Sistema pubblico di cooperazione:
STANDARD E TECNOLOGIE

Versione 1.0

INDICE

1. MODIFICHE DOCUMENTO 3
2. RIFERIMENTI 4
3. TERMINI E DEFINIZIONI 5
4. STRUTTURA ED ORGANIZZAZIONE DEI DOCUMENTI 7
4.1. Lista dei documenti SPC 7
4.2. Note di lettura dei documenti 9
5. OBIETTIVI E CONTENUTI DEL DOCUMENTO 11
5.1. Struttura del Documento 11
5.2. Componenti del gruppo di lavoro 12
6. IL CONTESTO DI RIFERIMENTO 14
6.1. Differenze tra Specifica e Standard 14
6.1.1. Come si giunge a una Recommendation 15
7. SERVIZI INFRASTRUTTURALI PER LA COOPERAZIONE. 18
7.1. Il Registro dei servizi. 18
7.1.1. Funzionalità del Registro dei servizi. 18
7.1.1.1. Modalità di utilizzo del registro 19
7.1.1.2. Convenzioni per l'utilizzo del registry UDDI. 22
7.1.1.3. Modello dei dati di un registro UDDI 23
7.1.1.4. I link del registro dei servizi. 25
7.1.1.5. Architettura federata. 26
7.1.2. Indice dei soggetti - Indice delle amministrazioni pubbliche e delle aree organizzative omogenee PA (IPA) 29
7.1.3. Banche documentali 31
7.1.3.1. Modalità di utilizzo 32
7.1.3.2. Descrizione del formato dei dati 33
7.2. Porte di Dominio 34
7.2.1. Modelli di Cooperazione tra Porte di Dominio 34
7.2.1.1. Scenario di invocazione unidirezionale 37
7.2.1.2. Scenario di invocazione Richiesta/risposta sincrono 37
7.2.1.3. Scenario di invocazione Richiesta/risposta asincrono simmetrico. 37
7.2.1.4. Scenario di richiesta/risposta asincrono asimmetrico 38
7.2.1.5. Cooperazione per notifica di eventi 38
7.3. Gestore degli eventi. 40
7.4. Specifiche da definire 43
7.4.1. Gestione dei processi 44
7.4.1.1. Lo stato attuale 46
7.4.1.2. La convergenza 46
8. TASSONOMIA 48
8.1. Principi 48
8.2. Template 48

8.3. Iniziative per migliorare la qualità dei dati. 49

9. SICUREZZA NELLE INTERAZIONI TRA APPLICAZIONI 51

9.1. Premessa 51

9.2. Modello di riferimento 51

9.2.1. Funzioni di sicurezza 52

9.2.2. Misure di sicurezza 53

9.3. Sicurezza delle porte di dominio 54

9.3.1. Autenticazione dei messaggi 57

9.3.2. Confidenzialità 59

9.3.3. Integrità 62

9.4. Tracciatura 63

9.4.1. Tipologie di tracce 64

9.4.2. Correlazione delle tracce applicative 64

9.4.3. Compatibilità con il protocollo informatico 65

9.4.4. Caratteristiche delle tracce applicative 65

9.5. Criteri per la sicurezza dei servizi 65

9.5.1. Autorizzazione 66

9.5.2. Non ripudio 67

9.5.2.1. Firma digitale 67

9.5.2.2. Altre firme elettroniche 68

9.6. Profilo dei certificati 69

9.7. Stato dei certificati 69

APPENDICE 70

A1 ESEMPI DI UTILIZZO DEI REGISTRI 70

A1.1 Autenticazione del client per la pubblicazione di un documento 70

A1.2 Pubblicazione di un documento WSDL in un registro UDDI 70

A1.3 tModel con riferimenti a documenti HTML 74

A2 LE STRUTTURE DATI DEL MODELLO UDDI 75

A2.1 L'entità businessEntity 75

A2.2 L'entità businessService 76

A2.3 L'entità bindingTemplate 77

A2.4 L'entità tModel 78

A2.5 L'entità PublisherAssertion 79

A3 IL PROGETTO SIGMA TER 81

A3.1 Descrizione del progetto 81

A3.2 Il formato del campo indirizzo 82

A3.1.1 Toponimi 84

A3.2.1 Esempio di Stradario 95

1. MODIFICHE DOCUMENTO

Descrizione Modifica	Edizione	Data
Prima emissione versione "beta" da approvare da parte del Gdl	beta	30/07/2004
Seconda emissione della versione "beta" da approvare da parte del Gdl	beta 2	15/09/2004
Pubblicazione versione approvata da Gdl e TCP Stato, Regioni e EE.LL.	1.0	25/11/2004

2. RIFERIMENTI

Codice	Titolo
[Busta e-Government]	http://www.cnipa.gov.it/site/_files/4.SPC_Busta%20e-Gov%20v.1_0-21-04-2004.pdf http://www.cnipa.gov.it/site/_files/AbstractBusta-%20e-Gov-ver-%202.pdf
[INDICE PA]	http://www.cnipa.gov.it/site/_files/Schema_Interop_IndicePA.pdf
[LDAPv.2]	http://www.ietf.org/rfc/rfc1777.txt
[LDAPv.3]	http://www.ietf.org/rfc/rfc2251.txt
[Qualità dei Dati]	http://www.cnipa.gov.it/site/_contentfiles/00462900/462996_4_2002.pdf
[RELAX NG]	http://relaxng.org/
[UDDI 2.0]	www.uddi.org versione 2 delle specifiche
[UDDI 2.03 Data Structure Reference]	http://uddi.org/pubs/DataStructure-V2.03-Published-20020719.pdf
[UDDI 2.03 ReplicationSpecification]	http://uddi.org/pubs/Replication-V2.03-Published-20020719.pdf
[XML]	http://www.w3.org/TR/REC-xml/
[W3C XML Schema]	http://www.w3.org/XML/Schema/
[WSDL – UDDI 1.07]	http://www.uddi.org/pubs/wsdlbestpractices-V1.07-Open-20020521.pdf
[WSDL-UDDI 1.08]	http://www.oasis-open.org/committees/uddi-spec/doc/bp/uddi-spec-tc-bp-using-wsdl-v108-20021110.htm
[WSDL-UDDI 2.0]	http://www.oasis-open.org/committees/uddi-spec/doc/tn/uddi-spec-tc-tn-wsdl-v200-20031104.htm
[WS-I Basic Profile 1.0]	http://www.ws-i.org/Profiles/BasicProfile-1.0-2004-04-16.html

3. TERMINI E DEFINIZIONI

Termine/Acronimo	Descrizione
API	Application Programming Interface
CNIPA	Centro nazionale per l'informatica nella Pubblica Amministrazione
DEM	Document Exchange Model
Dominio	Si definisce il dominio come l'insieme delle risorse(in particolare le procedure, i dati e ei servizi) e delle politiche di una determinata organizzazione. Il dominio definisce il confine di responsabilità di una organizzazione, in particolare per ciò che riguarda le politiche afferenti al proprio sistema informativo.
DUNS	D&B (Dun and The Bradstreet Companies) è la società americana che nel 1963, introdusse il "Data Universal Numbering System" il numero DUNS®, utilizzato per identificare numericamente ed univocamente Enti, Società ed Organizzazioni per agevolare l'elaborazione automatica dei flussi dati tra esse scambiati. Il DUNS® è diventato l'identificativo standard delle Aziende per le Nazioni Unite, la Commissione Europea ed il Governo degli Stati Uniti d'America.
ebXML: Electronic Business XML	Protocollo basato su XML utilizzato per incapsulare i dati da trasmettere tra processi applicativi automatizzati complessi
Porta Applicativa	Ruolo assunto da una Porta di Dominio nell'ambito di un episodio di collaborazione applicativa. Assume tale ruolo la Porta di Dominio che , a seguito della ricezione di un messaggio di richiesta, proveniente da un'altra Porta di Dominio (Porta Delegata), invia al mittente un messaggio di risposta.
Porta Delegata	Ruolo assunto da una Porta di Dominio nell'ambito di un episodio di collaborazione applicativa. Assume tale ruolo la Porta di Dominio che origina una richiesta di servizio destinato ad un'altra Porta di Dominio (Porta Applicativa).
Porta di Dominio	La Porta di Dominio rappresenta un elemento concettuale che ha la funzione di proxy per l'accesso alle risorse applicative del Dominio.
R.U.P.A.	Rete Unitaria della Pubblica Amministrazione
SPC	Sistema Pubblico di Connettività e Cooperazione
UDDI: Universal Description, Discovery and Integration	UDDI è un protocollo per la descrizione e la ricerca di servizi attraverso l'uso di un Registry. UDDI definisce le specifiche, indipendenti dalle piattaforme, necessarie per implementare i servizi UDDI che permettono ai Web Services di pubblicare le caratteristiche dei servizi da loro offerti e gli elementi di interfaccia necessari per utilizzarli e ricercare i servizi Web disponibili effettuando ricerche per nome, identificativi, categorie oppure in base alle specifiche del servizio. Normalmente i repository UDDI vengono considerati una sorta di "pagine gialle" e sono utilizzati in fase di progettazione, quando cioè l'implementatore preleva dal repository il WSDL e le informazioni di binding per costruire un client per l'accesso al servizio. I registri UDDI, però, sono dotati anche di interfacce standard (web service) per l'acceso al repository in fase di esecuzione. Il controllo delle informazioni contenute nel repository rispetto al servizio come: disponibilità, riferimenti attuali, fino ad arrivare potenzialmente allo SLA potrebbe fornire la possibilità reale di affrontare problemi di indisponibilità del rervizio a runtime ed in maniera automatica.

	Con una ricerca UDDI in fase di esecuzione, per esempio, un client potrebbe determinare il miglior punto di accesso in base alla classificazione geografica dei vari servizi o ad altri metadati associati a tale implementazione.
XML	Linguaggio derivato dall'SGML (Standard Generalized Markup Language) il metalinguaggio, che permette di creare altri linguaggi. Mentre l'HTML è un'istanza specifica dell'SGML, XML costituisce a sua volta un metalinguaggio, più semplice dell'SGML, largamente utilizzato per la descrizione di documenti sul Web. L'XML viene utilizzato per definire le strutture dei dati invece che per descrivere come questi ultimi devono essere presentati. Tali strutture vengono definite utilizzando dei marcatori (markup tags). Diversamente dall'HTML, l'XML consente all'utente di definire marcatori personalizzati, dandogli il controllo completo sulla struttura di un documento. Si possono definire liberamente anche gli attributi dei singoli marcatori. La specifica XML, largamente utilizzata in ambito internet, è lo standard per la definizione di documenti. Per questa ragione, nei progetti in esame, è previsto un ampio uso di tale specifica.
XML Schema	Linguaggio con il quale è possibile descrivere la grammatica (struttura e vincoli) di una particolare classe di documenti XML.

4. STRUTTURA ED ORGANIZZAZIONE DEI DOCUMENTI

Nel mese di dicembre 2003 è stato costituito presso il Centro nazionale per l'informatica nella pubblica amministrazione (CNIPA) un Gruppo di lavoro con il compito di definire il modello, l'architettura e le regole per l'interoperabilità, la cooperazione applicativa e l'accesso ai servizi telematici erogati dalle amministrazioni pubbliche nell'ambito del Sistema Pubblico di Connettività e Cooperazione (SPC).

Ai lavori del gruppo hanno partecipato oltre 120 persone in rappresentanza delle amministrazioni pubbliche centrali e locali, del mondo accademico e delle principali associazioni di categoria di fornitori di servizi ICT.

Le attività del Gdl hanno portato alla redazione di una serie di documenti relativi a differenti aspetti ed argomenti in materia di cooperazione sul SPC; tali documenti sono stati pubblicati in diverse fasi ed altri saranno pubblicati in futuro sia come evoluzione del modello che come approfondimento di alcuni temi.

4.1. Lista dei documenti SPC

Al fine di agevolarne la lettura e la corretta collocazione nel quadro d'insieme, e quindi facilitare la comprensione del disegno complessivo del Sistema Pubblico di Cooperazione, di seguito è riepilogata la struttura sia della documentazione prodotta, sia di quella prevista per il completamento del modello che sarà a breve prodotta:

Titolo documento/ Nome file/ URL	Oggetto	Stato/ Data pubblicazione/ Versione
Prima fase		
Risultati 1^ fase dei lavori SPC_PrincipiCondivisi.pdf http://www.cnipa.gov.it/site/_files/1.SPC_PrincipiCondivisi.pdf	Concetti preliminari condivisi nel corso della 1^fase dei lavori conclusa il 31/3/2004.	Approvato Gdl 31/3/2004 Ver.1.0
Rilevazione delle esigenze SPC_AnEsigenze v3-11-3-2004.pdf http://www.cnipa.gov.it/site/_files/2.SPC_AnEsigenze%20v3-11-3-2004.pdf	Rilevazione ed analisi delle esigenze di cooperazione applicativa delle amministrazioni pubbliche.	Approvato Gdl 31/3/2004 Ver.3.0

Titolo documento/ Nome file/ URL	Oggetto	Stato/ Data pubblicazione/ Versione
Requisiti del modello di interoperabilità ed accesso del SPC SPC-IntAcc_RequisitiMod-20040326.pdf http://www.cnipa.gov.it/site/_files/3.SPC-IntAcc_RequisitiMod-20040326.pdf	Definizione del modello e dei requisiti di riferimento per i servizi di interoperabilità, cooperazione ed accesso del SPC.	Approvato Gdl 31/3/2004 Ver.1.1
Abstract Busta e-government AbstractBusta- e-Gov-ver- 2.pdf http://www.cnipa.gov.it/site/_files/Abstract Busta-%20e-Gov-ver-%202.pdf	Sinetesi delle specifiche della busta di e-government	Approvato Gdl 31/3/2004 Ver.2.0
Specifiche della busta di e-government SPC_Busta e-Gov v.1_0-21-04-2004.pdf http://www.cnipa.gov.it/site/_files/4.SPC_Busta%20e-Gov%20v.1_0-21-04-2004.pdf	Specifiche di dettaglio della busta di e-government	Approvato Gdl 31/3/2004 Ver.1.0
Dizionario SPC_Dizionario v1.2.pdf http://www.cnipa.gov.it/site/_files/5.SPC_Dizionario%20v1.2.pdf	Dizionario dei termini usati	Approvato Gdl 31/3/2004 Ver.1.2
Seconda fase		
Sistema pubblico di cooperazione: Executive Summary SPCoop-ExecutiveSummary_v2.1_20041125.doc N.D.	Sintesi del modello del SP di Cooperazione	Approvato 25/11/2004 Ver.2.1
Sistema pubblico di cooperazione: Architettura SPCoop-Architettura_v1.0_20041125.doc N.D.	Modello di architettura, struttura e contenuti dell'accordo di servizio, architettura dei componenti e dei servizi infrastrutturali	Approvato 25/11/2004 Ver.1.0
Sistema pubblico di cooperazione: Organizzazione SPCoop-Organizzazione_v1.0_20041125.doc N.D.	Modello di funzionamento organizzativo e regole di governo e coordinamento del SP di Cooperazione	Approvato 25/11/2004 Ver.1.0
Sistema pubblico di cooperazione: Standard e tecnologie SPCoop-Standard_v1.0_20041125.doc N.D.	Individuazione e definizione dell'insieme di standard e tecnologie a cui si farà riferimento nell'ambito del SP di Cooperazione secondo le modalità che saranno specificate in fase di dettaglio dei singoli componenti.	Approvato 25/11/2004 Ver.1.0

Titolo documento/ Nome file/ URL	Oggetto	Stato/ Data pubblicazione/ Versione
Prossima emissione		
Sistema pubblico di cooperazione: regole e procedure di nomenclatura SPCoop-Nomenclatura_v*X.Y_aaaammgg*.doc N.D.	Regole di formazione degli identificatori (URI) e degli indirizzi (URL) dei soggetti, entità, documenti, punti di accesso. Procedure di attribuzione degli identificatori	*Da redigere*
Sistema pubblico di cooperazione: Accordo di Servizio SPCoop-AccordoServizio_v*X.Y_aaaammgg*.doc N.D.	Struttura, formato e contenuti dell'accordo di servizio standard SPCoop.	*Da redigere*
Sistema pubblico di cooperazione: Servizi di Registro SPCoop-ServiziRegistro_v*X.Y_aaaammgg*.doc N.D.	Requisiti, specifiche funzionali, accordo di servizio, architettura, specifiche tecniche, organizzazione e procedure di gestione ed accesso, standard di riferimento per i componenti ed i servizi di registro SICA	*Da redigere*
Sistema pubblico di cooperazione: Porta di dominio SPCoop-PortaDominio_v*X.Y_aaaammgg*.doc N.D.	Componenti, requisiti e specifiche funzionali, organizzazione e procedure di gestione ed accesso, standard di riferimento della porta di dominio	Bozza 25/11/2004 Ver.Alfa
Sistema pubblico di cooperazione: Servizi di sicurezza SPCoop-ServiziSicurezza_v*X.Y_aaaammgg*.doc N.D.	Componenti, requisiti e specifiche funzionali, organizzazione e procedure di gestione ed accesso, standard di riferimento dei servizi di sicurezza del SP di Cooperazione.	*Da redigere*
Sistema pubblico di cooperazione: Esercizio e gestione SPCoop-EsercizioGestione_v*X.Y_aaaammgg*.doc N.D.	Modalità di esercizio, gestione, verifica e controllo del SP di Cooperazione; modalità di gestione del transitorio e della fase di start-up.	*Da redigere*

4.2.Note di lettura dei documenti

Nella definizione dei requisiti, delle specifiche e delle regole descritte nei documenti precedentemente indicati sono utilizzate le parole chiave DEVE, NON DEVE, OBBLIGATORIO, VIETATO, DOVREBBE, CONSIGLIATO, NON DOVREBBE, SCONSIGLIATO, POTREBBE, OPZIONALE che devono essere interpretate in conformita con [RFC2119]. In particolare:

- DEVE, OBBLIGATORIO significano che la definizione è un requisito assoluto, la specifica deve essere implementata, la consegna è inderogabile.

- DOVREBBE, CONSIGLIATO significano che in particolari circostanze possono esistere validi motivi per ignorare un requisito, non implementare una specifica, derogare alla consegna, ma che occorre esaminare e valutare con attenzione le implicazioni correlate alla scelta.
- PUÒ, OPZIONALE significano che un elemento della specifica è a implementazione facoltativa.
- NON DOVREBBE, SCONSIGLIATO significano che in particolari circostanze possono esistere validi di motivi per cui un elemento di specifica è accettabile o persino utile, ma, prima di implementarlo, le implicazioni correlate dovrebbero essere esaminate e valutate con attenzione.
- NON DEVE, VIETATO significano che c'e proibizione assoluta di implementazione di un determinato elemento di specifica.

5. OBIETTIVI E CONTENUTI DEL DOCUMENTO

Questo documento è frutto delle attività del gruppo di lavoro per la definizione degli standard relativi ai servizi di accesso, interoperabilità e cooperazione del Sistema Pubblico di Connettività e Cooperazione.

Gli scopi del documento sono:

- determinare gli standard di riferimento dei dati e dei servizi applicativi ed infrastrutturali;
- definire le modalità di utilizzo dei servizi infrastrutturali e le specifiche tecniche relative agli aspetti non coperti dagli standard.

Ciò viene ottenuto prendendo in considerazione standard internazionali indipendenti dagli strumenti di sviluppo e dai prodotti di mercato. Ogni Ente, pertanto, nel recepire tali specifiche, può concentrare i propri sforzi nella graduale realizzazione delle logiche di business dei propri servizi, scegliendo i prodotti di mercato più adatti alle proprie esigenze, nel rispetto, comunque, delle regole e degli standard definiti nell'ambito dell'SPC.

Nel documento sono esposte le considerazioni e le valutazioni emerse nel corso delle riunioni del GdL ed i contributi dei partecipanti in merito agli aspetti esaminati.

L'elaborato costituisce un compendio degli standard applicabili alle principali componenti di una architettura di cooperazione applicativa e rappresenta un punto di partenza per i successivi documenti di specifica di dettaglio relativi alle singole componenti architetturali dell'SPC – SICA. Per ciascuno di tali documenti verranno ulteriormente definiti e dettagliati gli standard da applicare in termini di specifiche.

5.1. Struttura del Documento

Il presente documento si articola nei seguenti capitoli:

Capitolo 6 – Il Contesto di riferimento: il capitolo fornisce le indicazioni sul contesto architetturale, sulle tecnologie e sui vari documenti di riferimento che caratterizzano lo scenario di impiego del presente documento

Capitolo 7 - Servizi infrastrutturali per la cooperazione: obiettivo del capitolo è fornire l'indicazione sugli standard e sui formati dei dati relativi ai servizi infrastrutturali e applicativi

Capitolo 8 – Tassonomia: obiettivo del capitolo è la definizione della modalità con cui descrivere i servizi e i dati di interesse nazionale operando una ricognizione dell'esistente

Capitolo 9 – Sicurezza nelle interazioni tra applicazioni: il capitolo definisce le regole di sicurezza nelle interazioni tra sistemi, verificando gli scenari di utilizzo dei ruoli e gli impatti sulle infrastruttura di sicurezza dell'SPC

Capitolo 10 – Appendice:

A1 Esempi di utilizzo dei Registri

A2 Le strutture dati del Modello UDDI

A3 Il progetto SIGMA TER

5.2. Componenti del gruppo di lavoro

Il Gruppo di lavoro è composto dai seguenti partecipanti in rappresentanza delle rispettive amministrazioni :

Barattieri, Monica	Ministero Giustizia
Bellifemine, Giuseppe	Ministero Salute
Bellini Rossella	SUN
Bianchini, Vincenzo	Regione Lazio
Carota Serenella	Regione Marche
Cascioli Tiziana	SOGEI
Castellini, Alessandro	Provincia di Brescia
Craca Paolo	Neta
Dell'Anno Claudio	Regione Lazio
De Vecchis Massimo	Ministero del Lavoro e Politiche Sociali
Filippello Giuseppe	EDS
Gargiulo, Erasmo	CNIPA
Giovannini, Maria Pia	CNIPA
Grillo Fabrizio	Agenzia Entrate
Guetti Patrizia	SOGEI
Lupo, Mariano	Ministero Economia (Finanze)
Maraglino, Antonio	Microsoft
Mariotti, Emanuela	CNIPA
Massobrio Sonia	Comune Ancona – ANCI Marche

Mastroianni Aldo	SOGEI
Migliorini Raffaella	CONSIP
Mognato, Francesco	Agenzia Entrate
Neri Maurizio	Agenzia Entrate
Nicoletti, Luca	CONSIP
Palaia Egidio	Agenzia Entrate
Pastore, Maurizio	Datasiel - Regione Liguria
Pogliani Stefano	IBM
Pontevolpe, Gianfranco	CNIPA
Romanazzi Pietro	CT_RUPAR Puglia
Sala, Annarita	INPS
Tabet, Elena	CNIPA
Tamietti Corrado	CSI-Piemonte
Tongiani Marco	Comune Perugia ANCI Marche
Ugolini Leonardo	Oracle

6. IL CONTESTO DI RIFERIMENTO

Il contesto di riferimento è costituito dai documenti prodotti nel corso delle attività dei precedenti gruppi di lavoro e dalle specifiche della Busta di e-Government, approvate dal Gruppo di lavoro "Servizi per l'interoperabilità, la cooperazione applicativa e l'accesso del SPC" ed aventi una valenza nazionale.

Il ***Sistema Pubblico di Connettività e Cooperazione (SPC)*** rappresenta l'infrastruttura comune per l'interconnessione, fino al livello applicativo, delle amministrazioni pubbliche, centrali e locali. La sua realizzazione costituisce il presupposto essenziale per integrare, velocizzare ed armonizzare i processi di comunicazione tra i back-office delle amministrazioni, attività propedeutiche per una efficiente erogazione di servizi on-line a cittadini ed imprese.

Per attuare tale disegno occorre che tutti gli attori (amministrazioni centrali e locali, enti ed aziende) condividano le specifiche, gli standard e le modalità di realizzazione e gestione dei complessi elementi infrastrutturali comuni che disaccoppiano i sistemi (eventualmente legacy in senso generale) delle amministrazioni ed implementano i servizi che abilitano la cooperazione applicativa tra sistemi e si impegnino ad esporre ed utilizzare (in qualità di fruitori) servizi erogati da terzi secondo modalità standard predefinite e consolidate tecnologie di mercato.

6.1. Differenze tra Specifica e Standard

Prima di affrontare gli standard e le tecnologie del SPC è importante comprendere la differenza tra il termine "SPECIFICA" ed il termine "STANDARD" per la comunità Internet.

Una "SPECIFICA" e' un insieme di regole tecniche che definiscono come devono essere costruiti degli oggetti software, allo scopo di permettere differenti implementazioni interoperanti tra di loro. Se la specifica e' definita da una o più aziende, può essere protetta da Copyright.

Uno STANDARD e' tale se e' disponibile una specifica liberamente implementabile e ha il riconoscimento da parte di uno dei seguenti organismi internazionali: ISO, IEEE , Nazioni Unite.

Agli organismi legalmente riconosciuti si aggiungono, poi, organizzazioni che elaborano promuovono specifiche e raccomandazioni che si sono affermate come standard. Tra queste organizzazioni citiamo W3C OASIS e più di recente WS-I.

Questa differenza impone che nella definizione delle specifiche tecniche per l'SPC siano adottati soltanto gli standard, quindi liberamente implementabili **per garantire a tutti i fornitori la possibilità di partecipare alla realizzazione del sistema.**

A titolo di esempio viene di seguito descritto il processo tramite il quale l'organizzazione W3C definisce le Raccommendation sulle specifiche tecniche.

6.1.1. Come si giunge a una Recommendation

Le W3C Recommendation sono il risultato di un processo cooperativo, regolato dal *Process Document*, che prevede una serie di passi e di documenti prodotti. Alcuni documenti sono riservati ai partecipanti ai gruppi di lavoro, altri sono disponibili per i membri, che votano per approvarli o modificarli, altri sono pubblici.

Nello sviluppo delle specifiche tecniche e delle linee guida (in generale identificate come Technical Report) si possono individuare quattro scenari:

- *Avanzamento* di un technical report da una prima bozza ad un documento stabile ("Recommendation");
- *Interruzione* del lavoro su un technical report prima che diventi una Recommendation, o quando si ritiene opportuno che non lo diventi;
- *Modifica* di una W3C Recommendation;
- *Eliminazione* di una Recommendation non più supportata dal W3C.

L' intera procedura prevista dalla *Recommendation Track* è stata progettata per ottenere il massimo consenso sul contenuto, e assicurare il pieno appoggio da parte del W3C e dell' intera comunità web.

Per comprendere bene la procedura, occorre prima definire i cosiddetti *maturity level* dei documenti nelle varie fasi. Va altresì tenuto presente che non c'è una corrispondenza biunivoca tra i maturity level e i passi che si susseguono.

