ALLEGATO n. 2

Rete Nazionale: caratteristiche e principi di cooperazione applicativa

Premessa 3
La Rete Nazionale 3
Premessa 3
Il modello di Rete nazionale 3
La Rete nazionale e le reti territoriali 4
La Rete Nazionale come interconnessione di reti 6
I Fornitori dei servizi di accesso 6
Principi di cooperazione applicativa 8
Organizzazione per domini 8
Porte di dominio 8
Modello delle interazioni 10
Profili di collaborazione 11
Modalità di scambio telematico 12
Principi di sicurezza 12
La busta di e-government 13
Struttura generale della busta di egovernment 14
Standard tecnologici per l'interoperabilità 17
Lo standard XML 17
La famiglia di standard XML 17
Standard di interoperabilità 17
Standard di sicurezza 18

Premessa

Il presente documento propone, allo stato attuale della normativa e della tecnologia, le principali linee guida per le amministrazioni che vogliano realizzare servizi on-line ai cittadini ed alle imprese, interagendo anche con i sistemi di altre amministrazioni.
In generale, l'interazione dei servizi messi a disposizione da amministrazioni diverse, prevede sia il collegamento alla Rete Nazionale della Pubblica Amministrazione, sia l'adesione alle indicazioni di interoperabilità e cooperazione applicativa, proposte nel presente documento

La Rete Nazionale

Premessa

La rete nazionale si pone come obiettivo fondamentale quello di creare una infrastruttura, per l'interconnessione di tutte le pubbliche amministrazioni, caratterizzata da livelli di servizio, relativi al trasporto delle informazioni e alla sicurezza di queste, con caratteristiche, per ciò che riguarda prestazioni e qualità, omogenee su tutto il territorio nazionale, monitorate e rispondenti a politiche definite a livello nazionale fra tutti gli attori coinvolti.
Tale rete, aderente al modello IP (Internet Protocol) è delineata nel documento "Rete Nazionale: architettura e caratteristiche" reperibile all'indirizzo: http://www.pianoegov.it/ . La Rete Nazionale fornisce un servizio di interconnessione che consente agli utenti, che su di essa insistono, di effettuare operazioni sicure di comunicazione, scambio dati e più in generale, di interoperabilità applicativa. La Rete nazionale può definirsi una Extranet, cioè una rete basata su tecnologia Internet, che interconnette in maniera sicura e controllata una serie di reti di enti ed amministrazioni (Intranet) che costituiscono i domini informativi delle diverse amministrazioni.
La Rete Nazionale in questa logica di extranet della pubblica amministrazione costituisce il presupposto per l' attuazione di ambiti di cooperazione applicativa per i quali fornisce i servizi di trasporto in modo del tutto trasparente rispetto alla topologia e ai fornitori di servizio che concorrono alla sua costituzione e gestione.
In tal senso la Rete Nazionale e le reti di servizi applicativi che attuano la cooperazione applicativa sono interrelati ma indipendenti.
Un ente sarà pertanto connesso, in linea di principio, ad una sola sottorete della Rete Nazionale (Rete Unitaria della Pubblica Amministrazione, rete territoriale, rete regionale, rete di ISP, ecc..) ma parteciperà allo sviluppo di più reti sotto il profilo applicativo (rete delle sanità, rete delle scuole, rete del lavoro, ecc..).
L'adesione alla Rete Nazionale avviene:

- per le amministrazioni centrali mediante il collegamento alla Rete Unitaria della Pubblica Amministrazione (RUPA)
- per le amministrazioni locali aderendo alla RUPA, alle RUPAR, alle reti territoriali o scegliendo un *Service Provider* (SP) con il solo vincolo rappresentato dalle prescrizioni tecniche in materia di sicurezza e di qualità dei servizi che dovranno essere predisposte dal Dipartimento per l'innovazione e le tecnologie.

I servizi di interconnessione della Rete nazionale sono realizzati attraverso la connessione di ciascun SP ad un *Neutral Access Point* (NAP) o, in futuro, ad un Exchange Point (EP). I *provider* dovranno anche fornire servizi di sicurezza in linea con quanto stabilito dal Dipartimento.

Il modello di Rete nazionale

I principi ai quali si ispira la Rete Nazionale possono essere riassunti come segue:

- La Rete Nazionale si pone l'obiettivo di permettere l'interconnessione, any to any, tra tutti i soggetti rappresentati dalle amministrazioni dello stato, dalle regioni e dagli enti locali sfruttando pienamente le potenzialità offerte dallo sviluppo e dalla diffusione delle tecnologie,
- La Rete Nazionale completa un quadro che vede da un lato il consolidamento della RUPA e dall'altro lo sviluppo ed il consolidamento di reti regionali, territoriali o RUPAR garantendo l' interoperabilità ed estendendo la possibilità di accesso e di cooperazione attraverso l'offerta di mercato costituita dai servizi qualificati di ISP,
- La Rete Nazionale è concepita per una utilizzazione rapida ed ottimale delle opportunità offerte attualmente dal mercato dei servizi di telecomunicazione e rappresentano una domanda qualificata di servizi agli operatori del settore capace di potenziare e far evolvere su livelli qualitativamente migliori l'intera infrastruttura Internet del Paese.

La Rete nazionale si configura come una **internetwork di reti paritetiche**, su dorsale TCP/IP, che interconnette i diversi soggetti della pubblica amministrazione locale e centrale.

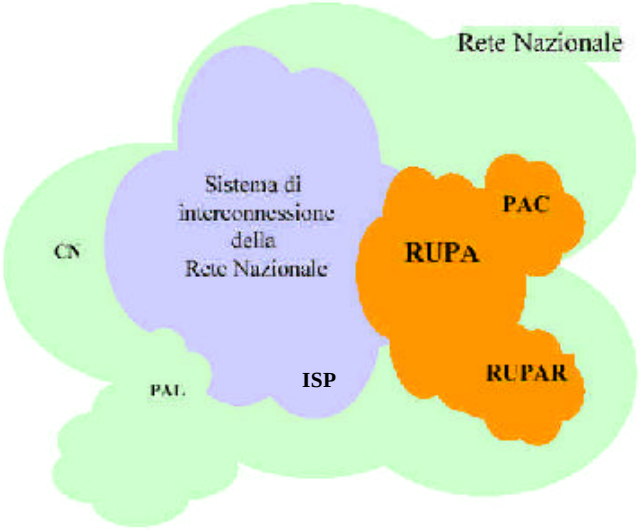

Figura 1 – La Rete Nazionale delle Pubbliche Amministrazioni (RNPA)

