le Tecnologie e dall'AIPA.

La seconda parte descrive la soluzione di Cooperazione applicativa in termini di soluzioni tecnologiche.

2. Il quadro di riferimento

L'incremento dell'efficienza interna alla P.A. e l'erogazione di servizi ai cittadini e alle imprese tramite un unico punto d'accesso al sistema amministrativo (sportello virtuale unico) richiedono l'integrazione tra i servizi di diverse Amministrazioni e quindi l'adozione di soluzioni di interoperabilità fra sistemi eterogenei.

Il quadro di riferimento è già stato tracciato nelle sue linee generali dall'Autorità di Governo, ed è riassunto nel documento "Rete Nazionale: architettura applicativa" pubblicato nel febbraio 2002. In esso, si fa riferimento specifico a:

- la Rete Nazionale della Pubblica Amministrazione (Rete Nazionale), come infrastruttura per lo scambio di dati e servizi tra tutte le Amministrazioni ed Enti Pubblici centrali o periferici;
- soluzioni di interoperabilità "neutrali" per quanto riguarda le scelte tecnologiche e le politiche di servizio di ciascun Ente.

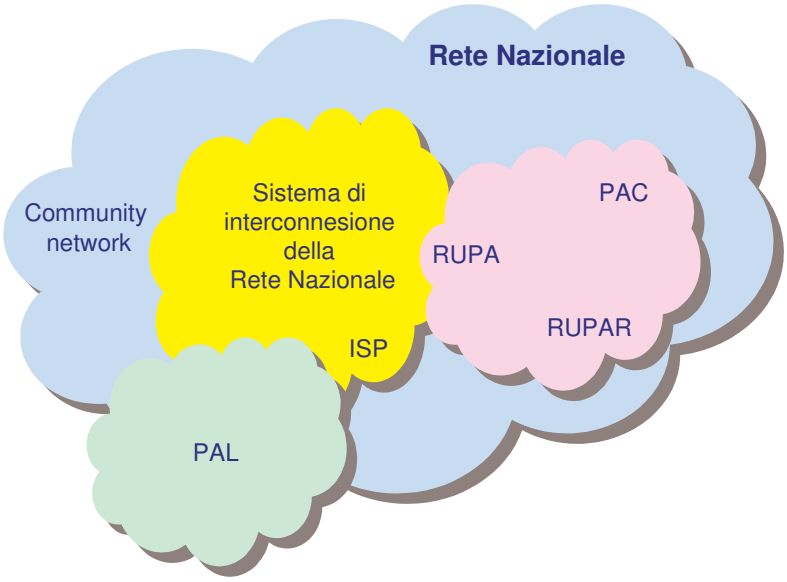
2.1 La Rete Nazionale della Pubblica Amministrazione

La Rete Nazionale è stata definita in modo tale da:

- permettere l'interconnessione "any to any" tra tutti i soggetti rappresentati dalle Amministrazioni dello Stato, dalle Regioni e dagli Enti Locali;
- definire un internetwork di **reti paritetiche** (figura 1) su dorsale TCP/IP, accessibile dalle singole reti di riferimento per gli Enti (RUPA, reti regionali, territoriali o RUPAR, consortili o anche di singoli Enti o categorie di Enti);
- fornire sicurezza a tutte le operazioni di scambio dati e interoperabilità.

Per queste sue connotazioni, la Rete Nazionale può essere vista come una Extranet, e cioè come una rete basata su tecnologia Internet, che interconnette in maniera controllata le Intranet dei domini informativi delle diverse Amministrazioni.

Figura 1 La Rete Nazionale della Pubblica Amministrazione (RNPA) (Fonte: Dipartimento per l'Innovazione e le Tecnologie – DIT)



2.2 I principi di Cooperazione applicativa

La Cooperazione applicativa permette a sistemi eterogenei (per ambienti operativi, linguaggi di implementazione, sistemi di gestione e accesso alle risorse) di scambiarsi servizi sulla base di messaggi standardizzati e dunque interpretabili da ciascuno di essi.
La Rete Nazionale, oltre all'infrastruttura di connessione, definisce anche il modo in cui ciò deve avvenire per far sì che sia rispettata l'autonomia degli Enti. Più in particolare impone un modello che:

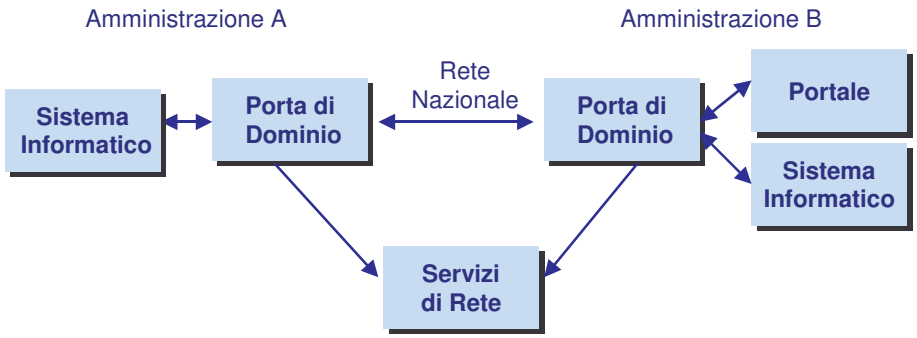
- vede la Rete Nazionale come una **federazione di "domini";**
- fa corrispondere ciascun "dominio" all'insieme delle risorse (procedure, dati e servizi) e delle politiche di servizio di una determinata organizzazione;
- definisce un'architettura di cooperazione che abilita l'integrazione degli oggetti informativi (procedure e dati) di domini diversi, quali che siano i sistemi informativi operanti nei singoli domini;

- assume a riferimento per gli interscambi telematici interdominio i protocolli standard caratteristici di Internet (prioritariamente HTTP, ma anche SMTP e FTP);
- identifica gli standard di base cui si devono attenere i messaggi di richiesta e di scambio di servizi fra sistemi (buste di e-Government), che sono il linguaggio XML (eXtensible Markup Language) per definire un formato dei dati condivisibile da sistemi eterogenei, e il protocollo SOAP (Single Object Access Protocol), per la veicolazione delle informazioni codificate XML sulla rete, mediante il protocollo HTTP.