I maturity level sono:

- *Working Draft (WD)*: è un documento pubblicato per essere sottoposto a revisione da parte di tutta la comunità, quindi sia i membri W3C che altre organizzazioni o in generale il pubblico.
- *Candidate Recommendation (CR)*: è un documento che, a parere del W3C, ha subito un' estesa revisione, e soddisfa i requisiti tecnici definiti dal WG. La pubblicazione della CR ha l' obiettivo di poter conseguire una adeguata esperienza implementativa.
- *Proposed Recommendation (PR)*: è un technical report che ha subito un' ampia valutazione tecnica, e per il quale è stata maturata una adeguata esperienza implementativa, che viene sottoposto al giudizio dell' Advisory Committee per l' avallo finale.
- *W3C Recommendation (REC)*: è una specifica o un insieme di linee guida che, dopo aver maturato il consenso da parte di tutti, ha ricevuto l' approvazione da parte del W3C e del suo direttore, che ne auspicano un' ampia diffusione.
- *Working Group Note:* viene pubblicata da un Working Group per indicare che il lavoro su quel particolare argomento è terminato, e può essere pubblicata indipendentemente da una sua precedente diffusione come Working Draft. Il W3C può anche pubblicare delle "*Interest Group Notes*" e "*Coordination Group Notes*[1]". Gli Interest Group e i Coordination Group non producono technical report destinati a diventare Recommendation.
- *Proposed Edited Recommendation:* è una Recommendation pubblicata per sottoporre la Recommendation a modifiche, che possono anche influenzare la conformità alle specifiche. Una volta ottenuto il consenso sulle modifiche proposte, il documento viene pubblicato come Recommendation.

[1] Per evitare confusione sul significato del termine "Note", che può designare sia il risultato di un gruppo costituito, che un documento sottoposto da uno o più membri, il W3C prevede di abolire il maturity level "Note" senza alcuna specifica addizionale.

- *Rescinded Recommendation:* è una Recommendation che il W3C non supporta più.

I maturity level di un technical report indicano la sua posizione nella Recommendation Track, in cui "*Working Draft*" e "*Working Group Note*" rappresentano i possibili stati iniziali, e "*Recommendation*", "*Working Group Note*", e "*Rescinded Recommendation*" costituiscono i possibili stati finali.

Nel passaggio da technical report a Recommendation si succedono questi passi:

1. Pubblicazione del primo *Public Working Draft*;
2. *Last Call announcement*;
3. *Call for Implementations* (a discrezione del Direttore, se sono già soddisfatti i criteri per passare alla fase successiva, questo passo può essere eliminato);
4. *Call for Review of a Proposed Recommendation*;
5. pubblicazione come *Recommendation*.

In genere un Working Group finalizza la sua attività alla pubblicazione di una o più Recommendation. Tuttavia, il W3C può decidere di concludere il lavoro in qualunque momento, oppure richiedere un lavoro supplementare, che potrebbe richiedere anche la ripetizione di qualche fase.

La figura 1 illustra schematicamente il processo che porta alla pubblicazione di una Recommendation, ed evidenzia la possibilità che un documento ritorni ad uno stato precedente. Il passaggio da uno stato all' altro avviene mediante votazione da parte dei membri. Il passaggio dallo stato di "*Last Call Working Draft*" a quello di "*Candidate Recommendation*" comporta una "*Call for implementations*", e il livello di "*Proposed Recommendation*" viene raggiunto solo dopo aver maturato una soddisfacente esperienza implementativa. Quindi possiamo dire che si ha sia una "*proof of the concept*" che una "*proof of implementation*". Le W3C Recommendation, perciò, non sono meri documenti cartacei, ma specifiche di cui è stata dimostrata l' efficacia e che sono implementabili con uno sforzo ragionevole.

Nel prossimo paragrafo vengono forniti dettagli sulla procedura di avanzamento e revisione delle specifiche tecniche.

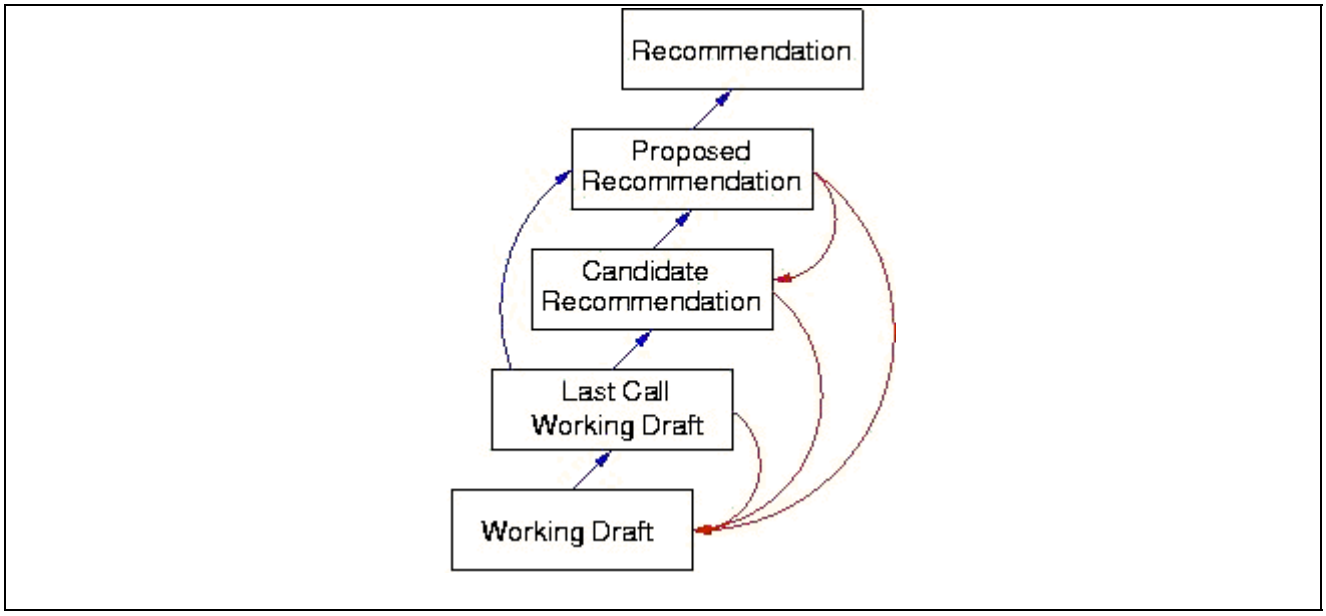


Figura 1 - La W3C Recommendation Track

Anche se *Network Computing* cita il W3C nella sua lista dei *"Ten Most Significant Standards Groups"*, dal punto di vista formale il W3C non è un organo di standardizzazione, ma una comunità di membri che cooperano spontaneamente, e con entusiasmo, per definire le linee guida e le specifiche, verificando che esse siano realmente implementabili, e mantiene stretti contatti con gli organi di standardizzazione e con gli User Forum.

Le W3C Recommendation non possono quindi essere definite degli standard in senso proprio, e vengono spesso citate come "*standard de facto*". È però importante sottolineare che esse non sono originate da posizioni dominanti del mercato, ma sono specifiche tecniche sulle quali è stato raggiunto, da parte di tutta la comunità del Web, un pieno accordo.

7. SERVIZI INFRASTRUTTURALI PER LA COOPERAZIONE.

I servizi infrastrutturali per la cooperazione applicativa, denominati anche servizi SICA, come meglio specificato nel modello architetturale, sono costituiti dalle seguenti componenti:

- **Registro dei servizi (SICA)**, e Banche dati documentali. Il Registro dei servizi, come meglio indicato nel documento dell'Architettura dei servizi SICA, comprende l'indice dei soggetti, l'elenco degli erogatori, il catalogo degli accordi e la rubrica degli indirizzi ;
- **Porte di Dominio** (componente di integrazione ed interoperabilità);

La definizione degli standard per lo sviluppo delle predette componenti infrastrutturali avrà uno sviluppo "incrementale" guidato dai progetti istituzionali sviluppati dalle PA sia locali che centrali.

Gli standard verranno prescelti osservando gli standard *"de facto"*[2] e le indicazioni emanate dagli enti preposti alla emissione di standard internazionali; le specifiche di dettaglio, invece approfondiranno gli aspetti non trattati dagli standard, o comunque non consolidati in base anche alle indicazioni del mercato.

7.1. Il Registro dei servizi.

Il Registro contiene le informazioni necessarie alla implementazione delle interazioni tra soggetti pubblici e privati attraverso il SPC. I dati contenuti nei registri possono essere utilizzati sia in fase di progettazione che durante le interazioni telematiche (*run time*).

Nel seguito vengono definite le funzioni, lo schema e le modalità di utilizzo di tale registro, focalizzando l'attenzione su un indice dei soggetti esistente e costituito dall'indice della PA (IPA) e sulle Banche dati documentali. Per ciascun elemento vengono indicati gli standard e le tecnologie utilizzati ed utilizzabili.

7.1.1. Funzionalità del Registro dei servizi.

Come previsto dal documento che descrive l'architettura SPC, il Registro dei servizi contiene informazioni rilevanti per le interazioni tra le applicazioni delle PA. La scelta della tipologia del registro deve tener conto dei seguenti requisiti:

- deve essere quanto più possibile rispondente a specifiche e/o standard, implementati da prodotti commerciali e open di mercato;
- deve essere interfacciabile sia da utenti che da applicazioni;

[2] Esempio il protocollo TCP/IP derivato dalle specifiche ISO/OSI, e gli standard più importanti che si sono affermati sul mercato internazionale.

- deve essere indipendente da una specifica piattaforma software;
- deve fornire funzionalità di ricerca e pubblicazione;
- deve essere corredato da API supportate dai principali linguaggi, nonché architetture applicative di sviluppo per servizi web;
- deve fornire informazioni per la determinazione delle interfacce con le quali vengono esposti i servizi web,
- deve consentire di catalogare servizi secondo diversi indici di classificazione;
- deve consentire di realizzare una struttura federata di replica di informazioni.

Oasis (Organtization for Advacement of Structured Information Standard) ha standardizzato due tipologie di registry federabili che rispondono ai requisiti richiesti: UDDI ver. 2 ed ebXML 3.0.

La specifica UDDI [UDDI 2.0], supportata da un maggior numero di vendor, propone la creazione di una directory di cosiddetti "business services", e prevede la catalogazione di servizi, applicazioni e altri componenti software sviluppati per facilitare la comunicazione tra diverse organizzazioni. La specifica definisce le modalità di registrazione e ricerca delle informazioni relative a un servizio e alle sue interfacce applicative ed è basata sull'utilizzo di standard esistenti quali XML e SOAP. In particolare la specifica definisce:

- la struttura di un registro di distributori di servizi e dei servizi stessi;
- le API che possono essere utilizzate per accedere o aggiornare il registro stesso;

Le informazioni presenti in un registro UDDI possono essere organizzate secondo i seguenti schemi logici:

- White Pages, contengono le informazioni anagrafiche di una organizzazione, quale il nome, l'indirizzo, il numero di telefono oltre ad identificativi del settore quali il numero DUNS;
- Yellow Pages, contengono le informazioni sui vari servizi messi a disposizione dalle organizzazioni;
- Green Pages, contengono le informazioni tecniche sul servizio Web e possono includere anche la descrizione tecnica del servizio (WSDL). Le "Green Pages" contengono informazioni relative a protocolli o specifiche necessarie per accedere ai servizi.

7.1.1.1. Modalità di utilizzo del registro

E' possibile interagire con un registro UDDI sia attraverso pagine web, per facilitare l'interrogazione o la pubblicazione dei servizi direttamente da utenti, oppure attraverso API di programmazione che possono essere utilizzate da applicazioni per effettuare il "discovering" automatico dei servizi.

Le API UDDI sono classificabili in due principali categorie:

- Inquiry API;
- Publish API;

Le prime sono utilizzate per effettuare ricerche sul registro al fine di ottenere informazioni relative alla descrizione di un servizio o dell'organizzazione che distribuisce il servizio, mentre le seconde vengono utilizzate per pubblicare nel registro informazioni relative a servizi o ad organizzazioni.

Le API UDDI sono aperte a qualsiasi linguaggio di sviluppo e si basano su un modello di programmazione denominato DEM (Document Exchange Model): la comunicazione tra oggetti applicativi avviene attraverso documenti strutturati su protocollo SOAP.

In particolare, le API UDDI sono costituite dagli schemi XML dei messaggi da utilizzare per interagire con i registri UDDI (messaggi SOAP contenenti sia le richieste inviate, sia le risposte ricevute). Le API di linguaggio presenti sul mercato, inoltre, come indicato in figura 1, consentono di dialogare con i registri UDDI (effettuare ricerche o pubblicare servizi) senza conoscere la specifica dei messaggi SOAP.

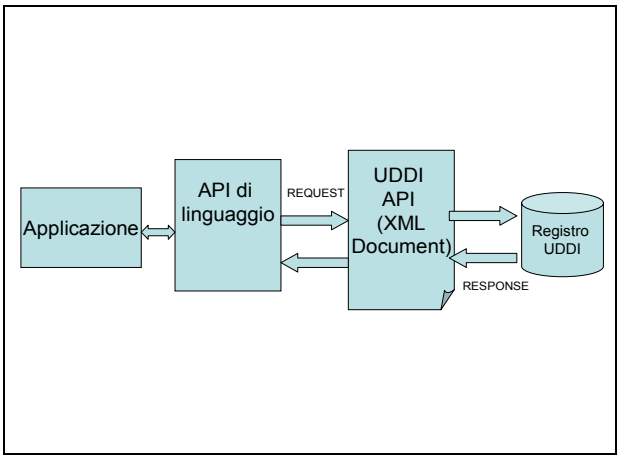
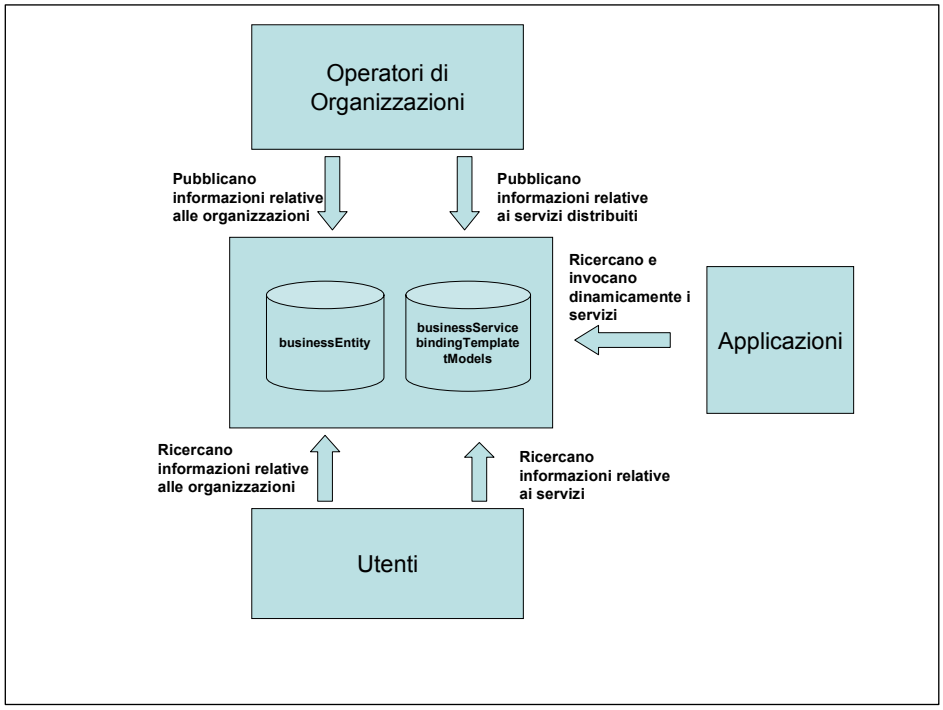


Fig.2 Schema di interazione attraverso le API di linguaggio.

Esistono diversi tipi di informazioni che vengono memorizzate in un registro UDDI, tra le quali:

- informazioni relative a organizzazioni (in UDDI chiamate "businessEntity") che offrono servizi,
- descrizione dei servizi esposti, incluse le specifiche di interfaccia nonché il riferimento alle "porte applicative" che erogano tali servizi.

Il modello dei dati usato da UDDI (cfr. §7.1.2.3) prevede l'utilizzo di cinque tipologie di strutture dati ed è abbastanza flessibile. Esso consente di memorizzare più informazioni tecniche relative ad un servizio (una ad esempio che fornisce una formale specifica dell'utilizzo del e una per esempio che rimanda ad un tutorial).



In figura 3 sono sintetizzate le modalità di interazione tra un registro UDDI e soggetti esterni.

Un registro UDDI viene aggiornato da "operatori" che pubblicano informazioni relative alle organizzazioni ai quali appartengono e ai servizi che si vogliono distribuire.

Fig. 3. Sintesi interazioni Registro UDDI

Al contempo il registro può essere interrogato da persone che, attraverso l'utilizzo di un web browser, possono ricercare informazioni relative ai servizi messi a disposizione dalle organizzazioni.

Infine, il registro può essere interrogato da programmi che effettuano il "discovery" dei servizi per una invocazione dinamica.

Una delle differenze sostanziali tra le funzioni di interrogazione e quelle di pubblicazione sta nel diverso livello di sicurezza richiesto.

Mentre le funzioni di ricerca consentono a chiunque di ottenere informazioni relative a organizzazioni o servizi pubblicati in un registro UDDI, le funzioni di pubblicazione richiedono un processo di autenticazione e autorizzazione (cfr. Appendice §10.1.1).

Le tipologie di ricerche effettuabili su un registro UDDI sono riportate in tabella 1:

Tipo di richiesta	Descrizione
find_business	Permette di ricercare una organizzazione in base a parametri di ricerca relativi alla ragione sociale, alla categoria di attività.
find_relatedBusinesses	Consente di ricercare una attività che ha quale correlazione con un'altra attività
find_binding	Consente la ricerca di un modello di binding associato ad un particolare servizio.

find_service	Consente di ricercare un servizio in base a criteri previsti per la richiesta "find business"
find_tModel	Consente di ricercare tutte le strutture tModel che rispondono al criterio di ricerca.
Get_bindingDetail	Consente di ottenere i dettagli relativi alla struttura di un binding template.
Get_businessDetail	Consente di ottenere i dettagli relativi ad una specifica organizzazione.
Get_serviceDetail	Consente di ottenere i dettagli relativi ad uno specifico servizio.
Get_tModelDetail	Consente di ottenere i dettagli relativi ad uno specifico tModel.

Tab. 1 Tipi di ricerche

Le tipologie di pubblicazioni effettuabili su un registro UDDI sono invece le seguenti:

- salvataggio e cancellazione di Business Entity;
- salvataggio e cancellazione di servizi (Business Service);
- salvataggio e cancellazione di Binding Template;
- salvataggio e cancellazione di tModel.

7.1.1.2. Convenzioni per l'utilizzo del registry UDDI.

Le modalità di pubblicazione di un servizio, come indicato dal WS-I Basic Profile [WS-I Basic Profile 1.0], sono descritte nelle linee guida per la pubblicazione (Requisito R3010) [WSDL-UDDI 1.08].

Lo schema di utilizzo generale di un registro UDDI potrebbe essere il seguente:

- Individuare un servizio Web in UDDI. Utilizzare il file WSDL del servizio (rappresentato da un "tModel"[3] UDDI) e i dettagli di implementazione, quali il punto di accesso e qualsiasi altra informazione di configurazione, contenuti in un "bindingTemplate" UDDI.
- Preparare un'applicazione client per il servizio Web. Nell'applicazione client, memorizzare nella cache la "bindingKey" univoca del servizio Web in modo che, quando l'applicazione viene utilizzata per la prima volta, possa richiamare tutte le informazioni necessarie da UDDI.
- Quando l'applicazione invoca il servizio Web remoto, utilizzare i dati memorizzati che sono stati ottenuti da un elenco Web UDDI.

[3] La fase di registrazione di un servizio WEB prevede che il file WSDL del servizio venga registrato come tModel. I tModel UDDI, infatti, sono entità XML utilizzate per rappresentare interfacce e metadati astratti. Dopo la registrazione del tModel il punto di accesso al servizio viene registrato come bindingTemplate. I bindingTemplate UDDI, infatti, sono strutture che consentono di rappresentarte i dettagli implementativi di uno specifico servizio WEB.

- Se l'invocazione non riesce, utilizzare il valore della "bindingKey" e la chiamata API "get_bindingTemplate" a un elenco UDDI per ottenere una copia aggiornata delle informazioni di binding.
- Confrontare le nuove informazioni con quelle precedenti: se sono diverse (è cambiata la URL del servizio) riprovare ad eseguire la chiamata non riuscita. Se il tentativo ha buon esito, sostituire i dati nella cache con quelli nuovi, memorizzandoli per le chiamate successive. Comunque, se le informazioni di binding ottenute sono identiche a quelle già memorizzate, significa che il fornitore non ha eseguito alcun aggiornamento e l'applicazione dovrebbe generare un errore. Analogamente, se le informazioni di binding sono nuove e la chiamata non riesce, l'applicazione dovrebbe generare un errore[4].

In appendice (§10.1), sono riportati alcuni esempi di utilizzo di un registro UDDI.

7.1.1.3. Modello dei dati di un registro UDDI

In figura 4 viene vengono indicate e descritte le principali Entità gestite da un registro UDDI.

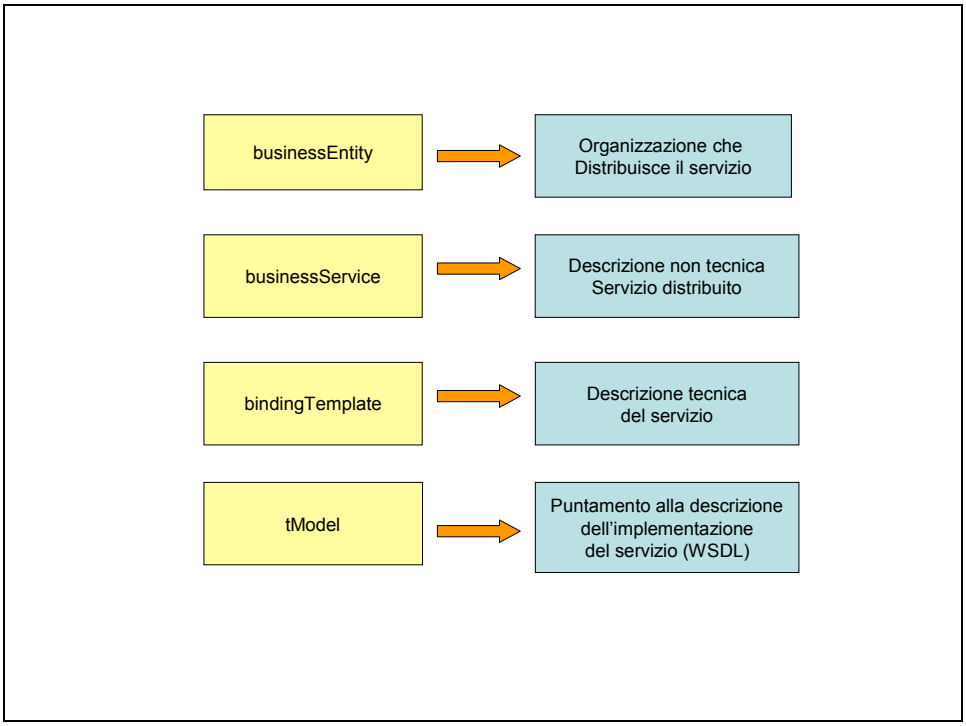


Fig. 4. Principali Entità gestite dal registro UDDI.

In particolare, il modello dei dati è costituito dalle seguenti tipologie di informazioni:

[4]Oltre che in fase di progettazione l'UDDI potrebbe essere utilizzato a runtime per la soluzione automatica di alcuni problemi relativi alla disponibilità di servizio, limitando così i messaggi di errore alle sole situazioni realmente critiche che necessitano l'intervento del fornitore del servizio e/o del gestore dello stesso registro.

- "businessEntity": La lista delle "businessEntity" è similare a quelle delle pagine bianche e delle pagine gialle. Una "businessEntity" rappresenta una organizzazione della quale vengono conservati: dati anagrafici, contatti, descrizioni e categorie di appartenenza.
- "businessService": Contengono informazioni non tecniche relative ai servizi che una organizzazione mette a disposizione. Un "businessService" è un raggruppamento di servizi web relativi ad un determinato processo applicativo. Un "businessService" corrisponde a un servizio WSDL.
- "bindingTemplate": Sono contenute informazioni relative all'accesso ai servizi, in particolare sono contenute descrizioni tecniche dei servizi web utili per le applicazioni che le devono invocare. In molti casi un binding template punta ad un indirizzo di implementazione (ad esempio URL) e mappa a un port WSDL. Questa entità è talvolta chiamata "access locator".
- "tModel": un tModel (technical model) è l'impronta digitale del servizio e rappresenta la specifica tecnica del servizio stesso.
- "Tassonomie": Rappresentano schemi di classificazione delle informazioni entro le quali le principali entità descritte all'interno dei registri vengono identificate. Esistono una serie di tassonomie standard supportate nei registri UDDI, tra le quali NAICS ("North American Industry Classification") e UNSPSC (Universal Standard Products and Services Classification). E' possibile comunque definire nuove tassonomie all'interno di un registro UDDI.
- "Asserzioni": Normalmente esiste una corrispondenza tra persona giuridica e business entity; tuttavia esistono situazioni nelle quali singole unità di una organizzazione possano registrare i propri servizi come se fossero entità autonome. UDDI consente in questo caso di mantenere una relazione tra le varie unità che fanno parte di una unica organizzazione: il meccanismo è denominato delle asserzioni ("publisher assertions"). Attraverso questo meccanismo è dunque possibile dichiarare la relazione tra più organizzazioni all'interno di un registro UDDI, attraverso una procedura che preveda il consenso di entrambe le organizzazioni nella definizione di questo legame.

In un registro UDDI, una businessEntity contiene riferimenti a una o più businessService. Un businessService referenzia uno o più bindingTemplate che puntano a loro volta ad un URL con il quale il servizio può essere invocato. Non è escluso tuttavia che un bindingTemplate contenga al posto di un URL, un riferimento ad un numero di telefono o ad un indirizzo.

Un tModel invece referenzia un documento WSDL, anche se è da sottolineare come nel registro UDDI è contenuto solamente l'URL che punta al sito web dove è possibile scaricare il file WSDL.

In figura 5 vengono riproposte le relazioni e le dipendenze tra le varie entità del modello dati di un registro UDDI.

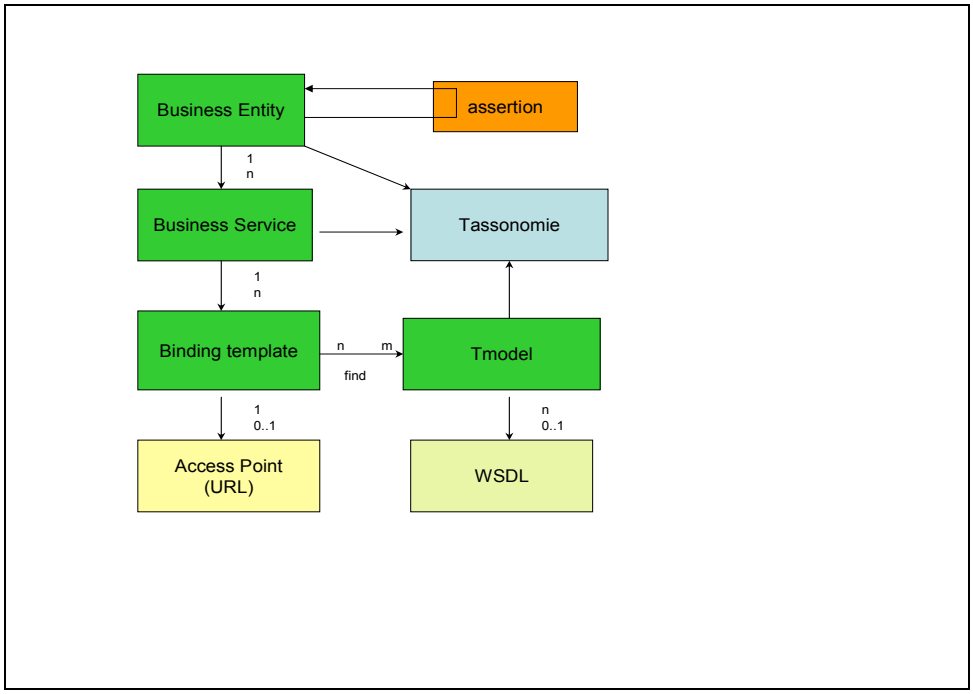


Fig. 5. Modello dati UDDI

Ulteriori dettagli sul formato dei dati sono stati riportati in appendice (§10.2).