I servizi di interconnessione della Rete nazionale sono quindi forniti, oltre che dalla RUPA, dalle Reti regionali, dalle *community network* (CN) e dalle altre reti di settore e di categoria.
Inoltre gli utenti possono stipulare contratti con gli *Internet Service Provider* (ISP) che sono responsabili dei livelli di sicurezza e di qualità dei propri sistemi. A loro volta, gli ISP stipulano un contratto con gli *Exchange Point Operator* (EPO) che garantiscono l'interconnessione delle amministrazioni locali e centrali. Anche la RUPA stessa è connessa all'EPO mediante un Service Provider.
Tutte le reti che usufruiscono direttamente del sistema di interconnessione della RN sono connesse tra loro attraverso gli EPO cui sono assegnate diverse funzioni. Al fine di garantire la massima copertura territoriale e prestazionale sono state previste due categorie di EPO: *nazionali* e *locali*, con differenti requisiti di accesso da parte dei *provider* (SP) e con funzionalità particolari.
L'affidabilità del sistema di interconnessione è garantita dai requisiti richiesti ai provider della RN. In figura viene rappresentato uno schema della Rete nazionale comprendente le amministrazioni centrali (PAC), quelle locali (PAL) e le *community network* (CN).

La Rete nazionale e le reti territoriali

Già da diversi anni, intuendo le potenzialità che venivano messe a disposizione dalla

tecnologia dell'informazione e della comunicazione, diverse realtà, in ambito centrale ma soprattutto locale, hanno iniziato un percorso progettuale con l'obiettivo di intervenire non solo nei propri processi interni, ma anche e soprattutto per :

1. integrare i sistemi informativi delle amministrazioni pubbliche del territorio di riferimento
2. realizzare un sistema di accesso pubblico da parte di cittadini ed imprese alle informazioni ed ai servizi delle amministrazioni.

Sono state, in tal senso, realizzate reti telematiche territoriali e settoriali, ed è cosi iniziata, nel nostro paese per migliaia di Enti locali, l'esperienza di lavorare "secondo un modello reticolare" sfruttando le opportunità offerte dalle tecnologie dell'informazione e della comunicazione.
Nell'ambito di queste iniziative le Reti telematiche regionali, come altre realtà territoriali, sono state elemento fondamentale:

- nell'affermare la necessità di una nuova mentalità nel management pubblico per affrontare, in una logica di sistema unitario il ri-disegno della Pubblica Amministrazione,
- nel mettere a punto un patrimonio di conoscenze su come si gestisce il cambiamento e sui fattori critici di successo di progetti complessi,
- nel sostenere e stimolare la consapevolezza della priorità da attribuire alla valorizzazione del fattore umano e alla solidità del reticolo dei soggetti che partecipano al "progetto di rete".

Le reti regionali e territoriali nella loro accezione di "reti di trasporto" ma anche e soprattutto di "reti di soggetti", costituiscono un punto di partenza, un modello di riferimento e una concreta garanzia nella realizzazione in tempi ridotti della Rete nazionale.
In considerazione dell'attuale offerta di mercato nel settore delle reti basate su IP e con l'obiettivo di fornire una opportunità di accesso alla rete a tutte le amministrazioni in tempi brevi, la Rete Nazionale si basa sui servizi delle reti esistenti e sui servizi di ISP.
Il modello organizzativo cui tendere è la costituzione di "reti di soggetti" nell'ambito di un reticolo istituzionale che realizzi o rafforzi la progettazione e la cooperazione interistituzionale per il ridisegno della pubblica amministrazione in una logica di sistema orientato ai cittadini e alle imprese.
L'essere comunque "in rete" aiuta la pubblica amministrazione ad operare con tale ottica" e pertanto l'accesso alla rete anche attraverso soluzioni non organiche e' ritenuto prioritario nel piano di azione e-government e di conseguenza nelle modalità di realizzazione della Rete Nazionale.
Al fine di estendere il concetto di rete al di fuori dei limiti amministrativi tradizionali, è stata inoltre introdotta una modalità di aggregazione denominata **Community Network,** la quale prevede che più soggetti, che manifestino il loro interesse alla cooperazione attraverso specifici protocolli d'intesa, gestiscano autonomamente gli aspetti del trasporto, della cooperazione applicativa e della sicurezza.
Le Community network, rappresentando un modello che si affianca a quello delle reti regionali, sono chiamate a:

- sviluppare efficientemente la cooperazione applicativa tra i sistemi informativi degli enti locali (modello front office – back office territoriale) e tra questi e quelli degli enti della Pubblica Amministrazione Centrale,
- organizzare i portali territoriali per l'accesso alle informazioni della P.A. locale e per l'erogazione dei servizi telematici ai cittadini ed alle imprese del territorio, sostenendo e diffondendo le esperienze ed i progetti degli enti locali,

La Rete Nazionale come interconnessione di reti

Limitatamente ai servizi di connettività e nel rispetto del principio di realizzare la massima coesione possibile a livello territoriale locale in modo da garantire il massimo della efficienza possibile, la struttura logica della Rete Nazionale è composta da:

- servizi di interconnessione, realizzati attraverso nodi di aggregazione che costituiscono l'equivalente di una dorsale di rete IP
- servizi di accesso dalle singole sottoreti (reti regionali, reti territoriali, singoli enti, RUPA, ecc..) alla dorsale IP.

Gli utenti dei servizi di accesso possono essere classificati in:

- *Pubbliche amministrazioni centrali* (PAC). Le PAC continueranno ad utilizzare i contratti RUPA sia per realizzare le proprie intranet sia per connettersi alla Rete Nazionale. Il Centro di Gestione dell'Interoperabilità della RUPA diviene un fornitore di servizi di interoperabilità anch'esso interconnesso alla Rete Nazionale. Le PAC quindi usufruiranno dei servizi della Rete Nazionale attraverso i propri contratti RUPA.
- *Rete regionale*. Ogni rete regionale potrà autonomamente interconnettersi alla Rete Nazionale acquisendo un accesso al servizio di interconnessione o direttamente alla RUPA secondo modalità tecniche definite.
- *Community Network*. Gruppi di reti possono, ove lo ritengano opportuno, realizzare un punto comune di accesso alla Rete Nazionale e quindi anche alla RUPA. La costituzione di un punto comune di accesso è a carico dei gestori di tali reti. Anche l'interconnessione del punto comune di accesso con la Rete Nazionale avverrà secondo le modalità tecniche che verranno definite dal Dipartimento.
- *Altre reti*. Ogni rete di settore o di categoria potrà essere collegata direttamente alla Rete Nazionale e quindi alla RUPA secondo gli stessi principi seguiti nel caso delle reti regionali.
- *Singolo ente*. Un singolo ente potrà accedere direttamente ai servizi della Rete Nazionale e quindi alla RUPA secondo le procedure che verranno definite dal Dipartimento.