2.2.1 Le Porte di Dominio

Le Porte di Dominio sono l'elemento tecnologico chiave dell'architettura di Cooperazione applicativa nell'ambito della Rete Nazionale. Esse corrispondono all'insieme delle funzionalità software attivabili in ciascun dominio come proxy unico ed esclusivo per l'accesso alle risorse applicative di altri domini attraverso al rete, e viceversa, senza introdurre variazioni significative agli ambienti esistenti.

Figura 2 Modello di riferimento per l'integrazione delle Porte di Dominio (Fonte: DIT)

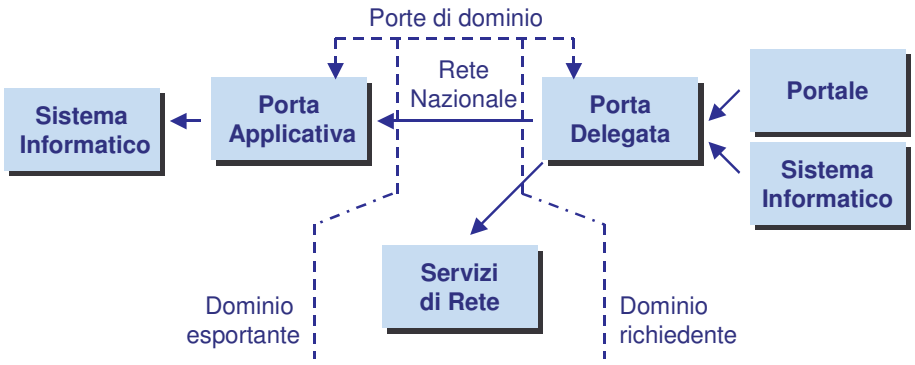


Nella logica delle Porte di Dominio (figura 2):

- i domini cui appartengono i sistemi informativi sono visti di volta in volta come ***domini client*** o come ***domini server***, a seconda del fatto che essi richiedano un servizio o rispondano a una richiesta di servizio;

- le porte assumono la denominazione di ***Porte Delegate*** quando chiedono un servizio e di Porte ***Applicative*** quando lo erogano (figura 3).

Figura 3 Schematizzazione delle Porte di Dominio (Fonte: DIT)



Sotto il profilo tecnico, le Porte di Dominio, pur essendo realizzate all'interno di ogni dominio:

- rendono palese l'architettura a tre livelli della Rete Nazionale (dominio client, Porta di Dominio e dominio server);
- mascherano i dettagli del sistema informativo della singola Amministrazione esponendo i suoi servizi sulla Rete Nazionale con modalità comuni e standardizzate basate su XML;
- sono implementabili con soluzioni basate sui Web Services;
- dialogano attraverso servizi di rete che comprendono anche un indice ove sono mappati i domini, i servizi che questi rendono disponibili e le modalità di interlocuzione.

2.2.2 I Web Services e le Porte di Dominio

Il termine Web Services indica le funzionalità che un sistema espone attraverso una connessione Internet ad altri sistemi, affinché questi ultimi possano rilevare le modalità di richiesta di un servizio, informativo o applicativo, quali che siano gli ambienti e le applicazioni interessate.

Più in particolare, i Web Services sono componenti applicative, accessibili tramite i protocolli standard di Internet (HTTP, SMTP e FTP) e registrati in directory pubbliche (in senso proprio o con restrizioni a specifici gruppi di operatori o sistemi) che:

- descrivono in un formato standardizzato (XML), quindi riconosciuto da sistemi eterogenei, le operazioni accessibili/richiedibili;
- possono essere avviati dinamicamente in un ambiente distribuito anche in automatico da applicazioni strutturate per effettuare richieste di servizio ad altri sistemi.

Queste caratteristiche, fanno di essi la base tecnologica delle Porte di Dominio per l'implementazione delle componenti funzionali di cooperazione più generiche (per il livello telematico e i profili di collaborazione). Tutte le altre principali funzionalità di integrazione - per l'adattamento verso il sistema informatico (o i sistemi informatici) di dominio e la garanzia del rispetto dei formati di codifica, per il contenuto applicativo di messaggi, e così via – sono invece assicurate da altre componenti delle porte applicative che si integrano a mezzo di interfacce e protocolli standard.

Dunque, le Porte di Dominio si avvalgono dei Web Services, ma associano e integrano componenti di middleware che si conformano alle caratteristiche specifiche dei sistemi informatici da integrare (ad esempio tecnologia e schema dei database, oltre che dalla presenza di middleware come sistemi a code o di accesso a mainframe, interfacce funzionali o di accesso remoto). Per questo le Porte di Dominio vanno viste come estensione rispetto ai Web Services.

2.2.3 Modelli e profili di cooperazione

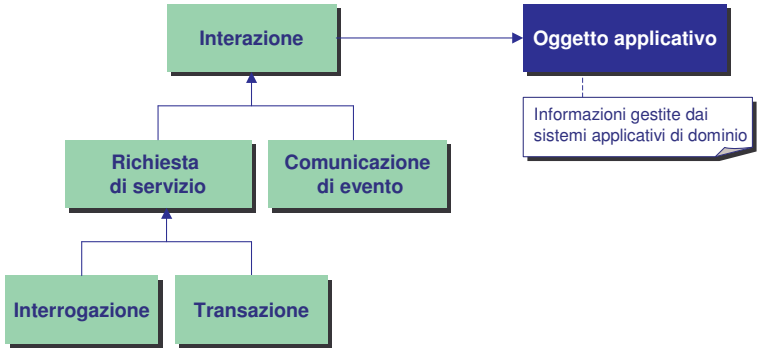
Anche nel caso delle Porte di Dominio, i paradigmi della Cooperazione applicativa, sono riconducibili a due tipologie (figura 4):

- la richiesta di servizio, quando un messaggio prodotto da una applicazione di un dominio client è diretto a una applicazione di un dominio server, determinando l'esecuzione di una applicazione del dominio server e l'invio di una risposta all'applicazione client. In particolare, la richiesta di servizio può essere:

- di interrogazione, quando non modifica alcun oggetto applicativo interno al dominio server;
- di transazione, quando produce una variazione permanente in un oggetto applicativo del dominio server;

- la comunicazione di evento, quando l'applicazione di un dominio genera un messaggio per informare altre applicazioni di uno o più domini destinatari dell'avvenuto cambiamento delle informazioni relative a un oggetto applicativo (ad esempio il cambio di residenza) o della creazione di un nuovo oggetto applicativo (ad esempio a seguito della registrazione di una nascita).

