Il progetto "**SI-II-06 Estensione del sistema per l'interoperabilità e la cooperazione applicativa tra le regioni - ICAR-Abruzzo** " ha come obiettivo la realizzazione, nell'ambito della Regione Abruzzo, delle infrastrutture fisiche e logiche capaci di erogare i servizi di base necessari per consentire l'interoperabilità e la cooperazione applicativa tra gli Enti della Pubblica Amministrazione nel contesto del Sistema Pubblico di Connettività (SPC).

Con tale progetto, la Regione Abruzzo si propone, attraverso l'implementazione delle necessarie infrastrutture tecnologiche, di fornire un grado di consolidamento generale all'infrastruttura elaborativa, applicativa e rete integrata all'interno del Centro Tecnico della ComNet-RA in modo da fornire ai diversi attori, erogatori di servizi e per il bacino d'utenza finale sia del territorio regionale sia nazionale, gli strumenti in grado di interoperare attraverso i propri sistemi informativi.

Inoltre l'implementazione dei meccanismi e l'integrazione tra l'infrastruttura del progetto e la restante Community Network regionale (ComNet-RA) permetterà di interagire con maggior efficacia e con un maggior numero di strutture della P.A., degli Enti Locali regionali e, più in generale, di utenti. Pertanto questo intervento, in aggiunta ad altri interventi di natura infrastrutturale ed applicativa nel settore ICT, alcuni attualmente in corso, altri in fase di start-up, intende consolidare le basi per un utilizzo efficace e capillare dei servizi informativi e telematici messi a disposizione dalla Regione Abruzzo.

Il progetto costituisce un modello di riferimento da estendere all'intero territorio regionale sia in termini di standardizzazione, sia in termini di diffusione agli Enti connessi alla ComNet – RA ed ai cittadini che intendono utilizzare i servizi messi a disposizione su tale infrastruttura. Il progetto consente alla Regione Abruzzo di agire sul gap preesistente rispetto alle realtà più avanzate e costituisce la base sulla quale la Regione, le Province, i Comuni, le Comunità Montane ed in generale gli Enti Locali potranno diffondere in maniera organica servizi applicativi avanzati in modalità IP oriented.

APPROFONDIMENTI:

LINK: Sito Ufficiale del progetto ICAR

LINK: Il Fumetto di ICAR

LINK: ICartoni di ICAR

LINK: ICarQuiz

Nell'ambito del progetto ICAR il **Centro Tecnico di Tortoreto Lido – ARIT** si è dotato dell'infrastruttura elaborativa necessaria all'erogazione di servizi in ambito SPC (Sistema Pubblico di Connettività). Grazie alla flessibilità e alla modularità delle componenti Hardware e Software configurate, ARIT è in grado di fornire tutti gli strumenti e le funzionalità richieste alle Pubbliche Amministrazioni per l'erogazione e la fruizione di servizi in cooperazione applicativa tramite Porte di Dominio.

Scopo dell'approfondimento è di:

- spiegare le potenzialità di Hosting che ARIT può offrire agli Enti della Regione Abruzzo per la realizzazione della cooperazione applicativa regionale e interregionale;

- fornire una guida logica per la realizzazione autonoma dell'intera infrastruttura necessaria alla messa in produzione della propria Porta di Dominio e della relativa certificazione presso il CNIPA-DigitPA.

Il contesto normativo di riferimento, di seguito riportato, si compone di un insieme di normative nazionali affiancate da un insieme di norme specifiche della Regione Abruzzo.