La comunicazione sicura all'interno dei confini del servizio di interconnessione della Rete Nazionale (per esempio nel segmento che unisce una intranet PAC a una rete regionale) avverrà sotto il controllo di un Centro per la sicurezza. La gestione della sicurezza e di qualsiasi altro requisito di servizio entro i confini di una rete regionale, di una rete di settore o categoria o delle Intranet delle amministrazioni è a carico dei rispettivi gestori. Questa suddivisione della responsabilità di gestione della sicurezza rappresenta un aspetto critico ma necessario per rispettare la autonomia gestionale di ogni singola amministrazione per ciò che concerne la sicurezza della propria rete.
Questa criticità può essere superata dalla definizione, da parte del Dipartimento, di requisiti tecnici ed architetturali standard per le reti che vogliono interconnettersi alla Rete Nazionale e che permettano una gestione integrata di livelli minimi di sicurezza end-to-end.
La responsabilità di gestione della comunicazione tra due punti interni di due diverse amministrazioni è individuabile in tre aree:

- all'interno della intranet della prima amministrazione;
- all'interno del servizio di interconnessione della Rete Nazionale;
- all'interno della intranet della seconda amministrazione

I Fornitori dei servizi di accesso

Per quanto riguarda i fornitori dei servizi di accesso alla Rete Nazionale, gli ISP, non e' prevista una selezione su scala nazionale mentre è auspicabile che un processo di

validazione/accreditamento di tali fornitori avvenga su scala locale al fine di garantire i singoli enti e avviare un'opera di sensibilizzazione del mercato sulla necessità di fornire servizi di connettività di qualità.
Le singole amministrazioni (o aggregazione di enti/amministrazioni) che intendono acquisire una connessione alla Rete Nazionale attiveranno procedure autonome di acquisizione dei servizi e sono tenute a richiedere nei contratti sottoscritti con il proprio fornitore di servizi di accesso il rispetto dei requisiti minimi. Ciò vale sia per i contratti RUPA sia per i contratti sottoscritti con altri Provider.
La Rete Nazionale è inoltre fondata sull'esistenza di ulteriori operatori, denominati EPO (Exchange Point Operator) che non intervengono direttamente nel rapporto contrattuale con le singole amministrazioni, ma che garantiscono l'interconnessione tra i diversi SP (Service Provider) dei servizi di accesso alla Rete Nazionale e che permettono la creazione dell'unico backbone IP virtuale.

Riassumendo, un'amministrazione locale può collegarsi alla Rete Nazionale:

1. tramite un rete regionale, una Community Network, una rete di settore o di categoria già connesse alla Rete Nazionale;
2. tramite un Service Provider collegato ad uno dei NAP o EPO esistenti;
3. tramite la RUPA, aderendo ad uno dei contratti quadro esistenti.

Principi di cooperazione applicativa

L'erogazione di servizi integrati ai cittadini e alle imprese, fra gli obiettivi del piano di azione di e-government, implica l'integrazione tra i servizi di diverse amministrazioni. Sul piano tecnologico ciò si traduce nell'interoperabilità dei sistemi informatici delle amministrazioni, descritta, allo stato attuale della tecnologia, nel documento "Rete Nazionale: architettura applicativa", di cui, nel seguito, si fornisce una sintesi.

Organizzazione per domini

Per garantire autonomia alle singole Amministrazioni, lasciando inalterato il loro patrimonio informativo, si definisce il **dominio** come "l'insieme delle risorse (in particolare le procedure, i dati e i servizi) e delle politiche di una determinata organizzazione ". Il dominio è anche il **confine di responsabilità** di un'organizzazione, in particolare per quanto riguarda le politiche che definiscono il suo sistema informativo. La Rete nazionale è concepita come una federazione di domini.
Secondo questo modello, la comunicazione avviene tra entità omogenee (i domini appunto) e lo scopo dell'architettura cooperativa è abilitare l'integrazione degli oggetti informativi (procedure e dati) e delle politiche di domini diversi. L'elemento fondamentale è rappresentato dalla definizione delle modalità in base alle quali un dominio *servente* esporta i propri servizi ed un dominio *cliente* vi accede.
L'interoperabilità fra amministrazioni dovrà svilupparsi sulla base di standard definiti a livello nazionale in modo tale che:

1. siano identificati **i servizi ed i dati** che ogni amministrazione deciderà di rendere disponibili sulla rete;
2. siano rispettati, per ogni servizio esposto, le **politiche di sicurezza e di accesso** e **di controllo di qualità e correttezza dei servizi erogati, stabilite dall'Amministrazione erogante di concerto con il Dipartimento**.

Porte di dominio

L'elemento tecnologico che realizza la cooperazione è la **porta di dominio**, che ha la funzione di *proxy* per l'accesso alle risorse applicative. È bene sottolineare che la porta di dominio fa parte prima di tutto del modello organizzativo della Rete nazionale, e come tale trova naturalmente posto nella progettazione concettuale piuttosto che in quella logica o fisica. In particolare, a livello concettuale esiste una sola porta per ogni dominio, che rappresenta la somma di tutti gli apparati preposti all'accesso delle risorse del dominio.
Dal punto di vista dell'architettura applicativa, le porte di dominio possono essere viste come degli **adattatori**, che consentono a sistemi informatici esistenti, o comunque progettati e realizzati in base alle esigenze del dominio specifico, di affacciarsi sulla Rete nazionale e partecipare all'interscambio telematico delle informazioni.