7.1.1.4. I link del registro dei servizi.

Il registro dei servizi nasce essenzialmente con lo scopo di fornire una descrizione tecnica del servizio (strutture bindingTemplates e tModel), della sua localizzazione e soprattutto della sua interfaccia di invocazione (WSDL).

Tra gli obiettivi del SPC si pone anche quello di fornire ulteriori informazioni (ad esempio tutorial, informazioni descrittive relative all'utilizzo del servizio e/o delle modalità di accesso a convenzioni), che non facilmente si prestano ad una memorizzazione all'interno del registro UDDI.

Tuttavia nell'implementazione della struttura dati di un registro UDDI vi è la possibilità di inserire puntamenti a URL per ottenere ulteriori referenze ed informazioni a supporto dell'utente.

Infatti, la struttura tModel contiene un elemento opzionale, "*overviewDoc*" (cfr. appendice §10.1.3), a sua volta strutturato come nella seguente tabella [UDDI 2.03 Data Structure Reference]. Tale struttura può essere utilizzata per puntare ad una (eventuale) banca dati documentale accessibile mediante protocollo http ed implementata, possibilmente, da un sito web.

Elemento	Descrizione	Tipo dato	lunghezza
Description	Elemento opzionale. Descrive brevemente come utilizzare il particolare tModel. E' consentita una descrizione per ogni lingua supportata.	string	255

overviewURL	Elemento opzionale. Questo campo contiene la URL del documento che descrive come utilizzare i particolare tModel nell'ambito della descrizione dell'intero Web service. E' preferibile utilizzare una URL in grado di restituire descrizioni HTML attraverso un web browser oppure attraverso una operazione HTTP-GET.	string	255

Tab. 2 Elementi della struttura overviewDoc

7.1.1.5. Architettura federata.

In una architettura federata dovrebbe essere possibile garantire l'esistenza di più registri interdipendenti che possano colloquiare per replicare le informazioni pubblicate su ognuno di essi.

Purtroppo, allo stato attuale, tale funzionalità è solo teorica. Le specifiche UDDI, infatti, prevedono un complicato meccanismo di replica delle informazioni tra più server, basato su file di configurazione e messaggi SOAP di allineamento[5].

E' auspicabile, pertanto, avere un unico registro UDDI dei servizi di livello Nazionale. Tutte le Amministrazioni dovrebbero registrarsi e pubblicare i propri servizi nel registro nazionale. Ogni Amministrazione potrebbe dotarsi di un registro UDDI "locale" su cui pubblicare i propri servizi. In tal caso deve registrare il registro UDDI "locale" nel Registro UDDI Nazionale, provvedendo autonomamente alla gestione del registro "locale".

Restano comunque da definire i criteri di ricerca, in quanto le "key" degli oggetti contenuti nei differenti UDDI services potrebbero non essere sincronizzate.

Di seguito vengono comunque illustrate le possibilità di architettura federata offerte dalle specifiche UDDI 2.0.

Come indicato in Fig.6, ogni nodo UDDI farebbe parte di un cosiddetto UDDI Service, entità logica in cui ogni nodo verrebbe identificato attraverso un UUID (Universal Inique Identifier) ed inserito in un cosiddetto Replication Configuration File..

[5] E' inoltre previsto un processo di autenticazione dei nodi basato su TLS (Transport layer Security) 1.0 con almeno uno dei seguenti livelli di cifratura: RC4 con 40-bit encryption e MD5, oppure RC2 con 40-bit encryption e MD5;

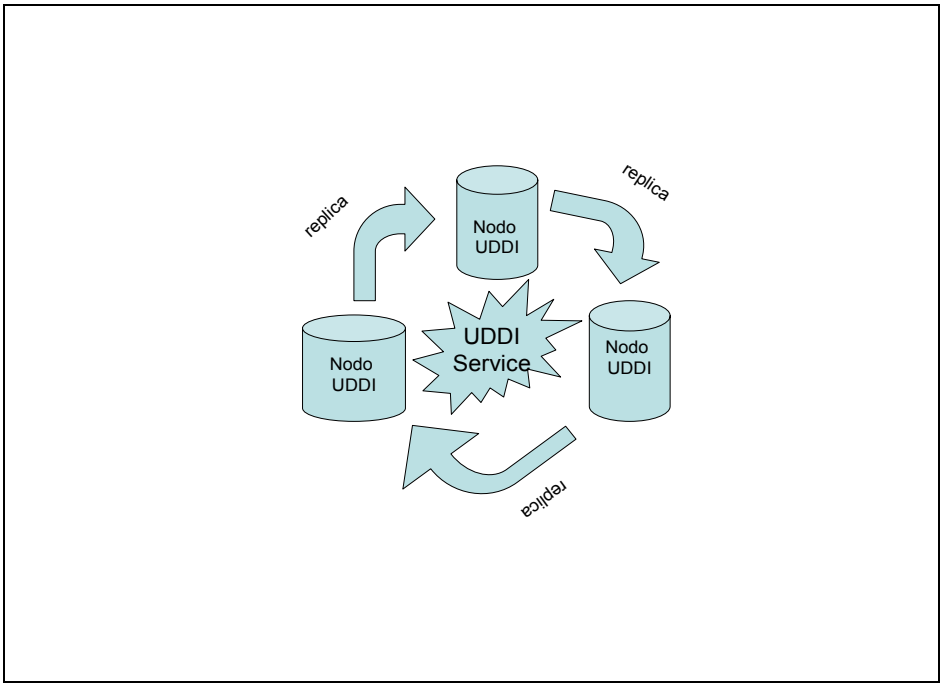


Fig. 6. UDDI Service composti da più nodi (UDDI operator)

L'obiettivo della replica in un UDDI Service è quello di assicurare che qualsiasi cambiamento originato in uno dei nodi che costituiscono la rete di un UDDI Service venga propagato agli altri nodi. Occorre notare che in caso di replica, con la versione 2.0 delle specifiche, il registro UDDI di replicazione consente di conservare il valore assunto dalla BusinessKey dell'amministrazione nel Registro di (prima) pubblicazione.

Ogni nodo ha la responsabilità di aggiornare una certa porzione dei dati gestiti dall'UDDI Service. I cambiamenti al dato possono essere fatti solo sul nodo che ha il dato in custodia, e da questo nodo vengono poi replicati agli altri nodi.

Quando un operatore cambia un dato su uno dei nodi, quest'ultimo crea un cosiddetto "change record", che descrive la modifica effettuata, e successivamente, lo trasmette agli altri nodi.

Il processo è descritto nella figura seguente:

- il nodo che origina la modifica, avvisa il nodo ricevente che un cambiamento è avvenuto nel registro (API notify_ChangeRecordsAvailable);
- il nodo ricevente, richiede al nodo che ha originato la modifica, il record cambiato.

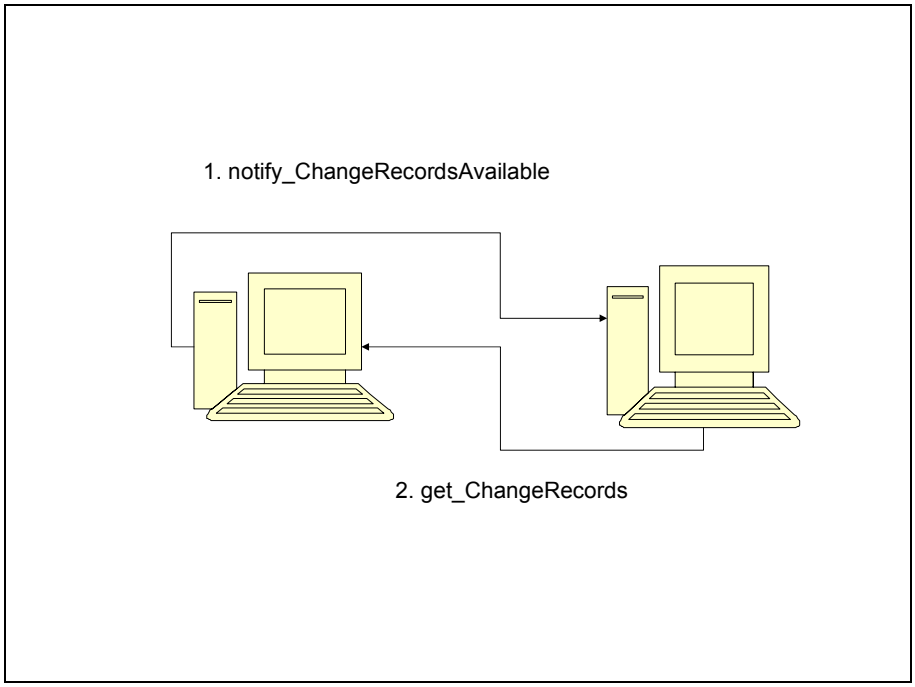


Fig. 7. Aggiornamento dei dati tra UDDI operator.

La replica dei dati è governata attraverso un file di configurazione denominato "UDDI Replication Configuration file". Questo file include informazioni per identificare in maniera univoca ogni nodo in un "UDDI Service". La descrizione del formato del file è specificato nello schema XML di seguito esposto [UDDI 2.03 ReplicationSpecification]:

```
<element name="replicationConfiguration">
  <complexType>
    <sequence>
      <element name="serialNumber" type="repl:USN_type"/>
      <element name="timeOfConfigurationUpdate"
         type="timeInstant"/>
      <element name="councilContact">
        <complexType>
          <sequence>
            <element ref="api_v2:contact"/>
          </sequence>
        </complexType>
      </element>
      <element ref="repl:operator" minOccurs="0"
          maxOccurs="unbounded"/>
      <element name="maximumTimeToSyncRegistry" type="integer"
          minOccurs="0" maxOccurs="1"/>
      <element name="maximumTimeToGetChanges" type="integer"/>
      <element ref="repl:communicationGraph" minOccurs="0"
          maxOccurs="1"/>
    </sequence>
  </complexType>
</element>
```

XML Schema dell'elemento replicationConfiguration.

Il file di configurazione contiene le seguenti informazioni:

- un identificativo (*serialNumber*) che viene aggiornato ogni volta che viene modificata la configurazione;
- un timestamp di aggiornamento della configurazione (*timeOfConfigurationUpdate*), che contiene il time in cui è avvenuto l'ultimo aggiornamento;
- il massimo numero di ore (*maximumTimeToSyncUBR*) in cui un cambiamento deve essere visibile a tutti i nodi in un UDDI Service;
- il massimo numero di ore (*maximumTimeToGetChanges*) che un nodo può attendere per richiedere un cambiamento;
- lista degli nodi (*operator*) che partecipano al UDDI Service e i path di comunicazione tra i nodi stessi
- configurazione dei percorsi (*communicationGraph*) attraverso i quali avviene la replica tra i nodi che partecipano ad un UDDI Service.

7.1.2. Indice dei soggetti - Indice delle amministrazioni pubbliche e delle aree organizzative omogenee PA (IPA)

Un particolare indice di risorse già esistente in SPC è costituito dall'Indice delle PA (IPA). Istituito con dpcm 31-12-2000 (Regole Tecniche sul Protocollo Informatico) contiene informazioni relative alla struttura organizzativa (Unità Organizzative) ed alle Aree Organizzative Omogenee (entità logiche associabili ad insiemi di UO) che compongono una Amministrazione.

L'indice è implementato da un sistema informatico gestito dal CNIPA ed è accessibile dalle Pubbliche Amministrazioni[6] e da tutti i soggetti pubblici o privati tramite un sito internet oppure mediante il protocollo LDAP v.3 [LDAP v.3].

In fase di accreditamento ciascuna Pubblica Amministrazione fornisce i dati relativi alla propria denominazione e l'indirizzo della sede principale, nonché i dati relativi alle Aree Organizzative Omogenee (AOO) ed alle Unità Organizzative (UO) in cui è articolata [INDICE PA]. Sempre in fase di accreditamento, inoltre, a ciascuna Amministrazione viene assegnato un codice identificativo (codice

[6] Art.1, comma2: Per amministrazioni pubbliche si intendono tutte le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le Regioni, le Province, i Comuni, le Comunità montane, e loro consorzi ed associazioni, le istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di commercio, industria, artigianato e agricoltura e loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale.

IPA), univoco a livello nazionale, composto da un massimo di 16 caratteri alfanumerici (compreso il carattere '_').

Le Amministrazioni accreditate, poi, sono tenute a comunicare le eventuali successive modifiche apportate ai dati di propria pertinenza pubblicati sull'indice.

L'indice dei soggetti può essere implementato utilizzando tecnologie LDAP (come nel caso dell'IPA) ovvero tecnologie UDDI [UDDI 2.0] (Web Services)

In quest'ottica, affinchè l'IPA possa costituire un riferimento per l'accesso ai dati relativi ai servizi applicativi esposti dalle singole Amministrazioni mediante Registri di servizi UDDI, potrebbe essere necessario inserire nella struttura dell'oggetto Amministrazione i seguenti attributi:

- un attributo contenente la URL del Registro dei servizi in cui sono pubblicati i servizi erogati dall'Amministrazione;
- un attributo che contiene la "business key" identificativa della Amministrazione nel Registro servizi che contiene l'elenco degli erogatori.

  Questi elementi verranno utilizzati tipicamente tramite le API UDDI per gli accessi effettuati dalle applicazioni o dai tool di sviluppo (*potrebbe essere opportuno avere anche una url per gli accessi via browser*).

Allo stato attuale, come riportato anche in §7.1.2.5, la possibilità di federazione dei registri UDDI è pressochè teorica (le specifiche UDDI 2.0 prevedono la funzionalità di replica). I dati relativi ai registri UDDI contenuti nell'IPA, pertanto dovrebbero riferire il registro dei servizi Nazionale (preferibilmente), oppure, in seconda istanza il Registro dei servizi gestito direttamente dall'Amministrazione.

In attesa della implementazione delle specifiche UDDI 3.0, che prevedono la federazione di registri UDDI, una possibile soluzione potrebbe essere la seguente:

l'IPA contiene la URL del registro UDDI Nazionale dei servizi (risorsa unica condivisa);

la struttura dell'oggetto Amministrazione contiene la "business key" identificativa della Amministrazione nel registro UDDI Nazionale dei servizi ("business entity");

la struttura dell'oggetto Amministrazione può contenere la "business key" identificativa della Amministrazione nel registro UDDI dei servizi gestito direttamente dall'Amministrazione[7];

Nel caso in cui l'Amministrazione gestisca un proprio registro UDDI dei servizi, il registro, che a tutti gli effetti costituisce un Web Service dell'Amministrazione, deve essere pubblicato sul registro UDDI Nazionale dei servizi.

L'indice della PA potrebbe anche costituire un indice guida di livello 0. L'oggetto Amministrazione relativo al CNIPA, in tal caso, conterrebbe i riferimenti di tutti i registri di risorse consultabili (un registro è un servizio); per ogni registro dovrebbe indicare scopi e finalità.

[7] Le Business Key di un dato registro UDDI non sono sincronizzate con le Business Key generate da un altro registro UDDI, a meno che non si tratti di nodi appartenenti allo stesso UDDI Service.

7.1.3. Banche documentali

Le Banche dati documentali sono dei registri che contengono documenti strutturati e non strutturati (descrittivi) a supporto della cooperazione su SPC. I documenti non strutturati costituiscono delle descrizioni in linguaggio naturale mentre i documenti strutturati utilizzano un formalismo XML.

XML, infatti, supportando sia la sintassi che la semantica dei dati, costituisce un must per l'interoperabilità e la diffusione dei documenti formali. I principali fattori che ne hanno determinato il successo sono i seguenti:

- Costituisce uno standard aperto;
- Utilizza supporti come file di testo e quindi richiede un livello tecnologico minimo;
- Incapsula dato e metadato (autodocumentante, persistenza nel tempo, …);
- E' caratterizzato da una *neutralità tecnologica* ;
- Esiste una vasta famiglia di tecnologie standard correlate (XSLT, XPath, WS, …);
- E' presente una grande disponibilità di *tool* e applicazioni;

Per poter condividere (scambio dati, applicazioni, ecc.) documenti XML è necessario conoscere la loro struttura. Questa è descritta attraverso metalinguaggi standard il cui prodotto è uno "schema XML".

Un repertorio mette a disposizione gli schemi XML relativi ad una categoria di dati e di applicazioni (p.e. contabilità, tasse, salute, …) e di utenti (p.e. ordini professionali, P.A., …).

I repertori di schemi XML favoriscono dunque l'interoperabilità, la diffusione delle migliori pratiche ed il riuso. Perciò sia organismi pubblici che privati hanno realizzato repertori di schemi e banche documentali dedicate.

Affinché un repertorio di schemi XML possa raggiungere gli obiettivi prefissati, è necessario che, nella progettazione, vengano considerati con la massima attenzione, fra gli altri, le banche documentali a supporto, gli aspetti concernenti gli standard e le modalità di pubblicazione degli schemi.

A livello unitario, dovranno essere costituite e mantenute le seguente banche documentali,:

1. repertorio degli schemi XML;
2. linee guida per la realizzazione di schemi XML;
3. repertorio dei metadati;
4. banche documentali a supporto.

A tal fine è indispensabile costituire un gruppo stabile per il coordinamento e monitoraggio delle attività.

Per quanto riguarda le banche documentali a supporto si può suggerire di rendere disponibili almeno le seguenti tipologie di documenti:

1. generalità sui metadati;

2. specifiche tecniche e standard di riferimento;
3. guide alla realizzazione di servizi e siti Web;
4. studi di fattibilità e progetti delle Amministrazioni;
5. strumenti di ausilio (tool);
6. archivio storico dei documenti;
7. riferimenti e link di interesse;
8. forum di discussione e FAQ.

Tutti i documenti dovranno essere resi disponibili attraverso le banche documentali in formato XML essi stessi ed almeno in un altro formato standard, per ogni documento dovranno essere adottati i seguenti criteri di classificazione:

1. sintesi dei contenuti;
2. versione corrente: data, versione, stato del documento, editore, commenti;
3. storia delle modifiche: data, versione, stato del documento, editore, autore,commenti.

7.1.3.1. Modalità di utilizzo

- MINIMALE: tale modalità sarà seguita nel caso in cui sia competente una sola Amministrazione ad erogare il servizio.

  Il repertorio si limita a rendere disponibili gli schemi ed eventuale relativa documentazione inviati da ciascuna amministrazione.

  E' consigliabile l'aggiunta di principi e standard di classificazione, commenti e strumenti di ricerca tramite sito Web.

- COOPERATIVA: tale modalità sarà seguita nel caso in cui la cooperazione avvenga tra più Amministrazioni.

  Si arriva alla pubblicazione finale attraverso un processo di discussione in rete da parte delle amministrazioni interessate che intervengono sulla bozza dello schema proponendo modifiche, aggiunte e quant'altro.

  Naturalmente tutta la procedura deve essere definita formalmente e coordinata da un apposito gruppo di lavoro che, eventualmente, può adottare anche strumenti di workflow.

L'approccio cooperativo ha, fra gli altri valori aggiunti, quello fondamentale di favorire l'accettazione e quindi il riuso degli schemi; questo perché la loro formazione è stata discussa e condivisa.

La mera pubblicazione degli schemi prodotti dalle amministrazioni individualmente non implica, infatti, *per se* l'adozione ed il riuso da parte di altre amministrazioni se non nei casi di forte virtuosità, pertanto è indispensabile il coordinamento a livello centrale.

7.1.3.2. Descrizione del formato dei dati

Focalizzando l'attenzione sui metalinguaggi adottati per descrivere il formato dei dati vengono di seguito commentate le caratteristiche dei formalismi standard o in via di standardizzazione da utilizzare:

- DTD (*Document Type Definition*)

  Rappresenta la sintassi implicitamente definita nella specifica standard di XML [XML]. Di fatto è un sottoinsieme, adattato alla "semplicità di XML", del metalinguaggio dell'antenato di XML, cioè SGML (*Standard Generalized Markup Language*) ISO8879, 1976.

  E' il metalinguaggio per la formazione di schemi XML più semplice e più diffuso. E' ampiamente supportato e sono disponibili numerosissimi *tools*.

  Ha alcuni limiti espressivi e non consente una vera e propria tipizzazione dei dati né la descrizione della loro struttura.

- W3C XML Schema

  E' il metalinguaggio per la produzione di schemi XML, elaborato e pubblicato come standard dal W3C [W3C XML Schema].

  Permette una descrizione granulare degli schemi, la tipizzazione dei dati e la definizione della loro struttura.

  E' ampiamente supportato e sono disponibili numerosi tools.

  E' molto complesso e l'apprendimento non è banale. E' scritto in XML e, anche per questo, è molto prolisso. Quindi non è adatto a far partecipare alla progettazione i non esperti (p.e. committenti).

  Non presenta un trattamento omogeneo degli elementi e degli attributi e per quanto concerne questi ultimo è affetto da alcune limitazioni espressive.

- RELAX NG

  E' il metalinguaggio [RELAX NG] realizzato da OASIS (http://www.oasis-open.org/), fondamentale organizzazione *non profit,* dedicata allo sviluppo e alla promozione degli standard relativi alle informazioni strutturate.

  E' allo stadio finale di standardizzazione come ISO/IEC 19757-2 da parte dello stesso gruppo di lavoro ISO che ha standardizzato SGML (l'antenato di XML) ISO/IEC JTC1/SC34/WG1.

  Permette di descrivere lo stesso schema con due sintassi totalmente equivalenti: una in XML e l'altra derivata da DTD con i suoi vantaggi in termini di semplicità e leggibilità (sono disponibili *tool* per la conversione fra le due sintassi).

Grazie ai presupposti logici, ha una espressività praticamente illimitata. Tratta omogeneamente elementi ed attributi.

Per scelte progettuali la sua sintassi non ha espressioni per la tipizzazione e la strutturazione del dato ma, per tali scopi, può far riferimento a librerie esterne (p.e. i tipi dati del W3C XML Schema).

Le applicazioni e i tool non sono numerosi come per i precedenti metalinguaggi ma stanno crescendo rapidamente.

7.2. Porte di Dominio

La Porta di Dominio [Busta e-Government] rappresenta un elemento concettuale che ha la funzione di proxy per l'accesso alle risorse applicative del Dominio di una Amministrazione. Come tale fa parte del modello organizzativo di cooperazione tra soggetti federati e trova la sua collocazione naturale nella progettazione concettuale piuttosto che in quella logica o fisica. Le differenti istanze di "Porta di Dominio" costituiscono gli elementi di una infrastruttura di cooperazione con funzioni di "proxy" dei servizi erogati dal dominio ed implementano funzionalità proprie di un layer di messaging. Gli scambi tra le Porte avvengono attraverso messaggi strutturati secondo le specifiche descritte in [Busta e-Government] . Come anticipato in [Busta e-Government] ed ulteriormente approfondito e descritto nel documento Architetturale dell'SPC, le Porte forniscono servizi di:

- Sicurezza nelle interazioni tra le Porte di Dominio:
- Identificazione;
- Autenticazione;
- Autorizzazione;
- Confidenzialità;
- Non ripudio;
- Indirizzamento delle richieste;
- Logging ed auditing delle interazioni;
- Servizi infrastrutturali aggiuntivi quali:
  affidabilità (eliminazione dei messaggi duplicati, certezza della consegna del messaggio);
  trasparenza temporale (rispetto della sequenza temporale dei messaggi tra gli end point).

7.2.1. Modelli di Cooperazione tra Porte di Dominio

L'interoperabilità tra i sistemi informativi delle diverse PA si realizza attraverso i servizi di Cooperazione Applicativa con l'interscambio di dati e di informazioni necessarie alle PA per la soddisfazione ultima del cittadino/impresa.

Definendo una scala ideale vista per complessità crescente di servizio, troviamo i seguenti modelli di cooperazione:

- la notifica evento (servizi di pubblicazione/abbonamento basati su tecnologie di tipo Publishing & Subscribe oppure Store&Forward);
- la cooperazione per richiesta di servizio (invocazione unidirezionale, richiesta/risposta, notifica, notifica/risposta);
- la cooperazione per collaborazione tra più soggetti (descritti come servizi composti opachi, trasparenti, a orchestrazione di processo e servizi di intermediazione nel documento architetturale) che può essere intesa come una combinazione di interazioni per notifica di evento o per richiesta tra più soggetti.

Tutti i modelli sono implementabili mediante il paradigma dei Web Service e sono supportati dalla Busta di e-Government [Busta e-Government].

Cooperazione per Eventi

L'interazione tra gli interlocutori avviene in modo indiretto, intermediata da una infrastruttura di servizio di Gestione Eventi (Publish and Subscribe oppure Publish&Forward). Questa infrastruttura fornisce servizi per la pubblicazione di un evento e di sottoscrizione agli eventi stessi. In questo paradigma una PA, a fronte di un evento (richiesta cittadino/impresa, risultato di un'elaborazione etc...), lo pubblica sul sistema di Gestione Eventi. Quest'ultimo si occupa di notificarlo poi, in modo opportuno, a tutte le amministrazioni che avevano preventivamente sottoscritto quell' evento specifico. Occorre notare che l'infrastruttura che implementa il servizio di Gestione degli eventi può essere implementata mediante un Web Service con cui interagire secondo il modello di cooperazione per richiesta di servizio.

Cooperazione per Richiesta

Con riferimento agli effetti sul dominio servente la richiesta può essere di due tipi, interrogazione oppure transazione:

- l'interrogazione è una richiesta di servizio che restituisce una informazione del dominio servente senza modificare alcun oggetto applicativo dello stesso dominio.
- la transazione è una richiesta di servizio che è destinata a produrre una variazione permanente in un qualche oggetto applicativo del dominio servente. La transazione può interessare anche oggetti di più domini. La transazione comporta sempre anche il supporto del paradigma informatico della transazione, nel senso tecnico del termine, perché la modifica permanente di un oggetto applicativo di un altro dominio deve essere garantita atomica e consistente e quindi, se non portata a compimento, deve essere reversibile. La risposta non contiene necessariamente una informazione applicativa, ma può anche ridursi alla semplice segnalazione che la transazione è stata completata oppure no.

Cooperazione per Collaborazione tra più soggetti

Tale metodologia permette il colloquio tra più soggetti e rende possibile sia la Cooperazione per Eventi che la Cooperazione per Richiesta a seconda delle esigenze

Nell'ambito della definizione degli standard per la cooperazione applicativa tra PA, è necessario normalizzare almeno in termini di definizioni i paradigmi di interazione necessari alla cooperazione tra

applicazioni e più in generale tra Porte di Dominio. A tal fine possiamo assumere che ciascun episodio di collaborazione applicativa preveda l'utilizzo di messaggi.

Le collaborazioni, di seguito descritte rientrano negli scenari di coordinamento di tipo invocazione unidirezionale oppure Richiesta/risposta e prevedono l'utilizzo di un messaggio unidirezionale, oppure di un messaggio/replica (richiesta/risposta), quest'ultimo in modalità *sincrona oppure asincrona*. Per convenzione, relativamente ai messaggi, 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.

L'utilizzo della modalità sincrona o asincrona dello scambio dei messaggi 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 ragioni 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 il cambio di stato di una corrispondente registrazione.