Figura 4 Interazioni e oggetti applicativi (Fonte: DIT)



Per le richieste di servizio, il modello di Cooperazione applicativa della Rete Nazionale prevede interlocuzioni:

- in modalità sincrona, quando la porta delegata invia la propria richiesta ed attende la risposta della porta applicativa;
- in modalità asincrona quando la risposta della porta applicativa può essere inviata in un tempo successivo e la porta delegata non rimane in attesa.

E' possibile che lo stesso servizio possa essere esportato con modalità diverse da domini diversi, e questo risulta dall'indice dei servizi in rete.

La notifica degli eventi è invece sempre in asincrono, pur avvenendo in modalità diverse, e cioè:

- Publish/Subscribe, quando le applicazioni generano messaggi e li inviano al repository di un sistema gestore di eventi, che poi li rende accessibili a chiunque risponda a regole predeterminate di accesso, contenuto o intestazione;
- Point–to-point, quando nel sistema gestore di eventi le applicazioni di specifici domini si interrogano reciprocamente tramite le procedure di "gestione delle code";
- Publish/Forward, quando i riferimenti di chi emette la comunicazione di evento e di chi deve riceverla sono già organizzati nella directory de gestore degli eventi.

2.2.4 La busta di e-Government

L'elemento fondamentale che caratterizza i messaggi per la Cooperazione applicativa è la completa e preliminare definizione della loro struttura e contenuto. Questi messaggi devono infatti essere totalmente interpretabili in modo automatico.

La struttura generale di ciascun messaggio si articola in due parti principali:

- una parte di busta, con le indicazioni relative al mittente e al destinatario (intese come Porte di Dominio), al servizio richiesto e al profilo di collaborazione utilizzato.
- una parte di contenuto applicativo, con le informazioni effettive previste per il servizio e lo scambio (ad esempio i dati identificativi di una richiesta di informazioni anagrafica).

Una visione più articolata e precisa della struttura del messaggio è descritta dalla figura 5.

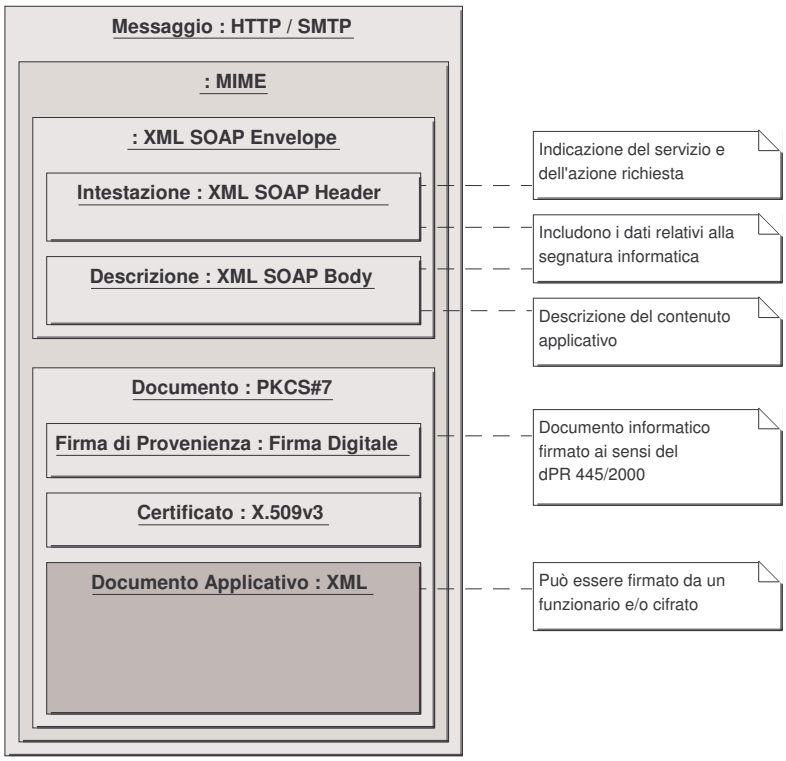


Figura 5 Struttura della busta di e-Government (Fonte: DIT)

La struttura di riferimento si avvale:

- del formato dati XML, per definire il contenuto dei dati di comune interesse e strutturare le stringhe di dati scambiati nei processi di cooperazione;
- del protocollo SOAP, e per il veicolamento delle informazioni codificate con XML sulla rete Internet, mediante il protocollo HTTP.
-

Più in particolare (si veda ancora la figura 5), la struttura XML SOAP è inclusa in una struttura MIME allo scopo di allegare al messaggio uno o più documenti applicativi, in base allo standard "XML SOAP with attachments". Una firma opzionale può essere inclusa nell'intestazione utilizzando gli standard XML SOAP Encription e XML Signature per garantire la fonte di provenienza delle informazioni (art. 43 del D.P.R. 445/2000). Nel caso di documenti informatici firmati, per la rilevanza legale è poi indicato il formato il PKCS#7 in base della circolare AIPA CR/24.

