CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

Gruppo di lavoro per i Servizi di interoperabilità, cooperazione applicativa ed accesso del Sistema Pubblico di Connettività e Cooperazione

SPC

Sistema pubblico di cooperazione:

ARCHITETTURA

Versione 1.0

INDICE

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
[DbC]	Building bug-free O-O software: An introduction to Design by Contract(TM) http://archive.eiffel.com/doc/manuals/technology/contract/
[HTTPR]	IBM – A Primer for HTTPR - An overview of the reliable HTTP protocol – 1 July 2001 http://www-106.ibm.com/developerworks/webservices/library/ws-phtt/
[MIME]	RFC 2045 – MIME Part One: Format of Internet Message Bodies RFC 2046 – MIME Part Two: Media types RFC 2047 – MIME Part Three: Message Header Extensions for Non-ASCII Text RFC 2048 – MIME Part Four: Registration Procedures RFC 2049 – MIME Part Five: Conformmance Criteria and Examples
[OCSP]	IETF – RFC 2560 - X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol – OCSP – June 1999 http://www.ietf.org/rfc/rfc2560.txt
[RFC2119]	IETF – RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels – March 1997 http://www.faqs.org/rfcs/rfc2119.html
[SOAP 1.1]	Simple Object Access Protocol (SOAP) 1.1 - W3C Note 08 May 2000 http://www.w3.org/TR/2000/NOTE-SOAP-20000508/
[SOAPAttach]	SOAP Messages with Attachments - W3C Note 11 December 2000 http://www.w3.org/TR/SOAP-attachments
[SPC Architettura]	CNIPA – Sistema pubblico di connettività – Architettura del SPC – 3.0 – 27/11/2003 http://www.cnipa.gov.it/site/_files/5.SPC,Architettura%20SPC,Q,3.0.pdf

Codice	Titolo
[UDDI - WSDL 2]	OASIS – UDDI Specification TC - Technical Note - Using WSDL in a UDDI Registry, Version 2.0 http://www.oasis-open.org/committees/uddi-spec/doc/tn/uddi-spec-tc-tn-wsdl-v200-20031104.htm
[UDDI API 2]	UDDI Version 2.04 API Specification - UDDI Committee Specification, 19 July 2002 http://uddi.org/pubs/ProgrammersAPI-V2.04-Published-20020719.htm
[UDDI Data Structure 2]	UDDI Version 2.03 Data Structure Reference - UDDI Committee Specification, 19 July 2002 http://uddi.org/pubs/DataStructure-V2.03-Published-20020719.htm
[URI]	IETF – RFC 2396 - Uniform Resource Identifiers (URI): Generic Syntax - August 1998 http://ftp.ics.uci.edu/pub/ietf/uri/rfc2396.txt
[W3C WS-Architecture]	Web Services Architecture - W3C Working Group Note 11 February 2004 http://www.w3.org/TR/2004/NOTE-ws-arch-20040211/
[W3C WS-Glossary]	Web Services Glossary - W3C Working Group Note 11 February 2004 http://www.w3.org/TR/2004/NOTE-ws-gloss-20040211/
[W3C WS-LifeCycle]	Web Service Management: Service Life Cycle - W3C Working Group Note 11 February 2004 http://www.w3.org/TR/2004/NOTE-wslc-20040211/
[WSBPEL 0.1]	OASIS - Web Services Business Process Execution Language - Working Draft 01, 30 July 2004 http://www.oasis-open.org/committees/download.php/8750/wsbpel-specification-draft-July-30-2004.html
[WSCI 1.0]	Web Service Choreography Interface (WSCI) 1.0 - W3C Note 8 August 2002 http://www.w3.org/TR/wsci/
[WSDL 1.1]	Web Services Description Language (WSDL) 1.1 - W3C Note 15 March 2001 http://www.w3.org/TR/2001/NOTE-wsdl-20010315
[WS-I AP 1.0]	WS-I Attachments Profile Verion 1.0 – Final Material – 20040824 http://www.ws-i.org/Profiles/AttachmentsProfile-1.0-2004-08-24.html

Codice	Titolo
[WS-I BP 1.0 errata]	WS-I - Basic Profile Version 1.0a Errata List - Revision: 1 - Date: 2003/11/12 http://www.ws-i.org/Profiles/Basic/2003-08/BasicProfile-1.0-errata-1.htm
[WS-I BP 1.0]	WS-I - Basic Profile Version 1.0a - Final Specification - Date: 2003/08/08 http://www.ws-i.org/Profiles/Basic/2003-08/BasicProfile-1.0a.html
[WS-I BP 1.1]	WS-I – Basic Profile Version 1.1 – Final Material – 20040824 http://www.ws-i.org/Profiles/BasicProfile-1.1-2004-08-24.html
[WS-I SCM Architecture 1.0]	WS-I - Supply Chain Management Sample Application – Architecture - Document Status: Final Specification - Version: 1.01 - Date: December 9, 2003 http://www.ws-i.org/SampleApplications/SupplyChainManagement/2003-12/SCMArchitecture1.01.pdf
[WS-I SCM Use Case 1.0]	WS-I - Supply Chain Management - Use Case Model - Document Status: Final Specification - Version: 1.0 - Date: December 1, 2003 http://www.ws-i.org/SampleApplications/SupplyChainManagement/2003-12/SCMUseCases1.0.pdf
[WS-I SSBP 1.0]	WS-I - Simple Soap Binding Profile Version 1.0 – Final Material – 20040824 http://www.ws-i.org/Profiles/SimpleSoapBindingProfile-1.0-2004-08-24.html
[WS-I Usage Scenarios 1.01]	WS-I Usage Scenarios - Document Status: Final Specification - Version: 1.01 - Date: December 9, 2003 http://www.ws-i.org/SampleApplications/SupplyChainManagement/2003-12/UsageScenarios-1.01.pdf
[WS-Reliability 1.1]	OASIS – Web Services Reliable Messaging TC – WS-Reliability 1.1 – Committee Draft 1.086, 24 August 2004-09-14 http://xml.coverpages.org/WSRM-CD1086-8936.pdf
[WS-ReliableMessaging]	BEA/IBM/Microsoft/TIBCO Software - Web Services Reliable Messaging Protocol (WS-ReliableMessaging) - March 2004 http://www-106.ibm.com/developerworks/library/ws-rm/

Codice	Titolo
[WSS TP X509]	OASIS – Web Services Security – X.509 Certificate Token Profile - OASIS Standard 200401, March 2004 http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0.pdf
[WS-Security 2004]	OASIS – Web Services Security: SOAP Message Security 1.0 (WS-Security 2004) – OASIS Standard 200401, March 2004 http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf
[XML 1.0]	Extensible Markup Language (XML) 1.0 (Third Edition) - W3C Recommendation 04 February 2004 http://www.w3.org/TR/2004/REC-xml-20040204/
[XML Encryption]	XML Encryption Syntax and Processing - W3C Recommendation 10 December 2002 http://www.w3.org/TR/xmlenc-core/
[XML Schema]	XML Schema Part 0: Primer - W3C Recommendation, 2 May 2001 http://www.w3.org/TR/xmlschema-0/
[XML Signature]	XML-Signature Syntax and Processing - W3C Recommendation 12 February 2002 http://www.w3.org/TR/xmldsig-core/
[XMLP].	W3C – XML Protocol (XMLP) Requirements – W3C Working Draft 26 June 2002 http://www.w3.org/TR/2002/WD-xmlp-reqs-20020626

3. TERMINI ED ACRONIMI

Termine/Acronimo	Descrizione
AC	Autorità di certificazione
AC SICA	Servizi SICA di autorità di certificazione
AC SICA nazionale	Servizio nazionale generale di AC SICA (radice di certificazione)
Accordo di cooperazione	Insieme di accordi di servizio di un dominio di cooperazione
Accordo di servizio	Definizione delle funzionalità, interfacce, requisiti di sicurezza e di qualità di servizio di un servizio
ACoop	Accordo di cooperazione
Architettura SPCoop	Architettura generale del S.P. di Cooperazione
AS	Accordo di servizio
CNIPA	Centro nazionale per l'informatica nella Pubblica Amministrazione
Comunità SPCoop	Insieme dei soggetti SPCoop
DC	Dominio di cooperazione
Dominio	Insieme dei sistemi di cui un soggetto è titolare
Dominio dei servizi applicativi	Insieme dei servizi di cui un soggetto è erogatore
DSA	Dominio dei Servizi Applicativi
ICP	Infrastruttura a chiave pubblica
ICP SICA	Servizi SICA di infrastruttura a chiave pubblica
PD	Porta di dominio
PDD	Porta di dominio delegata
R.U.P.A.	Rete Unitaria della Pubblica Amministrazione
Registro SICA	Servizi SICA di registrazione e ricerca
Registro SICA nazionale	Servizio nazionale generale di registro SICA
Registro SICA secondario	Servizio di registro SICA secondario
SA	Servizi applicativi
SICA	Servizi infrastrutturali di interoperabilità, cooperazione e accesso
Soggetto SPCoop	Soggetto emanante di una amministrazione, un'impresa o una associazione qualificata registrato sull'indice dei soggetti del Registro SICA nazionale
SPC	Sistema Pubblico di Connettività e Cooperazione
SPConn	Sistema Pubblico di Connettività
SPCoop	Sistema Pubblico di Cooperazione

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

L'obiettivo del documento è quello di definire l'architettura di riferimento del Sistema Pubblico di Cooperazione applicativa nell'ambito del SPC. Il documento è una specifica ufficiale di tale architettura.

5.1. Struttura del Documento

Nel § 6 è descritto il modello generale dell'architettura del S. P. di Cooperazione (Architettura SPCoop) come architettura di servizi.

Nel § 7 sono descritti i contenuti e indicato il formato dell'accordo di servizio (AS).

Nel § 8 sono descritti i componenti tecnici (Porta di dominio - PD) e i servizi infrastrutturali (SICA) del S. P. di Cooperazione.

5.2. Componenti del gruppo di lavoro

Hanno partecipato ai lavori del gruppo:

Nome	Amministrazione/società
Angelucci, Pietro Luigi	Agenzia delle Entrate
Arcese, Annamaria	EDS
Bucci, Stefano	Oracle
Bussotti, Ubaldo	CNIPA
Cammillacci, Vincenzo	Min. Economia (Tesoro)
Castellani, Laura	Reg. Toscana
Castiglioni, Fabio	IBM
Concordia, Giuseppe	Min. Economia (Finanze)
De Simone, Alessandro	Etnoteam
Filiaggi, Elvira	CNIPA
Fortuna, Paola	Finsiel
Fuligni, Stefano	CNIPA
Luisi, Piero	Progetto "people"
Maesano Libero	Consulente CNIPA
Milone, Francesco	SOGEI
Oldano, Giandomenico	EDS
Raiss, Gianluigi	Min. Lavoro
Sterpellone, Andrea	Etnoteam
Tortorelli, Francesco	CNIPA
Travascio, Vincenzo	Reg. Campania
Tufano, Giacomo	SUN
Veiluva, Enzo	CSI Piemonte
Vivaldo, Simona	Min. Salute

6. IL MODELLO DI ARCHITETTURA

Il Sistema Pubblico di Cooperazione (SPCoop) e un insieme di standards tecnologici e di servizi infrastrutturali il cui obiettivo è di permettere l'interoperabilità e la cooperazione di sistemi informatici per la realizzazione di adempimenti amministrativi. Tali sistemi sono sotto la responsabilità di *soggetti pubblici*, emananti da amministrazioni centrali, enti pubblici, regioni, provincie, comuni, comunità di enti locali, e *soggetti privati* (imprese e associazioni accreditate). L'insieme dei soggetti pubblici e privati operanti sul S.P. di Cooperazione costituiscono la *comunità dei soggetti* del S.P. di Cooperazione.

Tale cooperazione è motivata da due esigenze fondamentali:

- L'esigenza di coordinamento di processi realizzati con il concorso di trattamenti distribuiti tra sistemi informatici di cui sono responsabili soggetti pubblici e privati, al fine di assecondare l'esecuzione di *procedimenti amministrativi* e la produzione di *atti* e *provvedimenti amministrativi*. Il coordinamento e la collaborazione di detti sistemi devono essere corredati dalla capacità di ispezionare in ogni momento lo stato di avanzamento (gli adempimenti amministrativi effettuati e quelli ancora da effettuare) dei processi applicativi e l'origine di ogni atto amministrativo effettuato nell'ambito del processo applicativo, al fine di realizzare concretamente la trasparenza dell'azione amministrativa nel doveroso rispetto delle norme sulla confidenzialità e riservatezza dei dati.

- Il coordinamento e la collaborazione dei trattamenti distribuiti tra più sistemi informatici appartenenti a più soggetti pubblici e privati, al fine di assicurare il funzionamento interno delle amministazioni e di fornire *servizi di utilità* alle altre amministrazioni, ai cittadini, alle imprese e alle associazioni, in conformità con i compiti istituzionali delle diverse amministrazioni.

Il modello generale di riferimento dell'architettura del Sistema pubblico di cooperazione è il modello dell' *architettura di servizi sulla base di tecnologie Web services* [W3C WS-Architecture] descritto in questo paragrafo. I vantaggi principali che derivano dall'adozione di un tale modello per il Sistema Pubblico di Cooperazione sono:

- Il modello dell'architettura dei servizi è pienamente distribuito e permette l'interoperabilità e la cooperazione dei sistemi informatici sulla base di *accordi* sullo scambio di *funzionalità*, sulle *interfacce* che permettono tale scambio e sui suoi requisiti di *sicurezza* e *qualità di servizio*, nella piena autonomia delle scelte implementative e gestionali dei sistemi componenti l'architettura. L'indipendenza delle scelte implementative delle funzionalità applicative e delle funzionalità di infrastruttura (gestione dei messaggi, sicurezza, qualità di servizio) dei sistemi cooperanti rende tale modello perfettamente adatto alle esigenze di autonomia di gestione delle amministrazioni centrali e locali e all'interoperabilità con sistemi applicativi delle imprese e delle associazioni qualificate.

- La realizzazione delle funzionalità infrastrutturali di interfaccia, sicurezza e qualità di servizio necessarie alla cooperazione applicativa, sulla base degli standards tecnologici *Web services* [W3C WS-Glossary], permette di minimizzare l'impatto sull'implementazione delle funzionalità applicative già realizzate nei sistemi informativi dei soggetti, pubblici e

privati. Il modello non solo garantisce la salvaguardia del patrimonio applicativo dei soggetti pubblici e privati, ma ne stimola la valorizzazione attraverso il *riuso* in nuovi contesti di funzionalità applicative già implementate. La scelta del modello dell'architettura di servizi sulla base delle tecnologie Web services è quindi conforme alle esigenze di economia e di controllo della spesa pubblica e della qualità del servizio amministrativo.

Una caratteristica fondamentale del modello dell'architettura di servizi è che l'interazione tra i sistemi partecipanti avviene esclusivamente per mezzo dello scambio di messaggi in rete. Ne consegue che due sistemi interagenti devono essere connessi per mezzo di uno o più *canali* che trasportano i messaggi scambiati. **Il Sistema Pubblico di Cooperazione utilizza per il trasporto dei messaggi esclusivamente i canali e i meccanismi di trasporto forniti dal Sistema Pubblico di Connettività** [SPC Architettura].

Il S. P. di Connettività fornisce al S.P. di Cooperazione:

- l'infrastruttura di base per il trasporto dei messaggi,
- un insieme di funzionalità infrastrutturali di *sicurezza* e *qualità di servizio* applicabili al trasporto dei messaggi.

Dal punto di vista dei sistemi interagenti nel S. P. di Cooperazione, il S. P. di Connettività è semplicemente e esclusivamente il fornitore della infrastruttura per il trasporto dei messaggi. L'architettura logica e fisica dei sistemi partecipanti al S.P. di Cooperazione è indipendente dell'architettura logica, fisica, di rete del S.P. di Connettività: i soli punti di collegamento si trovano nell'uso del protocollo di trasporto utilizzato dal S.P. di Connettività (IP), e, eventualmente nell'uso di funzionalità di sicurezza (IPSec) e di qualità di servizio applicabili al trasporto fornite dal S.P. di Connettività.

L'architettura di servizi è un modello di architettura informatica distribuita che si diffonde grazie alla maturità e al consolidamento degli standards e delle tecnologie Web services. E' utile comunque precisare la differenza concettuale tra *architettura di servizi* e *Web services*:

- Il termine *architettura di servizi* designa un modello concettuale di architettura informatica distribuita costituita da un insieme di *sistemi* autonomi che comunicano per mezzo di *messaggi* scambiati attraverso *interfacce* standardizzate.
- Il termine *Web services* ricopre un insieme di standards tecnologici che permettono la realizzazione di architetture di servizi su larga scala, garantendo al tempo stesso l'interoperabilità e l'autonomia di implementazione dei sistemi componenti l'architettura.

Il modello d'architettura del Sistema Pubblico di Cooperazione (Architettura SPCoop) è un modello di architettura di servizi sulla base delle tecnologie Web services. Il modello dell'architettura SPCoop stabilisce tra i sistemi applicativi e infrastrutturali partecipanti delle relazioni che appartengono tutte alla stessa classe generale: la classe delle *relazioni di servizio*.

6.1. Le relazioni di servizio

6.1.1. *Definizione di servizio*

Tra due sistemi informatici si istaura una relazione di servizio se uno dei due sistemi, che riveste il ruolo di *fruitore*, utilizza i risultati di trattamenti informatici effettuati dall'altro sistema, che riveste il ruolo di *erogatore*. Nel seguito del documento parleremo, per ogni relazione specifica di servizio, rispettivamente di *sistema fruitore* (o direttamente di fruitore) e di *sistema erogatore* (o direttamente di erogatore) del servizio.

Un *servizio* è l'insieme dei risultati prodotti dai trattamenti effettuati dal sistema erogatore e utilizzati dai trattamenti effettuati dal sistema fruitore. In altri termini: la logica di trattamento del sistema fruitore utilizza determinate funzionalità (applicative o infrastrutturali) fornite da un altro sistema (l'erogatore). Chiameremo l'insieme dei risultati prodotti dai trattamenti effettuati dall'erogatore, che il fruitore utilizza nei suoi propri trattamenti interni, l'*insieme delle prestazioni di servizio*. L'insieme delle prestazioni di servizio è organizzato in *classi* (tipi) di prestazioni, che chiameremo *funzionalità di servizio*. La descrizione funzionale di un servizio è la descrizione delle classi di prestazioni (funzionalità) del servizio.

6.1.2. *Categorie di prestazioni di servizio*

Le prestazioni di servizio appartengono a quattro categorie:

- *prestazioni di calcolo*:
  fornitura da parte dell'erogatore al fruitore di dati risultato di puri trattamenti di calcolo, senza gestione di stato da parte dell'erogatore;
- *prestazioni di informazione di stato*:
  fornitura da parte dell'erogatore al fruitore di dati risultati di ricerche, semplici e complesse, su risorse e sorgenti di dati soggette à cambiamenti di stato;
- *prestazioni di cambiamento di stato*:
  gestione da parte dell'erogatore degli stati e delle transizioni di stato di risorse su richiesta diretta o indiretta del fruitore; gli stati e le transizioni di stato delle risorse gestite dall'erogatore possono presentare caratteristiche specifiche di qualità di servizio come la garanzia di coerenza degli stati, la gestione della persistenza degli stati, la gestione di transizioni indecomponibili (transazioni atomiche);
- *prestazioni di interazione*:
  produzione di interazioni da parte del sistema erogatore con l'ambiente esterno (altri sistemi, utenti, dispositivi diversi) su richiesta diretta o indiretta del fruitore.

Nel caso più generale, un servizio include prestazioni appartenenti a tutte le categorie sopraelencate.

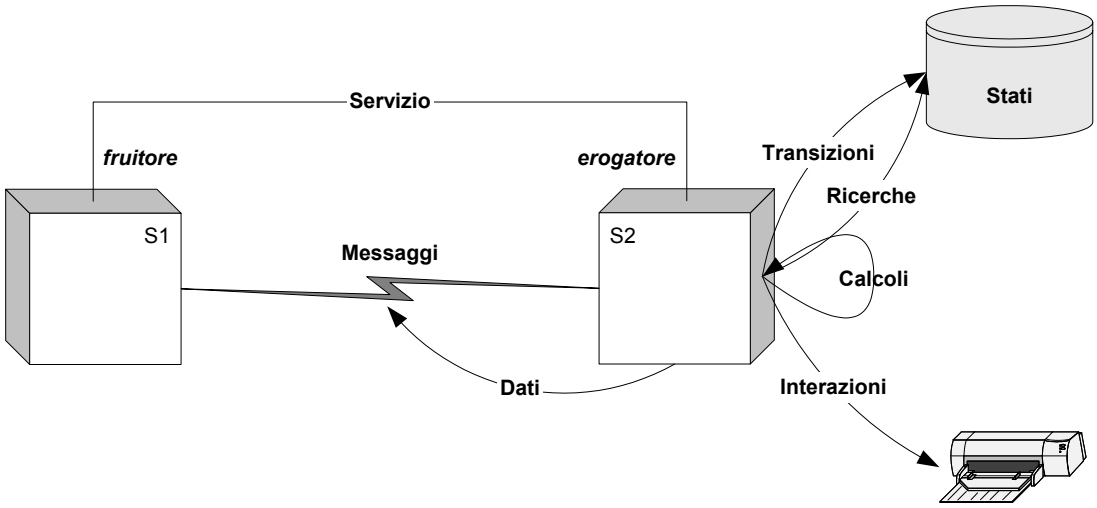


Figura 1. Relazione di servizio.

6.1.3. *La rete delle relazioni di servizio*

Un sistema che partecipa all'architettura SPCoop può, nel caso più generale, partecipare a più relazioni di servizio e ricoprire in queste relazioni alternativamente i ruoli di erogatore e fruitore: il sistema in questione eroga un sottoinsieme delle funzionalità che implementa come prestazioni e fruisce delle prestazioni fornite da altri sistemi dell'architettura. In una architettura di servizi, la cooperazione tra sistemi è realizzata quindi sotto forma di *scambio di prestazioni di servizio*.

L'architettura SPCoop si presenta quindi come una rete di relazioni di servizio tra sistemi autonomi e indipendenti dal punto di vista architetturale e tecnologico.

6.1.4. *Servizi applicativi e servizi infrastrutturali*

L'erogazione/fruizione di un servizio applicativo può richiedere la partecipazione di sistemi terzi che erogano le prestazioni infrastrutturali necessarie alla detta erogazione/fruizione. Esempi di prestazioni infrastrutturali sono (lista non esaustiva):

- le prestazioni di registrazione e ricerca di servizi e di indirizzi dei punti di accesso dei servizi;
- le prestazioni di autorità di registrazione e di certificazione in una infrastruttura a chiave pubblica.

Nell'architettura SPCoop, la cooperazioine tra sistemi applicativi e sistemi che implementano funzionalità infrastrutturali è realizzata per mezzo di relazioni di servizio: dette funzionalità infrastrutturali sono rese disponibili sotto forma di *servizi infrastrutturali*.

L'architettura SPCoop è una architettura di sistemi distribuiti in cui la cooperazione tra i sistemi partecipanti avviene esclusivamente sotto forma di scambio di prestazioni di servizi applicativi e infrastrutturali.

6.2. Lo scambio dei messaggi

Lo scambio di prestazioni di servizio tra sistemi richiede il coordinamento dell'erogazione/fruizione dei servizi scambiati, e quindi l'interazione tra i detti sistemi. **Nell'architettura SPCoop, la sola ed esclusiva modalità d'interazione tra il sistema erogatore e il sistema fruitore di un servizio è lo scambio di messaggi, sulla base degli standards tecnologici Web services** [XMLP].

Lo scambio di messaggi è utilizzato per coordinare l'erogazione/fruizione delle prestazioni di servizio e, eventualmente, per trasportare dati la cui fornitura fa parte di dette prestazioni.