In ogni caso, è da sottolineare che:

- la scelta delle modalità di interazione non dipende in generale dal tipo di servizio erogato ma dalle modalità organizzative ed implementative utilizzate per l'esportazione telematica;
- è quindi possibile, anche se non auspicabile, 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;
- di norma le porte di dominio esporteranno 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.

Si riportano, nel seguito, i dettagli relativi ad alcune tipologie di interazione che realizzano i modelli di cooperazione per Richiesta o per Eventi. In [Busta e-Government], inoltre, è riportato l'utilizzo della Busta di e-Government per ciascun modello .

7.2.1.1. Scenario di invocazione unidirezionale

Il caso di invocazione unidirezionale prevede l'invio di un messaggio unidirezionale (*MessaggioSingoloOneWay*, della Busta di e-Government). Come rappresentato in figura 8, la Porta Delegata invia un messaggio alla Porta Applicativa ma non resta in attesa di alcuna risposta.

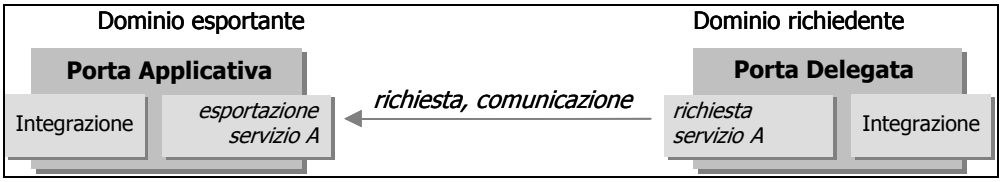


Fig. 8 Invocazione unidirezionale mediante messaggio One Way

7.2.1.2. Scenario di invocazione Richiesta/risposta sincrono

Lo scenario viene implementato dallo stile elementare di scambio messaggio/replica. Nel caso in esame, illustrato in figura 9 , il messaggio (richiesta) viene formato dal sistema informatico presso il dominio richiedente e quindi trasmesso dalla porta delegata. La porta delegata rimane in attesa della replica (risposta). Presso il dominio esportante il messaggio viene ricevuto ed elaborato, con la formazione e trasmissione della replica .

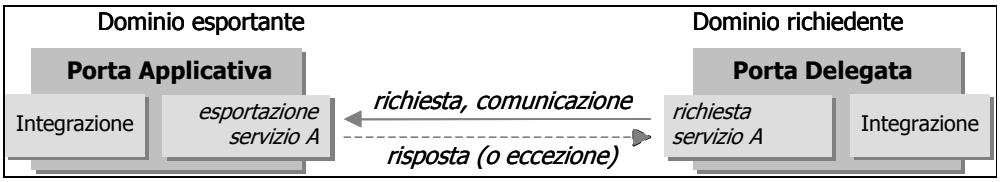


Fig. 9 Messaggio/replica sincroni

7.2.1.3. Scenario di invocazione Richiesta/risposta asincrono simmetrico.

Nel primo caso di cooperazione asincrona, ovvero nella tipologia asincrona simmetrica, come riportato in figura 10 , è previsto l'utilizzo di due scambi di tipo messaggio/replica, invece di uno. La collaborazione ha inizio con l'invio di un messaggio di richiesta da parte della porta delegata del Dominio richiedente, a cui fa seguito una replica (risposta) della porta applicativa del Dominio esportante contenente la sola ricevuta della richiesta. Successivamente, la Porta Delegata del Dominio esportante trasmette il messaggio contenente la risposta applicativa alla Porta Applicativa del Dominio Richiedente, mediante la seconda interazione sincrona di tipo messaggio/replica. Anche in questa seconda interazione, la Porta Applicativa del Dominio richiedente restituisce al mittente una ricevuta. In questa tipologia entrambi i domini devono avere implementato la coppia completa (Applicativa e Delegata) di porte di dominio.

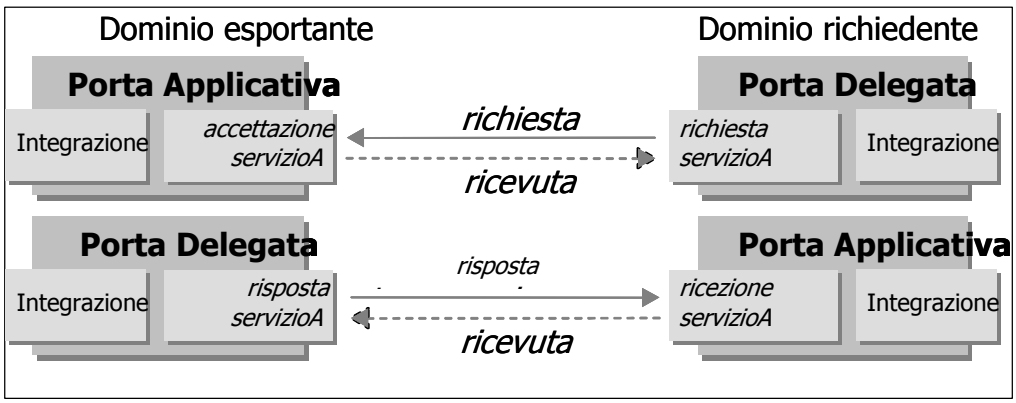


Fig. 10 Servizio asincrono simmetrico.

7.2.1.4. Scenario di richiesta/risposta asincrono asimmetrico

In una seconda tipologia di cooperazione asincrona, definita collaborazione asincrona asimmetrica, illustrata in figura 11, è compito della parte richiedente di contattare nuovamente in un tempo successivo alla richiesta la parte esportante al fine di ottenere la risposta effettiva. A questo scopo, la porta applicativa espone un secondo servizio apposito. Oltre alla richiesta originaria, la porta delegata invia un nuovo messaggio alla porta applicativa per verificare lo stato della richiesta e quindi ottenere la risposta. Questa seconda tipologia non prevede la necessità di una porta applicativa presso il dominio richiedente. Potrebbe essere utilizzata nel caso in cui la Porta Applicativa sia dietro un firewall e non accetti connessioni in ingresso, oppure nel caso in cui il Dominio richiedente non sia dotato di una Porta Applicativa (ed il Dominio esportante supporti il profilo AsincronoAsimmetrico).

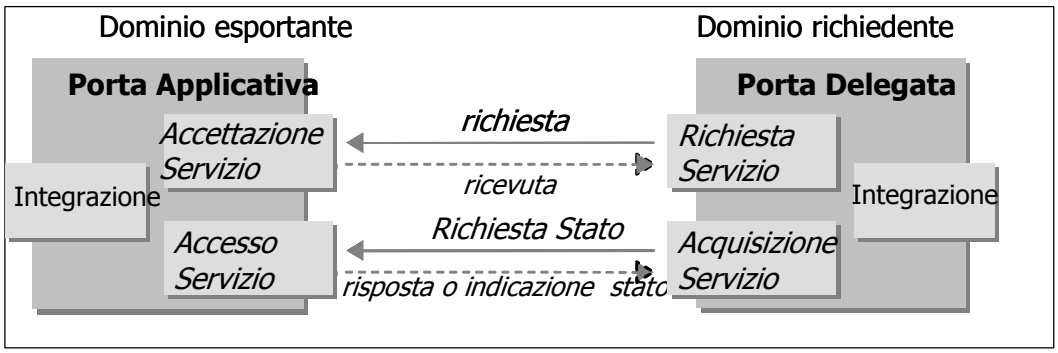


Fig.11 Servizio asincrono simmetrico.

Questo pattern di cooperazione, spesso utilizzato nel caso di "polling" sullo stato di esecuzione di una richiesta è naturalmente inefficiente . Deve essere utilizzato laddove effettivamente necessario secondo gli schemi descritti.

7.2.1.5. Cooperazione per notifica di eventi

Nel modello di cooperazione basato sul meccanismo di Publish & Subscribe la segnalazione o notifica di evento ha lo scopo di informare dell'evento le applicazioni di uno o più domini destinatari

che, sulla base del significato del messaggio associato all'evento, producono un cambiamento permanente del valore di propri oggetti applicativi. In questo modello cooperano domini che pubblicano o notificano eventi e domini che sottoscrivono eventi. Gli attori di questo sistema sono: i domini pubblicanti, quelli sottoscrittori ed il gestore del servizio di P&S. Il servizio di P&S è descritto dettagliatamente nel Quaderno Aipa "Servizio di cooperazione applicativa basato su eventi" del Dicembre 1999, a cui si rimanda per ulteriori approfondimenti.

In questa tipologia di cooperazione, a fronte di una precedente registrazione nel sistema di gestione eventi come dominio pubblicante e come dominio sottoscrittore, il messaggio viene formato dal sistema informatico presso il dominio pubblicante e viene inviato dalla porta delegata presso il sistema di gestione eventi. Il sistema di gestione eventi quindi notificherà (con il protocollo dichiarato al momento della sottoscrizione) sulla porta applicativa del dominio sottoscrittore l'esistenza di un nuovo evento.

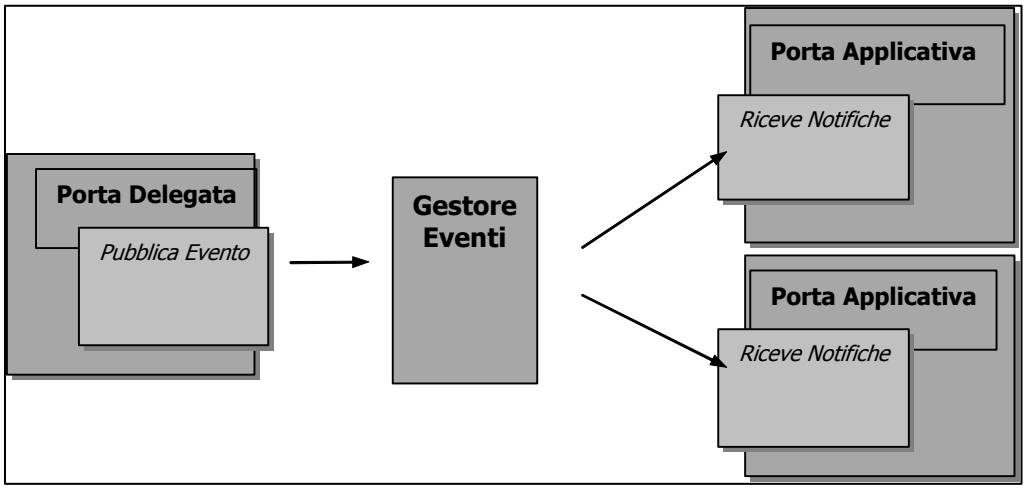


Fig.12 Servizio di Pubblicazione Eventi.

Generalmete l'integrazione tramite lo scambio di messaggi segue uno di questi due modelli:

Point – to - Point

Publish – Subscribe

Il più utilizzato modello di comunicazione Point – to - Point è basato sul meccanismo di tipo Poll o demand – driver. Il modello si basa sulle code. Mittente e Destinatario insieme una coda attraverso la quale scambiarsi messaggi. Le applicazioni interrogano ciclicamente la coda per verificare la presenza di messaggi.

Il modello di comunicazione Publish – Subscribe è basato sul meccanismo di Push o event-driven. Il produttore non indirizza il messaggio a nessuno.Il consumatore recupera i messaggi a lui indirizzati in base a regole definite nella fase di subscribe (rule-based routing), in base al loro contenuto (content-based) o in base a informazione contenute nell'header (subject-based).

Il modello di comunicazione di Publish & Forward, può essere visto come un caso particolare del modello Publish & Subscribe, in cui le informazioni sui pubblicatori e sui sottoscrittori sono già presenti nel Gestore degli Eventi.

Il Servizio di Gestione degli Eventi è basato su delle funzionalità di servizio:

connessione degli Enti secondo modalita' asincrone di scambio messaggi

scambio di messaggi in modo sicuro e certificato

monitoraggio del trasporto

integrazione con i sistemi informativi esistenti presso le aziende connesse al sistema

I Servizi offerti da Gestore degli Eventi permettono di collegare gli Enti in modo lineare secondo meccanismi di messagistica asincrona. Per esempio un utente non automatizzato potrà inviare un Evento o un Messaggio ad una coda e quindi a tutte gli altri Enti registrati per ricevere l'Evento per segnalare il cambio di residenza di un cittadino o la nascita di una nuova azienda. Il destinatario dell'Evento / Messaggio riceverà il dato e attiverà tutte le procedure necessarie ad aggiornare i propri dati. Il Gestore degli eventi dovrà garantire:

- paradigmi di interazione asincrona mediante scambio di messaggi
- sicurezza dei messaggi ricevuti/inviati e l'autenticazione degli utenti/sistemi esterni abilitati a scambiarli
- estrarre dai messaggi inviati le informazioni relative al logging
- supporto ai protocolli Internet più diffusi: HTTP, FTP, SMTP.
- delivery dei messaggi (nessuna perdita , nessuna duplicazione)
- gestione dei messaggi non inviati per condizione di errore o eccezione.
- trasformare un messaggio ricevuto prima di mandarlo al destinatario
- l'auditing sui messaggi ricevuti e inviati

7.3. Gestore degli eventi.

Nell'ambito dei servizi infrastrutturali presenti sull' SPC, gioca un ruolo rilevante il servizio di "Gestione Eventi". Si tratta infatti di un servizio applicativo necessario per poter implementare il modello di cooperazione per eventi, che prevede lo scambio di messaggi al fine di comunicare il verificarsi di uno specifico evento (es. nascita, matrimonio, iscrizione, derubricazione, etc.).

Dal punto di vista telematico, il modello di riferimento è quello del "Publish & Subscribe" (o in taluni casi del del "Publish & Forward"). In tale modello, il **Gestore degli Eventi** è il servizio applicativo che

si occupa di trasmettere le comunicazioni di evento tra i soggetti interessati (sistemi informativi oppure altri Gestori eventi).

Il Gestore degli Eventi potrebbe essere organizzato in modo federato ipotizzando uno scenario in cui siano presenti più istanze di tale servizio utilizzate differenti Domini di Cooperazione .

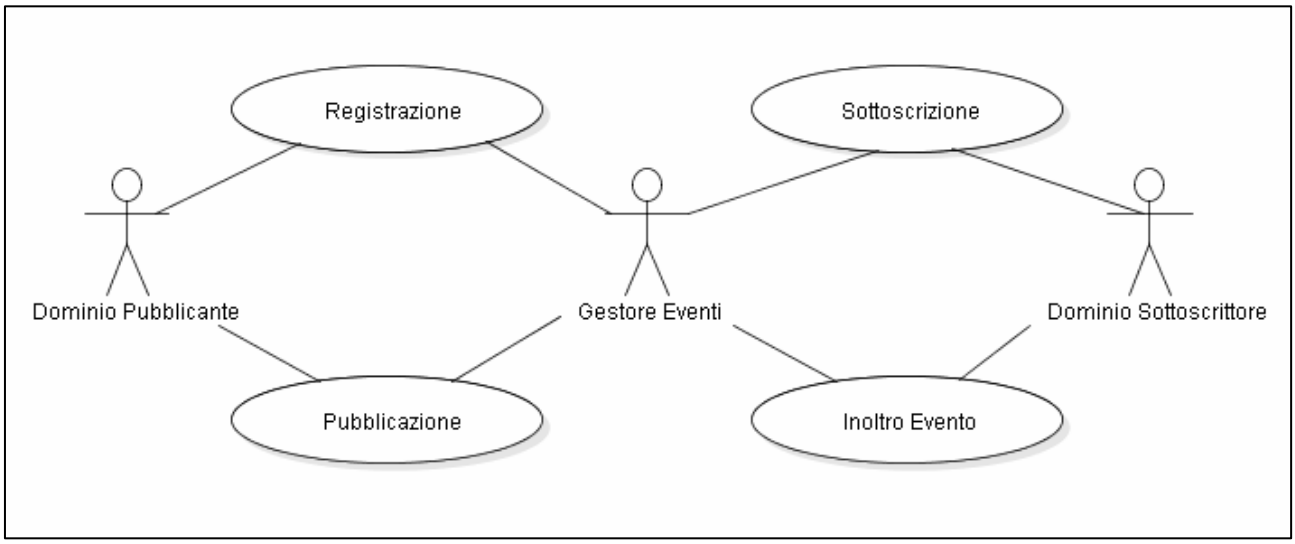


Fig.13 Il Gestore Eventi.

Il Gestore Eventi è strutturato come una porta applicativa con il compito di ricevere, e consegnare messaggi contenenti eventi amministrativi, utilizzando la busta standard di e-Government.

Come indicato in figura 13, il Gestore degli Eventi espone primariamente i seguenti servizi:

Sottoscrizione: consente ad una amministrazione di sottoscriversi alla ricezione di un evento fornendo i necessari parametri quali tipo di evento, protocollo per la notifica (http/SOAP o SMTP), etc…

Pubblicazione: consente di immettere un evento affinché sia propagato a chi è interessato a riceverlo (subscriber). L'operazione di Publishing consiste nell'invio di un messaggio contenente informazioni quali tipo evento, evento XML, priorità etc…

Inoltro: consente di inoltrare un evento ad una o più amministrazioni che sono sottoscritte per ricevere la particolare tipologia di evento.

Inoltro per competenza: consente di inoltrare un evento ad una o più amministrazioni che non sono direttamente sottoscritte per ricevere la particolare tipologia di evento ma che lo devono ricevere per competenza.

Notifica: consente di notificare ai sottoscrittori la presenza di un nuovo Evento per la classe di eventi sottoscritti. Il messaggio notificato dal Gestore ai sottoscrittori contenente informazioni quali tipo di evento, identificativo del messaggio, etc…

Ricezione: consente di attivare la ricezione di un evento di cui si sia ricevuta una notifica. L'operazione di Retrieve consiste nell'invio di un messaggio contenente informazioni quali tipo di evento, identificativo del messaggio, etc…

Garanzia di consegna: Consente di verificare la ricezione da parte delle amministrazioni destinatarie dell'evento, attraverso l'utilizzo della firma automatica e della ricevuta elettronica di ricezione.

L'Inoltro, l'Inoltro per Competenza e la Notifica definiscono delle interfacce che devono essere implementate dalle Porte di Dominio.

Il Gestore Eventi deve fornire un insieme di servizi in grado di:

- Garantire il delivery dei messaggi (nessuna perdita, nessuna duplicazione)
- Assicurare la gestione dei messaggi non inviati per condizione di errore o eccezione.
- Garantire l'auditing sui messaggi ricevuti e inviati, offrendo funzionalità di monitoraggio remoto.

Per il Gestore Eventi e' possibile ipotizzare differenti scenari d'implementazione:

Scenario Base: sono definite le sole interfacce di **Pubblicazione**, **Ricezione**, **Inoltro** e **Inoltro per Competenza**. In questo scenario non e' definita nessuna interfaccia Web Services per la sottoscrizione e neppure le interfacce per la propagazione delle sottoscrizioni tra differenti Gestori degli Eventi.

Scenario Completo: sono definite tutte le interfacce, compresa l'interfaccia per le sottoscrizioni e i meccanismi per realizzare un'architettura federata di Gestori degli Eventi. Le sottoscrizioni sono propagate automaticamente attraverso i differenti Gestori che costituiscono la federazione.

Definire tutti i dettagli per realizzare lo "Scenario Completo" e' molto complesso e troppo ambizioso, almeno in questa fase, mentre lo "Scenario Base", con qualche piccola aggiunta di tipo organizzativo, risulta essere realizzabile e copre la quasi totalità delle esigenze di una cooperazione per Notifica di Evento. Con lo scenario base e' possibile implementare un'architettura federata in cui la sottoscrizione non e' propagata automaticamente ma gestita dai singoli amministratori dei diversi Gestori degli Eventi. In pratica un Gestore degli eventi che volesse ricevere gli eventi da un altro gestore dovrebbe sottoscriversi come una qualunque altra applicazione / ente. Quindi non e' la sottoscrizione del singolo ente a propagarsi attraverso i gestori, ma sono i gestori che sono reciprocamente sottoscrittori e pubblicatori degli eventi. In questo modo la gestione delle sottoscrizione federata e' notevolmente semplificata. Ogni ente o Dominio di Cooperazione potrebbe avere un Gestore degli Eventi di riferimento per una particolare classe di Eventi (per esempio relativi alla persona fisica, alla persona giuridica, etc.).

Poiché il Gestore Eventi costituisce a tutti gli effetti un servizio, come tale dovrebbe essere inserito e descritto nel registro dei servizi. Insieme alla descrizione delle interfacce dovrebbe essere disponibile anche la lista degli eventi gestiti ed il riferimento alla relativa documentazione di dettaglio.

Per esempio, le informazioni presenti nel registro relative ad un Gestore Eventi potrebbero essere:

- Endpoint servizi di subscribe-unsubscribe;

- Certificati utilizzati per la firma del contenuto della busta (evento)
- Responsabile del servizio e relativi contatti
- Lista Eventi gestiti
- Lista Enti gestiti

In figura 14 è raffigurato il caso di due Amministrazioni che interoperano attraverso i propri Gestori Eventi.

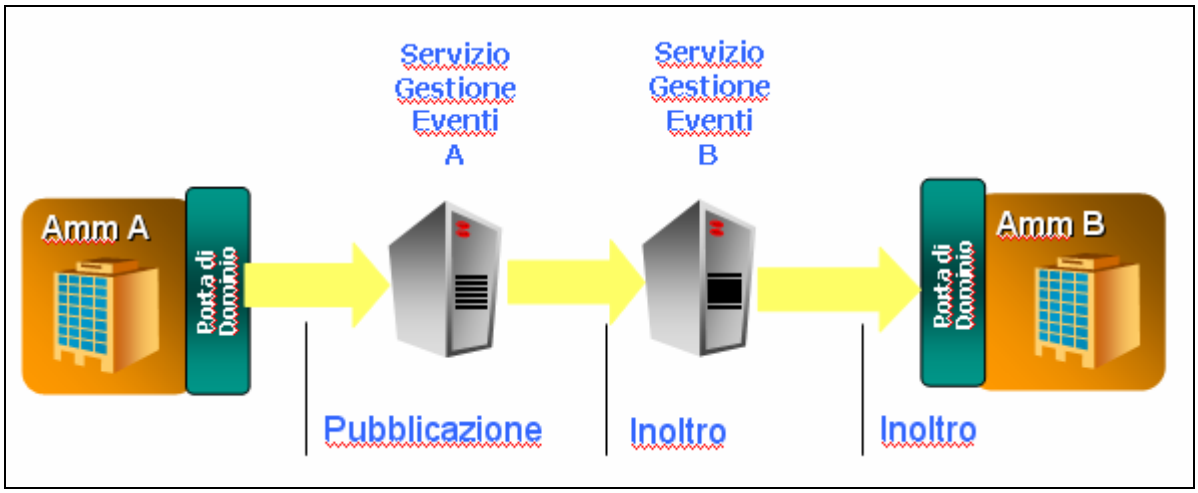


Fig. 14

In Allegato 1 sono riportate le specifiche di interfacciamento del Gestore Eventi.

7.4. Specifiche da definire

I Web Services si stanno rapidamente affermando come la principale via per integrare un ampio numero di servizi e applicazioni. Le specifiche base dei Web Services sembrano aver raggiunto un buon livello di maturazione e diffusione, diversa e' la situazione sulle specifiche di più altro livello dove sembra esserci stato un rallentamento dei processi di standardizzazione.

In questo paragrafo saranno introdotti gli standard piu' interessanti in via di definizione e che riguardano le seguenti aree:

- Gestione dei processi
- Transazioni
- Sicurezza
- Garanzia di consegna

Fig. 15 Schema degli standard

Esistono numerose specifiche in via di definizione, alcune definite da un gruppo di aziende e quindi protette da Copyright ed altre in via di definizione sui tavoli delle organizzazioni internazionionali quali W3C e OASIS:

- W3C: WS-Choreography

- OASIS: Orchestration - BPEL
- OASIS: WS-Reliability
- OASIS: WS-Security
- Spec: WS-Transaction
- Spec: WS-Coordination
- Spec: WS-Addressing

7.4.1. Gestione dei processi

La gestione dei processi costituisce uno dei argomenti più interessanti su cui si concentrano gli sforzi di molte aziende. Riuscire a definire uno standard con cui descrivere un processo aziendale costituisce un enorme passo avanti in termini di flessibilità e ritorno degli investimenti. Infatti se da un lato i web services sono visti come un elemento chiave per integrare i sistemi Legacy, dall'altro e' necessario disporre di strumenti e standard che permettano di descrivere il processo per poter intervenire in modo più semplice e flessibile alle richieste di cambiamento.

Gli enti OASIS e W3C stanno lavorando alla definizione degli standard per la gestione dei processi. Fino ad qualche tempo fa il lavoro di queste due organizzazioni poteva apparire in

sovrapposizione ed in complotto, questa situazione ha fatto pensare a molti come ad una guerra sugli standard.

In realtà, anche se sono deputati a svolgere le medesime mansioni, il loro approccio ai processi di business e alle applicazioni è sensibilmente differente.

Per le differenziare il lavoro di OASIS da quello di W3C si utilizzano spesso i termini Orchestrazione e Coreografia:

Orchestrazione: si riferisce all'esecuzione di un processo che può interagire con Web Services interni o esterni. L'orchestrazione definisce le interazioni dei Web Services a livello di messaggi, la logica di processo e l'ordine delle interazioni. Queste interazioni possono coinvolgere molte applicazioni e/o organizzazioni definendo un processo transazionale. L'orchestrazione e' sempre controllata da una sola organizzazione.

Coreografia: rappresenta uno scenario piu' collaborativi rispetto all'orchestrazione, in cui ogni organizzazione coinvolta nel processo descrive la sua parte di processo. La Coreografia traccia la sequenza dei messaggi che possono coinvolgere molteplici organizzazioni e molteplici fonti.

L'Orchestrazione si differenzia dalla Coreografia perche' descrive il flusso dei processi controllato da una sola organizzazione. La Coreografia e' piu' collaborativi e traccia i messaggi scambiati da piu' aorganizzazioni, dove nessuna e' proprietaria di tutta la collaboarazione[8].

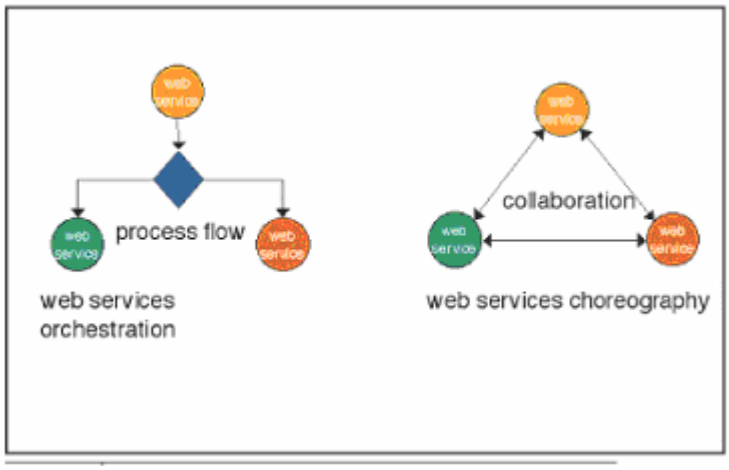
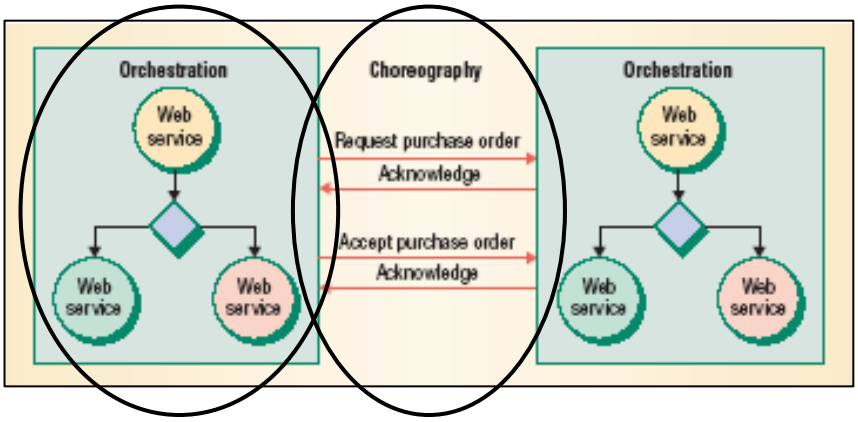


Fig. 16 – Schematizzazione del flusso dei processi nell'Orchestrazione e nella Coreografia

Fig. 17 – Schema di funzionamento dell'Orchestrazione e della Coreografia

[8] Definizioni introdotte da Chris Petz nell'articolo apparso sul Web Services Journal (http://www.sys-con.com/webservices/articleprint.cfm?id=592)



I due standard in via di definizione che rappresentano l'Orchestrazione e la Coreografia dei processi sono rispettivamente

- OASIS- Web Services Business Process Execution Language (BPEL4WS)
  http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsbpel

- W3C-Web Services Choreography Description Language (WS-CDL)
  http://www.w3.org/2002/ws/chor/

BPEL fornisce al singolo servizio regole e margini di movimento, lasciando che le interazioni tra più processi vengano governate dall'intervento di WS-CDL.