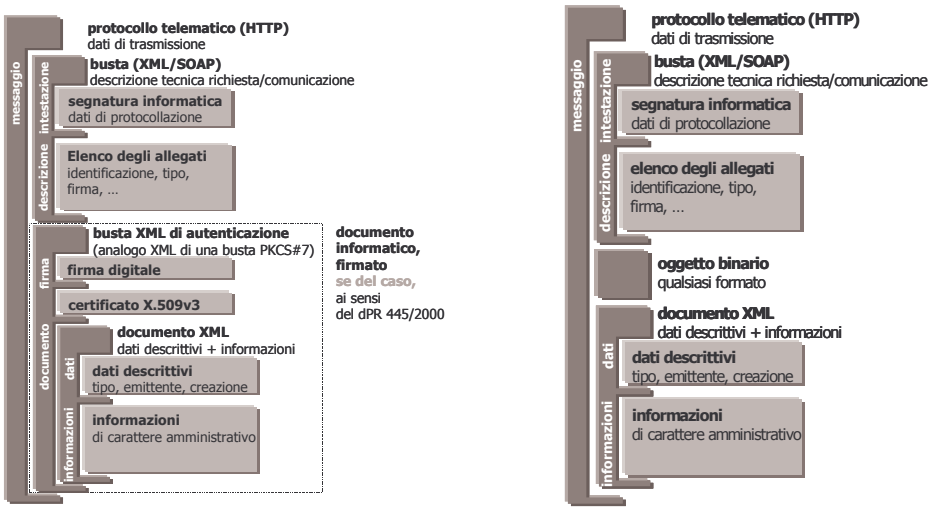


Figura 6 Firma di provenienza

Le specifiche tecniche per la Cooperazione applicativa sulla Rete Nazionale non entrano però nel merito della struttura informativa del messaggio, creando ad oggi la necessità di concordare fra vari enti/domini gli standard di riferimento al riguardo.

Di seguito viene descritta la busta di e-government gestita dalle Porte di Dominio. Il contenuto del messaggio è strutturato in più blocchi distinti di informazione sulla base della specifica XML SOAP 1.1 with attachments, che prevede l'aggregazione multipart in base allo standard MIME. In questo modo è possibile aggregare in un unico messaggio più blocchi distinti di informazioni anche eterogenee. La specifica non pone infatti restrizioni sul contenuto o la rappresentazione di ogni singolo blocco.

Il primo blocco di informazioni avrà una struttura prefissata e dovrà rispettare le specifiche XML SOAP per l'Envelope. Ciò impone che il formalismo utilizzato per la rappresentazione sarà XML. Per il contenuto si distinguono due sottostrutture di Envelope e precisamente:

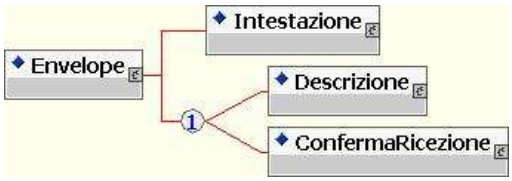
- una intestazione o Header;
- una descrizione o Body.

L'Header avrà tutte le informazioni legate alla logica di trasporto del messaggio mentre nel Body vi saranno i riferimenti agli altri blocchi dati o in alternativa contenuti informativi limitati e pre-classificati (conferma di ricezione ecc.). Nel successivo blocco di dati vi sarà il contenuto applicativo del messaggio. Per la verifica dell'autenticità, della

provenienza o per gestire la segretezza dell'informazione, si prevede che tale informazione possa essere contenuta in una busta PKCS#7 dove trovano posto l'eventuale firma di provenienza ed il certificato X.509. Come detto la Porta è in grado di generare anche buste XML-Signature.

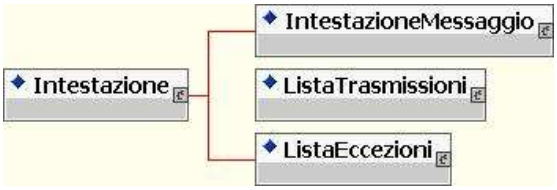
2.2.4.1 Il primo blocco dati

Come già detto il primo blocco dati prevede una struttura ed un formalismo prefissati. Il formalismo è l'XML, richiesto dal protocollo SOAP, il protocollo SOAP definisce anche la struttura esterna (Envelope) del blocco. Il contenuto è invece strutturato in due blocchi logici distinti, formalizzati sempre in XML e sono rispettivamente: l'intestazione ed il Body o Header.



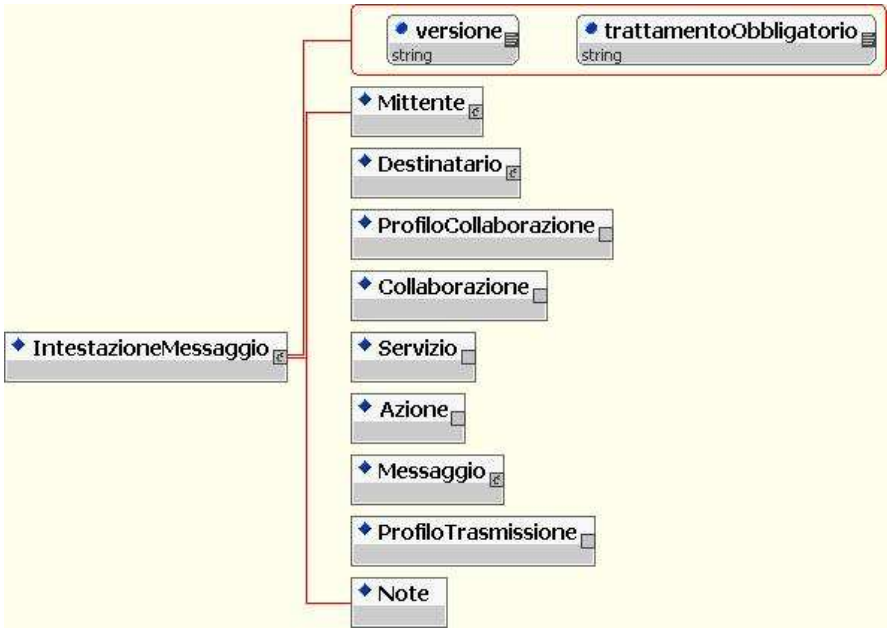
2.2.4.1.1 Intestazione

La testata si struttura in tre frammento XML: la Intestazione Messaggio, la Lista Intermediazioni e la Lista Eccezioni. In base alla specifica XML SOAP la testata sarà mappata su una "SOAP Header".