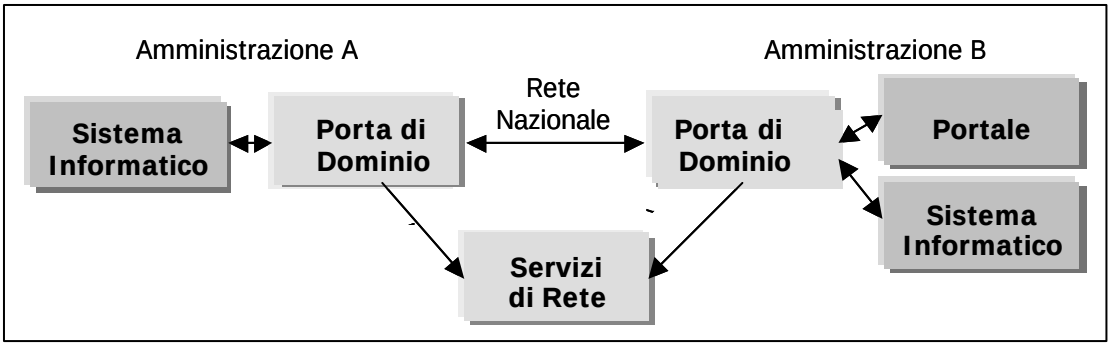

Figura 2 – Modello di riferimento per l'integrazione delle porte di dominio

Nella Figura 2 il termine "sistema informatico" deve essere inteso nella sua accezione più ampia. In particolare, può trattarsi di:

- un sistema 'monolitico', o comunque operante su un singolo nodo presso un'amministrazione di piccole dimensioni;
- un sistema distribuito su più nodi collegati in rete locale presso un'amministrazione di dimensioni maggiori;
- una rete di area (per es. aggregazione di comuni, comunità montana, rete provinciale o regionale), alla quale sono collegati i sistemi informatici di amministrazioni anche diverse, o di una singola amministrazione (ad esempio la rete territoriale gestita da un'agenzia o un ministero).

Risulta quindi chiaro che le porte di dominio, come componenti software di adattamento, possono essere chiamate a svolgere funzioni di integrazione diverse, a seconda del contesto di dispiegamento.
In quest'ottica, anche i sistemi di accesso ai servizi amministrativi per gli operatori umani, cioè i "portali", devono essere considerati dei sistemi informatici che accedono alla rete di cooperazione applicativa. In linea di principio, un "portale" potrebbe infatti essere:

- un sistema di accesso ai servizi di cooperazione applicativa funzionante presso una singola amministrazione, a cui hanno accesso solo gli operatori dell'amministrazione stessa (*intranet* locale);
- un portale di servizi integrato a cui hanno accesso solo operatori autorizzati ed identificati, anche attraverso procedure di *single sign-on* (*intranet* di area);
- un portale di servizi per la pubblica amministrazione cui hanno accesso solo operatori identificabili (portale di *back-office*);
- un portale di accesso orientato ai cittadini, al quale essi possono accedere utilizzando sistemi di identificazione opportuni (per es.. carta d'identità elettronica, carta nazionale dei servizi) ed ottenere servizi amministrativi di vario genere (portale di *front-office*).

Oltre alle porte di dominio, la cooperazione applicativa distribuita richiede la presenza di altri **servizi di rete** che consentano lo svolgimento di determinate forme di collaborazione tra domini. In particolare, i servizi di rete includono i servizi di individuazione degli indirizzi (***directory***), quello di trasferimento (***routing***) dei messaggi verso i domini destinatari e servizi di comunicazione eventi come ad esempio i servizi ***lagging consistency-based, publish-based, workflow-based*** basati su strati quali message-queuing, publish&subscribe e middleware similari.

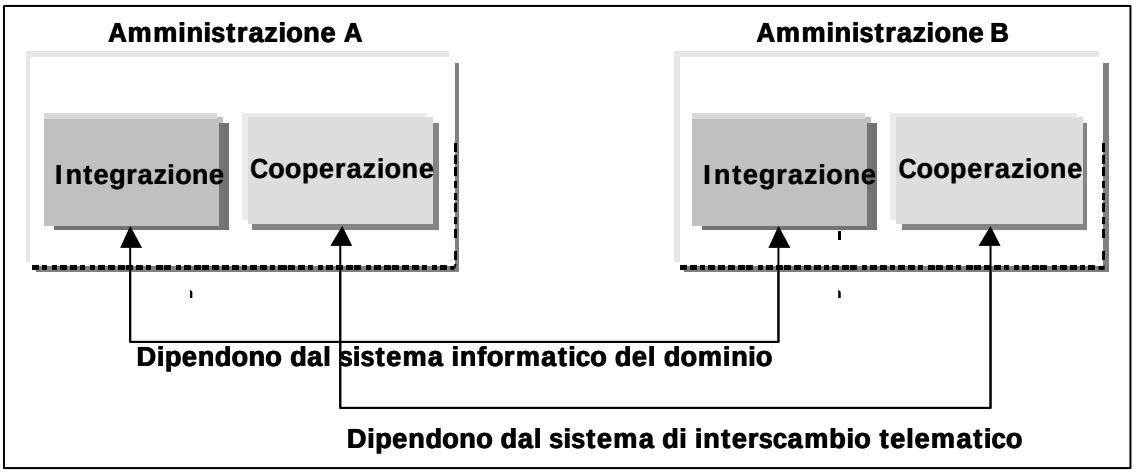

Figura 3 – Struttura interna delle porte di dominio

Dal punto di vista logico, ciascuna delle due porte di dominio è formata da due componenti distinti:

1. una componente che realizza le funzioni generiche, o di **cooperazione**, dipendenti dagli standard relativi alle **modalità telematiche** ed ai **profili di collaborazione**;
2. una componente che realizza le funzioni di **integrazione**, che realizza l'adattamento verso il sistema informatico (o i sistemi informatici) di dominio e garantisce tra l'altro il rispetto dei formati di codifica per il contenuto applicativo.

Come mostrato in Figura 3, le componenti che implementano le funzioni generiche dipendono unicamente dagli standard stabiliti per tutta la Rete nazionale. Al contrario, le componenti di integrazione dipendono dagli standard di tipo applicativo, che sono pure definiti per tutta la Rete nazionale, ma anche dalle caratteristiche specifiche dei sistemi informatici da integrare (e.g. tecnologia e schema dei database, presenza di middleware come sistemi a code o di accesso a *mainframe*, interfacce funzionali o di accesso remoto).