7.4.1.1. Lo stato attuale

W3C- Web Services Choreography Description Language (WS-CDL)- Gruppo di lavoro del W3C fondato nel gennaio 2003.- Il primo meeting è del 13 marzo 2003

Il primo draft di WS-CDL, acronimo di Web Services Choreography Description Language, è giunto infatti a compimento il 27 aprile 2004. Si tratta di una componente chiave, che disciplina i modi in cui i Web service interagiscono gli uni con gli altri e con gli utenti finali, permettendo alle applicazioni di comunicare tra loro. WS-CDL è basato su Xml e supporta la versione 1.2 di Soap e la 2.0 di Wsdl.

OASIS- Web Services Business Process Execution Language- Comitato tecnico di OASIS creato nell'aprile 2003.- Il primo incontro è del 16 maggio 2003

Il primo draft del BPEL4WS ad opera di OASIS e' stato pubblicato il 23 aprile 2004. Questa specifica nasce pero' da un lavoro precedente, la cui specifica 1.1 pubblicata il 5 maggio 2003, e' stata presentatala gruppo di lavoro OASIS nella riunione del 16 maggio 2003.

7.4.1.2. La convergenza

Entrambi gli enti di standardizzazione, l'Oasis e W3C, hanno costituito un gruppi di lavoro sulla gestione dei processi di Web Services. Oasis sta concentrando il proprio lavoro sulla definizione di risorse 'stateful' utilizzando i Web services e sulla questione delle notifiche. Come sempre quello di Oasis vuole essere un framework generale e aperto, ma anche privo di royalty.

Il W3C dal canto suo porta avanti un lavoro di choreography piuttosto astratto e dunque a priori adatto a diversi ambienti di utilizzo. L'ultimo draft è stato definito alla fine di marzo, ma lo scopo resta sempre quello iniziale: definire un modello astratto che descriva i dati e le loro relazioni, per poter realizzare una 'coreografia' che descriva la sequenza e le condizioni da soddisfare perché i dati scambiati da due o più applicazioni abbiano un senso ben definito.

Lo scenario proposto da W3C vede BPEL4WS per la definizione dei processi aziendali e WS-CDL per la coreografia di processi aziendali di differenti organizzazioni.9

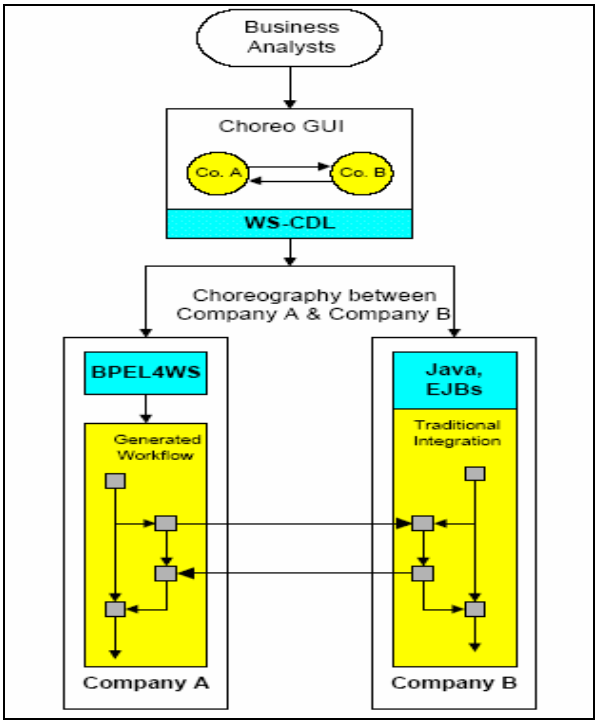


Fig. 18 –Scenario W3C per la coreografia dei processi

[9] Scenario proposto da W3C, nel documento Web Services Choreography Description Language Version 1.0 pubblicato in Working Draft il 27 Aprile 2004 (http://www.w3c.org/TR/ws-cdl-10/)

8. TASSONOMIA

Una tassonomia rappresenta un metodo di classificazione sistematica di oggetti. Nel contesto dell'SPC il termine viene utilizzato per indicare un insieme di specifiche formali per la raccolta ed archiviazione di metadati e dati in registri elettronici.

L'approccio scelto per effettuare tale classificazione è di tipo graduale e parte dalla rilevazione dell'esistente (progetti di e-Government in via di realizzazione o progetti già esistenti) per approdare alla raccolta sistematica degli schemi dei dati di interesse Nazionale.

Per la descrizione degli schemi dei dati, dei servizi e dei documenti verranno utilizzati, prevalentemente, formalismi basati sul linguaggio XML (XML Schema, Relax NG, WSDL).

La costruzione della tassonomia, nell'ambito SPS, prevede la classificazione delle differenti tipologie di servizi (sia applicativi che infrastrutturali), e dei dati. Tali classificazioni possono essere basate su diversi criteri di omogeneizzazione tra di loro anche intersecabili, ad esempio i dati ed i servizi anagrafici, territoriali, previdenziali, gli eventi della vita ecc.

8.1. Principi

La costruzione di una tassonomia in ambito SPC prevede che siano enunciati i principi a cui dovranno attenersi tutte le amministrazioni aderenti al programma di cooperazione pubblica. A puro titolo indicativo, di seguito ne vengono enunciati alcuni esempi:

- Precedenza degli standard usati nel catalogo (standard preesistenti);
- Regole di nomenclatura:
  - Formato dei nomi;
  - Designatori di standard (codice, descrizione, numero, tipologia);
  - Utilizzo di acronimi ;
- Contesto;
- Scopo;

8.2.Template

E' buona norma, inoltre, che ogni dato presente sul catalogo sia standardizzato e documentato secondo un template. Se ne propone, di seguito, un esempio:

Nome Elemento	Descrizione
Nome:	*Nome completo del dato in accordo con le regole di nomenclatura*
Status:	*'agreed' or 'draft'*
Data di validazione	*La data in cui il Cnipa ha adottato lo standard*
Descrizione:	*Una descrizione semplice ma non ambigua del dato*
Formato logico	*Il formato al quale il dato deve attenersi (minima e massima lunghezza, numero di caratteri, la struttura del dato, …)*
Schema XML	*Il collegamento agli schemi xml che utilizzano il dato*
Valori ammessi:	*Se significativi*
Titolare:	*Dipartimento, Agenzia, Organizzazione responsabile del dato*
Standard di riferimento:	*(es. BACS, ISO, BSI, BSEN, W3C)*
Commenti:	*Note eventuali*
Data di pubblicazione	
.....	

Tab. 3 Esempio di Template

8.3.Iniziative per migliorare la qualità dei dati.

L'AIPA a suo tempo ha avviato iniziative di studio e di sperimentazione per migliorare la qualità dei dati presentando agli inizi del 2002 il documento dal titolo "I dati pubblici: linee guida per la conoscibilità, l'accesso la comunicazione e la diffusione". Lo studio, sulla base dell'accordo di collaborazione stipulato successivamente tra l'Autorità e l'ISTAT [Qualità dei Dati], fornisce la definizione dei criteri guida per l'analisi e la gestione della qualità dei dati nella Pubblica Amministrazione, con riferimento specifico a due ambiti di particolare importanza e criticità:

1. i dati toponomastici presenti negli archivi Amministrativi per la localizzazione geografica dei soggetti fisici e delle unitàò economiche;

2. i dati Amministrativi utilizzati per la costruzione di indicatori statistici sulle imprese e le istituzioni provate riguardanti il mercato del lavoro.

I risultati di tale lavoro, una volta pubblicati, costituiranno il riferimento daranno lo spunto per le successive iniziative di standardizzazione e definizione della qualità dei dati in ambito Nazionale per il sistema SPC

L'indirizzo strategico del Cnipa in continuità con quanto già realizzato è quello di sviluppare le attività in modo incrementale sotto la guida dei progetti istituzionali sviluppati dalle pubbliche amministrazioni sia locali che centrali, in modo da poter riutilizzare le esperienze innovative che sono state già fatte in questo campo.

A esempio, tra i più recenti progetti innovativi, approvati dal Dipartimento per l'Innovazione e le Tecnologie nell'ambito dell'attuazione del Piano d'azione di e-government nazionale, troviamo il progetto denominato SIGMA TER, che si inquadra nel contesto caratterizzato dal Piano di Decentramento del Catasto ai Comuni, in esecuzione della Legge n. 59 del 1997, così come definito dal D.Lgs. n. 112 del 31/3/1998 che ridisegna i rapporti tra Stato ed Enti Locali ed assegna un ruolo determinante ai Comuni per quanto riguarda le funzioni catastali.

In linea con la metodologia incrementale scelta per effettuare la tassonomia, viene riportata in appendice, a titolo di esempio, la proposta di standardizzazione utilizzata per il campo 'INDIRIZZO' nell'ambito dei 'Servizi integrati catastali e geografici per il monitoraggio amministrativo del territorio' (SIGMA TER - Progetto di e-Government già finanziato con il primo bando) a cui partecipa l'Agenzia del Territorio, 5 regioni, 5 provincie, 12 comuni e 2 comunità montane. Al progetto partecipano anche 200 enti riusatori tra comuni, associazioni ed unioni di comuni, provincie e comunità montane per un totale di oltre 10 milioni di abitanti.

9. SICUREZZA NELLE INTERAZIONI TRA APPLICAZIONI

9.1. Premessa

Nel definire gli standard per le funzioni di sicurezza nella cooperazione applicativa occorre necessariamente fare riferimento ad un determinato sistema di sicurezza. Le misure di sicurezza sono a loro volta funzione dello scenario di rischio e devono essere individuate, caso per caso, in relazione alle peculiarità delle applicazioni.

Si assume che la scelta delle misure di sicurezza da mettere in atto ricada tra le responsabilità del dominio di cooperazione, che attuerà tale scelta in funzione delle caratteristiche delle applicazioni e del contesto organizzativo e tecnico.

Obiettivo di questo capitolo è invece la definizione delle regole o dei criteri che dovranno essere seguiti nella realizzazione delle misure di sicurezza individuate.

Poiché le misure di sicurezza possono variare alquanto in funzione dei livelli di rischio, si è scelto di prendere in considerazione, in prima battuta, misure di sicurezza idonee per sistemi caratterizzati da elevati requisiti di sicurezza, ma che non ricadono tra quelli idonei a trattare informazioni coperte dal segreto di stato.

9.2. Modello di riferimento

Per la definizione degli standard si è fatto riferimento al modello architetturale per la cooperazione applicativa che di seguito si schematizza[10].

L'attività di cooperazione può essere ricondotta ad uno scambio di messaggi tra due organizzazioni[11], veicolato da entità logiche definite con la locuzione "porte di dominio". La porta di dominio ha la funzione di normalizzare lo scambio informativo tra le due organizzazioni implementando i protocolli di cooperazione secondo gli standard propri del Sistema Pubblico di Connettività.. Il trattamento delle informazioni è invece eseguito dai "domini dei servizi", ossia gli insiemi di servizi che le organizzazioni rendono disponibili per realizzare funzioni cooperanti.

Secondo tale modello, gli standard per la sicurezza riguardano essenzialmente le funzioni svolte dalle porte di dominio che devono poter interagire in base a regole comuni.

[10] Per gli approfondimenti sul modello architetturale si rimanda allo specifico documento.
[11] Nei documenti di architettura si fa riferimento a scambi informativi tra pubbliche amministrazioni, in quanto il modello delineato è finalizzato a governare la realizzazione e la gestione di servizi cooperanti nel settore pubblico. Nel trattare gli aspetti di sicurezza si preferisce prescindere dalla natura dei soggetti coinvolti e fare riferimento a generiche organizzazioni.

Tuttavia occorre considerare che molti aspetti di sicurezza sono fortemente connessi alle logiche di trattamento delle informazioni, come ad esempio le regole di autorizzazione che dipendono dal contenuto informativo dei messaggi scambiati.

Inoltre il costante sviluppo dei prodotti di supporto alle applicazioni – ed in particolare dei web services – porta a separare sempre di più dal codice applicativo le logiche che attengono agli aspetti di sicurezza, consentendo di affrontare in modo generale ed integrato problematiche quali la gestione delle utenze, dei profili di accesso, delle regole di autorizzazione, ecc. Queste problematiche, generalmente referenziate con l'espressione "identità federata"[12], sono correntemente affrontate da modelli di cooperazione e specifiche che promettono di confluire in soluzioni standard, ma ancora non hanno raggiunto un sufficiente livello di maturità.

9.2.1. *Funzioni di sicurezza*

In seguito a quanto osservato viene definito il modello di sicurezza schematizzato dalla figura seguente.

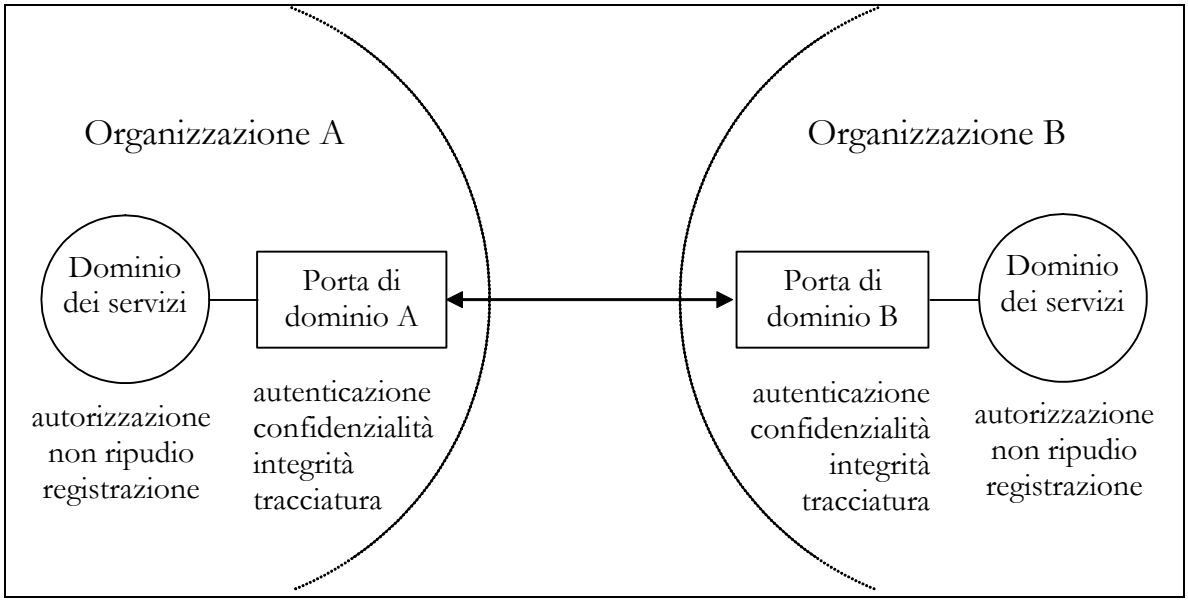


Fig. 19 – Schema del modello di sicurezza

Secondo tale modello presso ogni porta di dominio dovrà essere possibile realizzare in modo standard le seguenti funzioni di sicurezza:

- mutua autenticazione delle porte;
- autenticazione dei messaggi;
- confidenzialità dei messaggi;

[12] In un sistema di identità federata le credenziali dell'entità che attiva un servizio (ossia le informazioni che servono a verificare la titolarità ad eseguire l'intero processo) vengono trasmesse in modo standard tra i diversi servizi cooperanti in modo tale che ciascun servizio possa effettuare le verifiche necessarie per concedere l'autorizzazione.

– tracciatura applicativa.

Le funzioni di sicurezza svolte dalle porte di dominio dovranno basarsi su informazioni di sistema trasmesse dai protocolli di cooperazione applicativa.

Le funzioni di sicurezza che necessitano di trattare il contenuto dei messaggi saranno invece svolte dai domini dei servizi. Tra queste funzioni ricadono:

– l'autorizzazione al servizio;

– le funzioni applicative per la non ripudiabilità delle informazioni;

– le funzioni di registrazione delle prove non ripudiabili (registrazione delle istanze).

9.2.2. *Misure di sicurezza*

Le funzioni di sicurezza elencate possono essere implementate da componenti che logicamente fanno parte di livelli di comunicazione/cooperazione diversi.

– Il primo livello è quello di trasporto del Sistema Pubblico di Connettività e fa riferimento alle misure di sicurezza rese disponibili dalla infrastruttura di comunicazione. Nella figura viene evidenziata la possibilità di utilizzare la protezione di tipo VPN che assicura l'integrità e la confidenzialità dei messaggi. Le garanzie delle protezioni realizzate al livello di trasporto coprono lo scambio di dati tra porte di rete.

– Il secondo livello è quello del canale SSL che può essere attivato con le funzioni standard dei web server. Il canale SSL può garantire la l'integrità e la confidenzialità delle transazioni tra web server.

– Il terzo livello riguarda le funzioni per la protezione dei messaggi SOAP secondo gli standard definiti dal WS-security. Nel caso della cooperazione applicativa il messaggio soap sarà conforme alle specifiche della busta di e-government. Le protezioni realizzate a questo livello consentono di assicurare l'integrità, la confidenzialità e l'origine dei messaggi.

– Il quarto livello è quello delle applicazioni e può utilizzare sistemi per acquisire le informazioni utili all'autorizzazione o per l'attribuzione della responsabilità in merito a determinate informazioni. Tra questi strumenti sono previsti la firma digitale – il cui uso assicura anche l'integrità delle informazioni che sono state sottoscritte – e strumenti per la gestione dell'identità federata. Per la firma digitale si fa riferimento alla normativa Italiana, per le funzioni di identità federata si delega a funzioni applicative; si guarda comunque con attenzione allo standard SAML che, pur non essendo ancora integrato in modo standard con ws security, probabilmente diventerà il riferimento per i prodotti di gestione dell'identità federata.

Firma digitale/identità federata	Applicazione
WS - security	Porta di dominio
HTTPS	SSL (end to end)
VPN	SPC trasporto

Fig. 20 – Livelli di sicurezza

La scelta delle protezioni rese disponibili dai diversi livelli sarà effettuata dal dominio di cooperazione in base alle necessità di sicurezza ed in funzione del valore legale richiesto per le registrazioni.

Per quanto concerne gli standard:

- le regole per la protezione del livello SPC trasporto sono state definite dal gruppo di lavoro e sono pubblicate sul sito www.cnipa.it;
- la protezione SSL fa riferimento agli standard correntemente implementati dai prodotti di mercato che garantiscono l'interoperabilità tra i web server;
- le regole della porta di dominio sono definite nel presente documento;
- le regole applicative saranno stabilite dai domini di cooperazione, eventualmente basandosi su linee guida emesse dal gruppo di lavoro sulla cooperazione applicativa.

9.3.Sicurezza delle porte di dominio

Nell'ambito dei servizi di cooperazione previsti e dei modelli architetturali proposti per i servizi di cooperazione applicativa risulta naturale far riferimento agli standard di sicurezza proposti per i WEB Services.

In quest'ambito gli standard che si propone di utilizzare sono quelli basati sulle specifiche WS-Security.

Ad oggi, le specifiche di WS-Security non hanno ancora raggiunto lo status di standard, ma rappresentano, comunque, l'infrastruttura unanimemente riconosciuta per la messa in sicurezza delle transazioni effettuate a mezzo delle architetture applicative distribuite.

I Web Services utilizzano i pacchetti SOAP basati su XML al fine di rendere possibile il collegamento tra applicazioni all'interno di una stessa organizzazione o tra organizzazioni diverse in modo indipendente da specifiche piattaforme e linguaggi di programmazione.

Questa architettura si focalizza su due requisiti ritenuti fondamentali per la sicurezza nell'ambito *Web Service*:

La garanzia del raggiungimento dei requisiti di Integrità e Segretezza dei messaggi da capo a capo (*end to end*), senza trascurare gli stessi criteri anche nel transito attraverso intermediari;

La certezza che l'elaborazione dei servizi svolta ai due capi del collegamento avvenga in maniera sicura, cioè in aderenza alle regole di sicurezza definite.

L'architettura definisce le specifiche da rispettare ad alto livello con il preciso obiettivo di creare dei paradigmi di sicurezza in grado di far cooperare tra loro tecnologie di sicurezza gia esistenti e consolidate, senza trascurare l'apporto derivante dalle pratiche emergenti.

L'architettura WS Security si divide in un totale di sei raccomandazioni, ognuna delle quali affronta un'esigenza di sicurezza specifica.

WS-Security supporta, integra ed unifica numerosi modelli di sicurezza (PKI, SSL e Kerberos) e tutti meccanismi e tecnologie ad essi associati. In particolare fornisce un set standard di estensioni da applicare al protocollo SOAP. Queste estensioni sono in sostanza degli *header* da applicare ai messaggi SOAP per incrementare gli aspetti di integrità e confidenzialità delle applicazioni Web Services.

WS-Security stabilisce inoltre dei meccanismi standard per scambiare messaggi tra applicazioni Web Services in modo sicuro e con la garanzia di non ripudio.

Nell'individuazione di una soluzione standard di sicurezza per i servizi di cooperazione applicativa, basati su tecnologia SOAP alcuni requisiti devono essere previsti. In particolare, la soluzione:

- si deve basare su standard internazionali e de facto;
- deve essere integrabile con tecniche di scambio messaggi SOAP;
- deve prevedere implementazioni fornite dai principali software e piattaforme applicative di sviluppo di servizi web;
- deve gestire in maniera integrata gli aspetti relativi all'autenticazione dei clienti del servizio, nonché all'integrità e alla confidenzialità dei messaggi;

La soluzione che risponde ai requisiti predetti e quella nota con il nome di WS-Security che, nata come UDDI da iniziative di produttori di software, è successivamente stata trasferita al consorzio OASIS che ne ha approvato il 19 Aprile 2004 la specifica 1.0, alla cui definizione hanno contribuito i principali fornitori di prodotti di sicurezza e di soluzioni applicative basate su "web services".

Obiettivo di WS-Security è quello di abilitare le applicazioni a costruire tecniche di scambio messaggi SOAP sicuri. Per questo motivo WS-Security si propone di supportare diversi meccanismi di sicurezza che possono essere utilizzati per realizzare gli obiettivi della specifica.

WS-Security aggiunge ai messaggi SOAP le seguenti caratteristiche di sicurezza: l'integrità e la confidenzialità dei messaggi, nonché l'autenticazione.

WS-Security supporta molteplici security token, differenti trust domain, diversi formati di firma e diverse tecnologie di cifratura.

La specifica prevede tre meccanismi di gestione dei messaggi SOAP sicuri:

- autenticazione (security token);
- integrità del messaggio;

- confidenzialità del messaggio.

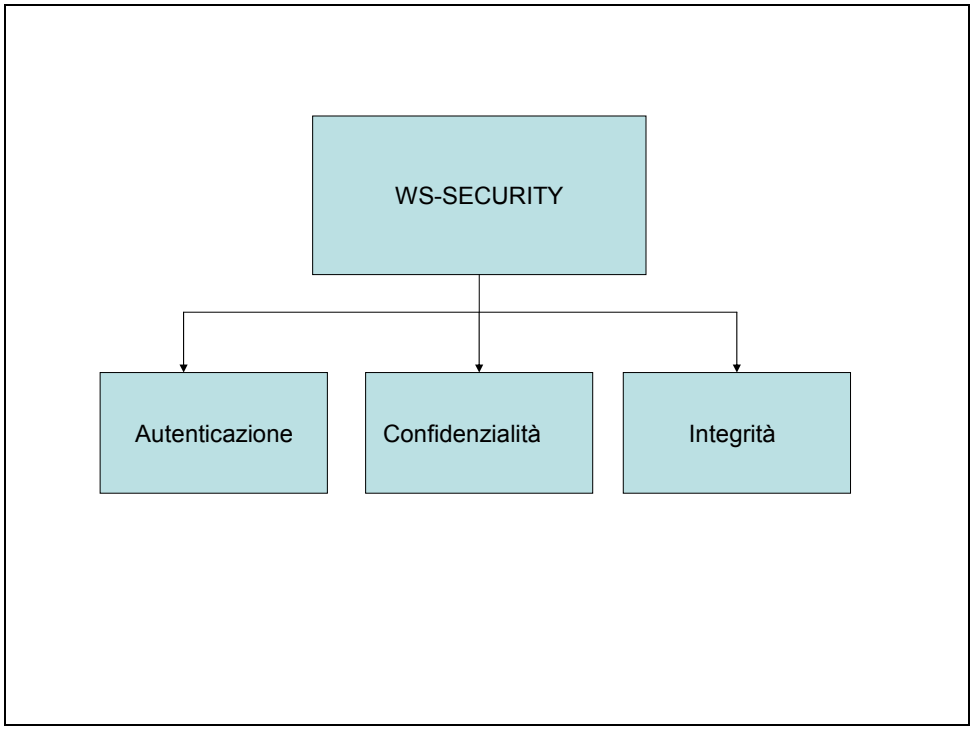


Fig. 21 – Meccanismi di gestione dei messaggi

Queste specifiche di per sé non definiscono una soluzione completa in termini di sicurezza. Piuttosto, i meccanismi che implementano WS-Security sono componenti che possono essere utilizzati in congiunzione con altre estensioni web e altri specifici protocolli per gestire una varietà di modelli di sicurezza.

Questi meccanismi inoltre possono essere utilizzati in maniera indipendente (ad esempio il passaggio di un security token per l'autenticazione) o in maniera integrata (firma e cifratura di un messaggio che contiene inoltre un security token)

La specifica prevede di utilizzare un blocco XML all'interno dell'header del messaggio SOAP per inserire informazioni relative alla sicurezza.

```
<soapenv:Header>
<wsse:Security
xmlns:wsse="http://schemas.xmlsoap.org/ws/2003/06/secext"
soapenv:mustUnderstand="1">
……..
</wsse:Security>
</soapenv:Header>
```

La sicurezza in WS-Security inoltre si basa sugli standard "XML digital segnature" per quanto riguarda gli aspetti relativi all'integrità, e sugli standard "XML encryption" per quanti riguarda gli aspetti di confidenzialità dei messaggi SOAP.