Nel caso più generale di scambio di messaggi nell'ambito dell'erogazione/fruizione di una prestazione di servizio, l'erogatore e il fruitore rivestono entrambi i ruoli di *mittenti* e *destinatari* di messaggi.

Lo scambio di messaggi come sola modalità d'interazione – che esclude, per esempio, l'interazione attraverso l'accesso diretto a basi di dati condivise - garantisce al tempo stesso l'interoperabilità dei sistemi partecipanti all'architettura SPCoop, l'autonomia e l'indipendenza nella scelta delle architetture e tecnologie di implementazione di tali sistemi.

Per realizzare l'interoperabilità tra sistemi (applicativi e infrastrutturali) messi in opera con architetture e tecniche d'implementazione eterogene è infatti sufficiente l'accordo:

- sul protocollo di trasporto dei messaggi,
- sul protocollo di connessione tra punti di accesso dei sistemi,
- sui formati dei messaggi e dei contenitori dei messaggi,
- sul contenuto dei messaggi,
- sui protocolli di conversazione.

L'accordo sul contenuto dei messaggi e sul protocollo di conversazione tra i sistemi che entrano in una relazione di servizio è realizzato a livello funzionale. La sola inter-dipendenza tecnologica tra sistemi partecipanti all'architettura SPCoop è quindi che essi devono implementare, ciascuno in piena autonomia e indipendenza, i componenti tecnici di gestione dei protocolli di trasporto, dei protocolli di connessione e dei formati conformi agli standards tecnologici SPCoop.

6.2.1. *Livelli architetturali di realizzazione dello scambio*

Nell'architettura SPCoop, si distinguono quattro livelli architetturali di messa in opera dello scambio di messaggi:

- Livello *servizio*: trattamento delle parti del messaggio direttamente utilizzate dai sistemi interagenti per coordinare l'erogazione/fruizione del servizio.
- Livello *porta*: trattamento del formato del contenitore generico del messaggio.
- Livello *connessione*: protocollo di connessione tra punti di accesso utilizzato per stabilire il canale di trasmissione dei messaggi.
- Livello *trasporto*: protocollo di trasporto dei messaggi.

Ad ogni livello architetturale dello scambio corrisponde un insieme di tecnologie di implementazione. **La Tabella 1 presenta le tecnologie standard prescritte dall'architettura SPCoop**.

LIVELLO	STANDARDS TECNOLOGICI
Servizio	Il formato del contenuto del messaggio è XML 1.0 [XML 1.0]. Il messaggio può comprendere allegati in formato binario [MIME].
Porta	Il formato del contenitore è la Busta SPCoop, estensione standard di SOAP 1.1 [SOAP 1.1], e di SOAP Message with attachments/MIME [SOAPAttach] [MIME]per messaggi con allegati binari, usato in conformità con le raccomandazioni WS-I [WS-I AP 1.0] [WS-I BP 1.1] [WS-I SSBP 1.0]. La Busta SPCoop distingue tra il *corpo* del messaggio, che ospita il contenuto del messaggio trattato a livello *servizio* e le *testate* del messaggio, contenenti dati trattati a livello *porta*.
Connessione	Il protocollo di connessione: HTTP 1/1. Gli identificatori dei punti di accesso sono in formato URI (schema "http" o "https") [RFC 2396]. Tali standards sono usati in conformità con le specifiche della connessione SOAP/HTTP di SOAP 1.1 [SOAP 1.1] e SOAP Message with attachments/HTTP 1.1 [SOAPAttach] [MIME] e con le raccomandazioni WS-I [WS-I AP 1.0] [WS-I BP 1.1] [WS-I SSBP 1.0].
Trasporto	Questo livello, e i livelli sottostanti, sono implementati nell'ambito del S.P. di Connettività (IP) [SPC Architettura]. Per realizzare il trasporto dei messaggi, l'architettura SPCoop utilizza l'architettura e gli standards tecnologici del Sistema Pubblico di Connettività.

Tabella 1. Standards tecnologici dello scambio di messaggi nell'architettura SPCoop.

6.2.2. Compiti dello scambio di messaggi

Nella trasmissione del messaggio, un sistema detto *mittente* invia un messaggio ad un sistema detto *destinatario*. La Tabella 2 riassume i compiti del sistema mittente e del sistema destinatario ai diversi livelli di realizzazione dello scambio.

Livello	Compiti mittente	Compiti destinatario
Servizio	Composizione del contenuto del messaggio (XML) e dei suoi eventuali allegati binari (MIME)	Analisi sintattica, valutazione semantica e trattamento del contenuto del messaggio (XML) e dei suoi eventuali allegati binari (MIME).
Porta	Imbustamento - inserimento del contenuto del messaggio nella struttura Busta SPCoop. Eventuale inclusione degli allegati binari nel formato MIME.	Validazione del formato e sbustamento - prelevamento del contenuto del messaggio dalla struttura Busta SPCoop. Prelevamento degli allegati binari dal formato MIME.
Connessione – richiesta HTTP POST	Apertura della connessione HTTP e inserimento della struttura Busta SPCoop nel carico di una richiesta HTTP POST, invio della richiesta alla URI destinataria.	Ricezione della richiesta HTTP POST, prelevamento del carico (Busta SPCoop)
Connessione – risposta HTTP	Inserimento della struttura Busta SPCoop nel carico di una risposta HTTP, invio della risposta sulla connessione aperta dalla richiesta HTTP.	Ricezione della risposta HTTP, prelevamento del carico (Busta SPCoop)

Tabella 2. Compiti del mittente e del destinatario del messaggio ai livelli "servizio", "porta" e "connessione".

I compiti del destinatario, a livello *servizio* e *porta*, possono essere classificati in quattro categorie:

- il *controllo di formato*: controllo di conformità del formato del messaggio con lo standard Busta SPCoop;
- l'*analisi sintattica*: verifica che il contenuto (corpo e testate) del messaggio ben formato ricevuto è sintatticamente corretto;
- la *valutazione semantica*: verifica che il mittente del messaggio (ben formato e sintatticamente corretto) ha la capacità, i diritti e l'autorizzazione per emetterlo e che il destinatario ha la capacità, i diritti e l'autorizzazione per trattarlo;
- il *trattamento* del messaggio (ben formato, sintatticamente corretto, semanticamente valido) è l'insieme delle operazioni che il destinatario deve compiere alla ricezione del

messaggio, nell'ambito del coordinamento della erogazione/fruizione del servizio a cui partecipa.

Un principio fondamentale dell'architettura SPCoop è che **il destinatario del messaggio non è autorizzato a intraprendere alcuna operazione di trattamento di qualsiasi messaggio ricevuto prima di avec completato la verifica di formato, sintattica e semantica del messaggio stesso**. Per altro, l'architettura SPCoop non impone nessuna sequenza nell'espletamento dei compiti di controllo di formato, analisi sintattica e valutazione semantica, così come non impone a priori al destinatario di non effettuare il trattamento di un messaggio mal formato, sintatticamente scorretto o semanticamente non valido.

6.2.3. *Tipi di scambio elementare*

Nell'ambito dell'architettura SPCoop, sono implementati tre tipi di scambio elementare, in conformità con le raccomandazioni WS-I [WS-I Usage Scenarios 1.01].

- *messaggio senza replica*,
- *messaggio/replica sincroni*,
- *messaggio/replica asincroni*.

Nell'architettura SPCoop, qualsiasi scambio di messaggi tra due o più sistemi risulta esclusivamente della composizione di scambi elementari appartenenti alle tre categorie messaggio senza replica, messaggio/replica sincroni, messaggio/replica asincroni. Dette categorie sono presentate nei paragrafi seguenti e sono dettagliate nelle specifiche della Busta SPCoop.

6.2.3.1. Messaggio senza replica

Nello scambio elementare di tipo *messaggio senza replica*, un sistema *mittente* invia un messaggio a un sistema *destinatario*.

Il mittente apre una connessione HTTP, invia un messaggio conforme allo standard Busta SPCoop nel carico di una richiesta HTTP 1.1 POST all'indirizzo del punto di accesso del destinatario e si mette in attesa della risposta HTTP. Il destinatario trasmette una risposta HTTP con carico vuoto sulla connessione HTTP aperta dal mittente. La risposta HTTP "`202 Accepted`" comunica la riuscita dello scambio a livello *connessione*. Gli altri codici di ritorno HTTP indicano altri eventi di errore o di eccezione a livello connessione. Il carico della risposta HTTP deve essere vuoto e in ogni caso non deve essere trattato dal mittente.

Il destinatario è libero di implementare qualsiasi sequenza tra i trattamenti a livello *servizio* e l'invio della risposta HTTP. Il mittente non può *in nessun caso* interpretare la ricezione della risposta HTTP come resoconto di un qualsiasi trattamento a livello *servizio* da parte del destinatario. In conformità con il principio enunciato nel § 6.2.2, il destinatario si impegna a non effettuare nessun trattamento conseguente alla ricezione del messaggio (a livello *servizio*) prima di aver completato il controllo di formato, l'analisi sintattica e la valutazione semantica del messaggio stesso.

Per implementare il mittente dello stile elementare di interazione *messaggio unidirezionale*, non è necessario disporre di una capacità di ricezione di richieste HTTP.

6.2.3.2. Messaggio/replica sincroni

Nello scambio elementare di tipo *messaggio/replica sincroni*, un sistema detto *richiedente* trasmette un *messaggio sincrono* a un sistema detto *rispondente* e si mette in attesa della *replica sincrona*. Successivamente il rispondente trasmette una *replica sincrona* al richiedente correlata logicamente con il messaggio.

Il richiedente apre una connessione HTTP con l'indirizzo del punto di accesso del rispondente, invia un messaggio conforme allo standard Busta SPCoop nel carico di una richiesta HTTP 1.1 POST e si mette in attesa della risposta HTTP.

La risposta HTTP trasporta nel carico la replica conforme allo standard Busta SPCoop. La correlazione a livello logico tra messaggio e replica sincroni è rappresentata implicitamente dall'inserzione della replica nel carico della risposta HTPP alla richiesta HTTP che contiene il messaggio.

Il rispondente è libero a priori di implementare qualsiasi sequenza tra i trattamenti del messaggio e la costituzione della replica che garantisce la conformità con il principio che il trattamento del messaggio può essere effettuato solo dopo la verifica di formato, sintattica e semantica del messaggio stesso. Ne consegue che il richiedente non può a priori interpretare la replica come un resoconto del trattamento completo a livello *servizio* del messaggio (il significato della replica rispetto al messaggio deve essere specificato nell'accordo di servizio – vedi § 7). La replica può essere utilizzata per trasportare i contenuti seguenti (lista non esaustiva):

- una *ricevuta di ritorno* del messaggio (comunica semplicemente che il richiedente ha ricevuto il messaggio),
- un *resoconto di validazione di formato* del messaggio,
- un *resoconto di validazione sintattica* del messaggio (ben formato),
- un *resoconto di validazione semantica* del messaggio (ben formato e sintatticamente valido),
- un *resoconto di tutti o parte dei trattamenti* che il rispondente deve eseguire alla ricezione del messaggio ben formato e sintatticamente e semanticamente valido e eventualmente i dati risultati di detti trattamenti,
- un *resoconto di errori* (di formato, sintattici, semantici, di trattamento).

Per implementare il richiedente dello scambio elementare *messaggio/replica sincroni*, non è necessario mettere in opera la capacità di ricezione di richieste HTTP. Il richiedente deve disporre all'esecuzione dell'indirizzo del punto di accesso (URI con schema "http" o "https") del rispondente.

6.2.3.3. Messaggio/replica asincroni

Nello scambio di tipo *messaggio/replica asincroni*, un sistema detto *richiedente* trasmette un *messaggio asincrono* a un sistema detto *rispondente*. Il rispondente trasmette in seguito una *replica asincrona* al richiedente correlata logicamente con il messaggio ricevuto.

Il richiedente apre una connessione HTTP con l'indirizzo (URI) del punto di accesso del rispondente e invia un messaggio dotato di un *identificatore di correlazione* conforme allo standard Busta SPCoop nel carico di una richiesta HTTP 1.1 POST. La risposta HTTP "200 OK" con carico vuoto comunica la riuscita dello scambio a livello *connessione*, e gli altri codici di ritorno HTTP indicano altri eventi di errore o di eccezione a livello *connessione* (o livelli più bassi). Il carico della risposta HTTP deve essere vuoto e in ogni caso non deve essere trattato dal richiedente.

Il rispondente apre una connessione HTTP con l'indirizzo (URI) del punto di accesso del richiedente, e invia una replica contenente l'*identificatore di correlazione* trasmesso nel messaggio correlato (in conformità allo standard Busta SPCoop) nel carico di una richiesta HTTP 1.1 POST, trasmette tale richiesta. La risposta HTTP "200 OK" con carico vuoto comunica la riuscita dello scambio a livello *connessione*, e gli altri codici di ritorno HTTP indicano altri eventi di errore o di eccezione a livello *connessione* (o livelli più bassi). Il carico della risposta HTTP deve essere vuoto e in ogni caso non deve essere trattato dal rispondente.

La correlazione a livello logico tra messaggio e replica asincroni è rappresentata esplicitamente dall'inserzione nella replica dell'identificatore di correlazione trasmesso nel messaggio (Busta SPCoop).

Il principio che detta che i trattamenti a livello *servizio* conseguenti alla ricezione del messaggio non devono essere intrapresi prima del completamento della verifica di formato, sintattica e semantica del messaggio si applica allo scambio elementare messaggio/replica asincroni. I differenti usi della replica presentati nel caso di messaggio/replica sincroni (ricevuta di ritorno, resoconto di validità sintattica...) si applicano anche allo scambio elementare messaggio/replica asincroni.

Per implementare sia il richiedente che il rispondente dello scambio elementare *messaggio/replica asincroni* è necessario disporre di una capacità di emissione e di ricezione di richieste/risposte HTTP.

6.2.4. Gestione della sessione

Nell'architettura SPCoop, lo scambio di messaggi tra due sistemi è utilizzato per coordinare l'erogazione/fruizione di una prestazione di servizio. Per effetture il coordinamento di tale prestazione, può essere necessario che lo scambio comprenda una sequenza di più scambi elementari di messaggi chiamata *sessione*. La sessione è generalmente dotata di un identificatore fornito dal messaggio di apertura della sessione stessa.

In sistemi partecipanti a una sessione devono ricostruire, alla ricezione di ogni messaggio:

- la sessione a cui appartiene il messaggio ricevuto,

- lo stato di avanzamento della sessione (e quindi dell'erogazione/fruizione della prestazione).

Per effettuare il riconoscimento della sessione e del suo stato di avanzamento alla ricezione del messaggio esistono due approcci di implementazione alternativi:

1. *Gestione implicita della sessione*:
   i messaggi scambiati sono autosufficienti, contengono cioè tutte le informazioni necessarie al destinatario per trattarli senza che quest'ultimo sia obbligato a mantenere una reppresentazione della sessione e del suo stato.
2. *Gestione esplicita della sessione*:
   ogni partecipante alla sessione mantiene esplicitamente una rappresentazione della sessione e del suo stato e i messaggi scambiati nella sessione contengono l'identificatore della sessione. Il sistema destinatario del messaggio è in grado di associarlo alla sessione a cui appartiene (e al suo stato corrente).

L'approccio (1) è certamente più efficace in termini di:

- *Scalabilità*: non occorre rappresentare la sessione e il suo stato (per ogni sessione in corso) e quindi l'occupazione della memoria non cresce meccanicamente con il numero di sessioni aperte.
- *Affidabilità*: il sistema non deve salvaguardare su memoria secondaria le sessioni e i loro stati, e quindi la ripartenza dopo un arresto non implica la ricarica di tali stati. Dopo la ripartenza, il sistema è in grado di gestire le sessioni senza particolari accorgimenti.
- *Visibilità*: ogni messaggio contiene la rappresentazione dello stato di avanzamento della sessione a cui appartiene.

L'approccio (2) può essere più efficace in termini di:

- *Economia di tempo di calcolo*: non occorre ricostruire lo stato a ogni ricezione di messaggio.
- *Economia di banda passante*: il messaggio ha una rappresentazione più concisa dato che non è necessario che contenga informazioni sullo stato.

Le architetture a gestione implicita della sessione (1) sono generalmente preferibili in quanto più semplici, robuste e scalabili. Ciononostante, in alcuni casi le soluzioni a gestione esplicita della sessione (2) non possono essere evitate, come per esempio quando è necessaria l'autentificazione reciproca dei partecipanti allo scambio e l'istaurazione una sessione sicura per mezzo di una chiave simmetrica di sessione condivisa evita costose operazione di autentificazione basate sulla coppia chiave pubblica / chiave privata ad ogni scambio di messaggi.

6.2.5. Scenari di coordinamento della prestazione di servizio

Nell'architettura SPCoop, lo scambio di messaggi è utilizzato per coordinare l'erogazione/fruizione delle prestazioni di servizio. Chiameremo uno scambio di messaggi

utilizzato per coordinare l'erogazione/fruizione di una prestazione di servizio *scenario di coordinamento* della prestazione di servizio. In conformità con il principio citato nel § 6.2.3, nell'architettura SPCoop qualsiasi scenario di coordinamento di una prestazione di servizio risulta esclusivamente della combinazione di scambi elementari di tipo *messaggio senza replica*, *messaggio/replica sincroni*, *messaggio/replica asincroni*.

Nei paragrafi seguenti sono presentati alcuni tipi di *scenari elementari di coordinamento* dell'erogazione/fruizione del servizio:

- *richiesta senza risposta*,
- *richiesta/risposta*,
- *notificazione senza risposta,*
- *notificazione/risposta.*

6.2.5.1. Richiesta senza risposta

Nello scenario *richiesta senza risposta*, il fruitore trasmette all'erogatore un messaggio contenente una richiesta di prestazione e continua il trattamento. Tale scenario può essere implementato utilizzando come tipo di interazione il *messaggio senza replica*.

Lo scenario di richiesta senza risposta coordina una modalità di erogazione della prestazione *asincrona* e *su iniziativa del fruitore*: i trattamenti per l'erogazione della prestazione di servizio seguono la ricezione dell'invocazione da parte dell'erogatore (precedute dalle verifiche di formato, sintattiche e semantiche), ma il sistema mittente della richiesta non ha nessuna informazione diretta sulla avvenuta erogazione della prestazione.

6.2.5.2. Richiesta/risposta

Nello scenario *richiesta/risposta*, il fruitore trasmette all'erogatore un messaggio contenente una richiesta di prestazione di servizio. L'erogatore esegue il trattamento di erogazione della prestazione (dopo aver effettuato le verifiche di formato, sintattiche e semantiche) e trasmette un messaggio di risposta contenente il resoconto di erogazione e eventualmente i dati la cui fornitura è parte della prestazione.

Lo scenario richiesta/risposta coordina una modalità di erogazione della prestazione *sincrona* e *su iniziativa del fruitore*: l'erogazione della prestazione avviene sempre *all'occasione e dopo* la ricezione della richiesta e *prima* dell'emissione della risposta e la fruizione avviene *dopo* la ricezione della risposta. In compenso, le modalità dell'interazione (dal punto di vista del fruitore) che implementano lo scenario di richiesta/risposta possono essere invece sia sincrone che asincrone:

- *Richiesta/risposta sincrone*
  Nello scenario *richiesta/risposta sincrone*, il sistema fruitore prepara e emette il messaggio di richiesta della prestazione e blocca la sua linea di esecuzione in attesa della risposta. Alla ricezione della risposta la linea di esecuzione del fruitore, riprende l'esecuzione. . Lo scenario richiesta/risposta sincrone può essere implementato direttamente utilizzando uno scambio elementare di tipo *messaggio/replica sincroni*.

- *Richiesta/risposta asincrone*
  Negli scenari di *richiesta/risposta asincrone*, il fruitore del servizio prepara la richiesta di prestazione, la trasmette all'erogatore e continua l'esecuzione. La richiesta viene trasmessa al sistema erogatore che effettua le verifiche, esegue i trattamenti, prepara e emette la risposta. La ricezione della risposta ha come effetto presso il fruitore l'avvio di una linea di esecuzione indipendente che esegue i trattamenti conseguenti alla ricezione della risposta.
  Lo scenario richiesta/risposta asincrone può essere implementato utilizzando lo scambio elementare di tipo *messaggio/replica asincroni*. L'identificatore di correlazione messaggio/replica può essere utilizzato come identificatore di correlazione richiesta/risposta

6.2.5.3. Notificazione senza risposta

Nello scenario *notificazione senza risposta*, l'erogatore del servizio trasmette di sua iniziativa un messaggio di notificazione al fruitore (che può contenente il resoconto di un trattamento effettuato o la *notifica di un evento*). Lo scenario di notificazione senza risposta coordina una modalità di fruizione di servizio *asincrona* e *su iniziativa dell'erogatore*. Come la richiesta senza risposta, tale scenario può essere implementato usando uno scambio elementare di tipo *messaggio senza replica*.

6.2.5.4. Notificazione/risposta

Lo scenario di *notificazione/risposta* è simmetrico allo scenario *richiesta/risposta*: l'erogatore trasmette un messaggio di notificazione e successivamente il fruitore trasmette un messaggio di risposta. Lo scenario di notificazione/risposta coordina una modalità di fruizione *sincrona* e *su iniziativa dell'erogatore*. Come nel caso della richiesta/risposta la notificazione/risposta può essere implementata con modalità sincrona o asincrona e quindi essere implementato rispettivamente dallo scambio elementare messaggio/replica sincrono o asincrono.

6.2.5.5. Altri scenari di coordinamento

Per implementare trattamenti complessi e distribuiti tra più sistemi (*processi distribuiti*) in termini di scambio di prestazioni di servizio tra i detti sistemi, può essere necessario mettere in opera scenari complessi di coordinamento dello scambio di servizi.

Tutti gli scenari di coordinamento della prestazione di servizio, indipendentemente dalla loro complessità, devono essere costruiti esclusivamente a partire dalla composizione di interazioni elementari di tipo *messaggio senza replica*, *messaggio/replica sincroni*, *messaggio/replica asincroni*.

In una architettura di servizi, la realizzazione di processi distribuiti complessi può essere effettuata seguendo due approcci fondamentali:

- L'*orchestrazione dei servizi*
  L'orchestrazione dei servizi prevede l'implementazione, oltre ai sistemi e servizi partecipanti al processo distribuito, di un ulteriore servizio specializzato (e del sistema erogatore di detto servizio) di *coordinamento* dello scambio di prestazioni di servizio tra i sistemi patecipanti al processo e di *mediazione* dello scambio di messaggi tra detti sistemi.

Il *coordinatore/mediatore* non eroga servizi applicativi nell'ambito del processo, non implementa logica applicativa altra che quella che presiede al coordinamento del processo e alla cooperazione dei sistemi. Il coordinatore/mediatore è l'interlocutore unico di tutti i sistemi e, se il processo implementa l'erogazione di un servizio verso sistemi terzi, svolge il ruolo di erogatore di tali servizi, così come svolge il ruolo di erogatore di servizi di pilotaggio e di monitoraggio del processo. Tecnologie come WSBPEL [WSBPEL 0.1] permettono di implementare l'approccio di orchestrazione dei servizi

- La *coreografia dei servizi*
  La coreografia dei servizi richiede l'implementazione del coordinamento dello scambio di servizi tra i sistemi partecipanti al processo per mezzo di un *protocollo di conversazione* che ordina lo scambio dei messaggi tra detti sistemi (senza prevedere l'implementazione di un servizio dedicato a un ruolo di coordinatore/mediatore). Il protocollo di conversazione è una macchina a stati in cui le transizioni sono messaggi scambiati tra i sistemi partecipanti al processo. Tecnologie come WSCI [WSCI 1.0] permettono di implementare l'approccio di coreografia dei servizi.