La porta di dominio, e più in particolare la sua componente delegata alla cooperazione, rappresenta dunque l'unico punto di contatto telematico tra domini: sulla propria porta di dominio ogni dominio veicola le richieste di servizio verso gli altri domini della Rete nazionale e, simmetricamente, riceve tutte le richieste di servizio provenienti dagli altri domini, identificandovi il confine della propria responsabilità.
Per garantire che ogni porta di dominio, e quindi ogni amministrazione, possa effettivamente colloquiare con tutte le altre porte, devono essere adottati formati standard di codifica per i messaggi che veicolano le richieste di servizio fra le varie porte di dominio. Di conseguenza, il contenuto informativo ed i formati di codifica dei messaggi devono essere chiaramente definiti prima che le informazioni possano essere effettivamente scambiate.
L'adattamento degli specifici applicativi ai formati standard definiti dei dati e delle informazioni prodotti all'interno del dominio, viene svolto dalla funzione di **integrazione** che dovrà essere quindi un componente software specifico del dominio ed adeguato alle realtà specifiche.
In particolare, al fine di garantire il più possibile l'uniformità delle porte di dominio, la conversione dei dati e dei documenti dai formati specifici delle applicazioni nei formati standard dovrà essere realizzata dal **solo** componente di integrazione. Viceversa, il componente di cooperazione dovrà gestire **solo** documenti codificati secondo standard definiti su base nazionale.

Modello delle interazioni

In base all'esperienza ed alla letteratura informatica, i paradigmi della cooperazione applicativa sono riconducibili a due tipologie principali: la richiesta di servizio e la comunicazione di evento.
La richiesta di servizio consiste in un messaggio prodotto da una applicazione di un dominio cliente e diretto ad una applicazione di un dominio servente. Il messaggio determina l'esecuzione di una applicazione del dominio servente che, in base alle informazioni contenute nel messaggio, esegue una procedura ed invia una risposta destinata all'applicazione cliente. La risposta è un'indicazione certa che l'applicazione servente ha attuato la richiesta e che abbia avuto esito positivo/negativo.
Dal punto di vista dell'interazione amministrativa, la richiesta di servizio è sempre sincrona, nel senso che prima o poi l'applicazione cliente si dovrà sincronizzare sulla risposta, perché dovrà utilizzarne le informazioni applicative, magari per successive nuove richieste.
La richiesta di servizio può essere di due tipi:

1. **interrogazione**: richiesta di servizio finalizzata all'acquisizione di un'informazione del dominio servente ma che non modifica alcun oggetto applicativo interno allo stesso dominio servente;
2. **transazione**: richiesta di servizio destinata a produrre una variazione permanente in un oggetto applicativo del dominio servente; il termine transazione è qui inteso in senso amministrativo più che informatico.

La comunicazione di evento è il messaggio che viene generato da un'applicazione allo scopo di informare altre applicazioni di uno o più domini destinatari dell'avvenuto cambiamento delle informazioni relative ad un oggetto applicativo (p. es. cambio di residenza) o della creazione di un nuovo oggetto applicativo (p. es. a seguito della registrazione di una nascita). Nel caso della comunicazione evento, il messaggio contiene anche le informazioni, nuove o modificate, che descrivono l'evento stesso.

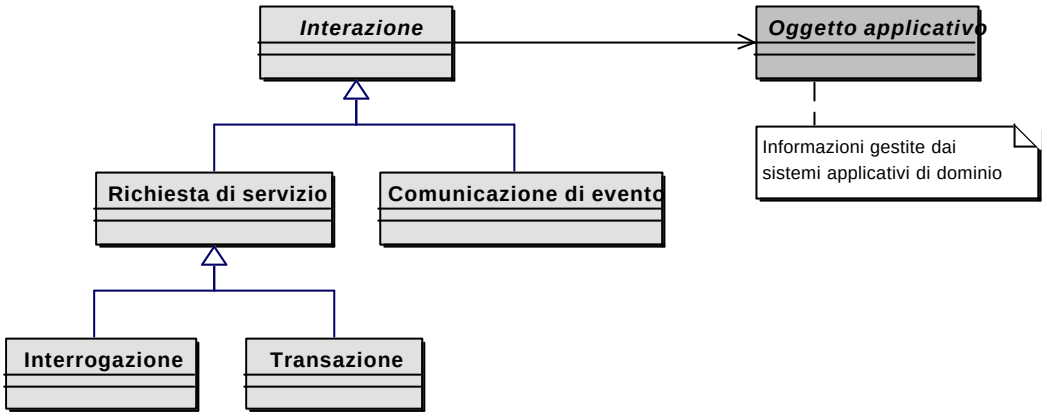

Figura 4 – Interazioni ed oggetti applicativi

Profili di collaborazione

Nell'ambito della definizione degli standard per la cooperazione applicativa, uno degli aspetti che devono essere normalizzati è quello dei profili di collaborazione, cioè degli schemi di interscambio di messaggi tra porte di dominio.
In termini generali, si assume che ciascun episodio di collaborazione applicativa preveda lo scambio di una coppia di messaggi: una richiesta inviata da una porta delegata a cui fa seguito una risposta da parte di una porta applicativa.
Le collaborazioni principali qui descritte prevedono lo scambio di messaggi in modalità *sincrona* e *asincrona*. Per convenzione, il sincronismo viene visto dal punto di vista della porta delegata, presso la quale ha inizio ogni episodio di collaborazione:

- in uno scambio *sincrono* la porta delegata invia la propria richiesta applicativa ed attende quindi la risposta della porta applicativa;
- al contrario, in uno scambio *asincrono*, la risposta della porta applicativa può essere inviata in un tempo successivo e la porta delegata non rimane quindi in attesa.

La scelta della modalità sincrona o asincrona può dipendere da aspetti legati alla latenza delle procedure amministrative (e.g. la necessità di intervento umano, ad esempio per l'apposizione della firma digitale di un pubblico ufficiale). Tuttavia, in linea di principio, tale scelta può dipendere anche da scelte di carattere esclusivamente tecnologico, come dimostra l'ampia diffusione nell'informatica gestionale dei sistemi basati su code, che adottano una modalità asincrona.