Le principali implementazioni software delle specifiche WS-Security presenti sul mercato ripropongono il modello architetturale esposto nella figura seguente. L' applicazione client e il servizio web gestiscono esclusivamente gli aspetti relativi al colloquio applicativo tramite messaggi SOAP, mentre specifici gestori della sicurezza si occupano della generazione delle informazioni di sicurezza da appendere al messaggio SOAP, della eventuale cifratura e decifratura dei messaggi, nonché della validazione delle credenziali.

Questo modello architetturale consente di separare in maniera netta le problematiche di logica applicativa e di colloquio, dagli aspetti inerenti alla sicurezza.

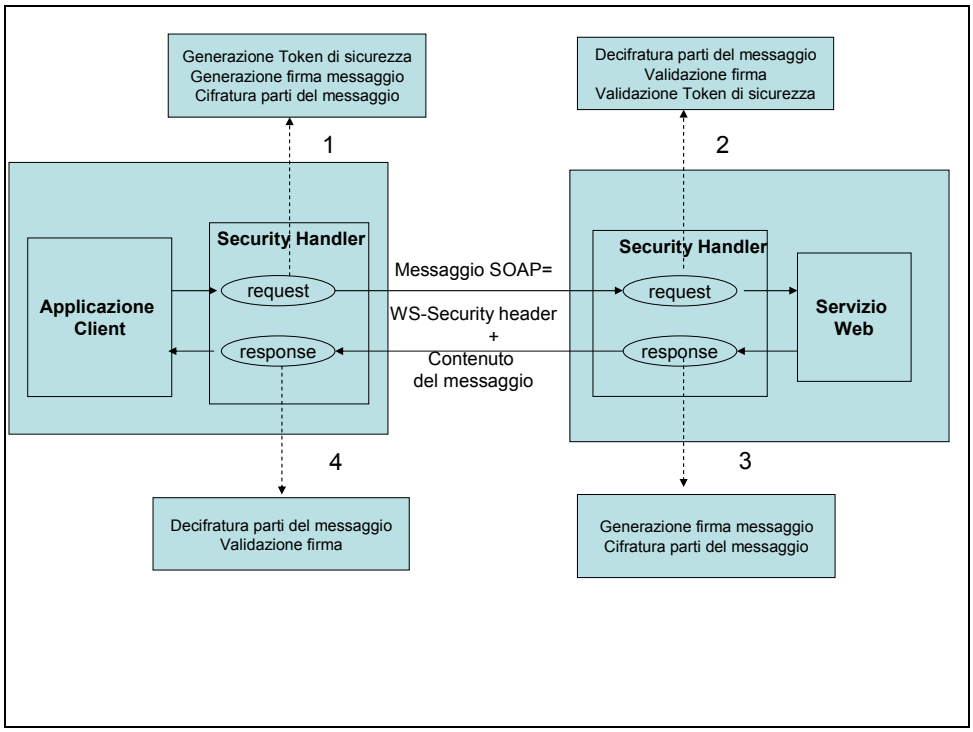


Fig. 22 – Modello architetturale delle specifiche WS-Securuty

9.3.1. *Autenticazione dei messaggi*

Le specifiche WS-Security prevedono che il processo di autenticazione avvenga attraverso la creazione di un contrassegno di sicurezza (*security token*) nel messaggio SOAP.

Il *security token* è inserito nel messaggio SOAP e contiene informazioni relative alle credenziali del client che richiede l'esecuzione del servizio web.

Attualmente le specifiche 1.0 di WS-Security prevedono le seguenti tipologie di security token:

Username Token Profile: che utilizza come credenziali per l'autenticazione una combinazione di userid e password;

X.509 Token Profile: che utilizza come credenziali per l'autenticazione un certificato digitale X.509

Il WS Technical Committee di OASIS sta inoltre lavorando per definire ulteriori security token e in particolare:

SAML token profile, che prevede l'utilizzo del protocollo SAML per l'autenticazione del client;

REL token profile, che specifica come utilizzare l'ISO/IEC 21000-5 Rights Expressions;

Kerberos token profile, che specifica come codificare ticket Kerberos all'interno di un messaggio SOAP.

Attualmente dunque i meccanismi da utilizzare sono quelli di Username Token profile e di x.509 Token profile.

Per quanto riguarda lo UserName Token profile, valgono le seguenti regole: viene inserito un elemento <wsse:UsernameToken> nel blocco <wsse:Security>, che serve per specificare la username del fruitore del servizio (client).

All'interno dell'elemento <wsse:UsernameToken> è possibile inserire un ulteriore elemento <wsse:Password> che contiene la password del client. La password può essere inviata all'interno del messaggio in un formato chiaro (wsse:PasswordText) oppure in un formato "digest" (wsse:PasswordDigest).

Esempio:

```
<wsse:UsernameToken wsu:Id="Example-1">
<wsse:Username> ... </wsse:Username>
<wsse:Password Type="..."> ... </wsse:Password>
<wsse:Nonce EncodingType="..."> ... </wsse:Nonce>
<wsu:Created> ... </wsu:Created>
</wsse:UsernameToken>
```

Per quanto riguarda invece il security token basato su X.509 le specifiche WS-Security prevedono che un elemento <wsse:SecurityTokenReference> all'interno dell'header <wsse:Security > venga utilizzato per referenziare la credenziale del client, che può essere rappresentata da:

- un subject Key Identifier (elemento <wsse:KeyIdentifier>);

- un binarySecurityToken, che rappresenta un certificato X.509 presente in binario all'interno di un elemento <wsse:BynarySecurityToken> nel messaggio soap, o su un data source remoto;
- un serial number che identifica il certificato attraverso l'emittente e il serial number.

Esempio:

```
<S11:Envelope xmlns:S11="...">
<S11:Header>
<wsse:Security xmlns:wsse="..." xmlns:wsu="...">
<wsse:BinarySecurityToken wsu:Id="binarytoken" ValueType="wsse:X509v3" EncodingType="wsse:Base64Binary">
MIIEZzCCA9CgAwIBAgIQEmtJZc0…
</wsse:BinarySecurityToken>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>…
<ds:Reference URI="#body">…</ds:Reference>
<ds:Reference URI="#binarytoken">…</ds:Reference>
</ds:SignedInfo> <ds:SignatureValue>HFLP…</ds:SignatureValue>
<ds:KeyInfo>
<wsse:SecurityTokenReference>
<wsse:Reference URI="#binarytoken" />
</wsse:SecurityTokenReference>
</ds:KeyInfo>
</ds:Signature>
</wsse:Security>
</S11:Header>
<S11:Body wsu:Id="body" xmlns:wsu="...">
…
</S11:Body>
</S11:Envelope>
```

9.3.2. Confidenzialità

Il modello proposto da WS-Security e' compatibile con modelli esistenti per l'autenticazione l'integrità e la confidenzialità dei dati. Infatti e' possibile integrare soluzioni basate sui web-services con altri modelli di sicurezza.

Ad esempio risulta naturale utilizzare la WS-security in congiunzione con la ***Sicurezza del trasporto***.

Tecnologie esistenti quali SSL e/o TLS sono assolutamente compatibili con Web Service che utilizzano WS-Security al fine di fornire integrità e crittografia *end-to-end*.

La cifratura viene realizzata attraverso le specifiche XML Encryption" e si applica alle seguenti parti del messaggio SOAP:

- il corpo del messaggio;
- blocchi di header.

Questa specifica permette in particolare di produrre una cifratura sia utilizzando una chiave simmetrica condivisa sia dal mittente che dal destinatario del messaggio SOAP, sia da una chiave simmetrica memorizzata in formato cifrato all'interno del messaggio SOAP.

Per garantire il massimo della flessibilità questa specifica si basa sugli standard XML Encryption.

La specifica infatti descrive come i seguenti tre elementi previsti dagli standard XML Encryption, possono essere utilizzati all'interno del blocco <wsse:Security> del messaggio SOAP.

L'elemento <xenc:ReferenceList> viene utilizzato per definire quali parti di dati (identificati da elementi <xenc:EncryptedData>) sono cifrati.

La specifica prevede inoltre che possano essere utilizzate più chiavi per cifrare un messaggio SOAP e di identificare la chiave con la quale la porzione di dati è stata cifrata (<xenc:EncryptedData>) utilizzando l'elemento <ds:KeyInfo>, come mostrato nell'esempio seguente.

Esempio:

```
<S11:Envelope xmlns:S11="..." xmlns:wsse="..." xmlns:wsu="..."
xmlns:ds="..." xmlns:xenc="...">
<S11:Header>
<wsse:Security>
<xenc:ReferenceList>
<xenc:DataReference URI="#bodyID"/>
</xenc:ReferenceList>
</wsse:Security>
</S11:Header>
<S11:Body>
<xenc:EncryptedData Id="bodyID">
<ds:KeyInfo>
<ds:KeyName>……</ds:KeyName>
</ds:KeyInfo>
<xenc:CipherData>
<xenc:CipherValue>...</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedData>
</S11:Body>
</S11:Envelope>
```

La specifica WS-Security prevede inoltre di utilizzare un elemento <xenc:EncryptedKey> per memorizzare la chiave simmetrica all'interno del messaggio SOAP.

```
<S11:Envelope xmlns:S11="..." xmlns:wsse="..." xmlns:wsu="..."
xmlns:ds="..." xmlns:xenc="...">
<S11:Header>
<wsse:Security>
<xenc:EncryptedKey>
...
<ds:KeyInfo>
<wsse:SecurityTokenReference>
<ds:X509IssuerSerial>
<ds:X509IssuerName>
……
</ds:X509IssuerName>
<ds:X509SerialNumber>12345678
</ds:X509SerialNumber>
</ds:X509IssuerSerial>
</wsse:SecurityTokenReference>
</ds:KeyInfo>
...
</xenc:EncryptedKey>
...
</wsse:Security>
</S11:Header>
<S11:Body>
<xenc:EncryptedData Id="bodyID">
<xenc:CipherData>
<xenc:CipherValue>...</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedData>
</S11:Body>
</S11:Envelope>
```

La cifratura di un messaggio SOAP prevede dunque i seguenti step:

- creazione di un <wsse:Security> header;
- creazione di un elemento <xenc:EncryptedKey> (in caso di utilizzo di chiave simmetrica), come sotto elemento di <wsse:Security>. L'elemento <xenc:EncryptedKey> conterrà a sua volta un sottoelemento <xenc:ReferenceList> che prevede un elemento<xenc:DataReference> per ogni elemento <xenc:EncryptedData> cifrato con quella chiave ;
- cifratura delle parti previste secondo le specifiche XML Encryption e rimpiazzare gli originali elementi con nuovi <xenc:EncryptedData>;
- creazione di un elemento <ds:KeyInfo> all'interno dell'elemento <xenc:EncryptedData>per referenziare una specifica chiave;

- creazione di un elemento<xenc:DataReference> che referenzia l'elemento <xenc:EncryptedData> generato. L'elemento <xenc:DataReference> va inserito come sottoelemento di <xenc:ReferenceList>.

9.3.3. Integrità

L'integrità assicura che i dati non siano stati manipolati in maniera accidentale o non autorizzata. "XML digital signature" è uno standard che definisce le regole per aggiungere ad un messaggio SOAP ulteriori informazioni che ne assicurano l'integrità. Le differenti parti che possono essere firmate sono:

- il corpo del messaggio SOAP;
- il security token;

La specifica permette di attaccare diverse firme e diversi formati di firma ad un messaggio e prevede di utilizzare gli stessi algoritmi di firma previsti dallo standard "XML Signature".

La firma va inserita all'interno dell'header block <wsse:security> utilizzando l'elemento <ds:Signature> che è conforme a quello specificato dallo standard "XML Signature".

Tutti gli elementi <ds:Reference> contenuti come sottoelementi di <ds:Signature> contengono il riferimento ad una parte del messaggio SOAP firmato.

Il seguente esempio illustra l'integrità in un messaggio SOAP nel corpo del messaggio.

```
<?xml version="1.0" encoding="utf-8"?>
<S11:Envelope xmlns:S11="..." xmlns:wsse="..." xmlns:wsu="..." xmlns:ds="...">
<S11:Header>
<wsse:Security>
<wsse:BinarySecurityToken ValueType="...#X509v3" EncodingType="...#Base64Binary" wsu:Id="X509Token">
MIIEZzCCA9CgAwIBAgIQEmtJZc0rqrKh5i...
</wsse:BinarySecurityToken>
<ds:Signature>
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<ds:Reference URI="#myBody">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>EULddytSo1...</ds:DigestValue>
</ds:Reference>
```

```
</ds:SignedInfo>
<ds:SignatureValue>
BL8jdfToEb1l/vXcMZNNjPOV...
</ds:SignatureValue>
<ds:KeyInfo>
<wsse:SecurityTokenReference>
<wsse:Reference URI="#X509Token"/>
</wsse:SecurityTokenReference>
</ds:KeyInfo>
</ds:Signature>
</wsse:Security>
</S11:Header>
<S11:Body wsu:Id="myBody">
<tru:StockSymbol xmlns:tru="http://www.fabrikam123.com/payloads">
QQQ
</tru:StockSymbol>
</S11:Body>
</S11:Envelope>
```

9.4.Tracciatura

Le funzioni di tracciatura consistono nella memorizzazione dei dati inerenti le operazioni che sono state eseguite presso le porte di dominio.

La tracciatura è un'operazione fondamentale per la sicurezza che ha i seguenti obiettivi:

a) consentire l'esame dell'attività svolta dalle singole porte di dominio al fine di individuare eventuali problemi prestazionali o di sicurezza;

b) ricostruire all'occorrenza le operazioni svolte da un processo cooperante per finalità diverse (trasparenza dei processi, messa a punto dei sistemi ed individuazione di eventuali colli di bottiglia, recupero di informazioni , attività investigative, ecc.);

c) conservare le informazioni in base a cui un dominio applicativo ha attivato un determinato procedimento amministrativo, al fine di utilizzarle in eventuali contenziosi.

Mentre l'obiettivo a) può essere raggiunto autonomamente dal gestore della porta di dominio, il raggiungimento degli obiettivi b) e c) presuppone un accordo tra i soggetti cooperanti. Si ritiene comunque che sia opportuno, anche nel primo caso, che l'operazione di tracciatura soddisfi regole

comuni, al fine di semplificare la gestione delle porte di dominio mediante l'uso di prodotti standard o il ricorso a servizi esterni.

In relazione ai requisiti espressi, non si ritiene necessario che le porte di dominio rendano disponibili *on line* le informazioni di tracciatura all'esterno. Al contrario, motivi di tutela della riservatezza delle informazioni fanno propendere per soluzioni in cui ciascuna porta di dominio gestisce e conserva autonomamente i dati di traccia che potranno essere forniti per indagini e correlazioni solo a seguito di eventi particolari e secondo procedure predefinite. Nel caso sussistano particolari requisiti di trasparenza dei procedimenti amministrativi, questi dovranno essere soddisfatti con soluzioni applicative, ad esempio memorizzando nelle banche dati delle amministrazioni le informazioni relative allo stato di avanzamento delle pratiche.

9.4.1. Tipologie di tracce

I record di traccia possono essere prodotti in modo automatico da diversi apparati e sistemi (router, firewall, sistemi operativi, web server, ecc.). I formati originali delle tracce prodotte da tali elementi variano in funzione della tipo di apparato, del produttore e delle opzioni che sono state scelte per l'attività di registrazione. Nel seguito del documento faremo riferimento a tali registrazione con la locuzione **tracce di sistema**.

Le tracce di sistema sono idonee per le attività di analisi locali (obiettivo a) ma non facilitano la condivisione delle informazioni registrate (obiettivi b, c).

Per gli obiettivi di cooperazione, ciascuna porta di dominio dovrà registrare delle ulteriori tracce secondo criteri comuni. Nel seguito del documento faremo riferimento a tali registrazioni con l'espressione **tracce applicative**.

9.4.2. Correlazione delle tracce applicative

Per raggiungere l'obiettivo b) è necessario che i record di traccia prodotti dalle diverse porte di dominio siano correlabili, ossia abbiano un formato noto e contengano informazioni che consentono di mettere in relazione le operazioni svolte da porte diverse.

Una conseguenza di tale requisito è l'esigenza di marcare le tracce con un tempo di rete ufficiale.

Ciascuna traccia applicativa dovrà inoltre contenere un insieme minimo di informazioni comuni. Si riporta di seguito un elenco di informazioni che si ritiene debbano essere contenute in ciascuna traccia applicativa:

- data
- ora
- identificativo della porta di dominio (id_porta)
- tipo di messaggio (invio, risposta, ack)
- *header* busta di e-government.

9.4.3. Compatibilità con il protocollo informatico

Le tracce applicative dovranno contenere le informazioni in base a cui un dominio applicativo ha attivato un determinato procedimento amministrativo (obiettivo c).

La finalità di queste tracce è simile a quella delle registrazioni di protocollo previste dal DPCM 31 ottobre 2000. Inoltre è presumibile che in molti casi la stessa funzione possa essere attivata in due diversi modi:

- da un operatore interno, a seguito di una richiesta trasmessa mediante documenti registrati dall'ufficio protocollo;
- attraverso un processo di cooperazione applicativa finalizzato a soddisfare una istanza veicolata da un'altra amministrazione.

Dal punto di vista organizzativo le due modalità sono equivalenti: in entrambi i casi l'amministrazione riceve una richiesta dall'esterno e deve mantenere traccia di tale richiesta, anche per risolvere eventuali contenziosi.

Questa considerazione suggerisce di rendere il più possibile uniformi, per contenuti e formati, le registrazioni del protocollo e le tracce applicative.

9.4.4. Caratteristiche delle tracce applicative

A seguito delle considerazioni espresse, si ritiene che la funzione di tracciatura a carico della porta di dominio debba generare una traccia applicativa per ogni messaggio SOAP ricevuto o inviato.

Ciascuna traccia avrà un formato XML compatibile con le registrazioni di protocollo (il formato di tali registrazioni è specificato dalla Circolare Aipa n. 28 del 7 maggio 2001).

Per la generazione delle tracce applicative potranno essere utilizzate sia informazioni presenti nelle tracce di sistema, sia le informazioni presenti nella busta di e-government (in particolare l'header della busta).

Le tracce applicative generate dalle porte di dominio non conterranno informazioni relative ai contenuti del messaggio (*body* della busta di *e-government*).

9.5. Criteri per la sicurezza dei servizi

In questo capitolo vengono riportati alcuni criteri per la realizzazione di funzioni di sicurezza tipiche dei domini dei servizi.

In generale ciascuna organizzazione sarà autonoma nella scelta delle modalità di realizzazione dei servizi resi disponibili dal proprio dominio, dunque potrà scegliere autonomamente le tecniche per implementare le misure di sicurezza necessarie a questo livello.

Tuttavia è consigliabile seguire criteri comuni, in moda da rendere il più possibile omogenei i trattamenti delle applicazioni distribuite con l'obiettivo da semplificarne il disegno e favorire l'uso di prodotti commerciali.

Inoltre le informazioni prodotte da alcune misure di sicurezza informazioni, come ad esempio le prove non ripudiabili, devono avere valore anche al di fuori del dominio dei servizi e dunque, per essere efficaci, devono rispettare standard comuni.

In questo capitolo vengono delineati i criteri "base" lasciando agli specifici gruppi di lavoro il compito di definire i formati e le tassonomie.

9.5.1. *Autorizzazione*

In un processo cooperativo assumono particolare rilevanza le problematiche di Identificazione, Autenticazione e Autorizzazione, in quanto il processo stesso è per sua natura distribuito fra sistemi informativi organizzati in piena autonomia dai singoli Enti che li gestiscono.

In tale quadro risulta fondamentale definire i confini di responsabilità di ciascun Ente coinvolto nel processo, al fine di evitare sia la ridondanza nei controlli sia il rischio di parziale assenza di questi.

Relativamente alla Identificazione e Autenticazione dell'utente, ovvero il meccanismo volto ad individuare con certezza la sua identità, è auspicabile che avvenga una sola volta, a carico dell'Ente che innesca il processo. In questo modo l'utente comunica al sistema la sua identità al sistema che tramite password, certificato, impronte isometriche ,etc lo autentica.

Tale fase, essendo volta solo ad individuare l'identità dell'utente, non richiede in linea di principio la conoscenza di particolari informazioni sull'utente stesso e può quindi essere svolta da uno qualsiasi dei sistemi coinvolti nel processo cooperativo, passando poi tale informazione agli altri.

Diversamente, per la fase di autorizzazione dove si accerta *cosa* l'utente è abilitato a fare, risulta complesso, ma soprattutto lesivo della autonomia dei diversi Enti cooperanti, delegare ad altri tali controlli.

Appare evidente che ciascun dominio applicativo deve avere la piena autonomia di concedere o revocare autorizzazioni in qualsiasi momento sulle funzioni che eroga. Autorizzazione che per la natura stessa delle funzioni erogate possono richiedere la conoscenza di informazioni di tale livello di dettaglio che risulta ingestibile centralizzare o distribuire ad altri. Ad esempio non è sufficiente essere un medico per esaminare un referto di un paziente, deve essere il medico curante (o un medico di proto soccorso per le emergenze), ed inoltre il paziente ha la facoltà di negare l'accesso anche ad singolo referto.

Il processo di Autorizzazione richiede quindi informazioni che possono essere gestite solo da ciascun dominio per le funzioni di sua competenza, mentre non esistono ragionevoli vincoli nel delegare ad altri le fasi di identificazione e l'autorizzazione.

Si delinea quindi un quadro in cui l'utente che richiede la fruizione di un servizio erogato in modalità cooperativa da enti appartenenti a domini applicativi diversi, si Identifica e viene Autenticato dal dominio del sistema di Front-End, che svolge anche le verifiche di Autorizzazione per la quota parte del processo di sua pertinenza. Le informazioni sull'identità dell'utente vengono poi trasmesse agli altri domini coinvolti, che non dovranno quindi più verificarle, ma dovranno controllare solo le Autorizzazioni a svolgere le funzioni richieste.

Tale processo è del tutto generale e si applica sia nel caso, appena descritto, di utente individuabile come persona fisica, sia di utente individuabile come figura logica impersonificata da un sistema o applicazione.

Da quanto affermato deriva che la fase di Autorizzazione rimane un aspetto interno al singolo dominio, mentre resta di pertinenza del processo cooperativo la trasmissione di credenziali dell'utente.

Tale aspetto pur essendo affrontato nell'ambito di diverse specifiche tecniche, come SAML, non ha ancora ad oggi prodotto uno standard condiviso e consolidato.

Si ritiene quindi che, pur rimanendo valido il quadro generale sopra delineato per la soluzione a regime, non sussistano al momento elementi sufficientemente consolidati per normare nell' ambito del SPC questo aspetto.

9.5.2. *Non ripudio*

Il termine "non ripudio" comunemente viene associato a funzioni applicative che consistono nella generazione di prove informatiche aventi caratteristiche tali da non poter essere ripudiate.

L'esempio più noto di questo tipo di applicazione è la firma digitale che nell'Unione europea è legalmente equivalente alla sottoscrizione autografa[13]. Questo tipo di prova attesta la validazione di un documento informatico da parte del soggetto firmatario.

9.5.2.1. Firma digitale

Le prove generate mediante firma digitale possono essere utilizzate dai domini dei servizi in molti casi pratici. La firma digitale può essere emessa dall'utente che ha originato il processo (ad esempio un cittadino che firma una istanza) oppure da soggetti che vi partecipano (ad esempio un funzionario che valida un determinato atto) e può essere trasmessa tra domini diversi secondo le regole del procedimento amministrativo. Ciascun dominio potrà verificare l'integrità del documento firmato, nonché la presenza e la validità delle necessarie sottoscrizioni, inoltre potrà memorizzare il documento per esibirlo all'occorrenza nel caso di contenziosi.

Per quanto concerne le regole e gli standard della firma digitale, occorre fare riferimento alla normativa corrente (DPR 29 dicembre 200 n.445 come modificato dal Decreto legislativo 29 gennaio 2002 n.10 e dal DPR 7 aprile 2003 n. 137, DPCM 13 gennaio 2004).

Con riferimento ai formati, si osserva che benché sia disponibile uno standard di firma adatto ai messaggi XML (XML signature) è opportuno effettuare delle scelte che facilitino l'utilizzo e la verifica della firma digitale anche al di fuori dei processi di cooperazione applicativa. In conseguenza di tale considerazione, è opportuno attenersi alle regole per l'interoperabilità tra i certificatori stabilite dalla circolare 19 giugno 2000 n. AIPA/CR/24 (G.U. 30 giugno 2000, Serie generale n. 151)[14].

I documenti firmati, eventualmente costituiti da tracciati XML, dovranno perciò essere completati con le informazioni previste dal formato RFC 2315 (PKCS#7).

[13] La locuzione "firma digitale" è ovviamente utilizzata solo in Italia. Nel contesto europeo il termine firma digitale corrisponde all'espressione "advanced electronic signature based on a qualified certificate and created by a secure-signature-creation device".

[14] L'uso dello standard XML Signature non è in contrasto con la normativa sulla firma digitale, per cui un documento conforme a tale standard può avere valore legale (perché vengano seguite le regole di carattere generale prescritte dalle norme). Tuttavia, per avere una utilità pratica, la firma digitale deve poter essere verificata in modo semplice da chiunque, dunque è opportuno che segua i formati definiti dalla citata circolare, pienamente supportati dai prodotti distribuiti dai certificatori italiani iscritti nell'elenco pubblico.

Tali informazioni, costituenti la busta PKCS#7, possono essere contenute all'interno del messaggio (*body* della busta di e-government), purché le informazioni di firma vengano codificate in formato BASE64 (RFC 3548).

Si ricorda che la firma digitale è l'equivalente informatico della firma autografa e dunque:

- può essere emessa solo da persone fisiche,
- deve avvenire sotto il pieno controllo del firmatario.

Queste condizioni escludono l'uso della firma digitale nei casi in cui è necessario che la prova venga generata da un sistema elaborativo.

9.5.2.2. Altre firme elettroniche

La firma digitale non è il solo modo con cui si possono generare prove valide ai fini legali, infatti l'articolo 10 del DPR 29 dicembre 200 n.445, modificato dall'articolo 6 del Decreto legislativo 29 gennaio 2002 n.10, al comma 2 recita: *Il documento informatico, sottoscritto con firma elettronica, soddisfa il requisito legale della forma scritta. Sul piano probatorio il documento stesso è liberamente valutabile, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza.*

E' possibile dunque generare prove "non ripudiabili" anche con strumenti diversi dalla firma digitale[15]. Questa possibilità è di particolare interesse per la cooperazione applicativa in quanto un'amministrazione può avere la necessità di conservare tracce non ripudiabili delle richieste provenienti da altre amministrazioni, laddove le richieste non sono imputabili ad un determinato soggetto ma ad un processo.

In questo caso la firma elettronica non ha il compito di attestare l'approvazione del contenuto di un documento da parte di un soggetto (come la firma digitale), quanto di dimostrare la provenienza di una richiesta.

Risulta dunque evidente che la firma elettronica finalizzata al non ripudio delle tracce e la firma XML per l'autenticazione dei messaggi possono coincidere, se si decide di conservare come tracce delle richieste pervenute, anche ai fini della gestione di eventuali contenziosi, i messaggi SOAP firmati dalla porta di dominio. In questo caso lo standard di riferimento è "XML signature", è inoltre necessario che il processo di firma avvenga in condizioni tali da assicurare le *caratteristiche oggettive di qualità e sicurezza* richieste dalla normativa. Per raggiungere tale obiettivo è opportuno che i certificati elettronici necessari per la certificazione delle chiavi siano emessi da Certificatori iscritti nell'elenco pubblico di cui all'articolo 5, comma 4 del Decreto legislativo 29 gennaio 2002, n.10 (Certificatori accreditati).