2.2.4.2 Intestazione Messaggio

La testata contiene tutte le informazioni di instradamento. Vengono indicati in particolare il mittente ed il destinatario, il servizio e l'azione da svolgere, le informazioni sul messaggio la modalità di colloquio.



2.2.4.3 Lista Trasmissioni

Ogni volta che il messaggio viene preso in carico da una porta di dominio, deve essere tracciato. Potrà essere tracciata la partenza così come l'arrivo, ed eventuali passaggi intermedi.

2.2.4.4 Lista Eccezioni

In questa sezione vengono elencate tutte le eccezioni verificate nel trattamento del messaggio prima dell'innesco dell'attivazione del servizio applicativo. Sono dunque eccezioni rilevate dalla porta di dominio e non dal sistema informatico, queste ultime faranno parte della componente applicativa del messaggio

2.2.4.4.1 Descrizione

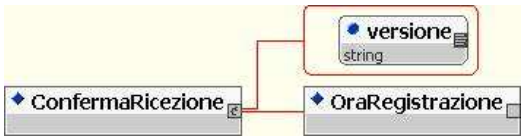
Il corpo del messaggio può essere strutturato in modo diverso a seconda della tipologia del messaggio. Ad esempio, nei casi di richiesta di stato, risposta di stato e ricevuta di ritorno, l'informazione sarà contenuta direttamente nel corpo e con una struttura predefinita. Negli altri casi sarà presente un manifesto, struttura informativa, con i riferimenti al contenuto dei singoli blocchi dati successivi al primo. In base alle specifiche XML SOAP il corpo sarà mappato da un "SOAP Body".

2.2.4.5 Descrizione Messaggio

La descrizione del messaggio contiene, come un manifesto, l'elenco di tutti i body part MIME, escluso il primo.

Conferma Ricezione

Questo elemento, presente in alternativa ai precedenti elementi, indica che il messaggio rappresenta una ricevuta di consegna, precedentemente richiesta dl mittente.



2.3 Le esigenze delle Amministrazioni

Alla luce di quanto esposto sin qui, un'Amministrazione che intenda avvalersi della Cooperazione applicativa, deve:

- organizzare l'accesso alla Rete Nazionale secondo il modello della Porta di Dominio;
- realizzare le interfacce fra i servizi disponibili sul proprio sistema informativo e la Porta di Dominio (componente di integrazione);
- essere anche in grado di utilizzare, all'occorrenza, anche formati concordati fra più Amministrazioni per i contenuti informativi inerenti a specifici servizi.

E' evidente che tutto questo si traduce, per gli Enti, nella necessità di avvalersi di interlocutori con competenze estese a tutti i livelli tecnologici, di progetto e di supporto implementativo.

3. La soluzione proposta

3.1 Le Porte di Domino

L'offerta risponde pienamente alle specifiche tecniche definite a livello istituzionale (SOAP/XML), attraverso un'architettura che garantisce:

- la completa apertura e indipendenza, in quanto basata su standard riconosciuti;
- la completa adattabilità e flessibilità a tutte le situazioni già esistenti, preservando la libertà di autonomia delle Amministrazioni in tema di scelte informatiche;
- la completa interoperabilità attraverso la Rete Nazionale tra le diverse applicazioni dei diversi domini;
- la scalabilità delle soluzioni;
- la sicurezza in termini di autenticità, autorizzazione, auditing.

In più *le soluzioni per le Porte di Dominio proposte rendono anche possibile superare il problema della mancanza di standard per il contenuto informativo di messaggi* inerenti a ciascun servizio (cfr. par.2.2.4) Esse infatti adottano una struttura informativa del messaggio funzionalmente compatibile con lo standard ebXML e adeguata alle normative sul protocollo e sulla segnatura informatica.

3.1.1 Indipendenza dalla piattaforma

Le componenti software di riferimento della soluzione sono state realizzate in linguaggio JAVA utilizzando tutte le interfacce standard disponibili: JMS,SOAP,DOM,XSLT,XSS,XML:DB,SAML. Questo per rendere la soluzione indipendente dai sistemi operativi e dalle piattaforme di infrastruttura (ad esempio l'application server).

Nel rispetto delle migliori pratiche di progettazione software è stata sempre definita un'interfaccia che consente di interagire con le applicazioni più eterogenee attraverso classi JAVA, Web Services, EJB, XML-RPC, CORBA, RMI.

Questo è ciò che consente di utilizzare in alternativa, liberamente e per specifiche componenti, anche i prodotti di mercato che incorporano le interfacce standard menzionate.

Nel seguito sono descritte più in dettaglio:

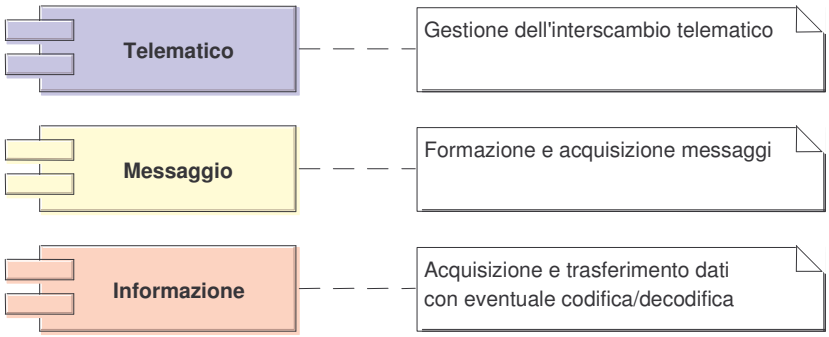
- le connotazioni dei servizi che supportano la Cooperazione applicativa utilizzati dalle Porte di Dominio e dai sistemi informatici da esse interessati;
- le soluzioni tecnologiche adottate.

3.1.2 I componenti logici

Come già sottolineato, le Porte di Dominio della soluzione, pur basandosi sulla tecnologia dei Web Services ne rappresentano una chiara evoluzione in termini applicativi, e non solo per la ricchezza delle componenti di integrazione. Infatti, attraverso un'implementazione dei costrutti di base della tecnologia ebXML, la soluzione proposta è anche in grado di fornire, a vari livelli, supporto alla normativa vigente in ambito amministrativo. Questo consente di concentrare aspetti soggetti a evoluzioni continue in un unico elemento infrastrutturale, senza darne carico ai singoli servizi applicativi.