Si noti che le modalità telematiche sincrona e asincrona adottate dalla porte di dominio non coincidono necessariamente con le modalità adottate dai sistemi informatici operanti nei domini coinvolti. In particolare, uno scambio asincrono non comporta affatto che il sistema informatico richiedente rimanga in uno stato di attesa. Come infatti accade già oggi per i sistemi di supporto alla gestione degli scambi tradizionali (p. es. sistemi di protocollo informatico), l'invio del messaggio di andata e la ricezione del messaggio di ritorno comportano semplicemente con il cambio di stato di una corrispondente registrazione.
In ogni caso, è da sottolineare che:

- la scelta del profilo di collaborazione non dipende in generale dal tipo di servizio erogato ma dalle modalità organizzative ed implementative utilizzate per l'esportazione telematica;
- è quindi possibile che lo stesso servizio possa essere esportato con modalità diverse da domini diversi;
- la definizione dei profili di collaborazione ammissibili per ciascun servizio esportato dalle amministrazioni è di fatto un pre-requisito per l'esportazione telematica e deve essere quindi stabilita in anticipo;
- è possibile che alcune porte di dominio esportino un servizio in base ad uno solo o comunque ad un sottoinsieme dei profili ammissibili; questo elemento deve essere comunque pubblicato nel sistema di *registry* dei servizi.

Modalità di scambio telematico

In linea di principio, gli scambi telematici possono avvenire utilizzando protocolli di trasporto diversi. Il successo del modello Internet ha avuto come effetto la grande diffusione dei protocolli leggeri basati su codifiche testuali (HTTP, SMTP) per l'interazione tra sistemi eterogenei. Appare quindi logico affermare che:

1. l'interscambio telematico interdominio viene effettuato utilizzando solamente il protocollo HTTP sia per gli scambi sincroni che per gli scambi asincroni e/o il protocollo SMTP per i soli scambi asincroni;
2. viceversa, all'interno di ciascun dominio l'interscambio telematico avviene in base a standard locali prescelti e definiti da ciascun dominio.
3. l'uso di protocolli crittografici deve essere ridotto al minimo ed utilizzato esclusivamente per le componenti sensibili delle informazioni scambiate

Dal punto di vista telematico, una simile scelta presenta i seguenti vantaggi:

- i protocolli HTTP ed SMTP utilizzano la codifica testuale dei messaggi ed è possibile adottare dei formati applicativi utilizzabili indifferentemente con entrambi;
- la definizione del formato dei messaggi può essere basata sugli standard riconosciuti ed accettati per lo scambio di servizi su web;
- le componenti generiche e fattorizzabili, delle porte di dominio possono prendersi carico di buna parte della gestione del formato dei messaggi senza dover interagire direttamente con gli applicativi.

Principi di sicurezza

Il modello di sicurezza si basa sui seguenti concetti:

- **entità**: utente o programma software che opera all'interno di un dominio;
- **servizio**: individua la funzionalità richiesta;
- **ruolo**: individua un utente astratto a cui vengono poi associati i richiedenti e gli esecutori del servizio;
- **profilo**: individua l'insieme di azioni che possono essere effettuate su un certo servizio; per ogni servizio viene associato un profilo ad ogni singolo ruolo.

Le funzionalità di sicurezza che devono essere fornite dalle porte di dominio sono le seguenti:

- **autenticazione e identificazione**: individuare in modo certo, attraverso le credenziali di sicurezza fornite, l'entità che sta accedendo ad una risorsa (dati o servizio);
- **autorizzazione**: verificare che l'entità riconosciuta abbia i diritti per fare l'azione richiesta, utilizzando il concetto di ruolo e profilo;
- **riservatezza**: garantire che solo il mittente ed il ricevente possano avere i dati della richiesta/risposta in chiaro;
- **integrità**: garantire che i dati della richiesta/risposta non siano modificati durante la trasmissione;
- **non ripudiabilità**: garantire che chi ha inviato una richiesta/risposta non possa rinnegare di averla emessa;
- **tracciabilità**: tracciare con modalità a terza parte tutte le richieste/risposte inviate e ricevute al fine garantire i necessari riscontri di sicurezza, generare allarmi applicativi e fornire la **garanzia di provenienza**.

Si prevede che i ruoli utilizzati all'interno della Rete nazionale siano definiti dagli Enti responsabili dell'erogazione dei diversi servizi e che per ogni servizio pubblicato vengano definiti i profili applicativi relativi a ciascun ruolo. Ruoli e profili saranno pubblicati sul registro dei servizi disponibili in rete.

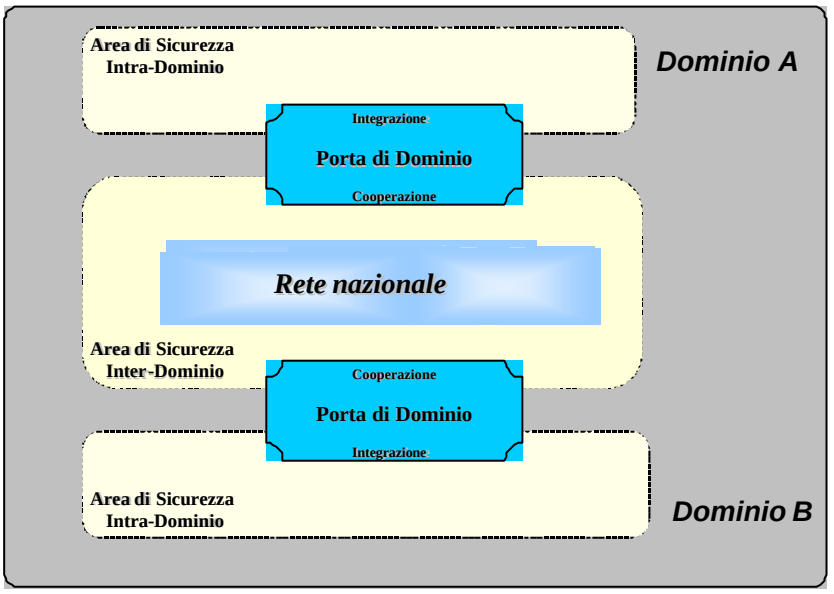

Figura 5 – Aree di sicurezza

A livello di trasporto telematico, la decisione di un soggetto di partecipare alla Rete nazionale comporta l'adozione di meccanismi di sicurezza ben precisi (p. es. utilizzo di protocolli a sicurezza intrinseca come IPSec, quest'ultimo non appena operante come standard di mercato in ambiente multifornitore). Anche dal punto di vista della cooperazione applicativa, la partecipazione alla Rete nazionale comporta l'adozione di politiche di sicurezza stabilite dal Ministro per l'Innovazione e le Tecnologie.

La busta di e-government

L'elemento fondamentale che caratterizza i messaggi per la cooperazione applicativa è la completa e preliminare definizione del contenuto e del formato di codifica. I messaggi tra le porte di dominio sono infatti parte integrante di uno scambio tra applicazioni e non tra operatori umani. Di conseguenza, il contenuto di questi messaggi deve essere totalmente interpretabile in modo automatico.