Ciascun dominio di cooperazione potrà determinare in autonomia le tipologie di firma che dovranno essere apposte ai fini del "non ripudio". Si sottolinea comunque che gli accordi di dominio possono prevedere il mutuo il riconoscimento delle tracce generate dalle applicazioni anche in assenza di funzioni di firma elettronica. Nel caso di utilizzo di funzioni di firma elettronica è opportuno utilizzare i servizi di certificazione erogati da Certificatori accreditati, in modo da garantire i necessari livelli di sicurezza e l'interoperabilità delle protezioni.

[15] Si ricorda che la firma digitale è una tipologia avanzata di firma elettronica, emessa con un dispositivo sicuro sulla base di un certificato qualificato (per le definizioni cfr. la direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999).

9.6. Profilo dei certificati

Alcune misure previste pel la sicurezza delle porte di dominio e per quelle dei servizi prevedono l'uso di certificati elettronici conformi allo standard X.509 V3.

Lo standard fissa solo alcuni degli elementi del certificato e non definisce il contenuto e la semantica dei diversi campi. Per garantire l'interoperabilità tra le protezioni che fanno uso di certificati è necessario fissare nel dettaglio i valori ed il significato dei campi definendo profili standard.

Tutti i certificati dovranno comunque essere conformi alla specifica RFC 3280, capitolo 4, recanti "Profilo dei certificati e delle liste di revoca dei certificati nell'Infrastruttura a chiave pubblica".

Il profilo dei certificati utilizzati per la firma digitale è definito dalla citata circolare 19 giugno 2000 n. AIPA/CR/24.

9.7. Stato dei certificati

Le protezioni che si avvalgono di certificati digitali devono essere in grado di verificarne lo stato, al fine di evitare l'utilizzo di chiavi crittografiche compromesse o per le quali vi è il sospetto che ne sia pregiudicata la sicurezza. Questo requisito viene in genere assolto inserendo i certificati relativi alle chiavi potenzialmente compromesse in opportune liste di revoca (CRL).

Nello scenario della cooperazione applicativa l'utilizzo delle liste di revoca non è consigliabile per il fatto che i web server oggi disponibili sul mercato non sono in grado di gestire efficacemente un numero di liste di revoca superiore a poche unità.

E' invece preferibile utilizzare sistemi che presentano un'unica interfaccia per l'interrogazione dello stato dei certificati e sono in grado di gestire un numero elevato di elenchi relativi allo stato dei medesimi.

Tali sistemi dovranno essere conformi al protocollo *Online Certificate Status Protocol* (OCSP), definito nello standard IETF RFC 2560.

In base a tale standard, ciascuna autorità di certificazione dovrà rendere disponibile un sistema in grado di fornire informazioni sullo stato dei certificati (OCSP *Responders*) che dovrà essere accessibile da sistemi di terze parti che forniscono il servizio OCSP.

APPENDICE

A1 ESEMPI DI UTILIZZO DEI REGISTRI

A1.1 AUTENTICAZIONE DEL CLIENT PER LA PUBBLICAZIONE DI UN DOCUMENTO

Prima di pubblicare qualsiasi servizio, il client deve prima autenticarsi fornendo al registro UDDI (il server) le proprie credenziali. Nell'esempio di seguito riportato ciò avviene mediante "userid" e "password" e viene effettuato attraverso la richiesta (API) "get_authToken" ed il relativo messaggio di risposta "authToken", che deve essere utilizzato per le successive richieste di pubblicazione. Al termine della interazione con il server, il client, invoca l'API discard_authToken richiedendo al server di cancellare il token di autorizzazione.

```
Request Body:
<get_authToken generic="2.0" userID="user1" cred="*****" xmlns="urn:uddi-org:api_v2" />

Response Body:
<authToken generic="2.0" operator="…." xmlns="urn:uddi-org:api_v2">
<authInfo>857629405456</authInfo>
</authToken>

Request Body:
<discard_authToken generic="2.0 xmlns="urn:uddi-org:api_v2" />
            <authInfo/>
</discard_authToken>
```

A1.2 PUBBLICAZIONE DI UN DOCUMENTO WSDL IN UN REGISTRO UDDI

L'esempio seguente riprende le specifiche Oasis per l'utilizzo di WSDL all'interno di un modello UDDI [WSDL-UDDI 1.07, WSDL-UDDI 1.08 e WSDL-UDDI 2.0] contestualizzandole nell'ambito della cooperazione applicativa.

Seguendo le specifiche[16] è possibile ottenere una descrizione dei servizi composta da una parte "riusabile" ed una "ad hoc", specifica per una determinata istanza del servizio.

In particolare, le informazioni relative al formato dei messages, portTypes e protocolBindings saranno comprese nella parte "riusabile" mentre l'informazione sul particolare "service endpoint" sarà compresa

[16] E' opportuno tener presente che ad oggi, la specifica WS-I Basic Profile [WS-I Basic Profile 1.0] prevede (Requisito R3010) che la pubblicazione del servizio venga effettuata secondo le linee guida OASIS UDDI Best Practice for Using WSDL in a UDDI Registry nella versione 1.08 (Novembre 2002)[WSDL-UDDI 1.08].

nella parte che descrive l'implementazione dello specifico servizio. Il WSDL che sarà pubblicato nel registro UDDI conterrà soltanto la parte detta "riusabile".

Il service endpoint sarà invece contenuto nel bindingTemplate dello specifico businessService.

Il seguente WSDL, che rispetta i principi sopra descritti, descrive il servizio di Protocollo Informatico attraverso porte di dominio.

```
<?xml version="1.0" encoding="UTF-8"?>
<definitions
    name="Protocollo"
    targetNamespace="http://localhost/schemas/Protocollo/Protocollo.wsdl"
    xmlns="http://schemas.xmlsoap.org/wsdl/"
    xmlns:addinf="http://localhost/schemas/Protocollo/AddProtInfo.xsd"
    xmlns:busta="http://localhost/schemas/BustaEgov/BustaEgov.xsd"
    xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/"
    xmlns:segn="http://localhost/schemas/Protocollo/Segnatura.xsd"
    xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
    xmlns:tns="http://localhost/schemas/Protocollo/Protocollo.wsdl"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <types>
        <schema
            targetNamespace="http://localhost/schemas/Protocollo/Segnatura.xsd"
            xmlns="http://www.w3.org/2001/XMLSchema">
            <import
                namespace="http://localhost/schemas/Protocollo/Segnatura.xsd"
                schemaLocation="http://localhost/schemas/Protocollo/Segnatura.xsd"/>
        </schema>
        <schema
            targetNamespace="http://localhost/schemas/Protocollo/AddProtInfo.xsd"
            xmlns="http://www.w3.org/2001/XMLSchema">
            <import
                namespace="http://localhost/schemas/Protocollo/AddProtInfo.xsd"
              schemaLocation="http://localhost/schemas/Protocollo/AddProtInfo.xsd"/>
        </schema>
        <schema
            targetNamespace="http://localhost/schemas/BustaEgov/BustaEgov.xsd"
            xmlns="http://www.w3.org/2001/XMLSchema">
            <import
                namespace="http://localhost/schemas/BustaEgov/BustaEgov.xsd"
                schemaLocation="http://localhost/schemas/BustaEgov/BustaEgov.xsd"/>
        </schema>
    </types>
    <message name="RichiestaRegistrazione">
        <part element="segn:Segnatura" name="arg1"/>
        <part element="busta:Descrizione" name="descr"/>
        <part element="addinf:AdditionalProtInfo" name="arg"/>
    </message>
    <message name="IntestazioneBusta">
        <part element="busta:Intestazione" name="arg1"/>
    </message>
    <message name="DescrizioneBusta">
        <part element="busta:Descrizione" name="descr"/>
    </message>
    <message name="RispostaRegistrazione">
        <part element="segn:Identificatore" name="arg2"/>
        <part element="busta:Descrizione" name="descr"/>
    </message>
    <portType name="ProtocolloPortType">
        <operation name="Registrazione">
            <input message="tns:RichiestaRegistrazione"/>
            <output message="tns:RispostaRegistrazione"/>
        </operation>
    </portType>
    <binding name="ProtocolloSoapBinding" type="tns:ProtocolloPortType">
        <documentation>Binding Soap alle funzioni di Registrazione protocollo</documentation>
        <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
```

```
        <operation name="Registrazione">
            <soap:operation
                soapAction="capeconnect:Protocollo:ProtocolloPortType#Registrazione"/>
            <input>
                <soap:body encodingStyle="" parts="descr" use="literal"/>
                <mime:multipartRelated>
                    <mime:part>
                        <mime:content part="arg"/>
                    </mime:part>
                    <mime:part>
                        <mime:content part="arg1"/>
                    </mime:part>
                </mime:multipartRelated>
                <soap:header
                    encodingStyle=""
                    message="tns:IntestazioneBusta"
                    part="arg1"
                    use="literal"> </soap:header>
            </input>
            <output>
                <mime:multipartRelated>
                    <mime:part>
                        <soap:body parts="descr" use="literal"/>
                    </mime:part>
                    <mime:part>
                        <mime:content part="arg2"/>
                    </mime:part>
                </mime:multipartRelated>
                <soap:header message="tns:IntestazioneBusta" part="arg1" use="literal">
                </soap:header>
            </output>
        </operation>
    </binding>
</definitions>
```

Esempio di WSDL da utilizzare in UDDI

Il PortType mapperà in un tModel come mostrato nel seguito. Si noti il richiamo del wsdl come overviewURL

```
<tModel tModelKey="uuid:e8cf1163-8234-4b35-865f-94a7322e40c3" >
    <name>
         ProtocolloPortType
    </name>
    <overviewDoc>
         <overviewURL>
            http://localhost/schemas/Protocollo/Protocollo.wsdl
         <overviewURL>
    <overviewDoc>
    <categoryBag>
         <keyedReference
             tModelKey="uuid:d01987d1-ab2e-3013-9be2-2a66eb99d824"
          keyName="portType namespace"
             keyValue="http://localhost/schemas/Protocollo/" />
         <keyedReference
             tModelKey="uuid:6e090afa-33e5-36eb-81b7-1ca18373f457"
         keyName="WSDL type"
             keyValue="portType" />
    </categoryBag>
</tModel>
```

Esempio di mapping di WSDL port type in UDDI

A sua volta il SOAP binding ProtocolloSoapBinding del wsdl mapperà in un'altro tModel come quello di seguito descritto

```
<tModel tModelKey="uuid:49662926-f4a5-4ba5-b8d0-32ab388dadda">
    <name>
         ProtocolloSoapBinding
    </name>
    <overviewDoc>
         <overviewURL>
            http://localhost/schemas/Protocollo/Protocollo.wsdl
         </overviewURL>
    </overviewDoc>
    <categoryBag>
         <keyedReference
             tModelKey="uuid:d01987d1-ab2e-3013-9be2-2a66eb99d824"
          keyName="binding namespace"
             keyValue=" http://localhost/schemas/Protocollo/"/>
         <keyedReference
             tModelKey="uuid:6e090afa-33e5-36eb-81b7-1ca18373f457"
          keyName="WSDL type"
             keyValue="binding" />
         <keyedReference
             tModelKey="uuid:082b0851-25d8-303c-b332-f24a6d53e38e"
          keyName="portType reference"
             keyValue="uuid:e8cf1163-8234-4b35-865f-94a7322e40c3" />
         <keyedReference
             tModelKey="uuid:4dc74177-7806-34d9-aecd-33c57dc3a865"
          keyName="SOAP protocol"
             keyValue= "uuid:aa254698-93de-3870-8df3-a5c075d64a0e" />
         <keyedReference
             tModelKey="uuid:e5c43936-86e4-37bf-8196-1d04b35c0099"
          keyName="HTTP transport"
             keyValue=" uuid:68DE9E80-AD09-469D-8A37-088422BFBC36" />
         <keyedReference
             tModelKey="uuid:c1acf26d-9672-4404-9d70-39b756e62ab4"
          keyName="uddi-org:types"
             keyValue="wsdlSpec" />
    </categoryBag>
</tModel>
```

Riferimento al portType

Esempio di mapping di un WSDL Binding in UDDI

Infine il dettaglio del servizio (accessPoint) sarà riportato in un bindingTemplate come nell'esempio di seguito riportato

```
<businessService
        serviceKey="102b114a-52e0-4af4-a292-02700da543d4"
        businessKey="1e65ea29-4e0f-4807-8098-d352d7b10368">
    <name>Protocollo Service</name>
    <bindingTemplates>
        <bindingTemplate
                bindingKey="f793c521-0daf-434c-8700-0e32da232e74"
                serviceKey="102b114a-52e0-4af4-a292-02700da543d4">
            <accessPoint URLType="http">
               http://localhost/protocollo
            </accessPoint>
            <tModelInstanceDetails>
                <tModelInstanceInfo
                     tModelKey="uuid:49662926-f4a5-4ba5-b8d0-32ab388dadda">
                     <description xml:lang="it">
                         Il ProtocolloSoapBinding implementato.
                         il tag instanceParms specifica il nome locale della porta.
                     </description>
                     <instanceDetails>
                         <instanceParms>ProtocolloPort</instanceParms>
                     </instanceDetails>
                </tModelInstanceInfo>
                <tModelInstanceInfo
                     tModelKey="uuid:e8cf1163-8234-4b35-865f-94a7322e40c3">
                     <description xml:lang="it">
                         Il ProtocolloPortType implementato.
                     </description>
                </tModelInstanceInfo>
            </tModelInstanceDetails>
        </bindingTemplate>
    </bindingTemplates>
    <categoryBag>
    <keyedReference
                tModelKey="uuid:6e090afa-33e5-36eb-81b7-1ca18373f457"
           keyName="WSDL type"
                keyValue="service" />
    <keyedReference
                tModelKey="uuid:d01987d1-ab2e-3013-9be2-2a66eb99d824"
           keyName="service namespace"
                keyValue=" http://localhost/schemas/Protocollo/" />
    <keyedReference
                tModelKey="uuid:2ec65201-9109-3919-9bec-c9dbefcaccf6"
           keyName="service local name"
                keyValue="ServizioProtocollo" />
</categoryBag>
</businessService>
```

Riferimento al soapBinding

Riferimento al portType

Esempio di Binding Template in un registro UDDI

A1.3 TMODEL CON RIFERIMENTI A DOCUMENTI HTML

Di seguito è riportato un breve esempio di tModel in cui compare anche l'elemento overviewDoc:

```
<tModel tModelKey="uuid:…….">
  <name>xyz:Tutorial</name>
  <description xml:lang="it"> Servizio xyz - Specifiche di utilizzo</description>
  <overviewDoc>
    <description xml:lang="it">
      Tutorial del servizio xyz.
    </description>
    <overviewURL>
```

```
      http://<ip addr>/xyz/tutorial/index.htm
    </overviewURL>
  </overviewDoc>
  ……..
```

Esempio di tModel con la struttura overviewDoc

A2 LE STRUTTURE DATI DEL MODELLO UDDI

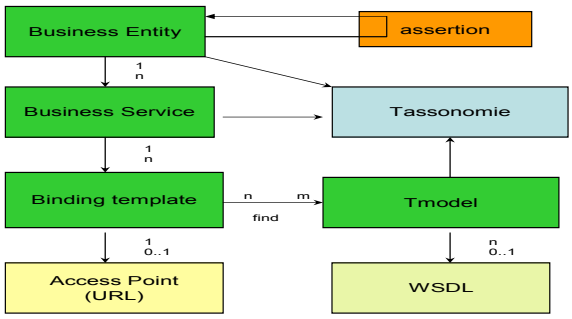


Fig.A1. Il Modello UDDI

Viene di seguito riportata la descrizione di dettaglio delle strutture dati relative alle entità del modello UDDI.

A2.1 L'ENTITÀ BUSINESSENTITY

Come già premesso, una struttura di tipo "businessEntity" rappresenta informazioni relative ad una attività o ad una organizzazione ed ai servizi che questa offre.

La struttura XML dell'entità è la seguente:

```
<element name="businessEntity" type="uddi:businessEntity" />
<complexType name="businessEntity">
<sequence>
<element ref="uddi:discoveryURLs" minOccurs="0" />
<element ref="uddi:name" maxOccurs="unbounded" />
<element ref="uddi:description" minOccurs="0" maxOccurs="unbounded" />
<element ref="uddi:contacts" minOccurs="0" />
<element ref="uddi:businessServices" minOccurs="0" />
<element ref="uddi:identifierBag" minOccurs="0" />
<element ref="uddi:categoryBag" minOccurs="0" />
</sequence>
<attribute name="businessKey" type="uddi:businessKey" use="required" />
<attribute name="operator" type="string" use="optional" />
<attribute name="authorizedName" type="string" use="optional" />
</complexType>
```

Struttura XML dell'entità businessEntity

La descrizione degli attributi è riportata in tabella A1

Attributo	Descrizione	Tipo dato	lunghezza
businessKey	Rappresenta l'identificativo univoco di una Business Entity.	UUID	41
authorizedName	Rappresenta il nome della persona che ha pubblicato i dati.	string	255
Operator	E' il nome certificate dell'operatore del registro UDDI.	String	255
discoveryURLs	(Elemento opzionale) Rappresenta una lista di URL che puntano alla struttura della singola Business Entity.	structure	
Name	(Elemento opzionale) Tanti elementi ripetibili quante sono le lingue con le quali esprimere il nome da assegnare ad una Business Entity.	string	255
description	(Elemento Opzionale) Contiene la descrizione della Business Entity. Come per l'attributo name è consentito una descrizione per lingua.	string	255
Contacts	(Elemento Opzionale) Contiene una lista di contatti.	structure	
businessServices	(Elemento opzionale). Contiene una lista di descrizione di servizi.	structure	
identifierBag	(Elemento opzionale). Contiene una lista di coppie chiave-valore utilizzate per identificare un Business Entity. Esempio: (D-U-N-S_ numbers, codice fiscale, etc).	structure	
categoryBag	(Elemento opzionale). Contiene una lista di coppie chiave-valore utilizzate per identificare la/e categoria/e di appartenenza del Business Entity.	structure	

Tabella A1 Gli attributi dell'entità businessEntity

A2.2 L'ENTITÀ BUSINESSSERVICE

La struttura businessService rappresenta una classificazione logica di servizi. Ogni businessService è figlio di una struttura businessEntity. Il legame tra le due strutture avviene attraverso l'attributo businessKey. Ogni businessService contiene informazioni descrittive di un servizio.

La struttura XML dell'entità è la seguente:

```
<element name="businessService" type="uddi:businessService" />
<complexType name="businessService">
<sequence>
<element ref="uddi:name" minOccurs="0" maxOccurs="unbounded" />
<element ref="uddi:description" minOccurs="0" maxOccurs="unbounded" />
<element ref="uddi:bindingTemplates" minOccurs="0" />
<element ref="uddi:categoryBag" minOccurs="0" />
</sequence>
```

```
<attribute name="serviceKey" type="uddi:serviceKey" use="required" />
<attribute name="businessKey" type="uddi:businessKey" use="optional" />
</complexType>
```

Struttura XML dell'entità businessService

La descrizione degli attributi è riportata in tabella A2

Attributo	Descrizione	Tipo dato	lunghezza
businessKey	Questo attributo è opzionale e contiene il universal unique identifier del Business Entity associate al servizio	UUID	41
serviceKey	Rappresenta la chiave per un determinato Business Service.	UUID	41
Name	(Elemento opzionale) Tanti elementi ripetibili quante sono le lingue con le quali esprimere il nome da assegnare ad un Business Service.	string	255
description	(Elemento Opzionale) Contiene la descrizione del Business Service. Come per l'attributo name è consentito una descrizione per lingua.	string	255
bindingTemplates	Questa struttura gestisce la descrizione tecnica dei servizi associate ad una famiglia di business service.	structure	
categoryBag	(Elemento opzionale). Contiene una lista di coppie chiave-valore utilizzate per identificare la/e categoria/e di appartenenza del Business Service.	structure	

Tabella A2 Gli attributi dell'entità businessService

A2.3 L'ENTITÀ BINDINGTEMPLATE

La struttura bindingTemplate fornisce informazioni per determinare un entry point di un servizio. Ogni bindingTemplate è parente di un businessService, il cui legame è determinato dall'attributo serviceKey.

La struttura XML dell'entità è la seguente:

```
<element name="bindingTemplate" type="uddi:bindingTemplate" />
<complexType name="bindingTemplate">
<sequence>
<element ref="uddi:description" minOccurs="0" maxOccurs="unbounded" />
<choice>
<element ref="uddi:accessPoint" />
<element ref="uddi:hostingRedirector" />
</choice>
<element ref="uddi:tModelInstanceDetails" />
</sequence>
<attribute name="serviceKey" type="uddi:serviceKey" use="optional" />
```

```
<attribute name="bindingKey" type="uddi:bindingKey" use="required" />
</complexType>
```

Struttura XML dell'entità bindingTemplate

La descrizione degli attributi è riportata in tabella A3

Attributo	Descrizione	Tipo dato	lunghezza
bindingKey	Rappresenta la chiave unica per identificare un Binding Template	UUID	41
serviceKey	Questo attributo è opzionale e contiene il universal unique identifier del Business Service	UUID	41
description	(Elemento Opzionale) Contiene la descrizione tecnica del servizio. E' consentito una descrizione per lingua.	string	255
accessPoint	Questo elemento identifica l'indirizzo per potere chiamare un particolare servizio Questo può essere un URL, un indirizzo e-mail, oppure un numero di telefono.	string	255
tModelInstanceDetails	Contiene una lista di elementi tModel associate a un Binding template.	structure	

Tabella A3 Gli attributi dell'entità bindingTemplate

A2.4 L'ENTITÀ TMODEL

Per essere in grado di descrivere un servizio web UDDI deve mantenere una struttura che contenga una descrizione comprensibile del servizio stesso per chi effettua una ricerca sul registro. Un altro requisito è quello di fornire delle informazioni relative al servizio che siano sufficienti per potere interagire con esso.

L'insieme delle informazioni contenute all'interno delle strutture tModel, cosiddette metadata, aggiungono un dettaglio tecnico rispetto a quelle descritte nella struttura bindingTemplate. Le informazioni gestite da un tModel sono le seguenti: una chiave, un nome, una descrizione opzionale e un URL che punta alla descrizione tecnica del servizio (ad esempio un WSDL).

La struttura XML dell'entità è la seguente:

```
<element name="tModel" type="uddi:tModel" />
<complexType name="tModel">
<sequence>
<element ref="uddi:name" />
<element ref="uddi:description" minOccurs="0" maxOccurs="unbounded" />
<element ref="uddi:overviewDoc" minOccurs="0" />
<element ref="uddi:identifierBag" minOccurs="0" />
<element ref="uddi:categoryBag" minOccurs="0" />
```

```
</sequence>
<attribute name="tModelKey" type="uddi:tModelKey" use="required" />
<attribute name="operator" type="string" use="optional" />
<attribute name="authorizedName" type="string" use="optional" />
</complexType>
```

Struttura XML dell'entità tModel

La descrizione degli attributi è riportata in tabella A4

Attributo	Descrizione	Tipo dato	Lunghezza
tModelKey	Rappresenta la chiave unica per identificare un tModel.	string	255
authorizedName	Rappresenta il nome della persona che ha pubblicato i dati.	string	255
operator	E' il nome certificate dell'operatore del registro UDDI.	string	255
Name	È il nome registrato per il tModel.	string	255
description	Elemento opzionale. Può essere presente più volte. Cntiene una breve descrizione dell'elemento. E' consentita una descrizione per ogni lingua supportata.	string	255
overviewDoc	Elemento opzionale. Utilizzato per referenziare informazioni documentali relative al tModel.	Structure	
identifierBag	(Elemento opzionale). Contiene una lista di coppie chiave-valore utilizzate per identificare un tModel.	Structure	
categoryBag	(Elemento opzionale). Contiene una lista di coppie chiave-valore utilizzate per identificare la/e categoria/e di appartenenza del tModel.	structure	

Tabella A4 Gli attributi dell'entità bindingTemplate

A2.5 L'ENTITÀ PUBLISHERASSERTION

Nella realtà molte organizzazioni che pubblicano servizi, sono a loro volta strutture dipendenti da altre organizzazioni. Il modello dati gestito dai registri UDDI consente tuttavia di evidenziare la relazione tra differenti organizzazioni attraverso il meccanismo delle asserzioni.

La struttura publisherAssertion, nel contesto, rappresenta dunque il legame tra due organizzazioni.

La struttura XML dell'entità è la seguente:

```
<element name="publisherAssertion" type="uddi:publisherAssertion" />
<complexType name="publisherAssertion">
<sequence>
<element ref="uddi:fromKey" />
<element ref="uddi:toKey" />
<element ref="uddi:keyedReference" />
</sequence>
</complexType>
```

Struttura XML dell'entità publisherAssertion

La descrizione degli attributi è riportata in tabella A5

Attributo	Descrizione	Tipo dato	lunghezza
fromKey	Rappresenta la chiave unica della prima business Entity che partecipa alla relazione.	string	255
toKey	Rappresenta la chiave unica della seconda business Entity che partecipa alla relazione.	string	255
keyedReference	Rappresenta la relazione tra le due business entity ed è rappresentata: da un tModelKey e descritta da una serie di coppie chiavi-valore.	attributes	255

Tabella A5 Gli attributi dell'entità publisherAssertion

A3 IL PROGETTO SIGMA TER

A3.1 DESCRIZIONE DEL PROGETTO

Il progetto SIGMA TER, cofinanziato dal Dipartimento per l'Innovazione e le tecnologie nell'ambito del piano di azione di e-Gov, nasce facilitare il processo di decentramento catastale e per migliorare la capacità di pianificazione e gestione amministrativa e fiscale del territorio e della qualità dei servizi per cittadini, professionisti ed imprese, che necessitano di integrare le informazioni catastali (a livello Agenzia del Territorio) con quelle territoriali (a livello di Regioni ed Enti Locali). Il progetto si pone quindi due obiettivi principali:

- creare un'infrastruttura per l'interscambio di informazioni catastali e territoriali fra Agenzia del Territorio e Regioni e fra queste e gli Enti Locali;
- sviluppare un ampio numero di servizi basati sull'informazione catastale e territoriale da fornire a cittadini, imprese e professionisti.

Una caratteristica chiave del progetto SIGMA TER è data dall'ampiezza dell'aggregazione in termini territoriali e di popolazione interessata e dei livelli istituzionali coinvolti: Pubblica Amministrazione Centrale, Regioni, Province, Comunità Montane, Comuni e loro aggregazioni.

Sin dalle prime fasi di progettazione gli enti promotori di SIGMA TER hanno mantenuto una forte attenzione all'adozione ed al rispetto di formati aperti e standard, sia per quanto attiene le informazioni di tipo cartografico e territoriali (documenti prodotti dall'Intesa GIS, ISO 19115, ecc.), sia per quanto riguarda gli strumenti informatici per la rappresentazione delle informazioni, la realizzazione degli applicativi e la trasferibilità delle soluzioni.

In particolare, oltre all'osservanza di tutte le disposizioni normative e le indicazioni relative alla cooperazione applicativa fornite dal DIT, viene prestata una forte attenzione all'utilizzo di soluzioni standard e "open" sia in termini di applicativi che per quanto riguarda i formati dati.

Si farà quindi ricorso anche a soluzioni open source (non solo per quanto riguarda i sistemi operativi), e per favorire il riuso e l'interoperabilità a XML, SOAP, J2EE, web services (WSDL), con particolare attenzione alla documentazione del software e delle banche dati, anche attraverso il ricorso a notazioni quali l'UML.

Il progetto SIGMA TER coinvolge numerosi enti impegnati (col supporto dei propri fornitori) nella realizzazione delle applicazioni.