- Decreto Legislativo 18 agosto 2000, n. 267 - "Testo unico delle leggi sull'ordinamento degli Enti locali"

- Piano di azione e-government (Decreto Presidente del Consiglio dei Ministri del 14 febbraio 2002)

- Decreto legislativo Consiglio dei Ministri del 11 febbraio 2005 – “Istituzione e regolazione Sistema Pubblico di Connettivita (SPC)”

- Decreto legislativo , testo coordinato, 07.03.2005 n° 82 – “Codice dell'amministrazione digitale”

- Delibera CIPE 35/05, Attribuzione risorse destinate al fondo per le aree sottoutilizzate per il periodo 2005/2008

- Decreto Legislativo 4 Aprile 2006, n. 159 – “Disposizioni integrative e correttive al codice dell'amministrazione digitale”

- Standard tecnologici definiti dal CNIPA e dal MIT in particolare quelli relativi alla banda larga e al Sistema Pubblico di Connettivita

- Norme di livello regionale o Legge n.25 del 2000 (Organizzazione del comparto sistemi informativi e telematici). o Delibera 27 dicembre 2001, n. 1319 – approvazione del Piano

d’Azione per lo sviluppo della Societa dell’Informazione E - Goverment” (P.A.S.I.)

Quasi la totalità delle Regioni (comprese le Province Autonome) sono impegnate per la realizzazione cooperativa del progetto interregionale ICAR (Interoperabilità e Cooperazione Applicativa tra le Regioni), inteso ad attivare la Community Network interregionale, rendendo disponibili un primo insieme di applicazioni cooperative attraverso Porte di Dominio a livello interregionale. Allo stesso tempo il progetto va di fatto ad implementare il nucleo iniziale e sperimentale del Sistema Pubblico di Connettività (SPC) nazionale. Per tale motivo il progetto prevede uno stretto rapporto tecnico-istituzionale con il DigitPA, in particolare per l’esigenza di allineamento delle soluzioni tecniche funzionali che devono essere specificate ed adottate nel progetto ICAR con quelle che devono essere ancora da specificare completamente anche nel sistema SPC nazionale secondo una visione condivisa tra Stato, Regioni ed Enti locali.

Il progetto “SI-II-06 Estensione del sistema per l'interoperabilità e la cooperazione applicativa tra le Regioni – ICAR-Abruzzo” nasce dalla presentazione separata, ma coordinata, di un progetto regionale da parte di ciascuna Regione aderente, in risposta all’avviso del CNIPA-DigitPA per la selezione dei progetti per “lo sviluppo dei servizi infrastrutturali locali e SPC”.

Le Regioni e le Province autonome aderenti al progetto interregionale ICAR sono: Abruzzo, Basilicata, Calabria, Campania, Emilia-Romagna, Friuli Venezia Giulia, Lazio, Liguria, Lombardia, Marche, Molise, Piemonte, Puglia, Sardegna, Sicilia, Toscana, Umbria, Valle d’Aosta, Veneto, Prov. Aut. di Trento, Prov. Aut. di Bolzano

---

I componenti infrastrutturali che ARIT mette a disposizione degli Enti regionali sono in grado di erogare i seguenti servizi in ambito SPC:

- **interconnessioni di base**: questi servizi permetteranno l'effettiva cooperazione tra le applicazioni interoperanti nelle diverse realtà regionali implementando funzionalità di relay, tracciatura e sicurezza;

- una **Porta di Dominio certificata** per ogni Ente regionale che decide di fruire del servizio di Hosting ARIT;

- un **Gestore di Eventi**, che abiliti alle comunicazioni applicative di tipo EDA;

- un **Registro** degli attori e dei servizi di secondo livello **SICA**;

- **Servizi di Tracciamento**: questa componente fornisce gli strumenti necessari per il **Monitoraggio** dei servizi erogati;

- Servizi di **Identificazione ed Autorizzazione** delle applicazioni cooperanti: questa componente si occupa di trasportare le asserzioni di identità secondo opportune regole di autenticazione e di accesso, realizzando, altresì, meccanismi di tracciamento ed audit degli stessi;

- un **Firewall XML** per la sicurezza nello scambio di messaggi SOAP nelle comunicazioni su SPC.

Tale ventaglio di offerta permette di coprire le esigenze di cooperazione applicativa di tutte quelle Amministrazioni che non sono intenzionate a dotarsi dei medesimi componenti presso il proprio dominio informatico, ma che vogliono affidare tale servizio all'ARIT.