La distinzione tra componenti delle porta di dominio che realizzano funzioni generiche e funzioni di integrazione applicativa specifica si riflette, in linea di principio, nella organizzazione della struttura generale di ciascun messaggio in due parti principali:

1. una parte di ***busta***, che contiene le indicazioni relative al mittente, il destinatario (intese come porte di dominio), al servizio richiesto ed al profilo di collaborazione utilizzato; tale busta viene in generale gestita dalle componenti di collaborazione delle porte di dominio e deve quindi essere il più generale possibile;
2. una parte di ***contenuto*** applicativo, rappresentato dalle informazioni effettive previste per quel tipo di servizio e di scambio (p. es. i dati identificativi personali di una richiesta di informazioni anagrafica).

In generale, il tipo di struttura da utilizzarsi per busta e contenuto dipende dal tipo di messaggio e dalle esigenze di carattere normativo.

Uno degli strumenti indicati per definire un formato dei dati condiviso in modo generalizzato tra tutte le amministrazioni, a prescindere dai sistemi *"legacy"* e dalle basi dati, è XML (eXtensible Markup Language, http://www.w3.org/XML/), in quanto consente di definire il contenuto dei dati di comune interesse e di strutturare le stringhe di dati scambiati nei processi di cooperazione.
Accanto ad esso, l'attuale scenario tecnologico indica SOAP (Single Object Access Protocol, http://www.w3.org/2000/xp/Group/) come standard emergente per il veicolamento delle informazioni codificate con XML sulla rete Internet, mediante il protocollo HTTP.

Struttura generale della busta di egovernment

In Figura 6 è descritta la struttura più generale dei messaggi scambiati tra le porte di dominio. Nella figura, la parte di *busta* è in grigio chiaro mentre la parte di *contenuto* è indicata in grigio più scuro.

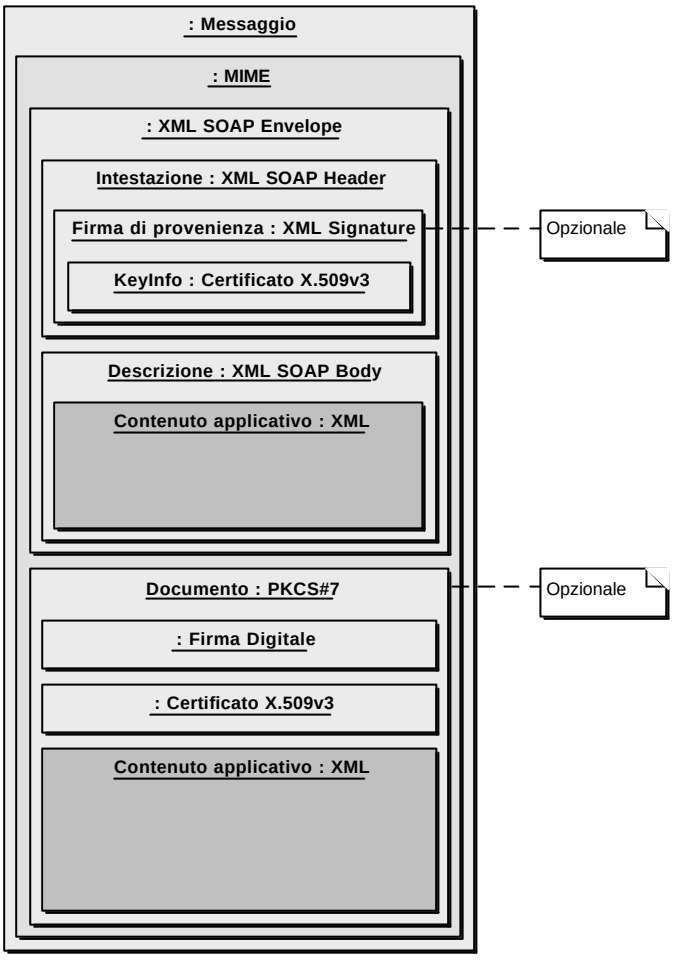

Figura 6 – Struttura generale della busta di e-government

La parte più esterna della struttura è formata da elementi specifici di codifica per i protocolli HTTP o SMTP (tipicamente *header fields*) ed è di fatto indipendente dal resto[1].
L'elemento principale di un messaggio è rappresentato da una struttura *XML SOAP* composta da due parti: *intestazione* e *descrizione*:

- l'intestazione (*XML SOAP Header*) contiene i dati relativi al messaggio ed in particolare contiene l'identificativo del messaggio, che coincide con l'identificatore di protocollo;
- la descrizione (*XML SOAP Body*) riporta i dati riguardanti il contenuto applicativo del servizio; tali dati possono includere l'insieme completo delle informazioni riguardanti la richiesta (o la risposta) oppure limitarsi alla semplice l'indicazione del tipo di documento informatico allegato e del relativo formato di codifica.

Dal punto di vista amministrativo, la struttura XML SOAP incorpora anche il ruolo della segnatura informatica in formato XML del messaggio in quanto riporta i dati minimi della registrazione di protocollo. La struttura XML SOAP può essere utilizzata in combinazione con lo standard WSDL per la descrizione dei servizi e con lo standard UDDI per la realizzazione dei *repository* di descrizione dei servizi.
La struttura XML SOAP può inoltre essere inclusa in una struttura MIME allo scopo di allegare al messaggio uno o più documenti applicativi, in base allo standard *XML SOAP with attachments*. Ad esempio potrebbe essere allegato un documento su cui è

[1] In teoria, come previsto dallo standard *XML Protocol*, il resto della struttura potrebbe utilizzato anche con un *protocol bidning* diverso da HTTP e SMTP.

stata apposta la firma di un pubblico ufficiale. La presenza degli allegati è comunque opzionale.
Una firma opzionale può essere inclusa nell'intestazione utilizzando gli standard *XML SOAP Security* e *XML Signature* e potrebbe, ad esempio, essere usata per garantire la fonte di provenienza delle informazioni (art. 43 del D.P.R. 445/2000).
Nel caso di documenti informatici firmati aventi rilevanza legale è adottato il formato il PKCS#7 in base della circolare AIPA CR/24, di cui si auspica, peraltro, un tempestivo aggiornamento. Tali documenti saranno, fino a tale aggiornamento, inclusi sotto forma di allegato.
Quando non è presente la XML *Signature* la struttura XML SOAP contiene unicamente le informazioni relative al protocollo e le informazioni necessarie alle porte di dominio per il *routing* applicativo, mentre il contenuto applicativo XML sarà riportato nell'allegato. Ciò ne consente, quando necessario, anche la cifratura (per esempio nella consultazione del casellario giudiziario), dato che lo standard *XML Encryption* si trova ancora in uno stadio di definizione preliminare.
La scelta delle strutture specifiche per la busta di e-government da utilizzare nello scambio dei messaggi costituisce una parte integrante della definizione preliminare dei servizi e non può costituire una variante da negoziarsi per ciascuno scambio.