L'approccio *orchestrazione* presenta dei vantaggi, rispetto all'approccio *coreografia*, in termini di maggiore leggibilità statica e di monitoraggio in esecuzione del processo. Questi vantaggi sono rilevanti in presenza di processi complessi. L'inconveniente è la necessità di implementare il coordinatore/mediatore, inconveniente che dovrebbe essere rapidamente rimosso dalla disponibilità di tecnologie specializzate (i motori di orchestrazione), basate su standards OASIS WSBPEL [WSBPEL 0.1].

L'approccio *coreografia* non necessita la presenza di un coordinatore/mediatore specializzato, ma può rivelarsi di difficile applicazione a processi di una certa complessità.

Modelli più specifici di coordinamento come la *catena di responsabilità* si rivelano adatti a processi totalmente sequenziali (vedi).

Un modello di coordinamento totalmente dinamico, e quello di pubblicazione/abbonamento (vedi § 9.1.6)

6.3. L'affidabilità dello scambio

Dato che nell'architettura SPCoop il coordinamento dell'erogazione/fruizione dei servizi è ottenuto esclusivamente attraverso lo scambio di messaggi, l'*affidabilità dello scambio* è un requisito di *qualità di servizio* (vedi § 7.5.3.3) che riveste una importanza particolare.

L'architettura SPCoop, come architettura distribuita in cui l'interazione tra sistemi è basata sullo scambio di messaggi, presenta dei problemi fondamentali di incertezza, che derivano:

- dall'attitudine propria dei sistemi partecipanti e delle connessioni componenti a cadere in avaria in modo indipendente gli uni dagli altri,
- dal tempo di latenza fondamentalmente imprevedibile delle connessioni.

Tali caratteristiche delle architetture distribuite provocano situazioni in cui, in una scambio elementare di tipo messaggio/replica, il richiedente, confrontato con l'assenza di risposta in un tempo dato, non è in grado di scegliere tra diverse ipotesi (non esclusive):

- la connessione utilizzata per la trasmissione del messaggio è in avaria,
- il rispondente è caduto in avaria dopo aver ricevuto il messaggio (sia prima di trattare il messaggio, sia mentre eseguiva il trattamento del messaggio oppure dopo aver trattato interamente il messaggio e prima dell'emissione della replica),
- la connessione utilizzata per la trasmissione della replica è in avaria,
- non ci sono avarie, ma semplicemente un tempo di latenza troppo lungo, e la replica deve ancora pervenire al richiedente.

Altre situazioni di incertezza si producono quando il richiedente cade in avaria dopo aver inviato il messaggio e prima di ricevere la replica e, dopo la ripartenza, "dimentica" di aver inviato il messaggio prima dell'avaria.

L'affidabilità dello scambio può essere migliorata in due modi:

- a livello fisico, con sistemi e connessioni più affidabili e di maggior rapidità e capacità;
- a livello infrastrutturale, con funzionalità che permettono di ridurre le incertezze descritte precedentemente.

L'affidabilità dello scambio a livello infrastrutturale è un insieme di funzionalità che permettono di garantire che, per ogni trasmissione di messaggio, si verifica solamente una delle due alternative seguenti (ad esclusione di tutte le altre):

- o il messaggio inviato dal mittente è effetivamente consegnato al destinatario,
- oppure il mittente riceve un resoconto *affidabile* della mancata consegna.

L'affidabilità dello scambio viene implementata per mezzo di

- protocolli di scambio specializzati,
- meccanismi distribuiti di persistenza transazionale dei messaggi in emissione e in ricezione; in particolare, tali meccanismi rendono lo scambio resistente alle avarie dei sistemi mittenti e destinatari.

I protocolli e meccanismi di scambio affidabile possono essere messi in opera:

- a livello *connessione*,
- a livello *porta*,
- a livello *servizio*.

A livello *connessione*, sono state effettivamente realizzate delle implementazioni di HTTP affidabile [HTTPR], che però non hanno raggiunto il grado di generalizzazione necessario per un protocollo a diffusione universale come HTTP.

A livello *porta*, nell'ambito delle tecnologie Web services, esistono due proposte concorrenti [WS-Reliability 1.1] [WS-ReliableMessaging] e un gruppo di lavoro OASIS (Web Services Reliable Messaging TC).

L'implementazione completa di protocolli e meccanismi di affidabilità dello scambio a livello *servizio* può essere ottenuta solo al prezzo di una complessificazione drastica della logica dei trattamenti dei sistemi partecipanti allo scambio.

Il piano di evoluzione dell'architettura SPCoop prevede la standardizzazione della affidabilità dello scambio a livello *porta*.

Allo stato attuale dell'architettura SPCoop, l'affidabilità completa dello scambio può essere ottenuta attraverso l'uso di protocolli e meccanismi Web services proprietari, ottenuti come estensioni degli standards esistenti e esplicitati nell'accordo tra i partecipanti allo scambio (per esempio in un dominio di cooperazione, vedi § 7.6.3) Per altro, la busta SPCoop prevede di ospitare le informazioni necessarie ai detti meccanismi e protocolli.

Una soluzione alternativa, raccomandata nella versione 1.0 dell'architettura SPCoop, consiste nell'implementare, a livello servizio, dei sistemi a *gestione implicita della sessione* che si scambiano dei *messaggi idempotenti*, ovvero dei messaggi la cui duplicazione produce lo stesso effetto del messaggio unico. I messaggi autosufficienti e idempotenti possono essere ricevuti in qualsiasi circostanza e contesto dal destinatario e permettono al mittente la ripetizione in caso di incidente di trasmissione o di incertezza.

6.4.La sicurezza

I meccanismi di sicurezza messi in opera nell'architettura SPCoop si applicano alla erogazione/fruizione del servizio e, in particolare, allo scambio dei messaggi. Tali meccanismi sono finalizzati al perseguimento di obiettivi come:

- La garanzia della riservatezza e confidenzialità dei dati amministrativi implicati nella collaborazione applicativa.
- Le necessità di imputabilità, di autenticazione e di non repudiabilità degli atti amministrativi e degli utenti e sistemi che li producono e concorrono a produrli.
- La protezione contro attacchi (intenzionali e no) da parte di utenti e sistemi che potrebbero prodursi anche in un ambiente protetto come il S.P. di Cooperazione.

Nella architettura SPCoop, i meccanismi di sicurezza si applicano alle *entità* coinvolte direttamente o indirettamente (via sistemi intermediari) nell'erogazione/fruizione dei servizi e nello scambio dei messaggi. Le entità in questione possono essere:

- *processori*,
- *componenti software* (applicativi o infrastrutturali),
- *utenti*.

Le entità posseggono un'*identità* rappresentata da un *codice identificatore* e un insieme di *attributi*. Occorre ribadire che l'architettura SPCoop organizza via lo scambio di servizi e di messaggi esclusivamente l'interazione tra sistemi e che quindi la partecipazione degli utenti all'erogazione/fruizione di servizi e lo scambio di messaggi è sempre *indiretta*.

I meccanismi di sicurezza messi in opera nell'architettura SPCoop implementano le seguenti funzionalità di sicurezza:

- *Autenticazione*:
  L'autenticazione delle entità è la prova dell'*identità* rivendicata dalle entità implicate direttamente o indirettamente nello scambio di messaggi e nella erogazione/fruizione dei servizi. L'autenticazione dei dati e messaggi è la garanzia che tali dati e messaggi sono stati effettivamente prodotti e emessi dalle entità che lo rivendicano.

- *Abilitazione/autorizzazione.*
  L'abilitazione e l'autorizzazione sono la prova, rispettivamente statica e dinamica, della *idoneità* delle entità, la cui identità è autenticata, all'erogazione/fruizione di servizi e all'accesso ai dati contenuti nei messaggi. L'abilitazione è la prova della idoneità generica a accedere (in erogazione e fruizione) a determinate funzionalità, mentre l'autorizzazione è la prova di tale idoneità in un determinato contesto di esecuzione. La distinzione serve generalmente a trattare le *liste nere*, cioè delle liste di entità a cui certe abilitazioni sono state ritirate dinamicamente in modo provvisorio o definitivo, oppure situazioni di eccezione.

- *Integrità.*
  L'integrità dei dati è la garanzia che i dati non possano essere modificati, in modo accidentale o intenzionale e, in ogni caso, non autorizzato, all'insaputa delle entità preposte alla produzione e al consumo di tali dati. Nel contesto dell'architettura SPCoop, la garanzia d'integrità riguarda i messaggi e le loro parti.

- *Riservatezza.*
  La riservatezza è la garanzia che le entità non autorizzate non possano accedere ai dati, ai messaggi e alle loro parti.

- *Non ripudiabilità.*
  La non ripudiabilità e la prova che una determinata azione è stata effettuata da una determinata entità, in un determinato contesto spazio/temporale di esecuzione.

- *Ispezione.*
  L'ispezione è la capacità di verificare staticamente e dinamicamente la tenuta dei requisiti di autenticazione, abilitazione/autorizzazione, integrità, riservatezza e non repudiabilità.

6.4.1. Tipologia dei rischi di attacco

I principali rischi di attacco a cui possono essere sottoposti i sistemi partecipanti al Sistema pubblico di cooperazione sono (lista non esaustiva):

- *Intrusione attraverso impersonificazione*: un'entità cerca di raggirare il processo di autenticazione e presentarsi sotto falsa identità (se l'attacco riesce, l'entità potrà accedere a dati e funzionalità anche senza esserne autorizzata). Le tecniche più usate per effettuare l'impersonificazione vanno dal *password guessing* sino allo sfruttamento delle anomalie presenti nel sistema operativo (presenti nel codice del sistema operativo o che possono essere state provocate in fase di configurazione). In presenza di meccanismi forti di autenticazione, la protezione ulteriore contro l'intrusione può essere ottenuta solo attraverso politiche rigorose di gestione degli

utenti e dei sistemi che esulano dal quadro specifico del Sistema Publico di Cooperazione

- *Abuso di privilegi*: un'entità sfrutta le vulnerabilità dei sistemi per accedere a funzionalità e dati al di là di ciò che è previsto nel suo profilo di autorizzazione ideale. Per evitare tale situazione occorre definire un meccanismo di controllo degli accessi.
- *Intercettazione dei dati*: un'entità cerca di acquisire dati senza essere autorizzata a farlo. Per ridurre il rischio devono essere implementate tecniche di *cifratura*.
- *Manomissione dei dati*: un'entità cerca di inserire dati non autentici alterando il contenuto dei messaggi. Per ovviare a questo attacco occorre che un controllo affidabile di eventuali manomissioni sia effettuato sistematicamente (controllo d'integrità).
- *Distruzione delle tracce*: un'entità all'origine di un attacco vuole evitare di essere identificata e/o che si ritrovi la traccia di talune operazioni che ha effettuato, quindi cerca di cancellare le tracce di tutte o parte delle operazioni effettuate. Per garantire l'imputabilità delle azioni devono essere custoditi con cura i giornali di tracciatura delle attività dei sistemi.
- *Riutilizzazione dei messaggi*: un'entità intercetta i messaggi trasmessi e li riutilizza effettuando nuovi invii. Per ovviare a questo attacco occorre che i produttori dei dati e i mittenti dei messaggi siano stati preventivamente autenticati, che i messaggi stessi siano identificati, autenticati e datati con garanzia di controllo di integrità.
- *Distruzione dei messaggi*: un'entità vuole evitare che vengano eseguite talune operazioni oppure vuole negare che esse siano state effettivamente richieste, attraverso la distruzione dei messaggi. Per prevenire tale tipo di attacco occorre garantire l'affidabilità dello scambio.

6.4.2. Sicurezza a livello trasporto, connessione e porta

I meccanismi di sicurezza sopraelencati possono essere messi in opera ai diversi livelli dell'architettura SPCoop/SPConn:

Livello *trasporto*	Il livello trasporto, implementato dal S.P. di Connettività, si basa sulla tecnologia IP. Il S.P. di Connettività fornisce le funzionalità di sicurezza IPsec che permettono: • l'*autenticazione* dell'origine e della destinazione dei pacchetti IP, • l'*autenticazione* dei pacchetti IP (l'origine), • l'*integrità* dei pacchetti IP, • la *riservatezza* dei pacchetti IP.

Livello *connessione*	Il livello connessione è implementato nel S.P. di Cooperazione e il protocollo imposto è HTTP 1/1. Il S. P. di Cooperazione implementa i protocolli di sicurezza SSL3 e TLS1 che permettono: • l'*autenticazione* reciproca dei punti di accesso (processori) che partecipano a una sessione HTTP, • l'*autenticazione del carico* delle richieste/risposte HTTP, • l'*integrità del carico* delle richieste/risposte HTTP. • la *riservatezza del carico* delle richieste/risposte HTTP.
Livello *porta*	Il livello porta è implementato sul S.P. di Cooperazione. Il protocollo imposto è SOAP 1.1. Il S.P. di Cooperazione implementa i meccanismi di sicurezza WS-Security [WS-Security 2004] che permettono: • l'*autenticazione delle entità* (macchine, applicazioni, utenti) che partecipano direttamente o indirettamente allo scambio di messaggi e all'erogazione/fruizione di servizi, • l'*autenticazione del contenuto* del messaggio (struttura SOAP 1.1/busta e-gov) o di parti di esso (in modo selettivo e differenziato), • la *riservatezza del contenuto* del messaggio o di parti di esso (in modo selettivo e differenziato), • l'*integrità del contenuto* del messaggio o di parti di esso (in modo selettivo e differenziato).

A livello *trasporto*, i protocolli IPsec permetto di implementare le *reti private virtuali* su una struttura di rete "pubblica" come Internet. Tali reti private virtuali possono essere messe in opera sul Sistema Pubblico di Connettività.

A livello *connessione*, i protocolli SSL e TLS permettono di implementare la sicurezza del canale che collega i punti di accesso di due sistemi. La sicurezza a livello "connessione" riguarda esclusivamente lo stabilimento della connessione e la trasmissione del carico (vedi Figura 2). Tali funzionalità di sicurezza sono sufficienti per soddisfare tutti i requisiti di sicurezza in una relazione di servizio *binaria* e per lo scambio di messaggi diretto e esclusivo tra l'erogatore e il fruitore.

Figura 2. Sicurezza a livello *connessione*.

In una architettura con più sistemi participanti, le funzionalità a livello connessione implementano quella che viene chiamata la sicurezza *punto a punto* (vedi Figura 3). Tale

architettura di sicurezza non resiste all'intrusione per impersonificazione: l'usurpazione riuscita dell'identità di S2 (attacco e presa di controllo) ha come conseguenze possibili la violazione della riservatezza e dell'integrità dei dati contenuti nei messaggi che transitano per S2.

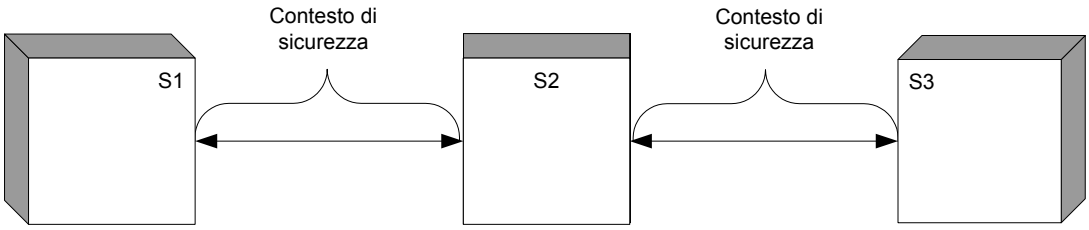


Figura 3. Sicurezza *punto a punto*.

Le funzionalità di sicurezza a livello *servizio* forniscono la sicurezza *da un estremo all'altro* (vedi Figura 4). Tale livello di sicurezza può essere indispensabile per mettere in opera un processo applicativo a cui partecipano più sistemi come erogatori/fruitori di servizi applicativi e infrastrutturali.

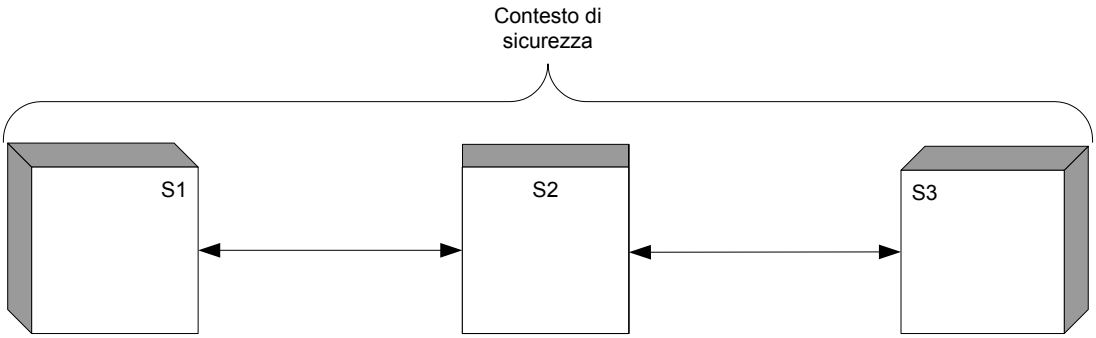


Figura 4. Sicurezza *da un estremo all'altro*.

Nel caso rappresentato dalla Figura 4:

- La *riservatezza da un estremo all'altro* vuol dire che S2 non può decifrare parti di messaggio che provengono da S1(S3) e sono destinati esclusivamente a S3 (S1). Tali dati o parti di messaggio sono cifrate da S1 (S3) in modo decifrabile solo da parte di S3 (S1).
- L'*integrità da un estremo all'altro* vuol dire che S2 non può modificare parti di messaggio provenienti da S1 (S3) a destinazione di S3 (S1) all'insaputa di S3 (S1).
- L'*autenticazione da un estremo all'altro* vuol dire che S2 non può usurpare l'identità di S1 o S3.
- La *non repudiabilità da un estremo all'altro* vuol dire che S3 (S1) è sicuro che una parte del messaggio viene da S1 (S3) e S1 (S3) non può negarlo.

6.4.3. Identificazione delle entità

L'identificazione univoca delle *entità* (processori, componenti software, utenti) che partecipano, in modo diretto e indiretto (attraverso sistemi intermediari), impersonando ruoli diversi, allo scambio di messaggi e alla erogazione/fruizione dei servizi è la condizione necessaria per implementare una qualsivoglia politica di sicurezza. Ogni entità non identificata la cui presenza e attività viene rilevata deve essere considerata come elemento che può arrecare pregiudizio al sistema.

L'identificazione delle entità coinvolte negli scambi di servizi e di messaggi segue le regole definite nel Sistema Pubblico di Cooperazione. Tutti i *processori* e i *componenti software* appartengono a un *dominio* (vedi) di cui un *soggetto della comunità del S.P. di Cooperazione* è titolare. Gli *utenti* sono sempre identificati sotto la responsabilità di un soggetto della comunità del S.P. di Cooperazione.

I *soggetti pubblici* (amministrazioni) e *privati* (imprese, associazioni) della comunità del S.P. di Cooperazione sono identificati (e autenticati) secondo le regole definite dagli standards SPCoop. Gli identificatori dei soggetti sono attribuiti centralmente dal Comitato di gestione del S.P. di Cooperazione e sono conformi a un formato URI specificato [URI]. SPCoop impone una procedura standard di gestione delle identità delle entità. Gli identificatori delle entità di cui un soggetto è responsabile sono attribuiti direttamente dal soggetto in questione in conformità al formato standard SPCoop.

I soggetti sono tutti registrati nel registro SICA nazionale generale (vedi 8.2.1).

Le richieste di registrazione dei soggetti, utenti, servizi, accordi di servizio, indirizzi dei punti di accesso sul registro SICA (nazionale generale) da parte di un utente autorizzato, devono essere autenticate mediante protocolli di autenticazione basati sull'uso di un certificato digitale in formato X.509 rilasciato da una autorità di certificazione centrale sotto la responsabilità del Comitato per l'SPC.

6.4.4. Meccanismi di autenticazione

I meccanismi di autenticazione sono messi in opera attraverso algoritmi e protocolli di *firma digitale* e di *calcolo di condensati* basati su una *infrastruttura a chiave pubblica*. L'autenticazione necessita quindi la partecipazione di servizi infrastrutturali (autorità di certificazione).

L'architettura SPCoop propone uno standard di infrastruttura a chiave pubblica e di servizi infrastrutturali di sicurezza SICA.

L'autenticazione a livello connessione (autenticazione dei punti di accesso) è messa in opera dai protocolli SSL3 o TLS1.

Per l'autenticazione a livello "servizio", SPCoop prescrive gli standards OASIS WS-Security [WS-Security 2004], che si appoggiano sugli standards W3C XML-Signature [XML Signature] e XML-Encryption [XML Encryption], e l'uso esclusivo del X509 token profile [WSS TP X509].

Ogni certificato digitale emesso deve contenere gli elementi minimi previsti da WS-Security (Subject, Key Identifier, serial number ed Issuer) e comunque il profilo del certificato deve

essere conforme al CPS previsto per lo scopo di certificazione. I CPS sono devono essere resi pubblici dalle infrastrutture a chiave pubblica autorizzate. Ai fini di verifica dello stato di validità del certificato, deve essere usato il protocollo OCSP [OCSP].

Per ogni messaggio di cui il destinatario richiede l'autenticazione (e quindi l'autenticazione del mittente), l'autenticazione reciproca del destinatario presso il mittente (*mutua autenticazione*) è obbligatoria.

6.4.5. Meccanismi di abilitazione/autorizzazione

Nell'ambito dell'erogazione/fruizione di prestazioni di servizio, i requisiti di abilitazione/autorizzazione possono riguardare i sistemi (processori e componenti software) erogatori e fruitori, diretti e indiretti, i sistemi terzi, erogatori di servizi infrastrutturali e di intermediazione (vedi § 9), gli utenti implicati nell'erogazione/fruizione del servizio. I requisiti di abilitazione/autorizzazione riguardano, per le posizioni di fruitori, diretti o indiretti, o di erogatori, diretti o indiretti, rispettivamente l'idoneità a usufruire o erogare determinati servizi.

Un meccanismo generale di abilitazione/autorizzazione necessità la messa in opera di:

- meccanismi di gestione delle *identità* (insiemi di attributi dotati di un codice identificatore) delle *entità* (macchine, applicazioni, utenti),
- meccanismi di *autenticazione* di dette entità,
- meccanismi di definizione di *ruoli* e di attribuzione dei detti ruoli alle entità,
- meccanismi di definizione di *azioni* e di associazione di dette azioni (da abilitare/autorizzare) ai ruoli (i ruoli sono abilitati /autorizzati a effettuare le azioni; la associazione può essere condizionata da regole contestuali.

L'architettura SPCoop V.1.0 non specifica un meccanismo standard di gestione delle abilitazioni/autorizzazioni. Meccanismi specifici possono essere messi in opera in contesti specifici di cooperazione applicativa.

6.4.6. Meccanismi di controllo di integrità

Il controllo di integrità dei dati e dei messaggi è realizzato attraverso l'uso di algoritmi e protocolli di calcolo di condensati e di firma digitale. La messa in opera di meccanismi di controllo di integrità necessita quindi la partecipazione di servizi infrastrutturali (infrastruttura a chiave pubblica, autorità di certificazione).

Il controllo d'integrità a livello *connessione* (integrità del carico HTTP) è messo in opera attraverso i protocolli SSL3 o TLS1.

Il controllo di integrità a livello servizio è messo in opera per mezzo delle tecnologie standard OASIS WS-Security [WS-Security 2004], che si appoggiano sugli standards di firma digitale W3C XML-Signature [XML-Signature].

L'architettura SPCoop specifica uno standard di infrastruttura a chiave pubblica e di servizi di sicurezza.

La firma digitale dei dati deve essere generata utilizzando le chiavi destinate a questo fine e contenute in un certificato digitale emesso da una autorità di certificazione qualificata nell'ambito del S.P. di Cooperazione. I sistemi coinvolti nella generazione/validazione delle firme devono essere in grado di verificare lo stato del certificato per mezzo del protocollo standard OCSP [OCSP].