Oltre alla Regione Emilia-Romagna (coordinatore), partecipano attivamente:

- l'Agenzia del Territorio;
- le Regioni, Abruzzo, Liguria, Toscana, Valle d'Aosta;

- le Province di Bologna, Genova, Parma, Piacenza, Pisa;
- le Comunità Montane Alta Val Polcevera e della Garfagnana;
- i Comuni di Bologna, Cesena, Collesalvetti, Faenza, Ferrara, Genova, La Spezia, Livorno, Lugo, Modena, Reggio Emilia, Rimini.

La serie di enti candidati al riuso delle soluzioni e delle esperienze sviluppate nel progetto porta ad oltre 150 il numero dei partner coinvolti ed altri enti hanno già manifestato l'interesse ad aderire.

A3.2 IL FORMATO DEL CAMPO INDIRIZZO

Nell'ambito del progetto è stato concordato il formato dei dati da esporre attraverso i servizi dell' dell'Agenzia del Territorio. Tali strutture dati sono state costruite, con la grammatica xml, riproponendo di massima le informazioni già fruibili dagli Enti, attraverso i servizi di sportello dell'ufficio provinciale dell' dell'Agenzia del Territorio, con le medesime regole di normalizzazione.

In particolare per lo scambio delle informazioni inerenti l'indirizzo degli immobili è stata definita una struttura che ripropone la standardizzazione delle medesime informazioni all'interno dei database degli uffici provinciali dell'AdT.

A ciascun immobile sono pertanto associati uno o più indirizzi, fino ad un massimo di 4, costituiti da:

- Codice nazionale del comune
- Sezione censuaria
- Codice toponimo
- Nomenclatura dell'indirizzo
- Numeri civici (massimo 3)
- Codice strada

Per ciascun immobile, indipendentemente dagli indirizzi presenti, sono inoltre esposte – se presenti nei database legali – le ulteriori informazioni:

- lotto
- edificio
- scala
- interno (massimo 2)
- piano (massimo 4)

Codice nazionale del Comune

I comuni sono identificati attraverso il codice nazionale utilizzato nel codice fiscale e l'AdT è titolare degli elenchi dei codici identificativi dei Comuni. E' però opportuno segnalare che l'istituzione di un comune è recepita nei data base catastali, e quindi negli indirizzi, a seguito della registrazione della

variazione circoscrizionale, operazione che può essere effettuata dall'uffici solo su richiesta del neo nato Ente.

Sezione censuaria

Codifica catastale che individua parti omogenee del territorio comunale, derivante da una suddivisione dello stesso per un più corretto procedimento estimativo catastale.

I comuni per i quali per gli indirizzi esiste questa ripartizione sono in numero limitato.

Codice toponimo

La tabella contiene la codifica di tutti i toponimi, oltre 500, utilizzati sul territorio nazionale (§10.3.1).

Nomenclatura dell'indirizzo e codice strada

Gli indirizzi degli immobili sono stati sottoposti ad una operazione massiva di normalizzazione e bonifica nel 1998 a seguito della quale le nomenclature, "ripulite" e correlate con uno stradario di riferimento, sono state ulteriormente lavorate dagli uffici anche con il diretto coinvolgimento dei comuni.

La bonifica iniziale ha trattato circa 5 milioni di indirizzi inseriti in 44 milioni di unità immobiliari urbane. La normalizzazione ha avuto esito positivo per l'87 % delle stringhe esaminate e il 61% di esse è stata anche correlata allo stradario di riferimento. La movimentazione di queste informazioni è oggi controllata in quanto i pacchetti software per l'aggiornamento possono utilizzare lo stradario di riferimento pubblicato sul sito dell'Agenzia del Territorio 'www.agenziaterritorio.gov.it' (un esempio è riportato in §10.3.2). benché sia previsto un margine di discrezionalità l'ufficio ha comunque a disposizione delle applicazioni mirate proprio al mantenimento del livello di qualità di dette informazioni.

Ad oggi le unità immobiliari ubicate su strade codificate sono oltre 61 milioni pari all'88,5% del totale.

CONCLUSIONI

Attualmente la titolarità dell'indirizzo è suddivisa tra diversi soggetti, in base alla sua qualificazione, infatti:

- **l'indirizzo dell'immobile** è un attributo dell'oggetto catastale gestito dall'Agenzia del Territorio (Ministero dell'Economia e delle Finanze);

- **l'indirizzo anagrafico** delle persone fisiche è di titolarità dei comuni (Ministero dell'Interno);

- **l'indirizzo fiscale** delle persone fisiche e delle persone non fisiche è di titolarità dell'Agenzia delle Entrate (Ministero dell'Economia e delle Finanze).

Tra i principali benefici che potrebbero derivare da una condivisione della struttura, del formato e della classificazione delle informazioni tra le strutture titolari dei dati possiamo individuare:

- la pubblicazione sul repository della Pubblica Amministrazione dello schema XML dell'indirizzo per rendere obbligatorio l'utilizzo del formato a tutte le strutture, pubbliche e private, per l'interscambio di informazioni con le pubbliche amministrazioni e gli enti pubblici, anche in recepimento della raccomandazione per le Amministrazioni fiscali, pubblicata nel mese di giugno dall'organismo di standardizzazione OASIS: *'XML position paper for Tax Amministration';*

- la standardizzazione e normalizzazione del campo indirizzo a livello nazionale;

- la possibilità di riuso delle applicazioni, degli schemi e dei servizi.

A3.1.1 TOPONIMI

CODICE	DESCRIZIONE
1	ALZATA
2	ANDRONA
4	ARCHIVOLTO
6	ARCO
8	ASCENSORE
10	ATRIO
12	BACINO
14	BAGLIO
16	BANCHINA
18	BASTIONI
20	BORGATA
22	BORGHETTO
24	BORGO
26	CALATA
28	CALLE
30	CALLESELLA
32	CAMPASSO
34	CAMPAZZO
36	CAMPIELLO
38	CAMPO
40	CASALE
42	CASE
44	CAVA
46	CAVALCAVIA
48	CHIASSO

50	CIRCONVALLAZIONE
52	CLIVIO
54	CONTRADA
56	CORSETTO
58	CORSO
60	CORTE
62	CORTICELLA
64	CORTILE
66	CUPA
68	DIRAMAZIONE
70	DISCESA
72	FONDACO
74	FONDAMENTA
76	FONDO
77	FRAZIONE
78	GALLERIA
80	GIARDINO
82	GRADINI
84	GRADONI
86	LARGO
88	LISTA
90	LOCALITA'
92	LOGGE
94	LUNGADIGE
96	LUNGARGINE
98	LUNGARNO
100	LUNGODORA
102	LUNGOMARE
106	LUNGOPO
108	LUNGOSTURA
110	LUNGOTEVERE
112	MASSERIA
114	MERCATO
116	MOLO
118	MULATTIERA
120	MURA
122	PARCO
124	PASSAGGIO
126	PASSEGGIATA
128	PASSETTO
130	PIAZZA
132	PIAZZALE
134	PIAZZETTA
136	PISCINA
138	PONTE
140	PONTILE
142	PORTA
144	PORTICO
146	PORTO
148	PROLUNGAMENTO
150	QUARTIERE
152	RAMI

154	RAMO
156	RAMPA
158	RAMPE
160	RECINTO
162	RIONE
164	RIVA
166	RIVIERA
168	ROTONDA
170	RUA
172	SALITA
174	SL
176	SALIZZATA
178	SCALA
180	SCALE
182	SCALEA
184	SCALETTA
186	SCALETTE
188	SCALI
190	SCALINATA
192	SCALONE
194	SDRUCCIOLO
196	SENTIERO
198	SESTRIERI
200	SITO
202	SOBBORGO
204	SOTTOPORTICO
206	SOTTOVIA
208	SPIANATA
210	STRADA
212	STRADALE
214	STRADELLA
216	STRADONE
218	SUPPORTICO
220	SVINCOLO
222	TRATTO
224	TRAVERSA
226	TRAVERSA VIA
228	TRESANDA
230	TRONCO
232	VALLONE
234	VARCO
236	VIA
238	VIADOTTO
240	VIALE
242	VIALETTO
244	VICO
246	VICOLETTO
248	VICOLO
250	VILLAGGIO
252	VIOTTOLO
254	VIUZZO
256	VO

258	VOLTA
260	PASSO
262	FORO
264	RIPA
266	RACCORDO
268	ALZAIA
300	ACCESSO
301	ACCESSO A CORSO
302	ACCESSO ALLA PIAZZA
303	ACCESSO ALLA VIA
304	ACCESSO VIALE
305	ACCESSO PRIVATO
306	ACCESSO STRADA
307	ACCESSO TRAVERSA
308	ALLEE
309	ALVEO
310	ANDRONE
311	ANGIPORTO
312	ARGINE
313	ARGINE DESTRO
314	ARGINE DI CANALE
315	ARGINE SINISTRO
316	AUTOSTRADA
317	AVENUE
318	BALUARDO
319	BARRIERA
320	BASTIONE
321	BASTIONI DI PORTA
322	BATTERIA
323	BISAGNO
324	BOCCA
325	BOULEVARD
326	CA'
327	CALA
328	CALETTA
329	CALLE DESTRA
330	CALLE LARGA
331	CALLE LITORANEA
332	CALLE SINISTRA
333	CALLE STRETTA
334	CALLESELLA DESTRA
335	CALLESELLA LARGA
336	CALLESELLA SINISTRA
337	CALLESELLE
338	CALLESELLE LARGHE
339	CALLESELLE STRETTE
340	CANALE
341	CANALE LARGO
342	CANTO
343	CANTONE
344	CAPO
345	CARRARA

346	CASCINA
347	CASE SPARSE
348	CAVALCAVIA DESTRO
349	CAVALCAVIA SINISTRO
350	CAVONE
351	CHIASSETTO
352	CHIASSUOLO
353	CIRCONVALLAZIONE DESTRA
354	CIRCONVALLAZIONE ESTERNA
355	CIRCONVALLAZIONE ESTRAMURALE
356	CIRCONVALLAZIONE INTERNA
357	CIRCONVALLAZIONE SINISTRA
358	CLAUSTRO
359	CLIVO
360	COMUNALE
361	CONTRA'
362	CORO
363	CORSIA
364	CORSIA DESTRA
365	CORSIA SINISTRA
366	CORSO PARALLELO
367	CORTINA
368	COSTA
369	COSTARELLA
370	CROSA
371	CROSINO
372	DARSENA
373	DIRAMAZIONE DEL CORSO
374	DIRAMAZIONE DEL VIALE
375	DIRAMAZIONE DI VIA
377	DIRUPO
378	DISTACCO
379	DORSO
380	EMICICLO
381	ERTA
382	FORTE
383	FOSSA
384	FOSSATO
385	FOSSO
386	GALLERIA DI CORSO
387	GRADINATA
388	GRADINATA DESTRA
389	GRADINATA SINISTRA
390	GRADINATA SUPERIORE
391	GRADINATE
392	GRADINATE SUPERIORI
393	GRANVIALE
394	LARGHETTO
395	LATERALE DI CORSO
396	LATERALE DI VIA
397	LATERALE DI VIALE
398	LIDO

399	LOGGIA
400	LUNGADIGE DESTRO
401	LUNGADIGE SINISTRO
402	LUNGARGINE DESTRO
403	LUNGARGINE SINISTRO
404	LUNGARNO DESTRO
405	LUNGARNO SINISTRO
406	LUNGOBISAGNO
407	LUNGOBISAGNO DESTRO
408	LUNGOBISAGNO SINISTRO
409	LUNGOCRATI
410	LUNGOCRATI DESTRO
411	LUNGOCRATI SINISTRO
412	LUNGODORA DESTRO
413	LUNGODORA SINISTRO
414	LUNGOFRIGIDO
415	LUNGOFRIGIDO DESTRO
416	LUNGOFRIGIDO SINISTRO
417	LUNGOGESSO
418	LUNGOGESSO DESTRO
419	LUNGOGESSO SINISTRO
420	LUNGOISARCO
421	LUNGOISARCO DESTRO
422	LUNGOISARCO SINISTRO
423	LUNGOLAGO
424	LUNGOLAGO DESTRO
425	LUNGOLAGO SINISTRO
426	LUNGOLARIO
427	LUNGOLARIO DESTRO
428	LUNGOLARIO SINISTRO
429	LUNGOMALLERO
430	LUNGOMALLERO DESTRO
431	LUNGOPARCO
432	LUNGOPO DESTRO
433	LUNGOPO SINISTRO
434	LUNGOSTURA DESTRO
435	LUNGOSTURA SINISTRO
436	LUNGOTALVERE
437	LUNGOTALVERE DESTRO
438	LUNGOTALVERE SINISTRO
439	LUNGOTEVERE DESTRO
440	LUNGOTEVERE SINISTRO
441	LUNGOTICINO
442	LUNGOTICINO DESTRO
443	LUNGOTICINO SINISTRO
444	LUNGOTORRENTE
445	LUNGOTORRENTE DESTRO
446	LUNGOTORRENTE SINISTRO
447	LUNGOTRONTO
448	LUNGOTRONTO DESTRO
449	LUNGOTRONTO SINISTRO
450	MARZARIA

451	MASSERIA VECCHIA
452	MERCERIA
453	MOLO ANTICO
454	MURAZZI
455	MURE
456	PARALLELA DESTRA
457	PARALLELA SINISTRA
458	PASSEGGIO
459	PENDICE
460	PENDIO
461	PENNINATO
462	PIAGGIA
463	PIANO
464	PIATTAFORMA
465	PIAZZA BELVEDERE
466	PIAZZA CHIUSA
467	PIAZZA COMUNALE
468	PIAZZA INFERIORE
469	PIAZZOLA
470	PLACE
471	POGGIO
472	PORTELLA
473	PORTICATO
474	PORTICCIOLO
475	PORTICHETTI
476	PORTICI
477	PRATO
478	PROLUNGAMENTO DI CORSO
479	PROLUNGAMENTO DEL VIALE
480	PROLUNGAMENTO DELLA VIA
481	PROVINCIALE
482	QUADRATO
483	RAMPA DEL CORSO
484	RAMPA DEL VIALE
485	RAMPA PIAZZA
486	RAMPA VIA
487	RAMPA DESTRA
488	RAMPA SINISTRA
489	RAMPA STRADA
490	RIALTO
491	RIGASTE
492	RIO
493	RIO TERRA'
494	RIPARTO
495	RIVETTA
496	RONCO
497	RONDO
498	ROUTE
499	RUE
500	RUGA
501	RUGA DESTRA
502	RUGA SINISTRA

503	RUGHETTA
504	RUGHETTA DESTRA
505	RUGHETTA SINISTRA
506	SALITA DESTRA
507	SALITA PER CORSO
508	SALITA PER PIAZZA
509	SALITA PER VIA
510	SALITA PER VIALE
511	SALITA SINISTRA
512	SALITA SUPERIORE
513	SALIZZATA DESTRA
514	SALIZADA SINISTRA
515	SBARCATOIO
516	SCALA DESTRA
517	SCALA SINISTRA
518	SCALEO
519	SCALETTA DESTRA
520	SCALETTA SINISTRA
521	SCALINATA DESTRA
522	SCALINATA SINISTRA
523	SCALO
524	SCESA
525	SCESE
526	SELCIATO
527	SENTIERO PANORAMICO
528	SESTIERE
529	SOTTOPASSAGGI
530	SOTTOPASSAGGIO
531	SOTTOPASSO
532	SPALTO
533	SPIAGGIA
534	SPIAZZO
535	STATALE
536	STAZZO
537	STRADA ACCORCIATOIA
538	STRADA ALTA
539	STRADA ANTICA
540	STRADA ARGINALE
541	STRADA BASSA
542	STRADA CANTONIERA
543	STRADA CHIUSA
544	STRADA CIECA
545	STRADA CIRCOLARE
546	STRADA COMUNALE
547	STRADA CONSORZIALE
548	STRADA DESTRA
549	STRADA DI LEVANTE
550	STRADA DI PONENTE
551	STRADA ESTERNA
552	STRADA EXTRAMURALE
553	STRADA INFERIORE
554	STRADA INTERCOMUNALE

555	STRADA INTERNA
556	STRADA INTERPODERALE
557	STRADA LARGA
558	STRADA LATERALE
559	STRADA LITORANEA
560	STRADA MULATTIERA
561	STRADA NUOVA
562	STRADA PANORAMICA
563	STRADA PARALLELA
564	STRADA PEDEMONTANA
565	STRADA PRIVATA
566	STRADA PROVINCIALE
567	STRADA ROMANA
568	STRADA ROTABILE
569	STRADA RURALE
570	STRADA SINISTRA
571	STRADA STATALE
572	STRADA STORTA
573	STRADA STRETTA
574	STRADA SUPERIORE
575	STRADA TANGENZIALE
576	STRADA TRASVERSALE
577	STRADA TRAVERSA
578	STRADA VECCHIA
579	STRADA VICINALE
580	STRADELLA DESTRA
581	STRADELLA SINISTRA
582	STRETTO
583	STRETTOIA
584	STRETTOIA DESTRA
585	STRETTOIA SINISTRA
586	STRETTOLA
587	STURA
588	SUPERSTRADA
589	TANGENZIALE
590	TERRAZZA
591	TRASVERSALE DEL CORSO
592	TRASVERSALE DI VIALE
593	TRASVERSALE VIA
594	TRAVERSALE PRIVATA
595	TRASVERSALE PROVINCIALE
596	TRAVERSALE STRADA
597	TRATTURO
598	TRAVERSA CORSO
599	TRAVERSA DEL VIALE
600	TRAVERSA DEL VILLAGGIO
601	TRAVERSA DELLA LOCALITA'
602	TRAVERSA DI VIA
603	TRAVERSA PRIVATA
604	TRAVERSA STRADA
605	VALCO
606	VALICO

607	VALLE
608	VIA ACCORCIATOIA
609	VIA ALTA
610	VIA ANTICA
611	VIA ARGINALE
612	VIA BASSA
613	VIA BELVEDERE
614	VIA CANTONIERA
615	VIA CHIUSA
616	VIA CIECA
617	VIA CIRCOLARE
618	VIA CIRCUMVALLAZIONE
619	VIA COMUNALE
620	VIA CONSORZIALE
621	VIA DESTRA
622	VIA DI LEVANTE
623	VIA DI PONENTE
624	VIA ESTERNA
625	VIA ESTRAMURALE
626	VIA INFERIORE
627	VIA INTERCOMUNALE
628	VIA INTERNA
629	VIA INTERPODERALE
630	VIA LARGA
631	VIA LATERALE
632	VIA LITORANEA
633	VIA LUNGOMARE
634	VIA MULATTIERA
635	VIA NUOVA
636	VIA PANORAMICA
637	VIA PARALLELA
638	VIA PEDEMONTANA
639	VIA PRIVATA
640	VIA PROVINCIALE
641	VIA ROMANA
642	VIA ROTABILE
643	VIA RURALE
644	VIA SINISTRA
645	VIA STATALE
646	VIA STORTA
647	VIA STRETTA
648	VIA SUPERIORE
649	VIA TANGENZIALE
650	VIA TRASVERSALE
651	VIA TRAVERSA
652	VIA VECCHIA
653	VIA VICINALE
654	VIALE BELVEDERE
655	VIALE LITORANEO
656	VIALE LUNGOMARE
657	VIALONE
658	VICO ALTO

659	VICO BASSO
660	VICO BELVEDERE
661	VICO CHIUSO
662	VICO CIECO
663	VICO DRITTO
664	VICO INFERIORE
665	VICO LUNGO
666	VICO NUOVO
667	VICO PRIVATO
668	VICO STORTO
669	VICO STRETTO
670	VICO VECCHIO
671	VICOLETTO CHIUSO
672	VICOLETTO CIECO
673	VICOLETTO DRITTO
674	VICOLETTO INFERIORE
675	VICOLETTO LUNGO
676	VICOLETTO NUOVO
677	VICOLETTO PRIVATO
678	VICOLETTO STORTO
679	VICOLETTO STRETTO
680	VICOLETTO VECCHIO
681	VICOLO ALTO
682	VICOLO BASSO
683	VICOLO BELVEDERE
684	VICOLO CHIUSO
685	VICOLO CIECO
686	VICOLO DRITTO
687	VICOLO INFERIORE
688	VICOLO LUNGO
689	VICOLO NUOVO
690	VICOLO PRIVATO
691	VICOLO STORTO
692	VICOLO STRETTO
693	VICOLO VECCHIO
694	VIELLA
695	VIETTA
696	VIOTTOLA
697	VIUZZA
698	VO'
699	VOCABOLO
700	VOLTE
701	VOLTO
702	VOLTONE
703	ZIPA
704	COLLE
705	ZONA
706	REGIONE
707	PODERE
708	PASSO PRIVATO
709	SALITA INFERIORE
710	LUNGO

711 VIAL

A3.2.1 ESEMPIO DI STRADARIO

1AA 1 AURELIA, STRADA STATALE	14004
M1AA 148 PONTINA, STRADA STATALE	14005
M1AA 2 CASSIA, STRADA STATALE	14006
M1AA 3 FLAMINIA, STRADA STATALE	14007
M1AA 4 SALARIA, STRADA STATALE	14008
M1AA 493 CLAUDIA BRACCIANESE, STRADA STATALE	14009
M1AA 5 TIBURTINA - VALERIA, STRADA STATALE	14010
M1AA 6 CASILINA, STRADA STATALE	14011
M1AA 601 OSTIA-ANZIO, STRADA STATALE	14012
M1AA 7 APPIA, STRADA STATALE	14013
M1AA 8 BIS OSTIENSE, STRADA STATALE	14014
M1AA ABANO TERME, VIA	01110
M1AA ABASCANTO, VIA	01111
M1AA ABATE DI TIVOLI, VIA	01112
M1AA ABATE UGONE, VIA	01113
M1AA ABBADIA SAN SALVATORE, VIA	01115
M1AA ABBASANTA, VIA	01116
M1AA ABBATEGGIO, VIA	01117
M1AA ABBATINI ANTONIO MARIA, VIA	01118
M1AA ABBAZIA, VIA	01119
M1AA ABBIATEGRASSO, VIA	01120
M1AA ABETONE, VIA	05154
M1AA ABRUZZI, VIA	14216
M1AA ACAIA, VIA	14218
M1AA ACATE, VIA	01125
M1AA ACCA LARENZIA, VIA	01126
M1AA ACCADEMIA DEGLI AGIATI, VIA	01127
M1AA ACCADEMIA DEI VIRTUOSI, VIA	01128
M1AA ACCADEMIA DI BRERA, VIA	01129

M1AA ACCADEMIA TIBERINA, LARGO	10541
M1AA ACCADEMIA TIBERINA, VIA	01130
M1AA ACCADIA, VIA	14220
M1AA ACCEGLIO, VIA	01134
M1AA ACCIAIOLI, VIA	01135
M1AA ACCIANO, VIA	01136
M1AA ACCINNI ENRICO, VIA	01138
M1AA ACCUMOLI, VIA	01141
M1AA ACCURSIO, VIA	01142
M1AA ACERENZA, VIA	01144
M1AA ACERNO, VIA	01145
M1AA ACERRA, VIA	14222
M1AA ACHELOO, VIA	01147
M1AA ACHEMENIDE, VIA	14233
M1AA ACHERUSIO, VIA	01149
M1AA ACHILLE BARILATTI, VIA	01938
M1AA ACHILLE BENEDETTI, VIA	02109
M1AA ACHILLE BERTELLI, VIA	02168
M1AA ACHILLE BIZZONI, VIA	14036
M1AA ACHILLE FUNI, VIA	07001
M1AA ACHILLE GAGGIA, VIA	07031
M1AA ACHILLE GRANDI, VIA	07450
M1AA ACHILLE LORIA, VIA	08114
M1AA ACHILLE LUIGI BONANOME, VIA	14209
M1AA ACHILLE MAURI, VIA	08587
M1AA ACHILLE PAPA, VIA	09711
M1AA ACHILLE PELLIZZARI, VIA	09849
M1AA ACHILLE RUSSO, VIA	10962
M1AA ACHILLE TAMBURLINI, VIA	11912
M1AA ACHILLE TEDESCHI, VIA	11962
M1AA ACHILLE TORELLI, VIA	12154
M1AA ACHILLE VERTUNNI, VIA	12645
M1AA ACHILLE VOGLIANO, VIA	12820

M1AA ACHILLE ZEZON, VIA	12902
M1AA ACI BONACCORSI, VIA	01151
M1AA ACI CASTELLO, VIA	01152
M1AA ACI CATENA, VIA	14234
M1AA ACI PLATANI, VIA	01154
M1AA ACI SANT`ANTONIO, VIA	01155
M1AA ACILIA, LOCALITA'	14235
M1AA ACILIA, PIAZZA	14237
M1AA ACILIO GLABRIONE, VIA	01157
M1AA ACIREALE, VIA	01158
M1AA ACQUA DEI CORSARI, VIA	01160
M1AA ACQUA DONZELLA, VIA	14244
M1AA ACQUACANINA, VIA	01162
M1AA ACQUAFONDATA, VIA	01164
M1AA ACQUAFORMOSA, VIA	14254
M1AA ACQUALAGNA, VIA	01165
M1AA ACQUALANDRONI, VIA	01166
M1AA ACQUAPENDENTE, VIA	01167
M1AA ACQUARO, VIA	01168
M1AA ACQUARONI, VIA	01169
M1AA ACQUAVIVA D`ISERNIA, VIA	01170
M1AA ACQUAVIVA DELLE FONTI, VIA	01171
M1AA ACQUAVIVA PLATANI, VIA	01172
M1AA ACQUI, VIA	01174
M1AA ACQUICELLA, VIA	01175
M1AA ACUSILAO, VIA	01178
M1AA ACUTO, VIA	14265
M1AA ACUZIA, VIA	01180
M1AA ADA NEGRI, VIA	09275
M1AA ADALBERTO CENCETTI, VIA	03315
M1AA ADALBERTO LIBERA, VIA	14236
M1AA ADALBERTO, VIA	01181
M1AA ADAMANTEA, VIA	14260

M1AA ADAMELLO, VIA	01182
M1AA ADDA, VIA	14270
M1AA ADDIS ABEBA, PIAZZA	00385
M1AA ADELAIDE BONO CAIROLI, VIA	02681
M1AA ADELAIDE RISTORI, VIA	10723
M1AA ADELE ZOAGLI MAMELI, PIAZZA	00801
M1AA ADELINA PATTI, VIA	09807
M1AA ADEMARO NICOLETTI ALTIMARI, VIA	09323
M1AA ADEODATO MATRICARDI, VIA	08580
M1AA ADEODATO RESSI, VIA	10656
M1AA ADIGE, VIA	14275
M1AA ADIGRAT, VIA	01191
M1AA ADOLFO ALBERTAZZI, VIA	14391
M1AA ADOLFO APOLLONI, VIA	01559
M1AA ADOLFO BORGOGNONI, VIA	02405
M1AA ADOLFO BRANCHINI, VIA	02492
M1AA ADOLFO CANCANI, VIA	14081
M1AA ADOLFO CONSOLINI, VIA	03769
M1AA ADOLFO COZZA, VIA	03901
M1AA ADOLFO GANDIGLIO, VIA	07102
M1AA ADOLFO GREGORETTI, VIA	07475
M1AA ADOLFO OMODEO, VIA	09470
M1AA ADOLFO PRASSO, VIA	10343
M1AA ADOLFO RAVA`, VIA	10601
M1AA ADOLFO TOMMASI, VIA	12126
M1AA ADOLFO VENTURI, VIA	12597
M1AA ADOLFO VIGORELLI, VIA	12708
M1AA ADONE FINARDI, VIA	06733