Per quanto riguarda l'adattamento dei servizi locali alla cooperazione ed alla interoperabilità, si intende la capacita di due o più sistemi informativi di scambiarsi informazioni e di attivare, a suddetto scopo, processi elaborativi nelle rispettive applicazioni. Ciascun sistema informativo può differenziarsi in genere dall'altro per le scelte implementative (linguaggio di programmazione, formato dei dati ecc.).

La cooperazione applicativa, quindi, attiene alla possibilità di uno o più sistemi informativi di avvalersi, ciascuno nella propria logica applicativa, dell'interscambio automatico di informazioni con gli altri sistemi, per le proprie finalità applicative. In altre parole, un'applicazione, nel corso del suo processo elaborativo, può far così uso di un'informazione elaborata da un'altra applicazione.

Le soluzioni per tali scopi dovranno puntare all'integrazione di nuove funzionalità, che mantengono comunque quelle autonomamente operanti nelle applicazioni già esistenti, con il ***pieno riuso dei relativi sistemi informativi***
. L'integrazione comporta l'attivazione di infrastrutture principalmente di tipo logico (software) per l'interoperabilità, nonché l'estensione delle funzioni dell'applicazione esistente per il trattamento dei dati oggetto di scambio con le applicazioni operanti negli altri sistemi informativi secondo le specifiche finalità della cooperazione applicativa. Le soluzioni per tale integrazione devono ammettere altresì l'eterogeneità delle caratteristiche tecniche e funzionali delle applicazioni già esistenti e dei relativi sistemi informativi.

Garantire l'interoperabilità e la cooperazione applicativa tra i sistemi informativi delle Pubbliche Amministrazioni (PA) operanti a livello centrale, regionale e locale, è diventato, quindi, un requisito di primaria importanza al fine di realizzare il pieno ed efficace sviluppo dell'e-government. Ciò risponde a due esigenze principali:

Integrare i processi automatizzati di back-office per l'erogazione di servizi interni (da una PA all'altra) ed esterni (dalle PA verso i cittadini);

Erogare servizi finali integrati in rete al cittadino in modo trasparente ed unitario.

In altre parole, l'obiettivo e garantire al cittadino la possibilità di rivolgersi ad un unico sportello (on-line) per la fruizione di un servizio, senza avere la percezione del coinvolgimento di più Amministrazioni nell'erogazione del servizio richiesto, ove ciò sia necessario (secondo il modello di servizi di e-government "one-stop").

Per far fronte a queste esigenze, le PA devono far evolvere i loro sistemi informativi in tale direzione con un approccio cooperativo e tra loro condiviso. Ciò comporta la necessità di realizzare delle infrastrutture che permettano ai sistemi ed applicazioni di e-government di interoperare, secondo le esigenze dei vari domini applicativi (quali il servizio sanitario, quello anagrafico, quello relativo alle Aree Organizzative Omogenee, quello relativo al servizio del lavoro, ecc...).

Dovranno essere intraprese le azioni per l'integrazione dei servizi locali sull'infrastruttura definita per la cooperazione applicativa, riguardante sia la comunicazione tra le Porte Di Dominio che l'interazione con la logica e l'architettura dell'infrastruttura che deve servire. Dovrà essere presa in considerazione l'integrazione del Gestore Eventi per permettere lo scambio di buste e-gov secondo l'architettura definita. L'uso del Gestore Eventi permette ai Sistemi Applicativi interessati ad un certo servizio di ricevere, previa iscrizione a quel servizio, le comunicazioni inviate dai Sistemi Applicativi pubblicatori. Da questo punto di vista, il Gestore Eventi potrà essere considerato un normale servizio SPCoop, con una sua logica applicativa che consiste appunto nel coordinare, richiedenti e fruitori dei servizi SPCoop.