6.4.7. *Meccanismi di riservatezza*

Dal punto di vista delle esigenze generali di riservatezza dei dati, l'architettura SPCoop distingue cinque categorie:

R1. *dato pubblico*,

R2. *dato interno* (al dominio del soggetto),

R3. *dato confidenziale*,

R4. *dato sensibile* (ai sensi del DL 196/2003),

R5. *dato riservato*.

Questa classificazione generale deve essere applicata ai dati contenuti nei messaggi.

I dati R3,R4,R5, per poter circolare in messaggi scambiati nel S.P. di Cooperazione, devono essere *cifrati* (e eventualmente condensati e firmati). Questa strategia si applica comunque ai dati personali sensibili e ai dati giudiziari (DL 196/2003).

I meccanismi di riservatezza sono messi in opera attraverso l'uso di algoritmi di *cifratura/decifratura*. La messa in opera di tali meccanismi di riservatezza necessita la partecipazione di servizi infrastrutturali (infrastruttura a chiave pubblica).

La riservatezza a livello *connessione* (riservatezza del carico) è messa in opera dai protocolli SSL3 o TLS1.

La riservatezza a livello *servizio* è messa in opera per mezzo delle tecnologie standard OASIS WS-Security [WS-Security 2004], basate sugli standards W3C XML-Encryption [XML-Encryption] e XML-Signature [XML-Signature]

SPCoop propone uno standard di infrastruttura a chiave pubblica e implementa dei servizi SICA (nazionale generale e secondari) di autorità di certificazione.

La cifratura/decifratura dei dati deve essere effettuata utilizzando le chiavi destinate a questo fine e contenute in un certificato digitale emesso da una autorità di certificazione qualificata nell'ambito del S.P. di Cooperazione. I sistemi coinvolti nella cifratura/decifratura devono essere in grado di verificare lo stato del certificato per mezzo del protocollo standard OCSP.

6.4.8. Meccanismi di imputabilità e di non ripudiabilità

L'imputabilità delle azioni delle entità identificate richiede la messa in opera di funzionalità di tracciatura L'architettura SPCoop specifica delle funzionalità di tracciatura che devono essere attivate in modo obbligatorio per ogni scambio di messaggi..

I meccanismi di non repudiabilità sono messi in opera attraverso algoritmi e protocolli di firma digitale, di calcolo di condensati, di marcatempo. La messa in opera meccanismi di non repudiabilità necessita la partecipazione di servizi infrastrutturali (per esempio, infrastrutture a chiave pubblica, autorità di certificazione, servizi marcatempo certificati).

L'architettura SPCoop V.1.0 non specifica un meccanismo standard di non ripudiabilità. Un dominio di cooperazione del S.P. di Cooperazione può specificare un meccanismo di non repudiabilità specifico.

6.4.9. Meccanismi di ispezione

I meccanismi di ispezione permettono di verificare staticamente e in esecuzione il corretto funzionamento dei meccanismi di sicurezza necessari alla erogazione/fruizione di servizi e allo scambio di messaggi. L'architettura SPCoop V.1 non specifica meccanismi standard di ispezione. Meccanismi specifici possono essere messi in opera in uno specifico contesto di cooperazione.

6.4.10. Classificazione dei servizi secondo le restrizioni di erogazione/fruizione

L'utilizzazione dei meccanismi di sicurezza permette una classificazione dei servizi a partire dalle restrizioni di erogazione/fruizione:

- *Servizi a erogazione/fruizione libera e anonima.*
  Sono servizi per cui non è richiesta l'identificazione di nessuna entità collegata direttamente o indirettamente ai sistemi erogatore e fruitore. **E' vietata la presentazione sul S. P. di Cooperazione di servizi a erogazione/fruizione libera e anonima.**

- *Servizi a erogazione/fruizione identificata.*
  I *servizi a fruizione identificata* sono servizi per cui è richiesta e messa in opera l'*identificazione* di entità collegate direttamente o indirettamente al sistema fruitore. I *servizi a erogazione identificata* sono servizi per cui è richiesta e messa in opera l'identificazione di entità collegate direttamente o indirettamente al sistema erogatore.

La mutua identificazione dei punti di accesso erogatore e fruitore a livello *connessione* è obbligatoria nel S.P. di Cooperazione.

- *Servizi a erogazione/fruizione autenticata.*
  Sono servizi per cui è messa in opera l'autenticazione dell'identità di entità collegate direttamente o indirettamente al sistema fruitore da parte di entità collegate direttamente o indirettamente al sistema erogatore. In questo caso, è obbligatoria sul S.P. di Cooperazione la mutua autenticazione delle entità coinvolte e allo stesso livello (trasporto, connessione, porta)

- *Servizi a erogazione/fruizione controllata.*
  I *servizi a fruizione controllata* sono servizi per cui è messa in opera l'identificazione, l'autenticazione, l'abilitazione e l'autorizzazione per l'accesso alla fruizione del servizio di entità collegate direttamente o indirettamente con il sistema fruitore (per esempio, di un utente la cui richiesta è all'origine di una richiesta di fruizione di servizio). I *servizi a erogazione controllata* sono servizi per cui è messa in opera l'identificazione, l'autenticazione e l'abilitazione/autorizzazione a partecipare all'erogazione del servizio di entità collegate direttamente o indirettamente con il sistema erogatore (per esempio di un utente la cui azione è all'origine di una risposta dell'erogatore).

- *Servizi a erogazione/fruizione non ripudiabile*
  I *servizi a fruizione non ripudiabile* sono servizi per cui è messa in opera la non ripudiabilità della partecipazione alla fruizione del servizio da parte di entità identificate, autenticate e autorizzate, collegate direttamente o indirettamente con il sistema fruitore. I *servizi a erogazione non ripudiabile* sono servizi per cui messa in opera la non ripudiabilità della partecipazione all'erogazione del servizio da parte di entità collegate direttamente o indirettamente al sistema erogatore (servizio non ripudiabile).

7. L'ACCORDO DI SERVIZIO (AS)

Nell'architettura SPCoop, per istaurare una relazione di servizio tra sistemi è obbligatorio definire un accordo esplicito sulla erogazione/fruizione delle prestazioni del servizio: l'*accordo di servizio*.

L'accordo di servizio (AS) porta sulle prestazioni del servizio e sulle modalità di erogazione/fruizione, ovvero più specificamente su:

- le *funzionalità* (classi di prestazioni) del servizio,
- le *interfacce* di scambio dei messaggi tra erogatore e fruitore,
- i *requisiti di sicurezza* dell'erogazione/fruizione,
- i *requisiti di qualità di servizio* dell'erogazione/fruizione.

I termini dell'accordo di servizio sono consegnati in un insieme di documenti, di cui una parte redatta in linguaggi formali e interpretabili da programma [WSDL 1.1]. Detto insieme di documenti costituisce una specifica per l'implementazione dei sistemi erogatore e fruitore. ed è utilizzato dai progettisti e dagli ambienti di sviluppo nelle fasi di implementazione dei sistemi erogatore e fruitore.

Alcune modalità operative dell'erogazione/fruizione del servizio possono essere lasciate non specificate al momento della progettazione e perfezionate automaticamente all'esecuzione - ciò richiede l'implementazione di capacità specifiche di contrattazione e di riconfigurazione dinamica da parte dei sistemi erogatore e fruitore. Un caso semplice di riconfigurazione dinamica si verifica quando l'URI del punto di accesso del sistema destinatario è sconosciuto al sistema mittente in esecuzione. In questo caso il mittente deve implementare una strategia dinamica di recupero dell'indirizzo (URI) del punto di accesso del destinatario, come per esempio l'interrogazione di un servizio di rubrica. Una modalità alternativa di recupero dell'URI è la trasmissione dello stesso nel contenuto del messaggio.

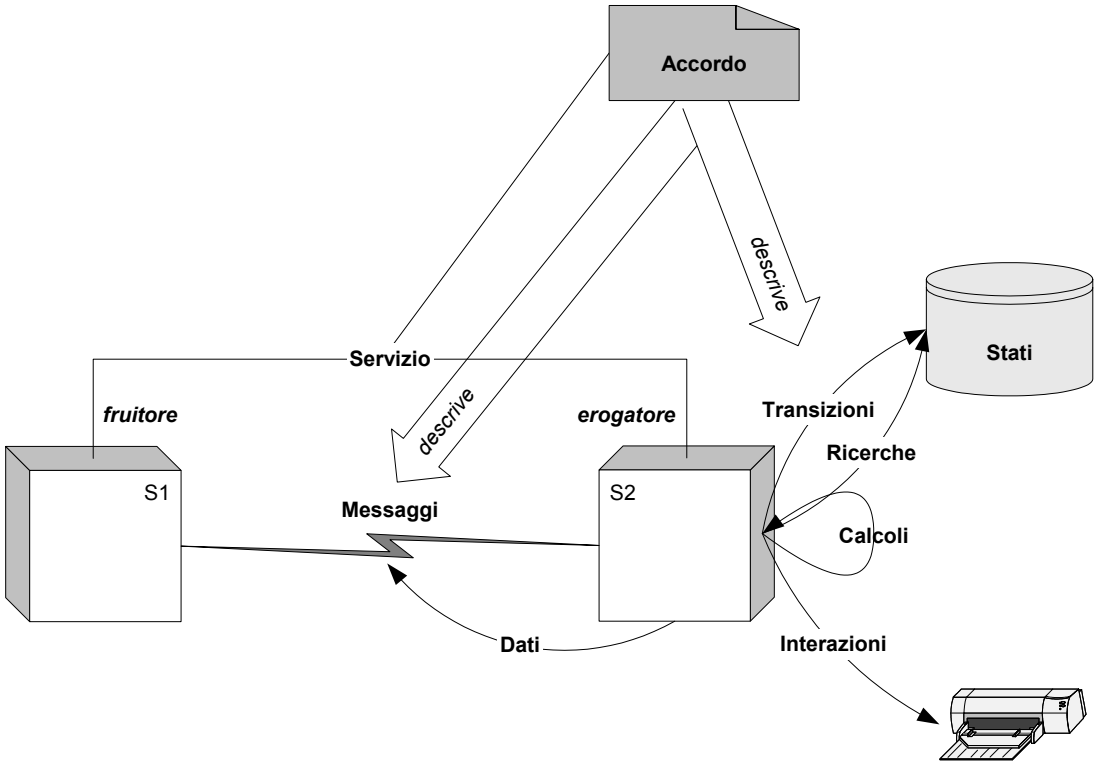


Figura 5. Accordo di servizio.

La rappresentazione dei termini dell'accordo di servizio in un insieme di documenti permette la dissociazione delle responsabilità di definizione del servizio da quelle dell'erogazione del servizio. Un servizio *standardizzato*:

- è definito da una autorità di definizione, che gestisce l'accordo e la pubblicazione dei documenti che ne rappresentano i termini,
- è erogato da uno o più sistemi erogatori, gestiti da differenti responsabili, che si impegnano a fornire prestazioni conformi con i termini dell'accordo di servizio.

L'accordo generale di un servizio standardizzato può essere incompleto: può limitarsi a definire le funzionalità, le interfacce, i requisiti di sicurezza e lasciare la definizione dei requisiti di qualità di servizio all'autonomia dell'offerta dei singoli erogatori o ad accordi specifici tra singoli fruitori e erogatori.

7.1. L'identificazione delle parti

L'accordo di servizio SPCoop impone l'identificazione delle parti coinvolte nella erogazione/fruizione del servizio.

Le parti in questione ricoprono i seguenti ruoli:

- Erogatori del servizio
- Fruitori del servizio
- Terzi (servizi di intermediazione e di supporto)

I titolari dei sistemi erogatori del servizio e dei servizi terzi devono essre identificati nell'accordo di servizio. I titolari dei sistemi fruitori possono essere identificati nell'accordo di servizio, e in ogni caso devono essere identificati (e registrati come fruitori) dagli erogatori e terzi.

I codici identificatori dei soggetti titolari sono conformi allo standard SPCoop, sono rilasciati esclusivamente dal Comitato di gestione del S.P. di Cooperazione e sono registrati sul registro SICA nazionale generale.

7.2. La descrizione delle funzionalità

L'accordo di servizio porta in primo luogo sulle funzionalità ovvero le *classi di prestazioni* fornite dall'erogatore del servizio. **L'accordo di servizio si limita alla descrizione puramente funzionale di tali classi di prestazioni: l'architettura, le tecniche e le risorse d'implementazione adottate dal sistema erogatore per fornire le prestazioni, cosi come quelle adottate dal sistema fruitore per utilizzare i risultati delle prestazioni, sono totalmente escluse dall'accordo (principio di occultamento dell'implementazione)**.

Lo standard di accordo di servizio SPCoop non impone né un linguaggio formale né un formato per la descrizione delle funzionalità del servizio.

7.3. La descrizione delle interfacce di scambio dei messaggi

La descrizione delle interfacce di scambio dei messaggi contiene:

- la descrizione degli eventuali protocolli di conversazione,
- la descrizione del formato del corpo e delle testate dei messaggi,
- la descrizione del *collegamento* con il protocollo di connessione,
- gli indirizzi (URI) dei punti di accesso,

e, infine, la descrizione delle relazioni funzionali tra i protocolli di conversazione, il contenuto dei messaggi e le modalità di erogazione/fruizione del servizio, cioè la descrizione della *semantica* (ciò che il mittente vuole significare con l'emissione del messaggio) e della *pragmatica* (ciò che il destinatario deve fare alla ricezione del messaggio).

L'accordo di servizio SPCoop V.1.0 non specifica un linguaggio standard per la descrizione dei protocolli di conversazione. Il piano di evoluzione dell'architettura e dell'accordo di

servizio SPCoop prevede l'introduzione in versioni successive di SPCoop del formalismo di orchestrazione OASIS WSBPEL [WSBPEL 0.1].

L'accordo di servizio SPCoop specifica il formalismo XML Schema [XML Schema] per la descrizione del formato del contenuto (corpo e testate) dei messaggi. L'accordo di servizio SPCoop V.1.0 prevede delle restrizioni, prescrizioni e raccomandazioni nell'uso dello standard XML Schema.

L'accordo di servizio SPCoop V.1.0 specifica come linguaggio di descrizione dei messaggi, delle connessioni e dei punti di accesso WSDL 1.1 [WSDL 1.1] con le restrizioni d'uso prescritte dalle raccomandazioni WS-I Basic Profile 1.1 [WS-I BP 1.1]. La specifica dell'accordo di servizio SPCoop fornisce gli elementi standard XML Schema e WSDL necessari alla generazione delle estensioni SOAP proprie alla Busta SPCoop.

Per la descrizione della semantica e della pragmatica dei messaggi, è raccomandato l'uso dell'approccio "Design by Contract" [DbC]. Tale approccio è particolarmente adatto per specificare le richiesta di prestazioni che producono transizioni di stato delle risorse gestite dall'erogatore. L'approccio "Design by Contract" prescrive, per ogni scenario di richiesta/risposta che coordina una transizione di stato, la definizione esplicita delle:

- *precondizioni*: condizioni verificabili prima della transizione e quindi prima della richiesta,
- *postcondizioni*: condizioni verificabili dopo la transizione, e quindi dopo la risposta contenete il resoconto della transizione,
- *invarianti*: condizioni sempre verificabili, prima e dopo la transizione.

La specifica dell'accordo di servizio SPCoop raccomanda la definizione, per ogni richiesta/risposta che coordina una transizione di stato, di richieste informative sulle precondizioni, postcondizioni e invarianti della transizione di stato. Tali richieste possono essere utilizzate in vario modo (per ispezione in esecuzione, per implementare degli scenari di test, ecc.).

7.4. La descrizione dei requisiti di sicurezza

I requisiti di sicurezza descritti nell'accordo di servizio SPCoop portano sull'uso dei protocolli e meccanismi standard di sicurezza del S. P. di Cooperazione e, eventualmente specificano l'uso di meccanismi specifici per prendere in conto problematiche di sicurezza per cui l'architettura SPCoop non specifica una soluzione standard.

I requisiti di sicurezza specificano quindi:

- L'uso dei meccanismi standard di *autenticazione*, ai livelli trasporto, connessione e porta.
- I meccanismi specifici di *abilitazione/autorizzazione*.
- L'uso dei meccanismi standard di *controllo di integrità*, ai livelli trasporto, connessione e porta.
- L'uso dei meccanismi standard di *riservatezza* ai livelli trasporto, connessione e porta.
- I meccanismi specifici di *non ripudiabilità*.

- I meccanismi e le regole di *ispezione*.

7.4.1. Requisiti di autenticazione

L'architettura SPCoop specifica una architettura di autenticazione (formati, protocolli e meccanismi, servizi di infrastruttura a chiave pubblica) ai livelli trasporto, connessione e porta delle entità che partecipano alla erogazione/fruizione delle prestazioni di servizio.

La specifica dell'accordo di servizio SPCoop V.1.0 non impone un linguaggio formale di descrizione dei requisiti di autenticazione ma raccomanda l'uso di formulari standardizzati.

Tali formulari sono dei documenti strutturati che permettono di specificare le entità da autentificare nella erogazione/fruizione delle prestazioni di servizio e i valori dei parametri dell'architettura standard di autenticazione SPCoop.

7.4.2. Requisiti di abilitazione/autorizzazione

L'architettura SPCoop V.1.0, non impone uno standard di gestione delle abilitazioni/autorizzazioni, né un linguaggio formale di descrizione dei requisiti di abilitazione/autorizzazione.

L'accordo di servizio può evidentemente specificare un sistema di gestione delle abilitazioni/autorizzazioni specifico. Tale sistema deve usare il sistema di gestione delle identità delle entità specificato dall'architettura SPCoop.

Se il meccanismo specifico di abilitazione/autorizzazione necessita la partecipazione di servizi di supporto, tali servizi devono essere definiti e i loro erogatori devono essere identificati nell'accordo di servizio.

7.4.3. Requisiti di controllo d'integrità

L'architettura SPCoop specifica una architettura di controllo di integrità (formati, protocolli e meccanismi, servizi di infrastruttura a chiave pubblica) ai livelli trasporto, connessione e porta dei dati e dei messaggi (o parti di essi) scambiati nel quadro della erogazione/fruizione di servizio.

La specifica dell'accordo di servizio SpCoop V.1.0 non impone un linguaggio formale di definizione dei requisiti di controllo di integrità, ma raccomanda l'uso di formulari standardizzati.

Tali formulari sono dei documenti strutturati che permettono di specificare i messaggi e le parti di messaggi su cui occorre esercitare il controllo di integrità, le entità coinvolte e i valori dei parametri dell'architettura standard SPCoop di controllo di integrità.

7.4.4. Requisiti di riservatezza

L'architettura SPCoop specifica una architettura di riservatezza (formati, protocolli e meccanismi, servizi di infrastruttura a chiave pubblica) ai livelli trasporto, connessione e porta dei messaggi (o di parti di essi) scambiati nel quadro della erogazione/fruizione delle prestazioni di servizio.

La specifica dell'accordo di servizio SpCoop V.1.0 non impone un linguaggio formale di definizione dei requisiti di controllo di integrità, ma raccomanda l'uso di formulari standardizzati.

Tali formulari sono dei documenti strutturati che permettono di specificare i messaggi e le parti di messaggi di cui occorre garantire la riservatezza, le entità coinvolte e i valori dei parametri dell'architettura standard SPCoop di riservatezza.

I formulari permettono di classificare i dati di cui occorre garantire la riservatezza secondo la classificazione presentata nel § 6.4.10.

7.4.5. Requisiti di imputazione e di non ripudiabilità

L'architettura SPCoop V.1.0, specifica una architettura di imputazione via dei formati, protocolli e meccanismi di tracciatura.

La specifica dell'accordo di servizio SpCoop V.1.0 non impone un linguaggio formale di definizione dei requisiti di imputazione, ma raccomanda l'uso di formulari standardizzati.

Tali formulari sono dei documenti strutturati che permettono di specificare i messaggi che devono fare l'oggetto di tracciatura, le entità coinvolte e i valori dei parametri dell'architettura standard SPCoop di tracciatura.

L'architettura SPCoop V.1.0 non impone uno standard di gestione della non ripudiabilità, né a maggior ragione un linguaggio formale di descrizione dei requisiti di non repudiabilità.

L'accordo di servizio può evidentemente specificare un sistema specifico di gestione della non repudiabilità. Tale sistema deve usare il sistema di gestione delle identità delle entità specificato dall'architettura SPCoop.

Se il meccanismo specifico di non repudiabilità necessita la partecipazione di servizi di supporto, tali servizi devono essere definiti e i loro erogatori devono essere identificati nell'accordo di servizio.

7.4.6. Requisiti di ispezione

L'architettura SPCoop V.1.0 non impone un'architettura standard (formati, protocolli, meccanismi) di ispezione, né a maggior ragione un linguaggio formale di descrizione dei requisiti di ispezione.

L'accordo di servizio può evidentemente specificare un sistema specifico di ispezione.

Se il meccanismo specifico che permette l'ispezione necessita la partecipazione di servizi di supporto, tali servizi devono essere definiti e i loro erogatori devono essere identificati nell'accordo di servizio.

7.5. La descrizione dei requisiti di qualità di servizio

I requisiti di qualità di servizio portano sulle *caratteristiche operative* (non funzionali) dell'erogazione/fruizione del servizio e dello scambio dei messaggi. I requisiti di qualità di servizio possono riguardare:

- i limiti quantitativi delle funzionalità del servizio: *volumetria*, *dimensionamento*, *accessibilità* del servizio;
- la qualità dei dati forniti dal servizio: *autenticità*, *coerenza*, *esattezza*, *precisione*, *freschezza*, *validità*;
- la robustezza dell'erogazione del servizio: *affidabilità*, *disponibilità*, *continuità*, *atomicità*, *isolamento*, *durevolezza* (qualità transazionali);
- la gestione dell'erogazione/fruizione del servizio: *tracciatura*, *monitoraggio*.

Determinati parametri della qualità di servizio possono essere contrattati e/o definiti dinamicamente tra l'erogatore e il fruitore nel contesto di esecuzione (ciò implica la capacità da parte dei sistemi a riconfigurare dinamicamente le modalità operative oggetto dell'accordo dinamico in esecuzione).

La specifica dell'accordo di servizio SpCoop V.1.0 non impone un linguaggio formale di definizione dei requisiti di qualità di servizio, ma raccomanda l'uso di formulari standardizzati.

7.5.1. Requisiti sui limiti quantitativi delle funzionalità

La descrizione dei limiti quantitativi delle funzionalità fornisce caratteristiche quantitative della erogazione di servizio che si traducono in impegni consegnati nell'accordo di servizio. L'accordo di servizio permette in questo caso di individuare direttamente gli indicatori che servono in seguito a misurare la tenuta dell'accordo.

7.5.1.1. Volumetria

I requisiti di volumetria si traducono in un insieme di impegni sulle quantità e le dimensioni (massime e minime) degli oggetti trattati nell'ambito della erogazione/fruizione del servizio. Esempio: lunghezza massima accettabile di un messaggio (quando l'informazione non può essere dedotta dallo schema XML del messaggio).

7.5.1.2. Dimensionamento

I requisiti di dimensionamento si traducono in un insieme di impegni sui tempi e i flussi di trattamenti (massimi e minimi, medie, varianze ...). Esempi:

- tempo di risposta massimo di una richiesta sincrona (fatto salvo il tempo di latenza della rete),
- numero massimo di richieste trattate nell'unità di tempo.

7.5.1.3. Accessibilità

I requisiti di accessibilità si traducono in un insieme di impegni sulla gestione statica e dinamica dei livelli di qualità di servizio. L'accordo di servizio può indicare dei livelli di priorità nella erogazione/fruizione del servizio, con delle garanzie di volumetria e dimensionamento per ogni livello di priorità.

Il problema per l'erogatore è prevenire problemi di saturazione e situazioni di inedia di fruitori a bassa priorità.

7.5.2. Requisiti sulla qualità dei dati

I requisiti di qualità dei dati si traducono in un insieme di impegni sulle caratteristiche dei dati forniti come parte dell'erogazione del servizio.