Di conseguenza nelle Porte di Dominio possiamo individuare tre livelli di componenti logici: Telematico, Messaggio, Informazione (figura 7).

Figura 7 Componenti logici della Porta di Dominio



Nel livello **Telematico** risiedono i componenti della Porta di Dominio che gestiscono l'interscambio telematico dei messaggi tra le Porte. Qui vengono:

- attivate le connessioni,
- sfruttati i vari strati di protocollo,
- risolti gli indirizzi logici delle porte,

- instradate le comunicazioni verso le porte di destinazione.

Nel livello **Messaggio**, vi sono i componenti che provvedono alle funzioni logico-amministrative legate allo scambio telematico dei messaggi. In particolar modo:

- vengono interfacciati i sistemi di protocollazione e archiviazione dei messaggi in entrata e in uscita,
- viene verificata la validità del messaggio rispetto alla firma di porta del mittente,
- viene apposta la firma di porta ai messaggi in uscita.

A questo livello non si entra comunque nel merito del contenuto applicativo del messaggio ma solo delle informazioni legate allo scambio, cioè quelle che si trovano nella busta di e-Government.

Nel livello **Informazione**, al contrario dei precedenti livelli, si entra nel merito del contenuto applicativo del messaggio. I componenti che si trovano a questo livello costituiscono il cosiddetto Wrapper verso il sistema informatico applicativo. Proprio perché si entra nel merito applicativo, qui si trovano i componenti in grado di registrare la traccia applicativa, codificare e decodificare i dati o i formati di presentazione del messaggio applicativo, ecc.. Sempre a questo livello sono eseguite le operazioni di:

- cifratura,
- decifratura,
- firma e verifica non di porta (applicazione, operatore),
- costruzione della credenziale (Porta delegata),
- gestione dell'accesso ai servizi (Porta Applicativa).

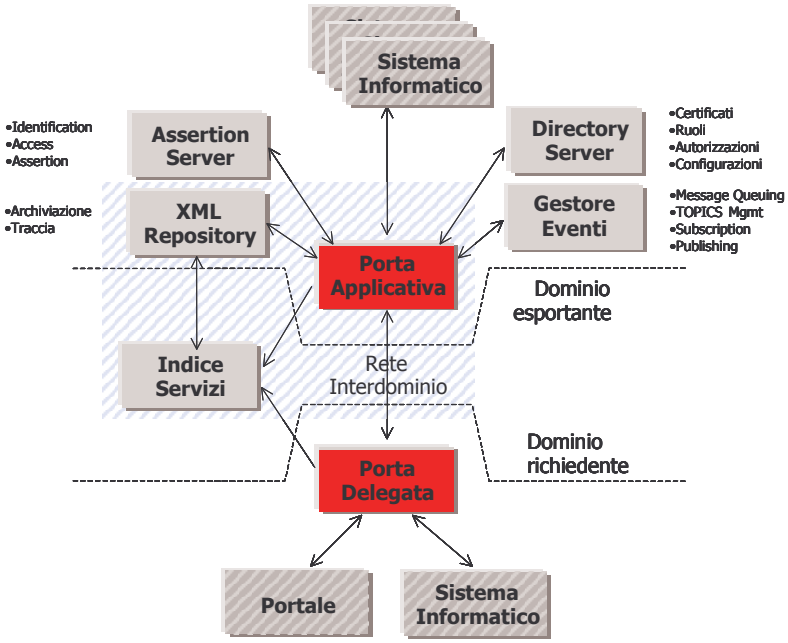
3.1.3 Le componenti architetturali

L'architettura della soluzione si basa sul concetto stesso di Porta di Dominio, con una Porta Applicativa per esportare i servizi applicativi verso le altre Amministrazioni dotate di una Porta Delegata e viceversa e ancora per notificare gli eventi ad altri domini e ricevere da essi notifiche.

La Porta Applicativa è stata concepita per offrire tutte le funzioni che, nell'ambito di servizi ed eventi amministrativi, danno validità ufficiale allo scambio d'informazioni. Per fare ciò la Porta di Dominio integra altri elementi (figura 8):

- l'**Indice dei servizi**, componente infrastrutturale presente di norma sulla rete condivisa tra le Amministrazioni, ove sono mappati i domini, i servizi che essi rendono disponibili e le modalità di interlocuzione;

- un **Gestore Eventi,** necessario per la pubblicazione e sottoscrizione degli eventi e, in seconda istanza, per la gestione delle code necessarie per la collaborazione di tipo asincrono;
- il **Directory Server**, con liste e informazioni di varia natura, come le configurazioni dei vari sistemi (es. dell'Assertion Server, con l'elenco di ruoli, servizi ed utenti interni al Dominio, i Certificati digitali, la configurazione delle code per il Gestore Eventi, ecc.);
- l'**Assertion Server**, su cui si basa il controllo d'accesso ai servizi e l'identificazione degli utenti interni per la collaborazione con le altre Amministrazioni;
- il **Repository XML**, per archiviare gli atti e i messaggi scambiati dalla Porte, contenere informazioni relative alla protocollazione, alla traccia dei messaggi, alla



configurazione delle Porte, e interfacciare l'Indice dei Servizi.

Figura 8 Architettura della soluzione

Più in dettaglio, si analizzano di seguito i singoli componenti.

3.1.3.1 Indice dei servizi

L'indice dei servizi è una componente software infrastrutturale (server) solitamente posta al di fuori delle porte, accessibile dalla Rete e che consente di risolvere gli indirizzamenti logici alle porte nei corrispondenti indirizzamenti fisici. Esso assolve questo compito attraverso uno scambio di informazioni strutturate in linguaggio XML su protocollo http.
L'indice dei servizi - basato su protocollo UDDI - di principale riferimento nell'offerta è quello incluso nel:

- Java Web Services Development Pack 1.1 di Sun Microsystems che si appoggia sul repository XML Open Source "Xindice" ed è compreso in un set che permette anche l'installazione dei server di comunicazione Open Source Tomcat e Apache.