Riassumendo, un'amministrazione che intenda realizzare servizi tramite la cooperazione applicativa, deve:

1. essere connessa alla Rete Nazionale;
2. organizzare il proprio accesso alla Rete Nazionale secondo il modello della porta di dominio;
3. realizzare le interfacce fra i servizi disponibili sul proprio sistema informativo e la porta di dominio (componente di integrazione)
4. controllare la qualità e la correttezza dei servizi erogati
5. fornire, alle altre amministrazioni, l'accesso ai propri servizi sulla porta di dominio (componente di cooperazione), utilizzando un formato standard di descrizione e scambio dei dati e dei servizi basato su XML/SOAP o, se necessario, utilizzando un formato concordato fra le diverse amministrazioni che concorrono all'erogazione del servizio

Standard tecnologici per l'interoperabilità

Lo standard XML

XML è stato studiato per consentire e facilitare scambi di dati anche tra applicazioni di tipo diverso, come ad esempio i database in ambienti eterogenei, e per facilitare i processi di cooperazione applicativa basati sullo scambio di dati.

La famiglia di standard XML

Nome	Descrizione	Stato	Riferimento
XML	Metalinguaggio che permette di definire marcature dell'informazione per generare classi di documenti e dati strutturati in modo gerarchico.	W3C Recommendation dal 6 ottobre 2000	http://www.w3.org/TR/REC-xml
DTD	*Document Type Definition*: formato di specifica e descrizione della struttura dei tag XML. DTD consente, con una sintassi simile alla Backus-Naur Form, di definire la grammaticaper una classe di documenti XML.		http://www.w3.org/TR/REC-xml
XML Schema	Formato di specifica e descrizione della struttura di documenti XML e consente di definire grammatiche più articolate e complesse dello schema dei documenti rispetto ai DTD.	W3C Recommendation dal 2 maggio 2001	http://www.w3.org/TR/xmlschema-0/
CSS	Linguaggio di *stylesheet* applicabile sia a XML che a HTML	W3C Recommendation dal 17 dicembre 1996	http://www.w3.org/TR/REC-CSS1
XSL (XSLT, XSL-FO)	Linguaggio di *stylesheet* per XML. Suddiviso in due parti: XSLT consente di trasformare un documento XML in un altro documento XML. XSL-FO associa ad ogni elemento le informazioni di *rendering* per la composizione di un documento finale.	W3C Candidate Recommendation dal 21 novembre 2000	http://www.w3.org/TR/xsl/
XML Protocol	Un modello generale ed astratto di protocollo per lo scambio di servizi basati su XML	W3C Working Draft del 9 luglio 2001	http://www.w3.org/TR/xmlp-am/
XML SOAP	Protocollo leggero ideato per permettere alle applicazioni di invocare metodi o funzioni che risiedono su server remoti e scambio semplice di messaggi.	W3C Note del 8 maggio 2000	http://www.w3.org/TR/SOAP/
UDDI	Protocollo per la descrizione e l'integrazione di servizi attraverso l'uso di un repository.	Versione 2.0 del 8 giugno 2001	http://Www.uddi.org
XML SOAP Security	Standard di regole sintattiche e funzionali per l'utilizzo della XML signature nei messaggi SOAP	W3C Note del 6 maggio 2001	http://www.w3.org/TR/SOAP-dsig/
ebXML	ebXML è un'iniziativa promossa dalle Nazioni Unite in collaborazione con l'organismo internazionale OASIS per creare una base tecnologica aperta, fondata su XML, per permettere lo scambio di informazioni e il commercio elettronico a livello globale.	Versione 1.0 del 16 febbraio 2001	http://www.ebxml.org/specs/index.html
WSDL	Specifica basata su XML per la definizione delle interfacce funzionali per l'accesso e l'interazione tra servizi sul Web	W3C Note del 15 marzo 2001	http://www.w3.org/TR/wsdl

Standard di interoperabilità

Nome	Descrizione	Stato	Riferimento
SMTP	Protocollo per l'invio di posta elettronica		RFC 821, 822, 1869
POP3	Protocollo per la lettura e lo scaricamento di messaggi di posta elettronica da un server remoto. Di semplice implementazione ed uso, questo protocollo risulta meno complesso di IMAP.	POP v3	RFC 1725,1939

	complesso di IMAP.		
IMAP	Protocollo per la lettura e lo scaricamento di messaggi di posta elettronica da un server remoto. A differenza di POP, questo protocollo consente funzionalità aggiuntive quali il mantenimento dei messaggi sul server e la ricerca avanzata.	IMAP v4	RFC 1730,1731
FTP	Protocollo per lo scambio di file su Internet.		RFC 354,683
MIME	Formato per la composizione di messaggi di posta elettronica formati da più parti di natura diversa.		RFC 2045-2049
HTTP	Protocollo a livello applicativo per sistemi distribuiti, collaborativi e multimediali. Si tratta di un protocollo generico e stateless che può essere usato per gli scopi più diversi. Oltre al semplice scambio di ipertesti, può implementare name servers o sistemi ad oggetti distribuiti con l'estensione dei metodi di interrogazione, dei codici di errore, degli header.	Versione 1.1 del giugno 1999	RFC 2616

Standard di sicurezza

Nome	Descrizione	Stato	Riferimento
X.509	Specifica del formato dei certificati e delle Certificate Revocation List (CRL) per i sistemi di sicurezza basti su Internet.	Versione 3.0	RFC 2459
XML Signature	Standard di firma digitale su XML	W3C Proposed Recommendation del 20 agosto 2001	http://www.w3.org/Signature/
PKCS	Public-Key Cryptography Standards: un insieme di protocolli standard per lo scambio sicuro di informazioni usando una infrastruttura a chiave pubblica (PKI).		http://www.rsasecurity.com/rsalabs/pkcs/index.html