7.5.2.1. Autenticità e coerenza

Gli impegni sull'*autenticità* e la *coerenza* dei dati forniti riguardano i servizi che erogano funzionalità di informazione di stato, ovvero che forniscono dati a partire da risorse e sorgenti di dati il cui stato è soggetto a modifiche. Ci sono tre livelli di garanzia dell'autenticità e coerenza dei dati:

Isolamento perfetto delle letture
Il sistema erogatore si impegna a isolare perfettamente le letture dalle modifiche (inserzioni, aggiornamenti, cancellazioni) delle risorse che gestisce. I dati forniti sono autentici e coerenti, nel senso che corrispondono strettamente a stati prodotti da transazioni di modifica atomiche, isolate e durevoli. Questa garanzia richiede la messa in opera di strategie costose (come il *two-phase locking* – i *locks* sui dati implicati in una transazione sono rimossi solo dopo essere stati tutti collocati) di tutte le risorse implicate in una interrogazione anche complessa (al costo dei locks si aggiunge il costo della sequenzializzazione delle transazioni di aggiornamento rispetto a quelle di lettura).

Stabilità del cursore
I *locks* sono collocati in lettura ma senza rispettare il principio *two-phase locking* (sono collocati solamente per il tempo necessario alla lettura del dato unitario e rimossi subito dopo). I dati possono essere incoerenti (afferenti a stati diversi), ma sono autentici. La strategia, che

funziona per la consolidazione statistica di dati afferenti a stati di scarsa variabilità, non è molto costosa (evita di sequenzializzare le transazioni di aggiornamento).

Letture "sporche"
La strategia delle letture dette sporche non prevede la collocazione di *locks* sui dati. I dati letti possono essere non autentici (possono non afferire a nessuno stato "legale" delle risorse ma solo a stati transitori) e, ovviamente, essere incoerenti (afferenti a stati diversi). Questa strategia, molto poco costosa, funziona, come le "stabilità del cursore", per la consolidazione statistica di dati afferenti a stati di scarsa variabilità.

La specifica dell'accordo di servizio SPCoop *raccomanda* l'indicazione del livello di qualità delle letture per ogni servizio con funzionalità di informazioni di stato.

7.5.2.2. Esattezza e precisione

L'*esattezza* e la *precisione* sono caratteristiche dei dati di tipo numerico. L'accordo di servizio può specificare impegni sulla misura dell'errore dei dati (deviazione rispetto al valore teorico esatto), sul numero di cifre dopo la virgola, sul livello di precisione a virgola mobile, ecc. Parte di questi impegni possono essere specificati negli schemi XML dei dati.

L'esattezza e la precisione dei dati numerici deve essere considerata con attenzione dato che è una delle cause principali di mancanza di interoperabilità tra sistemi a implementazione eterogenea (esempio: Java e .NET). In effetti, la trasformazione tra il formato XML e i formati interni, propri ai vari ambienti di esecuzione, non è generalmente standardizzata (soprattutto nei valori di *default*).

7.5.2.3. Freschezza e validità

La *freschezza* riguarda i dati forniti su iniziativa dell'erogatore (*notificazione*) e è la misura del rapporto tra l'intervallo in cui sono utilizzabili (tra la notificazione ricevuta e l'obsolescenza del dato) e l'intervallo totale (tra la creazione e l'obsolescenza). La freschezza misura l'impegno alla "reattività" di un servizio di notificazione.

La *validità* riguarda i dati forniti su richiesta del fruitore ed è la misura del rapporto tra l'intervallo tra la richiesta e la risposta e l'intervallo totale (tra la richiesta e l'obsolescenza). La validità misura l'impegno alla "reattività" di un servizio di interrogazione.

7.5.3. Requisiti sulla robustezza dell'erogazione

La robustezza è un insieme di requisiti sulle capacità dell'erogatore a restare "in servizio" e a fornire garanzie di buon funzionamento nei casi in cui si producono interruzioni nel servizio.

7.5.3.1. Affidabilità funzionale

L'affidabilità funzionale è un impegno in termini di *numero massimo di anomalie funzionali constatabili in un intervallo di tempo*. Gli impegni sull'affidabilità funzionale devono essere collegati con gli impegni sulla gestione delle anomalie e in generale sul ciclo di vita dell'erogatore.

7.5.3.2. Affidabilità dei sistemi

E' il complemento della probabilità di cadere in avaria del sistema erogatore. L'affidabilità dei sistemi viene tradotta in termini di MTTF (Mean Time To Failure), il tempo medio tra due avarie. La misura contribuisce alla determinazione della disponibilità del sistema erogatore (vedi § 7.5.3.4).

7.5.3.3. Affidabilità dello scambio

L'affidabilità dello scambio è stata introdotta nel § 6.3. Nell'accordo di servizio vanno precisati gli impegni sulle caratteristiche di detta affidabilità, e cioè:

La *consegna dei messaggi* (il messaggio viene consegnato al destinatario, oppure il mittente riceve un resoconto affidabile della mancata consegna).

L'*eliminazione dei doppioni* (il messaggio viene consegnato una sola volta).

Il *rispetto della sequenza* (i messaggi vengono consegnati nel rispetto della sequenza stretta – senza buchi - di emissione).

Gli impegni sulle caratteristiche listate configurano le politiche di affidabilità dello scambio presentate nella tabella seguente.

	GARANZIA DI CONSEGNA	ELIMINAZIONE DEI DOPPIONI	RISPETTO DELLA SEQUENZA
A1 (At most once)	NO	SI	NO (solo relazione d'ordine)
A2 (At least once)	SI	NO	NO
A3 (Exactly once)	SI	SI	SI
A4 (Exactly once + sequence)	SI	SI	SI
A5 (Exactly once + priority management)	SI	SI	SI (per classi di priorità dei messaggi)

Tabella 3. Livelli di affidabilità dello scambio.

A1. (*At most once*)
La politica A1 è direttamente implementata dall'uso standard dei tipi di scambio elementare (vedi § 6.2.3), con l'accortezza di non rinviare il messaggio in caso di

incidente di trasmissione o di tempo scaduto (il che esclude la possibilità di doppioni). La sequenza di emissione può essere rispettata solo come relazione d'ordine.

A2. (*At least once*)
L'invio del messaggio è ripetuto fino a ottenere riscontro positivo. Tale politica, applicata con messaggi è funzionalmente *idempotenti* (la coppia mittente/destinatario tollera i doppioni a livello *servizio*) e *auto-contenuti* (il ricevente implementa la gestione implicita della sessione, vedi § 6.2.4) permette di ottenere un livello elevato di affidabilità.

A3. (*Exactly once*)
La politica A3 richiede l'implementazione della gestione dell'identità esplicita e della persistenza transazionale dei messaggi sia presso il mittente che presso il destinatario. Il "motore" distribuito di gestione dello scambio affidabile si occupa della ripetizione della trasmissione su riscontro di errore o tempo scaduto e della eliminazione dei doppioni.

A4. (*Exactly once + sequence*)
La politica A4 aggiunge alla A3 la gestione della coerenza stretta tra sequenza di emissione e sequenza di ricezione. Ciò vuol dire che il "motore" ricostruisce in ricezione le sequenza stretta dei messaggi prima di consegnarli al programma applicativo (un messaggio non può essere consegnato al programma applicativo se *tutti* i suoi predecessori non sono stati consegnati).

A5. (*Exactly once + priority management*)
La politica A5 aggiunge alla A4 la gestione dei messaggi per gruppi di priorità (la sequenza è stretta tra i messaggi della stessa priorità). I messaggi ad alta priorità sono privilegiati, ma occorrono requisiti che scartano il pericolo di situazioni di inedia dei messaggi a bassa priorità.

7.5.3.4. Disponibilità

Gli impegni di disponibilità riguardano la capacità dell'erogatore a restare "in servizio" una certa percentuale di un intervallo di tempo. Nell'ambito dell'impegno di disponibilità, il tempo necessario al ristabilimento della erogazione dopo una interruzione (MTTR – *Mean Time To Repair*) è molto importante. La disponibilità è quindi la percentuale del tempo in cui l'erogatore è effettivamente "in servizio" e viene constatata e misurata sul periodo di servizio (che può non essere continuo) come MTTF/(MTTF+MTTR).

La classificazione usuale di disponibilità dei sistemi, descritta nella tabella seguente è perfettamente applicabile alla erogazione dei servizi.

Livello di gestione della disponibilità	Classe di sistema	Disponibilità	Indisponibilità annuale	Indisponibilità settimanale
Unmanaged	1	90%	< 52 560minuti	< 1008minuti
Managed	2	99%	< 5 256minuti	< 101,08minuti
Medium	3	99,9%	< 526minuti	< 10,11minuti
Fault tolerant	4	99,99%	< 53minuti	< 1,01minuti
High Availability	5	99,999%	< 5minuti	< 0,1minuti
Very high availability	6	99,9999%	< 0,5minuti	< 0,01minuti
Very very high availability	7	99,99999%	< 0,05minuti	< 0,001minuti

Tabella 4. Livelli di sisponibilità del servizio.

Gli impegni di disponibilità sono differenti degli impegni di *accessibilità* del servizio (vedi § 7.5.1.3) - un erogatore può essere in servizio ma inaccessibile per causa *saturazione*).

7.5.3.5. Continuità

La continuità di servizio è l'insieme di impegni dell'erogatore sugli arresti e le riprese dell'erogazione del servizio, tendenti a garantire un certo livello di continuità.

L'impegno alla continuità di servizio può essere organizzato per livelli:

C0. *Nessuna gestione della continuità*
In caso di interruzione del servizio, l'erogatore si impegna al più su un tempo massimo di ristabilimento del servizio e non fornisce nessun processore o punto d'accesso alternativo. In questo caso, l'onere della gestione della continuità grava interamente sul fruitore, che deve effetuare dei test per sapere se il processore e/o il punto di accesso è di nuovo in servizio.

C1. *Retry-on-failure*
In caso di interruzione del servizio, l'erogatore si impegna a fornire un processore e/o un punto d'accesso alternativo (eventualmente dopo un certo tempo massimo). Il fruitore può trovare l'indirizzo del punto di accesso alternativo su una rubrica degli indirizzi dei servizi. La pratica usuale per il fruitore è di ricercare sul registro dei servizi l'indirizzo (URI) del punto di accesso dell'erogatore e di memorizzarlo localmente. In caso di indisponibilità constatata, il fruitore accede di nuovo alla rubrica per ottenere l'indirizzo del punto di accesso alternativo.

C2. *Notification*
L'erogatore notifica al fruitore l'imminenza di un arresto improvviso o programmato e si impegna a fornire un processore e/o punto di accesso alternativo di cui comunica l'indirizzo al fruitore. Il fruitore riconfigura l'accesso al nuovo indirizzo. Questo livello di gestione della continuità funziona se il fruitore e in grado di ricevere notificazioni.

C3. *Fail over*

L'erogatore gestisce interamente e totalmente la continuità di servizio, nel senso che l'arresto di tutto o parte del sistema erogatore è trasparente per il fruitore. L'impegno *fail over* dell'erogatore richiede dei meccanismi di scambio automatico verso il sistema erogatore alternativo, che nel caso di servizi con funzionalita di informazione o di gestione di stato (vedi § 6.1.2) deve essere implementato come un sistema speculare al sistema indisponibile.

7.5.3.6. Gestione delle transazioni (atomicità, isolamento, durevolezza)

Gli impegni di gestione transazionale dell'erogatore riguardano le funzionalità di gestione di stato (vedi § 6.1.2) Si tratta dell'impegno a che il trattamento che segue una richiesta esegue una transizione di stato dotata di tutte le (o parte delle) caratteristiche transazionali classiche di *atomicità*, *isolamento* e *durevolezza*.

- *Atomicità.*
  La transizione invocata dalla richiesta deve essere indivisibile, ovvero deve essere effettuata interamente o non deve essere effettuata affatto. Gli stati intermedi tra lo stato iniziale e lo stato finale non possono mai divenire stati finali (sono provvisori e inaccessibili all'esterno del processo di transizione, salvo alle letture "sporche" – vedi § 7.5.2.2). Se la transizione è interrotta e non può riprendere, deve *fallire*: gli stati intermedi provvisori eventualmente già prodotti devono essere soppressi.

- *Isolamento.*
  La transizione invocata dalla richiesta in genere riguarda stati di risorse a accesso concorrente fra i fruitori del servizio, che sono in competizione per l'allocazione di dette risorse. La transizione deve essere isolata, nel senso che le risorse su cui opera la transizione devono essere allocate in modo esclusivo al trattamernto della richiesta. L'isolamento è ottenuto per mezzo del *lock* delle risorse coinvolte nella transizione (il cui stato sarà modificato dalla transizione) e l'isolamento totale è ottenuto attraverso la strategia del *two-phase locking* (vedi § 7.5.2.1): tutti i *lock* necessari sulle risorse implicate nella transizione sono collocati prima di cominciare a essere rimossi.
  L'isolamento mette in sequenza due transazioni concorrenti. Un impegno più gravoso da parte del fruitore è la garanzia della coerenza tra sequenzialità delle richieste e sequenzialità delle transazioni (la transazione invocata dalla richiesta immediatamente successiva viene eseguita immediatamente dopo – senza inserimenti - la transazione invocata dalla richiesta immediatamente precedente). L'impegno di stretta sequenza delle transazioni richiede il trattamento esplicito del *deadlock* (per mezzo del fallimento della transazione). Una politica alternativa è il trattamento trasparente del *deadlock* (se la transazione fallisce per *deadlock*, le richiesta originaria è rimessa in coda senza avvertire il richiedente).

- *Durevolezza.*
  La durevolezza degli stati è un insieme di impegni sulla permanenza degli stati (prodotti dalle transazioni) in presenza di interruzioni del sistema erogatore e di avarie del sistema di memorizzazione. Gli stati devono essere persistenti, devono cioè poter persistere in presenza dell'arresto temporaneo del sistema erogatore. La durevolezza è un impegno superiore di permanenza degli stati che devono poter persistere in presenza della avaria

o distruzione parziale del sistema di memoria di massa (ottenuta per mezzo della ridondanza di detti sistemi).

7.5.4. Requisiti di controllo e ispezione dell'erogazione/fruizione

La gestione dell'erogazione/fruizione è un insieme di funzionalità gestione del servizio che l'erogatore mette a disposizione del fruitore e di servizi terzi.

7.5.4.1. Tracciatura

La tracciatura dei messaggi è una funzionalità infrastrutturale standard dell'architettura SPCoop (vedi § 8.1.1). Il livello di tracciatura dell'erogazione fruizione del servizio deve essere specificato nell'accordo di servizio.

7.5.4.2. Monitoraggio

L'architettura SPCoop non specifica un ciclo di vita standard né dell'erogazione/fruizione del servizio nella sua globalità né delle singole prestazioni. Un accordo di servizio SPCoop può prevedere delle funzioni specifiche di monitoraggio della erogazione/fruizione del servizio e delle singole prestazioni. Tali funzioni devono essere implementate come delle prestazioni di servizio e quindi descritte in conformità con la specifica dell'accordo di servizio SPCoop.

7.6. Concetti organizzativi

L'erogazione/fruizione di un servizio sul S.P. di Cooperazione è effettuta in conformità con un accordo di servizio preliminare, i cui contenuti sono stati presentati nel paragrafo precedente.

Qesto paragrafo introduce dei concetti organizzativi (soggetti, ruoli, procedure e processi), che sono descritti in modo esauriente in un documento separato sull'organizzazione e le regole di funzionamento del S. P. di Cooperazione, che servono a comprendere la tipologia degli accordi di servizio (e dei servizi descritti).

7.6.1. Dominio

Il *dominio* di un *soggetto* (*pubblico* o *privato*) della *comunità* del S.P. di Cooperazione è l'insieme dei *sistemi* di cui il soggetto è titolare o responsabile. Per sistema, nella sua accezione più ampia, si intende l'implementazione di un trattamento informatico realizzata da o per un soggetto

(pubblico o privato), *titolare* del sistema, al fine di soddisfare una specifica necessità applicativa (amministrativa e istituzionale) o infrastrutturale (tecnica e di supporto al funzionamento dei sistemi applicativi).

I sistemi di un dominio possono essere:

- *erogatori di servizi inter-dominio*, di cui usufruiscoino sistemi di altri domini – l'erogazione/fruizione di tali servizi è messa in opera sul S.P. di Cooperazione, in conformità con l'architettura SPCoop e utilizzando le tecnologie standard SPCoop;
- *fruitori di servizi inter-dominio*, erogati da sistemi appartenenti a altri domini – l'erogazione/fruizione di tali servizi è messa in opera sul S.P. di Cooperazione, in conformità con l'architettura SPCoop e utilizzando le tecnologie standard SPCoop;
- *erogatori di servizi intra-dominio*, di cui usufruiscono altri sistemi all'interno del dominio – l'erogazione/fruizione di tali servizi è messa in opera sul S.P. di Cooperazione, in conformità con l'architettura SPCoop e utilizzando le tecnologie standard SPCoop;
- *fruitori di servizi intra-dominio*, erogati da altri sistemi dello stesso dominio, la cui erogazione/fruizione è messa in opera sul S.P. di Cooperazione, in conformità con l'architettura SPCoop e utilizzando le tecnologie standard SPCoop;
- *interni* - tali sistemi non partecipano direttamente alla erogazione/fruizione di servizi messa in opera sul S.P. di Cooperazione.

7.6.2. *Dominio dei servizi applicativi (DSA)*

Il dominio dei servizi applicativi di un soggetto (pubblico o privato) della comunità S.P. di Cooperazione è l'insieme dei servizi erogati sul S.P. di Cooperazione dai sistemi del suo dominio.

7.6.2.1. I servizi presentati e erogati sul S.P. di Cooperazione

In conformità con il modello dell'architettura SPCoop, la cooperazione di sistemi appartenenti a domini distinti è possibile solo se detti sistemi:

- entrano in relazioni di servizio in conformità con l'architettura SPCoop - tali relazioni di servizio sono rette da accordi di servizio formalizzati e conformi al modello di accordo di servizio SPCoop,
- coordinano l'erogazione/fruizione di detti servizi esclusivamente per attraverso scambi di messaggi in conformità con l'architettura SPCoop.

Peraltro, i sistemi di uno stesso dominio possono scegliere di cooperare tra di loro utilizzando il modello di architettura, gli standard tecnici e i servizi SPCoop e il S.P. di Connettività come base dello scambio di messaggi. L'uso del S.P. di Connettività per la connessione dei sistemi intra-dominio è incoraggiata per i soggetti pubblici, laddove la scelta è appropriata dal punto di vista tecnico (per esempio, in presenza di sistemi appartenenti a una amministrazione centrale ma localmente distribuiti sul territorio nazionale). Per i soggetti

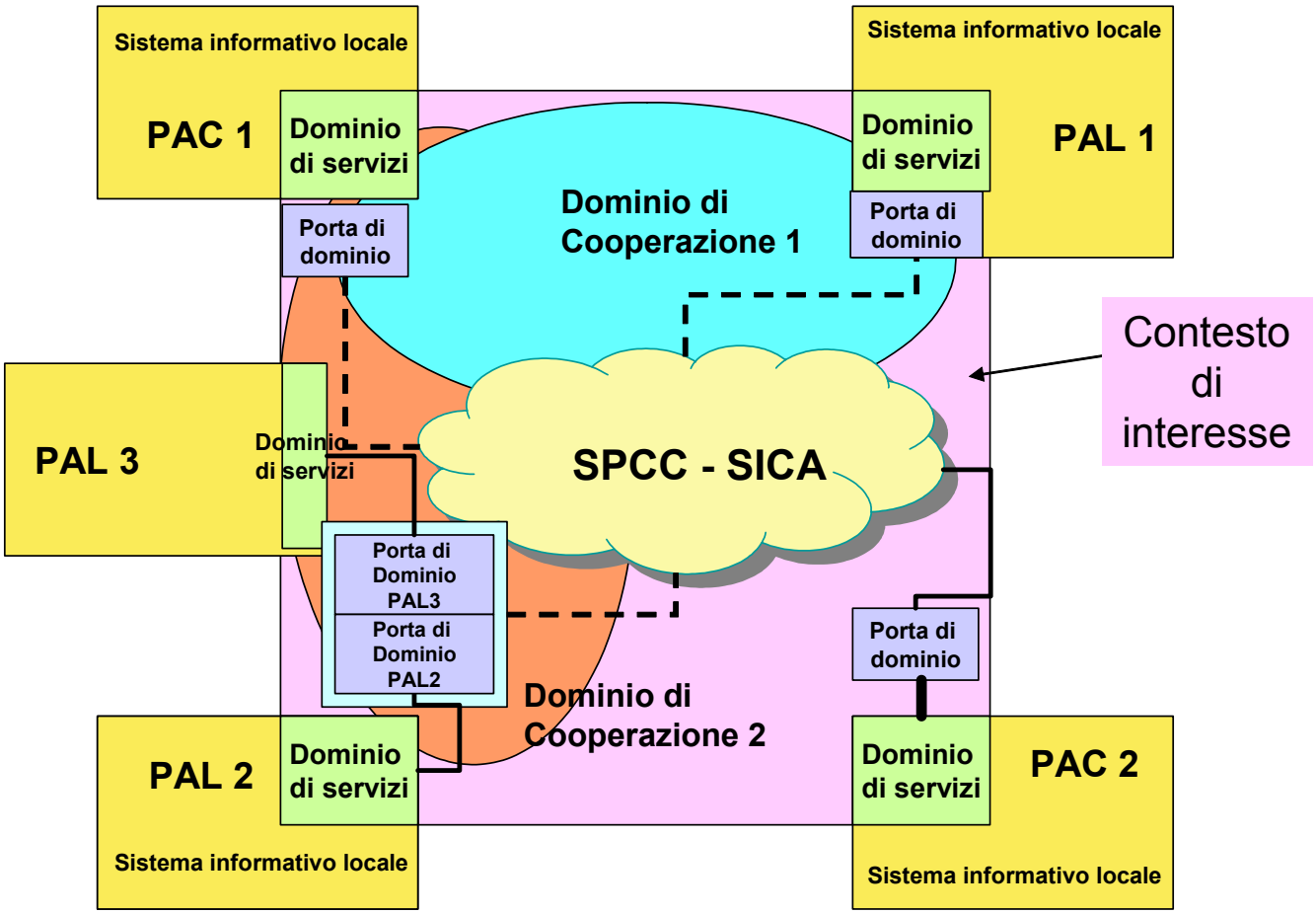
privati della comunità del S.P. di Cooperazione, l'uso dell'infrastruttura S.P. di Connettività per la connessione di sistemi intra-dominio è permessa previa qualificazione.

L'architettura SPCoop specifica un insieme unitario di servizi infrastrutturali standardizzati di supporto all'erogazione/fruizione dei servizi applicativi sul S.P. di Cooperazione, denominati Servizi Infrastrutturali di Interoperabilità, Cooperazione e Accesso (SICA – vedi § 8.2).

Gli *accordi di servizio* dei SICA sono pubblicati come standards SPCoop.

I SICA sono erogati sia:

- a *livello generale* come servizi nazionali generali (**SICA nazionali generali**), erogati da sistemi di cui è titolare il Comitato di gestione SPC, e accessibili come servizi SPCoop da parte tutti i sistemi che partecipano al S.P. di Cooperazione in conformità dei requisiti di controllo di accesso e le abilitazioni/autorizzazioni di tali sistemi, e come servizi all'utente (via una interfaccia utente) a tutti gli utenti afferenti ai soggetti della Comunità S.P. di Cooperazione, in conformità con i requisiti di controllo di accesso e le abilitazioni/autorizzazioni degli utenti;
- a *livello secondario* come servizi distribuiti (**SICA secondari**), erogati da sistemi di cui sono titolari soggetti specifici della comunità S.P. di Cooperazione – di tali servizi usufruiscono i sistemi della comunità S.P. Cooperazione, in conformità con accordi di servizio specifici – i SICA secondari sono conformi agli standard SICA e sono registrati obbligatoriamente nel registro nazionale generale dei servizi (SICA nazionale).