In alternativa, è possibile integrare come Indice qualsiasi altra soluzione di mercato che incorpori lo standard UDDI, come ad esempio:

- l'Indice compreso in Oracle AS (piattaforma per i Web Service che ha a bordo Xindice e anch'esso con i tool per installare i server di comunicazione Tomcat e Apache);
- l'Indice disponibile nell'ambito della piattaforma di sviluppo WebSphere di IBM, che può essere utilizzata anche per modalità di indicizzazione LDAP oltre che UDDI.

In modalità LDAP sono utilizzabili anche le soluzioni descritte nel seguito per il Directory Server.

3.1.3.2 Directory Server

Il Directory server è una componente importante dell'architettura della Porta. Su di esso si appoggiano diversi componenti per la gestione delle configurazioni o l'archiviazione di informazioni essenziali accedute con estrema frequenza. In questo modo è possibile centralizzare la gestione di più componenti come quelli del Gestore Eventi (incluso il Message Queuing) e dell'Assertion Server.
La soluzioni di riferimento principali nella Porta di Dominio sono:

- una qualsiasi soluzione Open LDAP, scelta fra le più solide nell'ambito del software open source di directory;

- Sun ONE Directory Server (parte di ONE Platform for Network Identity di Sun, soluzione estesa all'intero ambito delle infrastrutture di rete per il controllo delle identità digitali).

In alternativa sono utilizzabili soluzioni di mercato come:

- Oracle net Directory (compresa nella piattaforma Oracle 9i);
- Microsoft NT Directory Services;
- IBM Directory Server.

Quest'ultima è peraltro da considerarsi a tutti gli effetti una soluzione open source, per le modalità con cui è resa disponibile.

3.1.3.3 Assertion Server (Gestione Accessi)

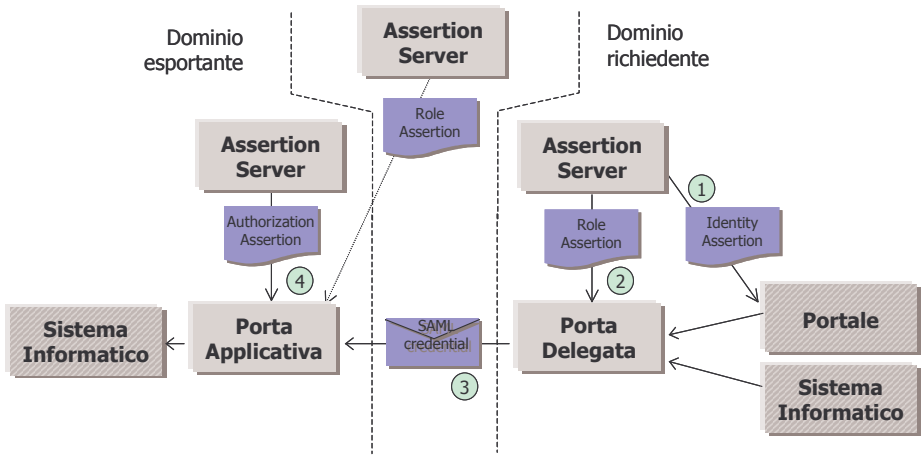
Per la gestione degli accessi sono proposte soluzioni basate sullo standard SAML (Security Assertion Markup Language), che permettono di gestire l'accesso a informazioni e servizi anche da parte di utenti non registrati nel dominio esportante.

Tale peculiarità deriva dal fatto che le verifiche d'identità e abilitazione dei singoli operatori avvengono all'interno del dominio d'appartenenza, consentendo al livello superiore (di dialogo fra domini) di limitarsi a controllare le credenziali richieste per attivare il dialogo tra domini.

Questa caratteristica è importante poiché, con l'estendersi della Cooperazione applicativa, risulterebbe prima o poi pesantissimo gestire, a livello centralizzato o di ciascun dominio, un repository con le abilitazioni ad operare per gli operatori di tutti i domini e per i diversi servizi.

Più in dettaglio, l'approccio dell'Assertion Server proposto è quello dello scambio di asserzioni (identità, ruolo o attributo e autorizzazione) validate da responsabili riconosciuti, che firmano digitalmente la credenziale dopo aver verificato al loro interno le abilitazioni. La credenziale verrà poi presentata dalla Porta Delegata alle Porte Applicative con la richiesta di servizio. Verificata l'autenticità della credenziale, il Dominio esportante l'utilizzerà per ottenere l'asserzione d'autorizzazione dal sistema che gestisce le politiche d'accesso allo specifico servizio. Il flusso procedurale è illustrato nella figura seguente.

Figura 9 La gestione degli accessi



La componente per la firma e la verifica di firma è implementata sia nella forma PKCS7 che XML Signature. E' anche contemplata l'integrazione del sistema di PKI della SA, tramite specifici servizi professionali.

La soluzione di principale riferimento in quest'ambito, ancora in evoluzione è Sun ONE Identity Server, anch'essa parte della già citata ONE Platform for Network Identity di Sun.

3.1.3.4 Repository XML

Per il Repository XML, preposto all'interfacciamento con l'indice dei servizi e al mantenimento della tracciatura degli scambi e delle richieste di servizio, le soluzioni di principale riferimento sono:

- l'Xindice di Apache;
- oppure, il SunOne Directory Services, anch'esso con funzionalità "Xindice" per l'archiviazione di documenti XML.

Le soluzioni citate permettono il rintraccio dei documenti XML relativi agli scambi attraverso lo standard XPath, e implementano l'interfaccia XML:DB API.