7.6.2.2. Definizione e erogazione dei servizi applicativi del S.P. di Cooperazione

La definizione di un servizio è il processo organizzativo il cui prodotto è l'*accordo di servizio*.

L'accordo di servizio è generalmente composto di un *accordo generale di servizio* (AGS), identifica le parti e formalizza gli elementi della descrizione del servizio (funzionalità, interfacce, requisiti di sicurezza, requisiti di qualità di servizio).

La qualità di servizio può fare l'oggetto di *accordi particolari* che precisano l'AGS. Chiameremo detti accordi particolari:

- *Accordo di livello di servizio* (LDS): il livello di servizio specifica determinate modalità operative di erogazione (come il tempo di latenza massimo, il livello di disponibilità e di continuità di servizio).
- *Accordo di livello di utilizzo* (LDU): il livello di utilizzo del servizio specifica determinate modalità operative di fruizione, come per esempio il numero massimo di richieste effettuabili nell'unità di tempo.

I servizi applicativi del S.P. di Cooperazione si distinguono, dal punto di vista della portata della loro erogazione/fruizione, in 4 classi:

- *Servizi mono-erogatore/mono-fruitore*
  Il servizio è erogato dal un solo sistema erogatore indipendente, di cui è titolare un soggetto della comunità S. P. Cooperazione, per la fruizione da parte di un unico altro sistema indipendente di cui il titolare è - nel caso di un servizio inter-dominio – un altro soggetto della comunità. Il titolare del sistema erogatore ha la responsabilità di gestione del ciclo di vita dell'accordo di servizio (indipendentemente dalle modalità del processo di definizione che ha condotto all'accordo) e dell'erogazione del servizio in conformità con l'accordo. Il titolare del sistema fruitore è responsabile della fruizione del servizio nei termini dell'accordo (e specificamente dell'accordo sul livello di utilizzo, che è direttamente integrato nell'accordo generale di servizio).

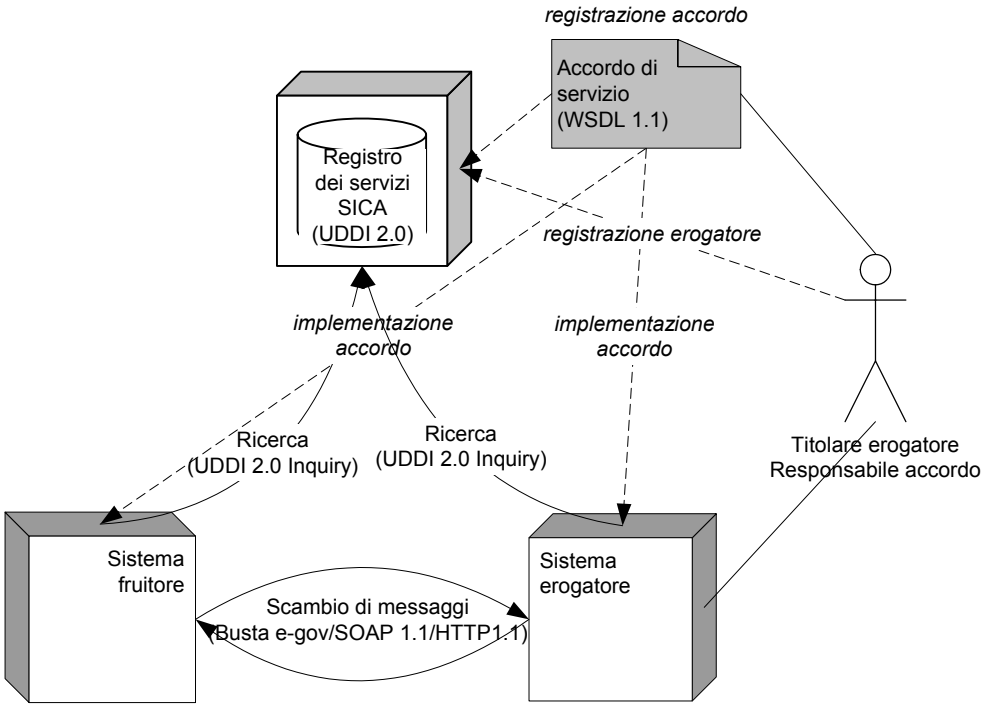


Figura 6. Servizio mono-erogatore/mono-fruitore.

- *Servizi mono-erogatore/multi-fruitore*
  Il servizio è erogato da un solo sistema erogatore indipendente, di cui è titolare un soggetto della comunità S.P. Cooperazione, e destinato alla fruizione di una classe di sistemi indipendenti (i fruitori) di cui sono responsabili - nel caso di servizio inter-dominio – altri soggetti della comunità S.P. Cooperazione. Il titolare del sistema erogatore ha la responsabilità di gestione del ciclo di vita dell'accordo di servizio (indipendentemente dalle modalità del processo che ha condotto all'accordo) e dell'erogazione del servizio in conformità con l'accordo. Ogni titolare di sistema fruitore è responsabile della fruizione del servizio nel rispetto dei termini dell'accordo generale di servizio (e eventualmente di accordi specifici sul livello di utilizzo del servizio).

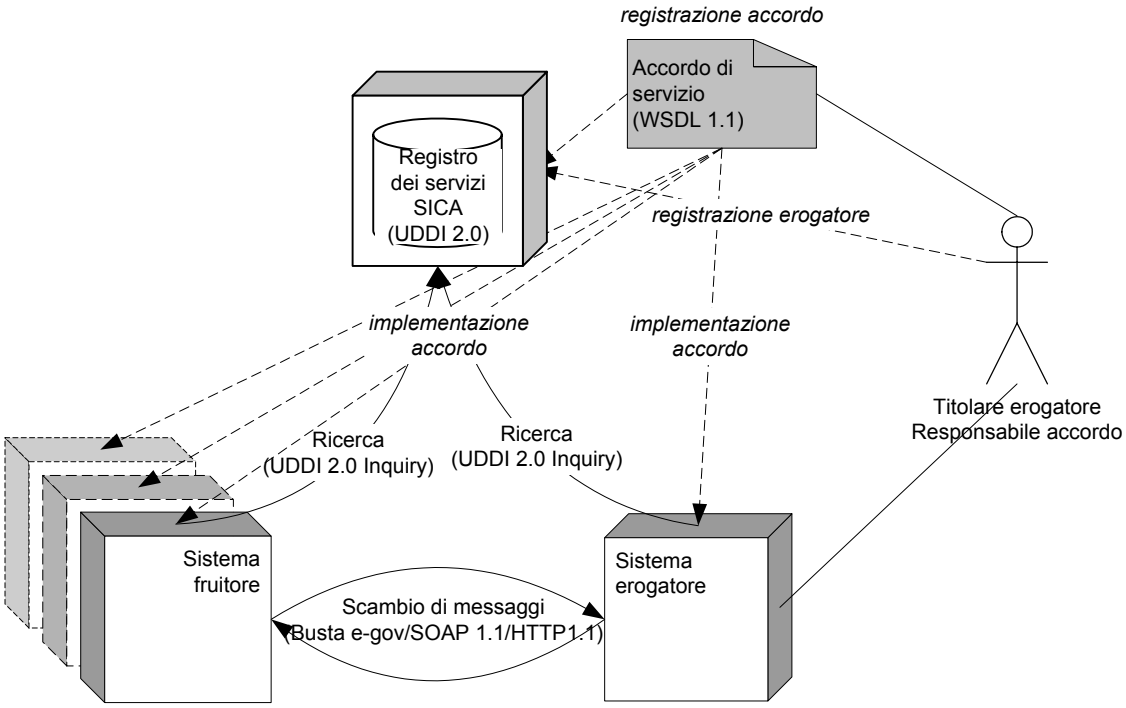


Figura 7. Servizio mono-erogatore/multi-fruitore.

- *Servizi multi-erogatore/mono-fruitore*
  Il servizio è erogato in conformità con l'accordo di servizio da un insieme di sistemi erogatori indipendenti, di cui sono titolari - nel caso di servizio inter-dominio - più soggetti differenti. Il servizio è destinato alla fruizione da parte di un sistema di cui il titolare è un altro soggetto della comunità del S.P. di Cooperazione. Il ciclo di vita dell'accordo di servizio è gestito da un soggetto a cui viene delegato il compito, (indipendentemente dal processo di definizione dell'accordo), eventualmente nel quadro di un dominio di cooperazione (vedi § 7.6.3). Ogni titolare di ogni singolo erogatore è responsabile dell'erogazione del servizio in conformità con l'accordo generale e, eventualmente di un accordo specifico di livello di servizio (LDS) che si impegna a rispettare. Il fruitore è responsabile della fruizione del servizio rispettando i termini dell'accordo generale e eventualmente di accordi specifici sul livello di utilizzo che si impegna a rispettare.

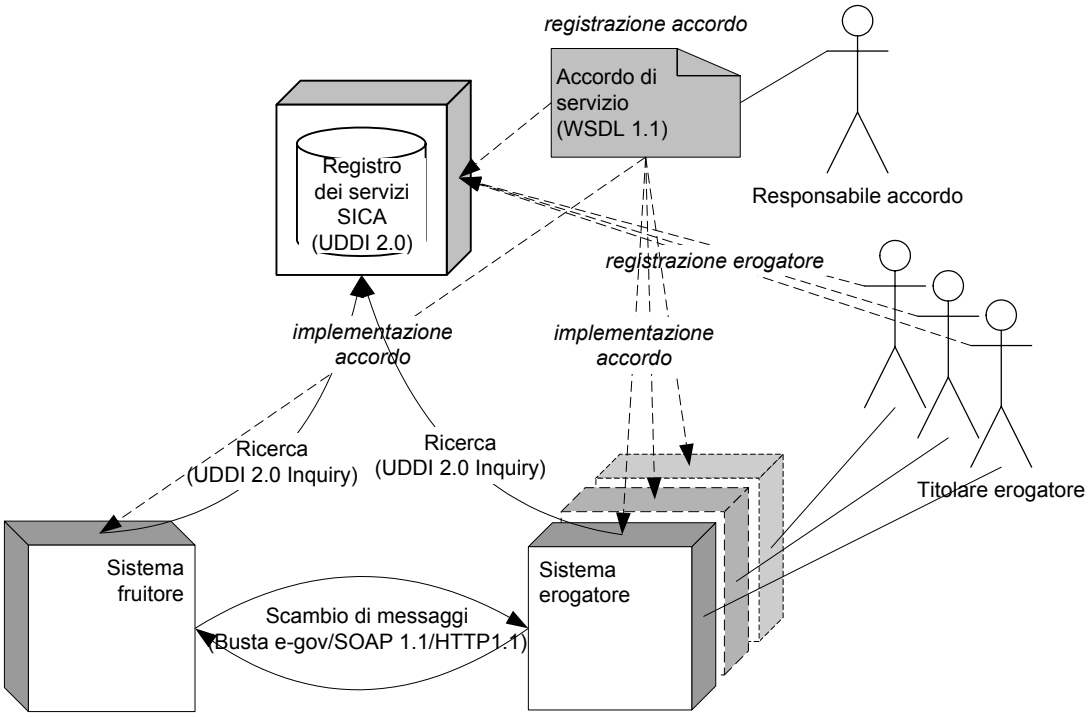


Figura 8. Servizio multi-erogatore/mono-fruitore.

- *Servizi multi-erogatore/multi-fruitore*
  Il servizio è erogato in conformità con l'accordo di servizio da un insieme di sistemi erogatori indipendenti, i cui titolari - nel caso di servizio inter-dominio – sono soggetti diversi. I servizi (tutti conformi alla stesso accordo) sono destinati alla fruizione di una classe di sistemi indipendenti (i fruitori) i cui titolari - nel caso di servizio inter-dominio – sono altri soggetti del S.P. di Cooperazione. Il ciclo di vita dell'accordo di servizio è gestito da un soggetto a cui viene delegato il compito, eventualmente nell'ambito di un dominio di cooperazione (vedi § 7.6.3). Ogni erogatore è responsabile dell'erogazione del proprio servizio in conformità all'accordo generale (che non gestisce direttamente) e eventualmente a clausole specifiche di livello di servizio. Ogni fruitore è responsabile della fruizione del servizio rispettando i termini dell'accordo generale e eventualmente clausole specifiche sul livello di utilizzo.

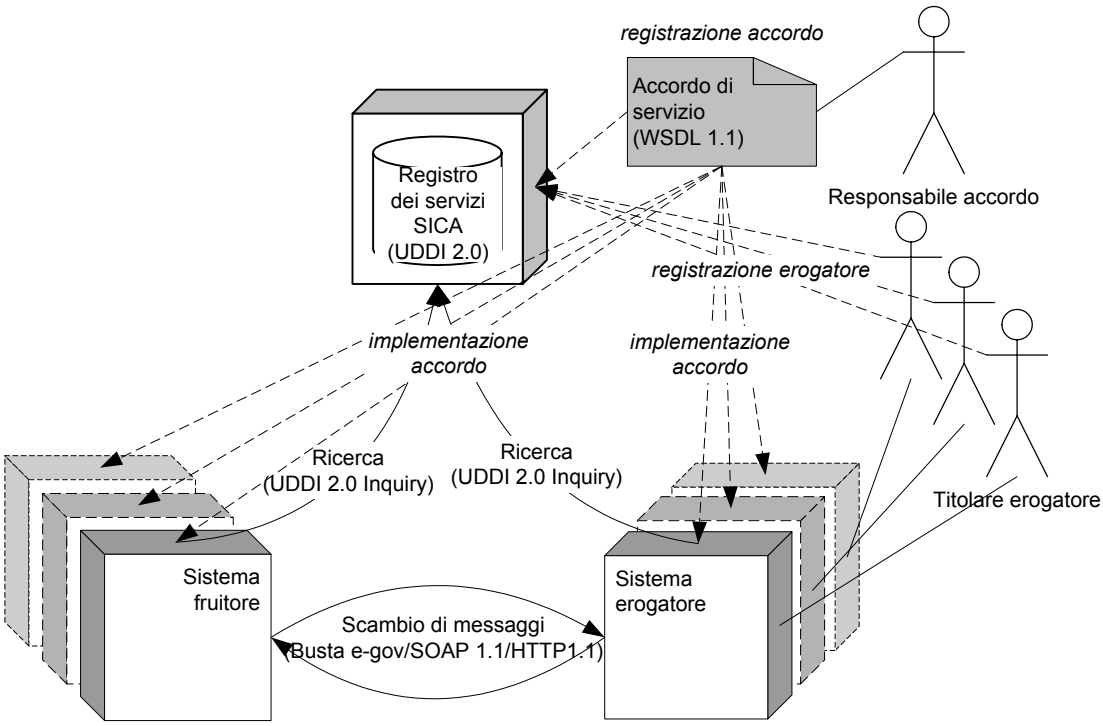


Figura 9. Servizio multi-erogatore/multi-fruitore.

7.6.2.3. Ciclo di vita dei servizi del S.P. di Cooperazione

L'accordo di servizio è il cardine del ciclo di vita del servizio. I servizi del S.P. di Cooperazione sono obbligatoriamente gestiti per versioni dell'accordo di servizio. Più versioni di uno stesso servizio (corrispondenti a versioni diverse dell'accordo di servizio) possono essere erogate nello stesso momento. Ogni versione segue un ciclo di vita autonomo, che è definito dal soggetto responsabile dell'accordo di servizio.

Per ogni versione del servizio applicativo, il ciclo di vita è composto da 6 fasi:

Fase 1. Definizione dell'accordo di servizio.

Fase 2. Registrazione dell'accordo di servizio sul registro SICA nazionale generale.

Fase 3. Implementazione del servizio.

Fase 4. Presentazione del servizio sul S.P. di Cooperazione.

Fase 5. Erogazione/fruizione del servizio sul S.P. di Cooperazione.

Fase 6. Dismissione dell'accordo di servizio e del servizio dal S.P. di Cooperazione.

Le fasi del clco di vita del servizio sono descritte nella Tabella 5.

Fase 1. Definizione dell'accordo di servizio	Nella fase di definizione del servizio, il servizio viene ideato e formalizzato nell'accordo generale di servizio e eventualmente negli accordi specifici sul livello di servizio e sul livello di utilizzo. Il processo che porta alla definizione del servizio segue fondamentalmente due approcci: • *Approccio unilaterale.* Nell'approccio unilaterale, l'accordo generale di servizio viene concepito unilateralmente dal soggetto titolare dell'erogatore, o da un soggetto delegato. Accordi specifici di livello di servizio o di livello di utilizzo possono seguire l'approccio unilaterale o l'approccio concordato (vedi il prossimo paragrafo). • *Approccio concordato.* Nell'approccio concordato, l'accordo di servizio è ideato in modo congiunto dall'erogatore (o il suo rappresentante) e dal fruitore (o il suo rappresentante). L'approccio concordato richiede l'apertura di un dominio di cooperazione (vedi § 7.6.3).
Fase 2. Registrazione dell'accordo di servizio sul registro SICA nazionale generale.	Nel S.P di Cooperazione, la registrazione del servizio è obbligatoria. La registrazione comprende molteplici attività da effettuare presso i registri SICA (generale o secondari): • registrazione dei titolari dei sistemi erogatori nell'indice dei soggetti della comunità S.P. Cooperazione (SICA generale), • registrazione degli accordi generali di servizio nel catalogo degli accordi (SICA generale), • registrazione degli accordi specifici (LDS e LDU) di servizio nel catalogo degli accordi (SICA generale o secondario), • registrazione dei servizi da presentare nel registro dei servizi (SICA generale o secondario), • registrazione dei porti di accesso ai sistemi erogatori nella rubrica degli indirizzi (SICA generale o secondario).

Fase 3. Implementazione del servizio.	Nella fase di implementazione, i titolari dei sistemi erogatori o fruitori implementano rispettivamente l'erogazione e la fruizione del servizio in conformità con l'accordo generale di servizio e gli eventuali accordi specifici di livello di servizio e di livello di utilizzo. Il modello dell'architettura SPCoop permette di minimizzare i livelli di aderenza e interdipendenza reciproca delle architetture e le tecnologie di implementazione dei sistemi erogatori e fruitori. In effetti, il solo punto di aderenza applicativo è situato nelle interfacce di scambio di messaggi e il solo punto di aderenza tecnica è nell'implementazione delle tecnologie di connessione e di trasporto (accoppiamento debole) – le interfacce di scambio dei messaggi sono esplicitamente specificate dall'accordo di servizio e le tecnologie di connessione e trasporto sono conformi allo standard SPCoop. La fase di implementazione dei sistemi erogatori può essere organizzata secondo seguendo differenti modelli del ciclo di realizzazione (incrementale, evolutivo) e diversi approcci di realizzazione (ciclo classico in cascata, concezione e realizzazione agile, programmazione "estrema"). Il carico di lavoro della fase di implementazione del sistema erogatore può essere estremamente variabile: se l'accordo di servizio prevede la presentazione come interfaccia di servizio di interfacce programmatiche già realizzate su un sistema patrimoniale, l'implementazione del servizio si riduce alla generazione semi-automatica (grazie agli ambienti di sviluppo) dell'interfaccia di servizio. Se, all'estremo opposto, occore sviluppare a partire da zero il sistema erogatore, la fase di implementazione del servizio si traduce in una fase di sviluppo applicativo classico. La fase di implementazione implica la disponibilità di un ambiente di test, dove sia possibile qualificare i sistemi erogatori e fruitori e l'erogazione/fruizione del servizio. Il ciclo di implementazione è un ciclo interno al ciclo generale del servizio: per la stessa versione dell'accordo di servizio, il ciclo interno di implementazione può essere ripreso più volte per interventi di manutenzione correttiva, adattativa e migliorativa. Il ciclo di implementazione si svolge sotto la responsabilità esclusiva del titolare del sistema erogatore, ma l'accordo di servizio può prevedere delle clausole sulla qualità dell'implementazione (affidabilità del software, impegno di non regressione, rapidità di correzione di anomalie, ecc.).
Fase 4. Presentazione del servizio sul S.P. di Cooperazione.	Nella fase di presentazione del servizio, i titolari dei sistemi erogatori presentano il servizio sulla rete, ovvero lo mettono in esercizio. La presentazione è la fase che precede immediatamente la fase di erogazione/fruizione.
Fase 5. Erogazione/fruizione del servizio sul S.P. di Cooperazione.	Nella fase di erogazione/fruizione il servizio è erogato in conformità con l'accordo di servizio. La fase di erogazione/fruizione comprende attività di tracciatura (standard SPCoop) e può comprendere attività di monitoraggio definite nell'accordo di servizio e effettuate dai soggetti designati da detto accordo.

Fase 6. Dismissione dell'accordo di servizio e del servizio dal S.P. di Cooperazione.	La fase di dismissione (di una versione) del servizio prevede l'archiviazione (della versione) del servizio e dell'accordo di servizio e dei giornali di tracciatura e può comprendere l'archiviazione di eventuali supporti di non repudiabilità definiti nell'accordo di servizio. La fase di dismissione prevede la sottrazione (della versione) del servizio dal S.P. di Cooperazione, dopo annuncio preventivo ai titolari dei sistemi fruitori.

Tabella 5. Fasi del ciclo di vita del servizio.

7.6.3. Dominio di cooperazione (DC)

7.6.3.1. Il processo applicativo inter-dominio

Un obiettivo della cooperazione applicativa inter-dominio è la realizzazione di *processi applicativi inter-dominio*. Un processo applicativo inter-dominio è un processo:

- il cui svolgimento segue uno scenario predeterminato,
- la cui finalità è un risultato applicativo (provvedimento amministrativo, insieme di atti amministrativi, ecc.),
- la cui implementazione coinvolge sistemi applicativi appartenenti a domini differenti; tali sistemi partecipano al processo applicativo inter-dominio esclusivamente attraverso l'erogazione/fruizione di servizi applicativi.

7.6.3.2. Dominio di cooperazione e accordo di cooperazione

Un *dominio di cooperazione* (DC) del S.P. di Cooperazione è un insieme di soggetti della comunità del S.P. di Cooperazione che si accordano per la realizzazione di un processo applicativo inter-dominio.

Uno dei soggetti partecipanti al dominio di cooperazione è designato come *coordinatore del dominio di cooperazione*. Se il processo applicativo implementa l'erogazione di un servizio applicativo, il coordinatore del DC è il responsabile del servizio.

I soggetti del DC sottoscrivono un *accordo di cooperazione*. Un accordo di cooperazione è l'insieme degli accordi di servizio necessari alla realizzazione di un processo applicativo inter-dominio come scambio di servizi tra i sistemi partecipanti. Gli accordi di servizio dell'accordo di cooperazione possono essere *organici* al dominio di cooperazione (stipulati espressamente per mettere in opera il processo applicativo oggetto del dominio di cooperazione) oppure *indipendenti* (preesistenti al dominio e riusati nell'ambito del processo applicativo). L'accordo di cooperazione contiene gli accordi di servizio organici e fa riferimento agli accordi di servizio indipendenti. L'accordo di cooperazione è definito collegialmente (approccio concordato) dai soggetti del DC e gestito (registrato sul registro SICA) dal coordinatore del DC che ne è responsabile. Il coordinatore del DC è particolarmente responsabile della coerenza e pertinenza degli accordi di servizio organici e dell'usabilità, ai fini della implementazione del processo applicativo come scambio di servizi, degli accordi indipendenti.

8. COMPONENTI TECNICI E SERVIZI INFRASTRUTTURALI DEL SISTEMA PUBBLICO DI COOPERAZIONE

L'architettura tecnica del Sistema Pubblico di Cooperazione è composta da:

- un insieme di componenti tecnici standard che costituiscono la Porta di Dominio (PD),
- un insieme di servizi infrastrutturali (SICA).

L'architettura per livelli degli standards tecnologici e infrastrutturali SPCoop è presentata nella Figura 10.

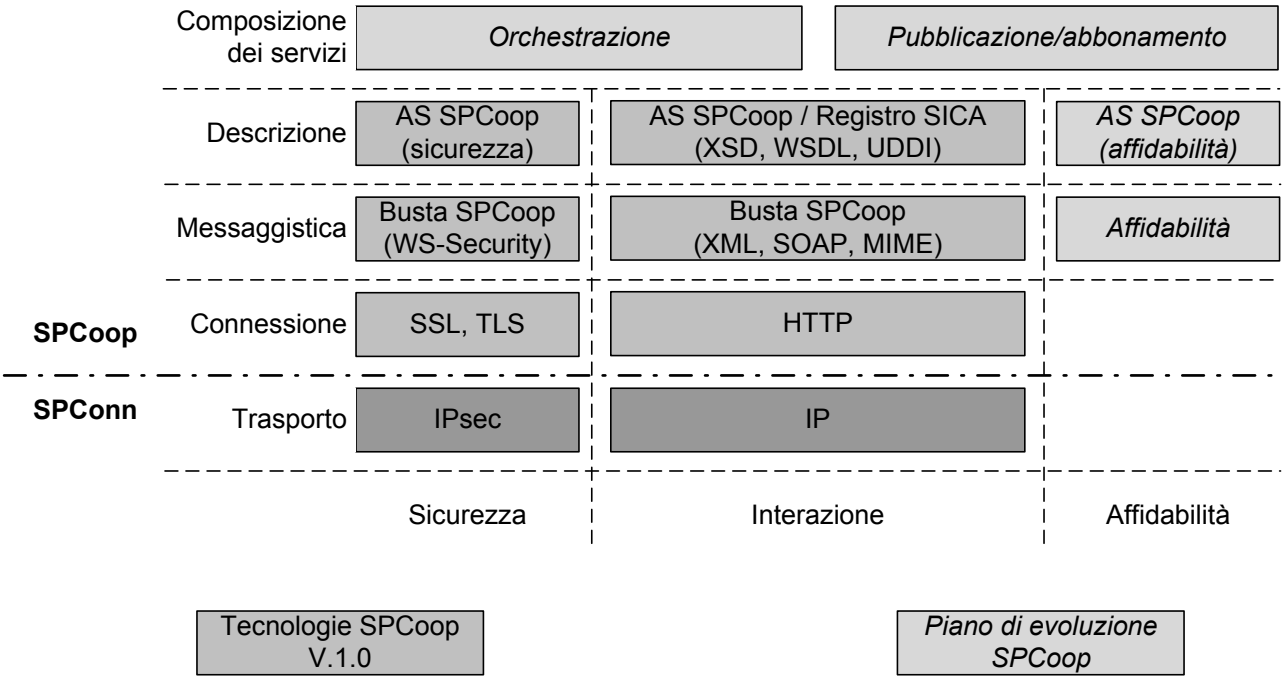


Figura 10. Architettura degli standards tecnologici SPCoop.

8.1. Porta di dominio (PD)

La Porta di dominio è l'insieme dei componenti distribuiti che implementano le funzionalità infrastrutturali che permettono la messa in opera dello scambio di messaggi e dei requisiti di sicurezza e di qualità di servizio, a livello *connessione* e *porta* in modo indipendente dalla logica applicativa.

Le funzionalità infrastrutturali implementate dai componenti standard della PD, e che ogni dominio è tenuto a implementare, sono:

F1. Funzionalità di gestione dello scambio al livello *connessione* (HTPP).

F2. Funzionalità di gestione della sicurezza a livello *connessione* (SSL, TLS).

F3. Funzionalità di gestione della Busta SPCoop (imbustamento, sbustamento).

F4. Funzionalità di tracciatura dei messaggi a livello *porta* (Busta SPCoop).

F5. Funzionalità di gestione dello smistamento a livello *porta*.

F6. Funzionalità di gestione della sicurezza a livello *porta* (WS-Security).

Le funzionalità F1, F2, F3 devono essere attive in ogni interazione (emissione e ricezione di messaggi) tra sistemi sul S.P. di Cooperazione.

Ogni dominio può arricchire la PD con altri componenti specifici che implementano altre funzionalità infrastrutturali di sicurezza e qualità di servizio (per esempio, l'affidabilità dello scambio, la non repudiazione). In questo caso, le specifiche funzionali e di interfaccia di tali componenti debbono essere descritte nell' accordo di servizio.

Per ogni funzionalità infrastrutturale la PD implementa due componenti:

- il componente che esegue le operazioni che precedono l'invio del messaggio,
- il componente che esegue le operazioni che seguono la ricezione del messaggio.

I componenti della PD sono organizzati come componenti intercettori in *pipeline* che eseguono delle operazioni che si situano:

- per il mittente del messaggio, tra la costruzione del contenuto applicativo del messaggio e l'invio del carico HTTP (richiesta o risposta HTTP) sulla connessione,
- per il destinatario del messaggio, tra la ricezione del carico HTTP (richiesta o risposta HTTP) e il trattamento del contenuto applicativo del messaggio.

8.1.1. Lista dei componenti della PD

La lista dei componenti standard della PD è descritta nella Tabella 6:

Funzionalità	*Componente*	*Descrizione*
Scambio di messaggi HTTP	Richiedente HTTP	Si tratta de classico "client" HTTP, che si incarica di aprire una connessione, di formare la richiesta HTTP e di trasmetterla sulla connessione, di mettersi in attesa della risposta e, alla ricezione della risposta di prelevare il carico per consegnarlo ai moduli applicativi.
	Rispondente HTTP	Si tratta del classico "server" HTTP, che si incarica di ricevere la richiesta HTTP su una connessione aperta, di prelevare il carico e di smistarlo ai moduli applicativi, di recuperare il risultato del

Funzionalità	*Componente*	*Descrizione*
		trattamento applicativo, di costruire il carico della risposta e di trasmetterla sulla connessione aperta.
Sicurezza a livello "connessione" (SSL3, TSL1)	Sicurezza a livello "connessione" (SSL3, TSL1)	Il componente di gestione della sicurezza a livello connessione del richiedente HTTP si incaricano dell'autenticazione del rispondente HTTP, dell'eventuale protocollo di autenticazione reciproca, del controllo di integrità del carico (calcolo del condensato, firma digitale, validazione della firma digitale), della riservatezza del carico (cifratura/decifratura), sulla base dei protocolli SSL e TLS. Il componente di sicurezza si avvale dei servizi infrastrutturali SICA proposti nella infrastruttura a chiave pubblica (gestione dei certificati, gestione delle chiavi, servizio marcatempo).
Smistamento dei messaggi a livello *connessione*	Smistamento in emissione delle richieste HTTP (reverse proxy)	Concentratore di richieste HTTP in emissione, che si incarica di lanciare la richiesta HTTP sul S.P. di Connettività.
	Smistamento in ricezione delle richieste HTTP (proxy)	Gateway HTTP che si incarica di smistare la richiesta in ricezione interpretando la URL della richiesta.
Tracciatura dei messaggi a livello *porta*	Tracciatura dei messaggi a livello *porta*	Il componente di tracciatura dei messaggi a livello *porta* si incarica di memorizzare i messaggi (busta SPCoop) in emissione e in ricezione su un giornale di formato standard SPCoop.
Gestione della Busta SPCoop	Costruzione della busta SPCoop (imbustamento)	Il componente si incarica di costruire la struttura della busta SPCoop e di riempire il corpo con contenuti forniti dai moduli applicativi.
	Trattamento della busta SPCoop (sbustamento)	Il componente si incarica di prelevare il corpo della busta SPCoop e di consegnarlo ai moduli applicativi.
Smistamento dei messaggi a livello porta	Smistamento dei messaggi a livello busta	Il componente interpreta le consegne di smistamento presenti nella testata della busta SPCoop e lancia i componenti dello scambio HTTP con l'indirizzo del nuovo destinatario.
Gestione della sicurezza à livello porta	Firma digitale (XML Signature)	Il componente applica i meccanismi di firma digitale in conformità con lo standard XML Signature/WS-Security agli elementi del messaggio. La scelta dell'agorotmo di firma è parametrabile. Utilizza i servizi dell'infrastruttura a chiave pubblica SPCoop.
	Validazione della firma digitale (XML Signature)	Il componente valida la firma digitale in conformità con lo standard XML Signature/WS-Security agli elementi del messaggio. La scelta dell'algoritmo di firma è parametrabile. Utilizza i servizi dell'infrastruttura a chiave pubblica SPCoop.

Funzionalità	*Componente*	*Descrizione*
	Calcolo di condensato	Il componente produce il condensato (digest) di un elemento del messaggio. La scelta dell'algoritmo è parametrabile.
	Cifratura (XML Encryption)	Il componente applica algoritmi di cifratura la cui scelta è parametrabile, agli elementi del messaggio, in conformità con lo standard XML Encryption/WS-Security. Utilizza i servizi dell'infrastruttura a chiave pubblica SPCoop.
	Decifratura (XML Encryption)	Il componente decifra gli elementi del messaggio, in conformità con lo standard XML Encryption/WS-Security. Utilizza i servizi delll'inbfrastruttura a chiave pubblica SPCoop.
	Construzione della testata WS-Security	Il componente costruisce le testate del messaggio in conformità con lo standard WS-Security e invoca i componenti di sicurezza implicati (firma, cifratura) per realizzare i requisiti di autenticazione, integrità e riservatezza (delle entità e dei messaggi).
	Trattamento della testata WS-Security	Il componente tratta le testate del messaggio in conformità con lo standard WS-Security e invoca i componenti di sicurezza implicati (validazione della firma, decifratura) per realizzare i requisiti di autenticazione, integrità e riservatezza (delle entità e dei messaggi).

Tabella 6. Componenti della PD.

8.1.2. *Configurazioni della PD*

La PD si presenta in due configurazioni:

- PD completa (configurazione completa),
- PD delegata (configurazione ridotta).

Ogni soggetto della comunità del S.P. di Cooperazione deve implementare almeno la configurazione ridotta (PD delegata) e può implementare la configurazione completa (PD completa).

8.1.2.1. Configurazione completa

La PD completa contiene tutti i componenti listati nel paragrafo 8.1.1.

8.1.2.2. Configurazione ridotta (PD delegata)

La PD in configurazione ridotta (PD delegata) deve contenere tutti i componenti listati nel paragrafo 8.1.1, salvo i componenti:

- Rispondente HTTP
- Smistamento delle richiesta a livello *connessione* in ricezione (proxy)
- Smistamento dei messaggi a livello *porta*

I sistemi che usufruiscono della porta delegata possono implementare esclusivamente:

- Il *mittente* nello scambio elementare *messaggio senza replica* (vedi § 6.2.3.1)
- Il *richiedente* nello scambio elementare *messaggio/replica sincroni* (vedi § 6.2.3.2)

Tali sistemi possono quindi interpretare il ruolo di fruitori negli scenari di coordinamento:

- Richiesta senza risposta (vedi § 6.2.5.1)
- Richiesta/risposta sincrone (vedi § 6.2.5.2)

Possono anche implementare il ruolo di erogatori negli scenari di coordinamento:

- Notificazione senza risposta (vedi § 6.2.5.3)
- Notificazione/risposta sincrone (vedi § 6.2.5.4)

La *PD delegata* (PDD) può essere implementata dai soggetti della comunità del S.P. di Cooperazione le cui necessità applicative non impongono l'implementazione di un *listener* HTTP.

8.1.3. Sequenza dei trattamenti di PD in emissione e ricezione del messaggio

I componenti della PD, la cui implementazione può essere distribuita, funzionano come moduli intercettori in *pipeline* nella costruzione del messaggio da emettere e nel trattamento del messaggio ricevuto. Alcuni componenti della PD (completa e delegata) devono essere attivi in ogni scambio sul S. P. di Cooperazione. Nei paragrafi seguenti, i componenti che *non* devono essere attivi in modo obbligatorio (in emissione e ricezione) sono qualificati a *attivazione opzionale*). Tali componenti sono attivati solo se le loro funzionalità sono necessarie alla soddisfazione dei requisiti formalizzati nell'accordo di servizio.

8.1.3.1. Emissione del messaggio

La sequenza dei trattamenti di PD in emissione del messaggio è la seguente:

1. Costruzione della Busta SPCoop (struttura e contenuto del corpo e delle testate standard SPCoop).
2. Costruzione della catena di smistamento a livello porta (*attivazione opzionale*).
3. Costruzione delle testata WS-Security (*attivazione opzionale*)
    a. Firma digitale degli elementi del messaggio
    b. Cifratura degli elementi del messaggio

4. Tracciatura della busta in emissione
5. Costruzione del messaggio (richiesta o risposta) HTTP
6. Sicurezza in emissione a livello *connessione* (*attivazione opzionale*)
    a. Autenticazione a livello *connessione*
    b. Firma digitale del carico
    c. Cifratura del carico
7. Smistamento della richiesta a livello *connessione* in emissione (reverse proxy).
8. Invio del messaggio (richiesta o risposta) HTTP.

8.1.3.2. Ricezione del messaggio

La sequenza dei trattamenti PD in ricezione del messaggio è la seguente:

1. Ricezione del messaggio (richiesta o risposta) HTTP
2. Smistamento delle richiesta a livello *connessione* in ricezione (proxy)
3. Sicurezza in ricezione a livello "connessione" (*attivazione opzionale*)
    a. Autenticazione a livello *connessione*
    b. Validazione della firma digitale del carico
    c. Decifratura del carico
4. Tracciatura della busta in ricezione.
5. Smistamento del messaggio a livello *porta* (*attivazione opzionale*).
6. Trattamento della testata WS-Security (*attivazione opzionale*)
    a. Validazione della firma digitale
    b. Decifratura (opzionale).
7. Selezione del contenuto applicativo dalla busta.

8.1.4. Installazione della PD

I componenti della PD sono generalmente distribuibili e replicabili. **L'architettura SPCoop impone come vincolo che la porta di dominio di un soggetto possegga un solo indirizzo di rete (un processore identificato e autenticabile) in emissione delle richieste HTTP e un solo indirizzo di rete (un processore identificato e autenticabile) in ricezione delle richieste HTTP**.

Da tale vincolo deriva una sola restrizione all'istallazione dei componenti della PD:

- la implementazione di un solo *proxy* (obbligatoria per la PD ma non per la PDD) per ogni dominio dei servizi su un processore identificato e autentificabile,

- la implementazione di un solo *reverse proxy* (obbligatoria per la PD e la PDD) per ogni dominio dei servizi su un processore identificato e autenticabile.

8.2. Servizi infrastrutturali di cooperazione ed accesso *(SICA)*

L'Architettura SPCoop V.1.0 specifica due insiemi di servizi infrastrutturali di supporto allo scambio di servizi e di messaggi nel S.P. di Cooperazione:

- Servizi di registrazione e ricerca (Registro SICA)
- Servizi di infrastruttura a chiave pubblica (ICP SICA)

Si tratta di servizi multi-erogatore a implementazione distribuita, definiti in accordi generali di servizio (AGS) e erogati da sistemi di cui sono responsabili soggetti della comunità SPCoop qualificati dal Comitatio di gestione SPC.

Il Comitato di gestione SPC è titolare e responsabile della erogazione di servizi SICA di valenza nazionale generale:

- *Registro SICA nazionale generale.*
- *Autorità di certificazione (AC) nazionale generale.*

Le altre occorrenze dei servizi Registro SICA e AC SICA sono chiamate, per opposizione, *Registri SICA secondari* e *AC SICA secondarie.*

8.2.1. *Servizi di registrazione e ricerca (Registro)*

Il registro SICA è un insieme di servizi infrastrutturali di registrazione e ricerca di informazioni. Gestisce gli stati, le transizioni di stato, l'accesso alle informazioni sullo stato delle risorse seguenti:

- sui soggetti della comunità SPCoop,
- sulle entità (processori, sistemi software, utenti) di cui tali soggetti sono responsabili,
- sui servizi presentati sul S.P. di Cooperazione, di cui i soggetti sono titolari,
- sugli accordi di servizio (AGS, ALU, ALS),
- sui punti di accesso dei servizi presentati sul S.P. di Cooperazione,
- sui domini di cooperazione e i soggetti partecipanti,
- sugli accordi di cooperazione.

Gli stati di tali risorse sono persistenti e durevoli, e le transizioni di detti stati sono non decomponibili (atomiche) e isolate. Il registro SICA gestisce la coerenza degli stati delle risorse (gestione transazionale).

L'architettura SPCoop specifica un *accordo generale di servizio* (AGS) per il registro SICA. Le implementazioni (occorrenze) del registro SICA devono essere conformi all'AGS Registro SICA. Le diverse occorrenze dei servizi SICA presentano requisiti di autorizzazione e qualità di servizio particolari (ALS).

Una occorrenza di registro SICA *dovrebbe* essere accessibile, oltre che ai sistemi dei soggetti della comunità del S.P. di Cooperazione in conformità con l'AGS, agli utenti afferenti ai soggetti della comunità SPCoop, per mezzo di una *interfaccia utente*. L'interfaccia utente potrebbe essere utilizzata dagli *amministratori* - utenti che agiscono sotto la responsabilità dei soggetti della comunità SPCoop - per inserire, aggiornare e cancellare le informazioni sulle risorse di cui tali soggetti sono responsabili. L'interfaccia utente è utilizzata dai responsabili e dai progettisti dei sistemi fruitori attuali e potenziali dei servizi, nelle fasi di analisi e progettazione, per ottenere informazioni sui soggetti, i servizi, gli erogatori, gli accordi di servizio e gli indirizzi dei punti di accesso.

La specifica SPCoop e l'AGS del registro SICA non contengono alcuna specifica dell'interfaccia utente del registro SICA. La concezione e l'implementazione di tale interfaccia è lasciata alla libera scelta dei singoli titolari dei registri SICA secondari.

Le specifiche dell'interfaccia utente del registro SICA nazionale generale sono prodotte dal Comitato di gestione SPC e possono essere utilizzate per implementare le interfacce utente dei registri SICA secondari. Al solo scopo di evitare confusioni, la presentazione visiva dell'interfaccia utente di un registro SICA secondario deve poter essere distinta facilmente dalla presentazione del registro SICA nazionale generale, la cui riproduzione esatta e completa in un registro SICA secondario è comunque rigorosamente vietata.

8.2.1.1. Descrizione funzionale

Dal punto di vista funzionale, il registro SICA è il risultato della composizione di quattro servizi (vedi Figura 11) che gestiscono le risorse seguenti:

- Il servizio di gestione dell'*indice dei soggetti* della comunità del S.P. di Cooperazione.
- Il servizio di gestione dell'*elenco degli erogatori* presenti sul S.P. di Cooperazione.
- Il servizio di gestione del *catalogo degli accordi di servizio* sottoscritti e implementati sul S.P. di Cooperazione.
- Il servizio di gestione della *rubrica degli indirizzi dei punti di accesso* dei sistemi erogatori e fruitori.

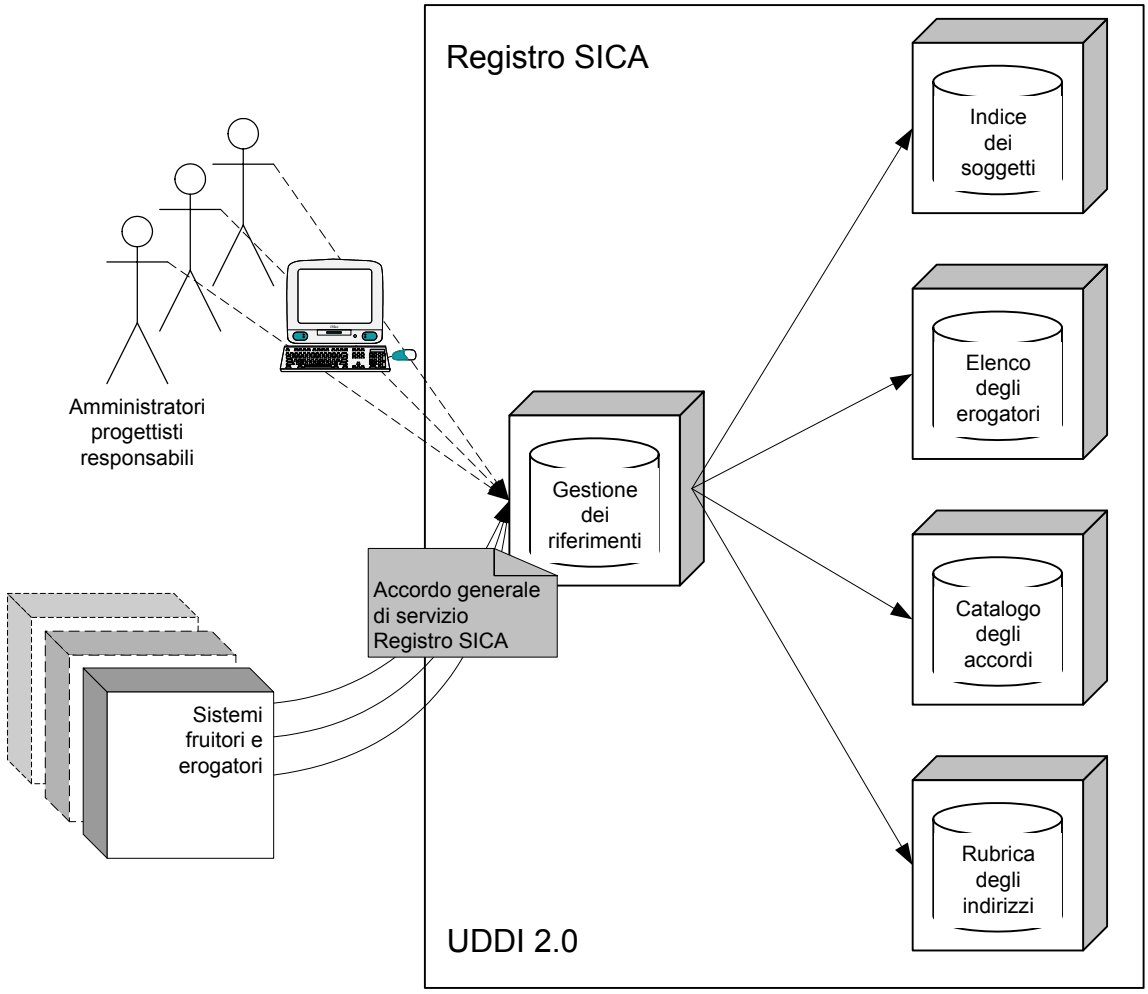


Figura 11. Architettura logica del registro dei servizi.

8.2.1.2. Tipologia di casi di utilizzo

Il registro dei servizi permette di effettuare richieste del tipo:

- ricercare tutti i servizi di cui è titolare un determinato soggetto (ciò corrisponde al Dominio dei Servizi Applictivi – DSA – del soggetto in questione),
- ricercare il documento WSDL 1.1 dell'accordo di servizio di un servizio,
- ricercare il documento XML Schema dell'accordo di servizio di un servizio,
- ricercare l'insieme dei soggetti erogatori di un servizio (servizio multi-erogatore),
- ricercare il soggetto responsabile dell'accordo di servizio di un servizio multi-erogatore,
- ricercare l'insieme dei punti di accesso dei soggetti erogatori di un servizio multi-erogatore,

- ricercare, a partire da un accordo di cooperazione, l'insieme degli accordi di servizio indipendenti (a cui l'accordo di cooperazione fa riferimento),
- ricercare le coordinate dell'utente responsabile di una porta di dominio,
- ricercare il coordinatore e i soggetti componenti di un dominio di cooperazione,
- ricercare il punto di accesso di un registro SICA (generale o secondario) identificato dal soggetto titolare,
- ricercare tutti gli erogatori del servizio registro SICA.