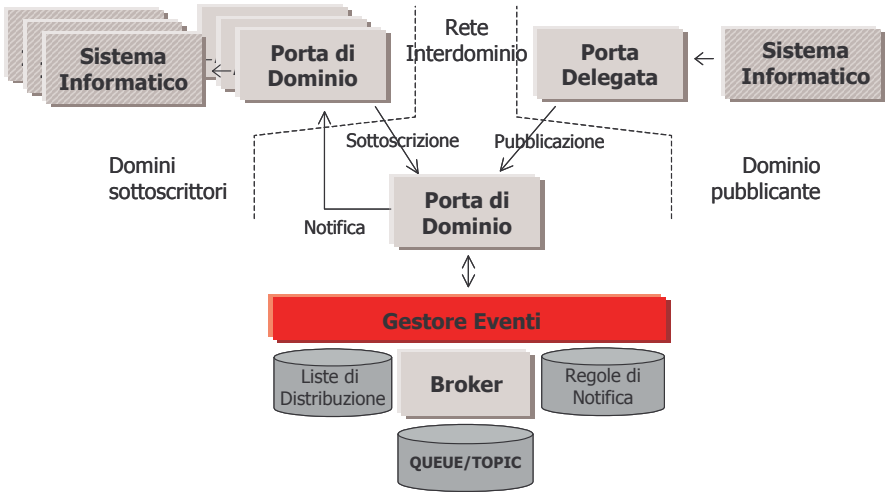
Anche in questo caso, e in coerenza con la massima libertà di implementazione, l'approccio dà la possibilità di utilizzare altre soluzioni alternative di mercato. Fra queste sono i repository:

- Oracle basati su modalità XQuery (Oracle XML DB);
- XML:DB e Xquery compliant disponibili in ambito Microsoft .Net.

3.1.3.5 Gestore Eventi

Integrato nel sistema di messaggistica, il Gestore degli Eventi (o Broker) sovrintende alle funzioni di propagazione dei messaggi nelle modalità volute (publish&subscribe, point-to-point o publish&forward) e alla gestione delle code (in eventuale accoppiata con un verso e proprio gestore di code), che è essenziale per definire il flusso delle operazioni. Lo schema del Gestore Eventi incluso nelle Porte di Dominio è illustrato dalla figura seguente

Figura 0 Il servizio di Gestione degli Eventi



Le soluzioni utilizzabili sono sia quella proprietaria con componenti full open, sia qualsiasi altra soluzione egualmente conforme allo standard JMS (Java Messaging System) incluso nello standard di interfaccia JAXM (Java API for Messaging).

La soluzione di primo riferimento, proprio perché open source, è OpenJMS (un'implementazione open source della specifica di interfaccia JMS 1.0.2 di Sun Microsystems) In alternativa, l'implementazione del Gestore può essere effettuata con:

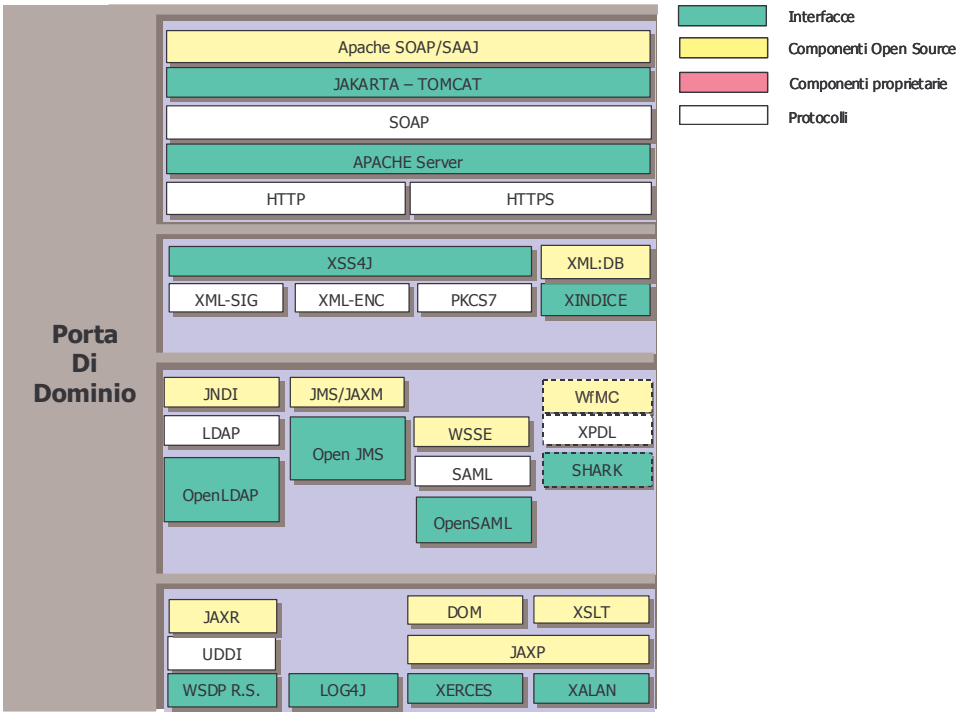
- Sun One Message Queuing, della piattaforma Sun ONE;
- Oracle Advanced Queuing , incluso in Oracle 9i Database;
- MQSeries, della piattaforma IBM WebSphere, e altri ancora.

In quest'ambito è anche allocato un sistema essenziale di Workflow Management, ad oggi sviluppato ad hoc con tool Java (Development Pack); ed è anche data la possibilità di impostare workflow specifici ad ogni servizio, associando all'identificativo del servizio la descrizione del workflow in linguaggio standard XPDL –WfMC.

3.1.3.6 – Connettività e overview sugli standard di riferimento

L'adozione di soluzioni di connettività standard open source (Apache Server e Jakarta Tomcat), illustrata dalla figura seguente (figura 11), riflette le scelte di riferimento open source più evolute, peraltro incorporate anche nelle componenti corrispondenti Oracle, Sun e IBM.

Figura 1 Architettura software della Porta di Dominio



La stessa figura rimanda ancora ai concetti di apertura dell'insieme delle soluzioni di Porta proposte, che meritano di essere richiamate a conclusione di questa sezione.

La flessibilità e la portabilità in tutti gli ambienti di riferimento – con soluzioni open source e/o con soluzioni di mercato richieste dai clienti - riflette infatti una visione che

predilige, per ciascun componente, la presenza di interfacce open e protocolli standard rispetto al produttore d'origine. E la stessa presenza di motori proprietari è qualificata dall'incorporazione degli standard di riferimento.