L'interfaccia di servizio del registro è usata in esecuzione per ottenere dinamicamente gli indirizzi dei porti di accesso. I casi più frequenti sono due:

Il servizio è identificato (dall'accordo) ed è erogato dal sistema applicativo di un soggetto titolare identificato (servizio mono-erogatore). In questo caso la ricerca à partire dalla coppia soggetto/accordo permette di ottenere gli indirizzi dei punti di accesso.

Il servizio, conforme à un accordo di servizio unico, è erogato da un insieme di sistemi applicativi gestiti da titolari differenti (servizio multi-erogatore), e il sistema fruitore deve interagire con tutti i sistemi. In questo caso la ricerca per servizio da come risultato la lista dei responsabili dei sistemi erogatori e, per ogni responsabile, gli indirizzi dei porti corrispondenti.

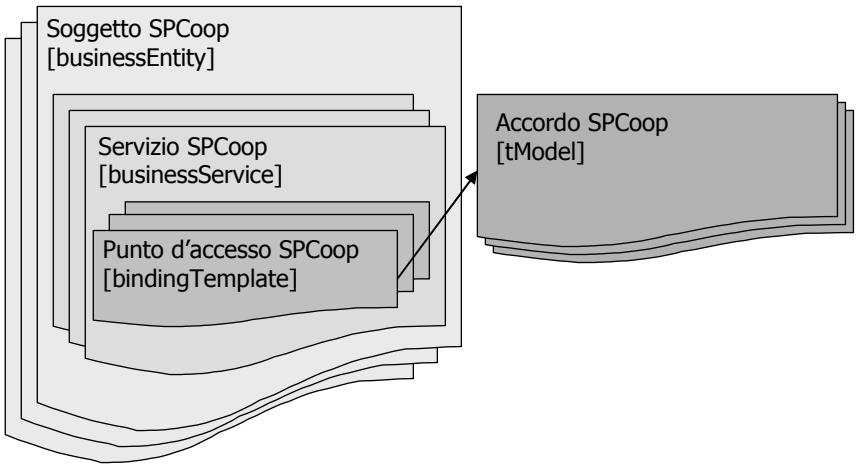


Figura 12. Struttura di dati (elementi XML) del registro dei servizi

8.2.1.3. L'indice dei soggetti

Il primo passo nella costruzione del registro SICA è la costruzione dell'indice dei soggetti.

L'identificazione dei soggetti pubblici e privati è un compito organizzativo svolto Comitato di gestione SPC, che rilascia al soggetto un codice identificatore unico (formato URI/URN) nell'ambito del S.P. di Cooperazione, conforme con le specifiche della.

La struttura di dati che rappresenta il soggetto è un elemento XML (*Soggetto SPCoop*) specializzazione della struttura UDDI 2.0 *businessEntity* (vedi Figura 12) [UDDI Data Structure 2].

Il dominio di un soggetto è rappresentato dal soggetto stesso (c'è identità tra soggetto e dominio).

L'attuale indice delle pubbliche amministrazioni (IndicePA) verrà asunto come partenza per la realizzazione di tale struttura.

8.2.1.4. L'elenco delle occorrenze dei servizi

La costituzione dell'indice dei soggetti permette in seguito la registrazione delle occorrenze di erogazione dei servizi. Le occorrenze dei servizi possono essere identificati se il titolare è identificato e registrato.

La struttura di dati che rappresenta l'occorrenza di un servizio è un elemento XML (*Servizio SPCoop*) specializzazione della struttura UDDI 2.0 *businessService* (vedi Figura 12) [UDDI Data Structure 2].

La relazione di inclusione tra elementi Soggetto SPCoop (*businessEntity*) e Servizio SPCoop (*businessService*) rappresenta le relazione di titolarità tra un soggetto del S.P. di Cooperazione e l'occorrenza di erogazione di un servizio.

Il DSA (dominio dei servizi applicativi) di un soggetto SPCoop è rappresentato dall'insieme dei Servizi SPCoop (*businessService*) inclusi in un Soggetto SPCoop (*businessEntity*).

Le occorrenze di erogazione dei servizi SPCoop (Servizi SPCoop) sono dotate di un codice identificatore unico in formato URI/URN standard SPCoop (URN) costruite combinando l'identificatore universale del soggetto SPCoop (titolare dell'occorrenza di erogazione del servizio) e l'identificatore dell'accordo di servizio SPCoop (registrato nel catalogo degli accordi). Ne consegue che il Servizio SPCoop (businessService) può essre registrato solo dopo la registrazione del soggetto SPCoop titolare (businessEntity) in cui è incluso e dell'accordo di servizio SPCoop, in accordo con le regole del ciclo di vita dei servizi che indicano che la presentazione del servizio applicativo sul S.P. di Cooperazione è successiva alla registrazione dell'accordo di servizio.

La registrazione dei servizi SICA è effettuata seguendo la stessa procedura dei servizi applicativi. I servizi SICA nazionali sono registrati dall'amministratore del soggetto titolare (il Comitato di gestione SPC) e fanno riferimento agli accordi di servizio SICA (di cui è responsabile lo stesso Comitato di gestione SPC). I servizi SICA secondari (occorrenze di servizi SICA) sono registrati sul registro SICA nazionale generale come occorrenze di servizi dei soggetti loro titolari.

8.2.1.5. Il catalogo degli accordi

L'accordo di servizio è rappresentato da un insieme di documenti il cui "manifesto" è contenuto in un elemento XML (Accordo SPCoop) specializzazione della struttura di dati UDDI 2.0 *tModel* (vedi Figura 12) [UDDI Data Structure 2].

L'accordo SPCoop ha un codice identificatore in formato URI/URN in conformità con lo standard SPCoop. Il codice identificatore di un accordo di servizio è unico in ambito SPCoop e è fornito dal responsabile dell'accordo e formato secondo le regole SPCoop. L'accordo SPCoop deve essere registrato nel registro SICA nazionale, in cui viene effettuato un controllo di universalità del codice identificatore in ambito SPCoop (nei fatti tale controllo riguarda la possibilità che un soggetto responsabile possa registrare due accordi con lo stesso nome).

A partire dalla registrazione dell'accordo SPCoop, è possibile registrare le occorrenze di erogazione del servizio conforme all'accordo (erogatori SPCoop).

L'insieme dei documenti dell'accordo SPCoop, organizzato dall'elemento tModel, in conformità con lo standard SPCoop, è composto da documenti in testo libero e da documenti XML (XML Schema, WSDL). La base documentaria che implementa il catalogo degli accordi permette delle ricerche sul contenuto dei documenti (in *full text* per i documenti in testo libero e utilizzando XQuery / XPath per i documenti XML), in maniera da ottenere logicamente un catalogo degli schemi.

8.2.1.6. La rubrica degli indirizzi

Per ogni occorrenza di servizio, il titolare può registrare più punti di accesso (*Punti d'accesso SPCoop*) specializzazioni della struttura UDDI 2.0 *bindingTemplate* (vedi Figura 12) [UDDI Data Structure 2]. La struttura contiene come elemento l'indirizzo del punto di accesso in formato URI/URL (schema HTTP) in conformità con lo standard SPCoop (Indirizzo SPCoop). L'indirizzo è in parte calcolato automaticamente e la parte dominio ("it"), sotto-dominio ("spc"), host (codice soggetto) è l'indirizzo del *proxy* de la porta di dominio del soggetto (il resto serve a localizzare il punto di accesso del servizio).

8.2.2. *Servizi di infrastruttura a chiave pubblica (ICP)*

I requisiti di sicurezza dell'accordo di servizio sono messi in opera dai componenti di sicurezza della PD. Tali componenti, addetti alla realizzazione delle funzionalità di autenticazione, integrità e riservatezza sulla base di gestioni di chiavi asimmetriche, richiedono l'uso di certificati digitali e quindi la fruizione di servizi di *infrastruttura a chiave pubblica* (ICP).

8.2.2.1. Accreditamento delle autorità di certificazione (AC)

Gli elementi essenziali per una infrastruttura a chiave pubblica sono i certificati e le autorità di certificazione. Per poter operare in ambito SPCoop, le AC devono essere accreditate. Le modalità di accreditamento sono stabilite dal Comitato di gestione SPC.

Il Comitato di gestione SPC gestisce la AC radice, che autentica i certificati delle AC distribuite.

I certificati radice di ogni AC devono essere pubblicati con modalità tali da essere immediatamente disponibili ad ogni soggetto della comunità SPCoop. Inoltre, devono essere disponibili strumenti per la verifica di tali certificati digitali, compreso lo stato di validità.

8.2.2.2. Servizi offerti dalle AC

Le CA accreditate devono offrire i seguenti servizi di certificazione:

- Registrazione dei richiedenti.
- Emissione di certificati con le seguenti tipologie:
  - certificati di autenticazione,
  - certificati di cifratura.
  - certificati sistema (processori e componenti software),
- Operazioni di gestione dei certificati:
  - revoca dei certificati,
  - sospensione dei certificati,
  - pubblicazione dei certificati,
  - rinnovo dei certificati.
- Marcatura temporale.
- Informazione in tempo reale dello stato dei certificati (OCSP).

8.2.2.3. Gestione delle richieste di certificati

Le regole e procedure per le richieste dei certificati sono definite in termini tecnici e organizzativi (autorizzazioni, tempi e modalità di consegna).

8.2.2.4. Profilo dei certificati

I certificati digitali sono emessi in conformità con lo standard X509v3. I profili dei certificati utilizzati in ambito SPCoop sono definiti in un apposito documento di standard SPCoop reso pubblico alle AC, al fine di garantire l'interoperabilità dei sistemi.

8.2.2.5. Verifica dello stato di validità dei certificati

Per verificare in tempo reale lo stato dei certificati digitali (valido/sospeso/revocato) è imposto il protocollo OCSP [OCSP]. Il profilo dei certificati di autenticazione presenti nella CNS prevede la possibilità di utilizzo di tale protocollo. Un profilo standard SPCoop è definito per i certificati sistema.

Le AC che emettono i certificati di autenticazione e certificati sistema devono assicurare la gestione di OCSP, cioè mettere a disposizione funzioni per la revoca dei certificati e per la verifica delle revoche.

9. ALLEGATO – TIPOLOGIA DI SERVIZI

In una architettura di servizi, i sistemi componenti sono collegati da una rete di relazioni di servizio. A parte i casi estremi dei puri fruitori di servizi (sistemi che non erogano servizi ma la cui implementazione si basa sulla fruizione di servizi) e degli erogatori puri (sistemi che erogano servizi ma che non usufruiscono di altri servizi), i sistemi dell'architettura sono al tempo stesso erogatori e fruitori di servizi. In tali sistemi la fruizione di servizi serve all'implementazione dell'erogazione di altri servizi: si tratta del meccanismo chiamato *composizione di servizi*. I servizi si distinguono quindi, dal punto di vista dell'implementazione dei sistemi che li erogano, in *semplici* e *composti*. La *composizione di servizi* (fruizione di servizi per implementare l'erogazione di altri servizi) segue diverse modalità che sono descritte nei paragrafi che seguono.

Un *servizio semplice* eroga un insieme di funzionalità la cui implementazione non necessita la fruizione di altri servizi. Un servizio semplice può essere implementato sia da un sistema dedicato, sia da un sistema applicativo complesso le cui funzionalità sono erogate attraverso un insieme di servizi componenti modulari (*disseminazione di servizi*). **La modularità di erogazione dei servizi è indipendente della modularità di implementatione dei sistemi erogatori**.

Un *servizio composto* eroga un insieme di funzionalità la cui implementazione necessita la fruizione di altri servizi semplici o composti, chiamati *servizi componenti*.

9.1.1. Servizi composti opachi

Il *servizio composto opaco* segue alla lettera il *principio di occultamento dell'implementazione*: l'accordo di servizio non menziona i servizi componenti e l'esistenza di tali servizi, dei loro sistemi erogatori e dei responsabili di tali sistemi deve essere ignorata nell'analisi, concezione e implementazione dei sistemi fruitori del servizio composto.

Ogni informazione sui servizi componenti, i sistemi erogatori di tali servizi, i responsabili di tali servizi non è garantita dall'accordo di servizio e la dipendenza della concezione dei sistemi fruitori del servizio composto da tali informazioni non garantisce la perennità di tale concezione.

In una architettura di servizi, un servizio composto che applica integralmente il principio di occultamento dell'implementazione (servizio composto opaco) è indistinguibile da un servizio semplice: la rete di dipendenza degli accordi di servizio è invisibile (ciò è vero anche in caso di pubblicazione dei servizi componenti su un registro accessibile: la dipendenza dell'implementazione del servizio composto dai servizi componenti non è pubblicata nel registro, dato che non è esplicita in nessun accordo di servizio).

9.1.2. Servizi composti trasparenti (catena di responsabilità)

Un *servizio composto trasparente* (*catena di responsabilità*) è un servizio composto caratterizzato dal fatto che l'esistenza, il ruolo e la responsabilità di tutti o parte dei servizi componenti, dei sistemi che li erogano, dei responsabili di detti sistemi nell'erogazione del servizio composto sono esplicitati *staticamente* nell'accordo di servizio: l'accordo di servizio del servizio composto esplicita le responsabilità di erogazione di parte delle funzionalità del servizio composto da parte dei servizi componenti (catena di responsabilità).

Il contributo dei sistemi erogatori componenti detti *erogatori indiretti* per opposizione all'erogatore diretto del servizio composto, può essere tracciato *dinamicamente* al momento dell'erogazione con vari metodi. Come l'accesso al servizio, la delega di erogazione ai servizi componenti può essere:

- identificata,
- autenticata,
- controllata,
- non ripudiabile.

Un metodo comunemente usato è l'autentica di dati e dei resoconti di erogazione forniti dai servizi componenti delegati per mezzo della firma digitale di tali dati e resoconti da parte dei sistemi erogatori indiretti. Il servizio composto fornisce tali dati e resoconti firmati ai fruitori del servizio.

Un erogatore indiretto che produce dati per i fruitori del servizio composto può cifrare detti dati in modo che essi non siano decifrabili da parte del sistema che implementa il servizio composto, ma solo dai fruitori di tale servizio. In questo caso, le responsabilità sulle caratteristiche di qualità di detti dati (autenticità, coerenza, esattezza, precisione, freschezza, validità) è esclusivamente dell'erogatore indiretto.

In una architettura a composizione ricorsiva di servizi, la trasparenza della catena di responsabilità rompe, nei suoi punti di applicazione, il principio di occultamento dell'implementazione nell'accordo di servizio (dando luogo ai servizi composti trasparenti).

9.1.3. Servizi composti a orchestrazione di processo

Un servizio composto a orchestrazione di processo è un servizio composto la cui architettura di composizione segue il modello specifico di orchestrazione di processo (vedi 6.2.5.5): il sistema erogatore del servizio composto svolge escusivamente il ruolo di *coordinatore* e *mediatore* dei servizi componenti, cioè implementa esclusivamente il coordinamento dell'erogazione dei servizi componenti e la mediazione dello scambio dei messaggi tra i sistemi erogatori. Tutte le funzionalità e le regole applicative che implementano il servizio composto sono implementate nei sistemi erogatori dei servizi componenti.

Il modello di esecuzione di un qualsivoglia servizio composto è quello di un processo distribuito a cui partecipano i sistemi erogatori dei servizi componenti che eseguono trattamenti e si scambiano servizi. Il punto distintivo dell'architettura di composizione per orchestrazione di processo è che il sistema erogatore del servizio composto interpreta esclusivamente i ruoli di coordinatore del processo e di mediatore dello scambio tra i servizi componenti:

- l'erogazione dei servizi componenti è escusivamente attivata e pilotata dal coordinatore/mediatore;
- i sistemi erogatori dei servizi componenti scambiano messaggi per coordinare l'erogazione del loro servizio esclusivamente con il coordinatore/mediatore;
- il coordinatore/mediatore non implementa regole applicative altre che le regole di coordinamento e di mediazione dei servizi componenti;
- il coordinatore/mediatore eroga il servizio composto, che può comprendere oltre che le dovute funzionalità di avvio del processo e di consumo dei risultati finali, il consumo dei risultati intermedi, il monitoraggio e il pilotaggio del processo stesso.

Il modello del servizio composto a orchestrazione di processo è un modello generale di composizione di servizi che è particolarmente adatto per i servizi in cui è necessario non solo ottenere dei risultati prodotti da trattamenti distribuiti, ma in cui anche che il processo che conduce alla produzione di detti risultati, nonché gli stati e i risultati intermedi di tale processo, devono essere accessibili.

I fruitori di tale servizio possono essere generalmente distinti in due categorie

- i fruitori delle funzionalità applicative primarie del servizio composto;
- i fruitori delle funzionalità di monitoraggio del processo a fini di controllo.

Lo scenario del processo può essere descritto esplicitamente nell'accordo di servizio (deve esserlo nell'accordo di cooperazione, vedi più avanti). In questo caso, l'esistenza e il ruolo dei servizi componenti fa parte dell'accordo di servizio, introducendo elementi di trasparenza del servizio composto. Alla esplicitazione dello scenario di processo può essere aggiunta la trasparenza della responsabilità dei servizi componenti: ciò permette di ottenere la tracciatura del processo, la tracciatura dei servizi componenti e la tracciatura dei messaggi. Il caso estremo si verifica quando il coordinatore/mediatore smista esclusivamente dati firmati e per lui indecifrabili (salvo quelli strettamente necessari al coordinamento e allo smistamento).

Il sistema coordinatore/mediatore può essere implementato per mezzo di uno scenario (*script*) scritto in un linguaggio di orchestrazione formale [WSBPEL 0.1], caricato automaticamente da un motore di processi alla ricezione di un messaggio di avvio di una occorrenza dello scenario di processo e interpretato dal motore stesso. Il motore di processi implementa funzionalità di:

- gestione della esecuzione concorrente di molteplici occorrenze degli scenari,
- salvaguardia di stati intermedi,
- monitoraggio e pilotaggio dell'occorrenza del processo.

Queste funzionalità sono erogate come servizi di supporto del motore di processi e dei coordinatori/mediatori (script in esecuzione) delle occorrenze dei processi in attività.

Il modello di servizio a orchestrazione di processo è assolutamente generale e può essere considerato come il modello per eccellenza della composizione ricorsiva di servizi: ogni servizio è o un sevizio semplice o un servizio composto a orchestrazione di processo. Si tratta di un modello che presenta vantaggi importanti in termini di rapidità e plasticità di implementazione di nuovi servizi e di evoluzione/manutenzione di servizi esistenzi.

Il modello di composizione di servizi per mezzo dell'orchestrazione di processo è particolarmente adatto all'erogazione di servizi prodotti da trattamenti discontinui, in cui l'occorrenza del processo è inattiva per periodi lunghi, in attesa, per esempio, che uno dei servizi partecipanti produca una risposta à una richiesta, risposta che a sua volta dipende dalla decisione di un utente.

L'approccio di servizio a orchestrazione di processo con catena di responsabilità è particolarmente adatto alla realizzazione di servizi la cui produzione implica l'esecuzione di procedimenti amministrativi a cui concorrono più amministrazioni e più responsabili amministrativi. Il modello di orchestrazione di processo non solo si adatta perfettamente alla realizzazione di sistemi che assecondano la produzione di atti amministrativi, ma soddisfa anche gli obblighi di trasparenza sugli stati di avanzamento e sui responsabili dei procedimenti dettati dalla normativa. La catena di responsabilità (trasparenza del processo) si adatta perfettamente al principio che la responsabilità di ogni amministrazione nella produzione di atti amministrativi informatici non può essere delegata.

9.1.4. Servizi di intermediazione

Un servizio di intermediazione è un tipo specifico di servizio composto (opaco o trasparente), invocato su iniziativa del fruitore via una richiesta, le cui uniche funzionalità sono:

- lo smistamento della richiesta verso uno dei servizi componente la cui scelta e effettuata sulla base di un insieme di regole,
- la trasformazione (eventuale) dei dati dalla richiesta del fruitore alle richieste verso i servizi componenti,
- la trasformazione (eventuale) dei dati dalle risposte dei servizi componenti alla risposta al fruitore.

Il sistema fruitore di un servizio di intermediazione (*fruitore finale*) usufruisce quindi direttamente dei servizi (applicativi o infrastrutturali) erogati dai servizi componenti (*erogatori originari*). Nel caso in cui non vi sia trasformazione di dati, il servizio di intermediazione degenera verso un puro servizio di smistamento. Lo smistamento della richiesta verso l'erogatore originario appropriato può essere effettuata sulla base della semplice analisi di un dato elementare contenuto nella richiesta, ma anche a partire da regole che effettuano una analisi complessa del contenuto della richiesta.

Un servizio di intermediazione può essere implementato:

- come un servizio opaco (il servizio di intermediazione funziona come se erogasse direttamente i servizi erogati dagli erogatori indiretti),

- oppure come un servizio trasparente: l'identità degli erogatori iniziali di una funzionalità richiesta appare esplicitamente nella risposta verso il fruitore finale. Dette identità, e i dati annessi, possono essere autenticati dall'erogatore componente per mezzo di firma digitale verificabile dal fruitore finale.

Indipendentemente dall'autentica dell'erogatore componente e dei suoi dati, nel caso di servizio di smistamento, l'erogatore iniziale può cifrare i dati che fornisce in modo tale che essi siano decifrabili solamente da parte del fruitore finale.

9.1.5. *Servizi informativi*

Un servizio informativo è un servizio che fornisce un meccanismo per accedere à una o più sorgenti di dati e altri servizi informativi per mezzo di una interfaccia di scambio di messaggi. I sistemi fruitori del servizio non consoscono ne l'implementazione fisica, ne il formato di memorizzazione, né la locazione della o delle sorgenti di dati. Il servizio informativo è responsabile della traduzione della richiesta nel o nei linguaggi di interrogazione appropriati, del suo smistamento alla o alle sorgenti di dati appropriate e di confezionare una risposta unitaria a partire dai risultati delle richieste alle varie sorgenti di dati.

9.1.6. *Servizi di pubblicazione/abbonamento*

I servizi di pubblicazione/abbonamento erogano servizi che possono essere raggruppati in due categorie di funzionalità (le funzionalità di pubblicazione e le funzionalità di abbonamento).

9.1.6.1. Servizi di pubblicazione

I servizi di pubblicazione accettano la fornitura di dati, che si presentano nella forma di "notizie di eventi di un certo tipo", da parte di sistemi fruitori della funzionalità di pubblicazione del servizio ("pubblicisti"). I dati forniti da parte dei fruitori "pubblicisti" sono classificati e gestiti in conformità con gli impegni formalizzati nell'accordo di servizio.

9.1.6.2. Servizi di abbonamento

I servizi di abbonamento accettano le richieste di abbonamento ai "tipi di notizie di eventi" emesse da sistemi fruitori della funzionalità di abbonamento (gli "abbonati"). Il servizio di abbonamento notifica le notizie di eventi fornite dai "pubblicisti" agli "abbonati", in conformità con gli abbonamenti che hanno sottoscritto. L'abbonamento a un tipo di notizie di eventi può essere sottoscritto e revocato dinamicamente. Una variante semplificata del servizio di abbonamento (*store and forward*) prevede la sottoscrizione e la revoca puramente statiche degli abbonamenti (come elementi di configurazione statica del sistema erogatore).

9.1.7. Servizi di gestione di eventi, eccezioni e servizi di compensazione

La gestione delle situazioni di ricezione di eventi asincroni o di eccezione nell'invocazione di servizi componenti da parte di un sistema che eroga un servizio composto può raggiungere livelli di complessità tali da richiede l'implementazione di servizi componenti specializzati nella gestione di detti eventi o eccezioni. Tali servizi possono effettuare il completamento o lo storno dei trattamenti interrotti e l'annullazione o la compensazione dei trattamenti già completati al momento dell'evento o eccezione. Nel caso di servizi a orchestrazione di processo, in cui il sistema erogatore passa attraverso stati intermedi visibili e eventualmente tracciati, può essere necessario di effettuare azioni e trattamenti di compensazione dei trattamenti effettuati prima dell'eccezione.