In definitiva, la realizzazione dell'infrastruttura composta dai moduli descritti in questo e nel precedente paragrafo renderà possibile alle Amministrazioni cooperanti l'utilizzo di web services offerti dalla rete SPCoop nazionale o la fornitura di web services alla medesima rete. Saranno evidenti gli enormi vantaggi derivanti da tale mutuo scambio di web services. Inoltre la presenza dell'infrastruttura creata potrà essere ulteriormente sfruttata per:

- la creazione di nuovi servizi composti con i servizi disponibili;

- la fornitura di servizi di gestione dell'identità;

- l‘abilitazione alla cooperazione applicativa anche degli Enti che non vogliano trasformare la propria architettura applicativa verso una SOA.

La Regione Abruzzo intende porsi anche come Ente in grado di offrire infrastrutture e servizi di cooperazione applicativa per quegli Enti che, invece di realizzare a propria volta la medesima infrastruttura di cooperazione, vorranno utilizzare l’infrastruttura presente presso il Centro Elaborazione Dati di ARIT. La scelta di fruire dell’Hosting consente agli Enti di ottenere Porte di Dominio personalizzate ed entrare a far parte del Sistema Pubblico di Connettività senza l’onere di procedure di gestione sistemistica e di sicurezza ed i relativi oneri di certificazione e messa in esercizio dei servizi infrastrutturali necessari usufruendo dei servizi descritti nelle successive sezioni, fermo restando l’autonomia degli Enti nel definire i flussi applicativi certificati da sottoporre alla propria Porta di Dominio ed i relativi oneri di procedura amministrativi previsti dal DigitPA per la richiesta formale della Porta di Dominio.

Per maggiori informazioni contattare l' Agenzia Regionale per l'Informatica e la Telematica .

Qualora invece l’Ente volesse realizzare autonomamente la propria Porta di Dominio dovrà farsi carico di realizzare l’infrastruttura logicamente descritta nei successivi paragrafi. Per un maggior approfondimento dei dettagli tecnico-progettuali delle componenti infrastrutturali si rimanda ai documenti del sito www.progettoicar.it , alcuni dei quali riportati nel paragrafo BIBLIOGRAFIA.

Con i termini interoperabilità e cooperazione applicativa ci si riferisce ad una specifica capacità di due o più sistemi informativi connessi in rete, ovvero la capacita che essi devono avere, affinché l’applicazione, operante in ciascun sistema, sia in grado di disporre automaticamente, per le proprie finalità applicative, dei dati che sono producibili e/o acquisibili solo attraverso il processo elaborativo delle applicazioni operanti negli altri sistemi informativi.

Interoperabilità applicativa

In particolare, l'interoperabilità attiene alla capacità di due o più sistemi informativi di scambiarsi informazioni e di attivare, a suddetto scopo, processi elaborativi nelle rispettive applicazioni. Ciascun sistema informativo può differenziarsi in genere dall'altro per le scelte implementative (e.g. linguaggio di programmazione e formato dei dati). In tal caso, un approccio che può garantire interoperabilità è ad esempio l'adozione di uno stesso formato di interscambio dei dati e di un protocollo di comunicazione condiviso. La cooperazione applicativa attiene alla capacità di uno o più sistemi informativi di avvalersi, ciascuno nella propria logica applicativa, dell'interscambio automatico di informazioni con gli altri sistemi, per le proprie finalità applicative. In altre parole, un'applicazione nel corso del suo processo elaborativo può far così uso di un'informazione elaborata da un'altra applicazione: ad esempio un applicativo sanitario può richiedere i dati anagrafici al programma di anagrafe civile del Comune di residenza del cittadino.

Cooperazione applicativa

La cooperazione applicativa costituisce l'elemento centrale per il collegamento delle infrastrutture dati in modalità distribuita. Tale meccanismo definisce le modalità di interscambio tra Enti e consente il trasferimento delle informazioni tra le diverse strutture. Nello specifico il progetto prevede uno schema di cooperazione sia a livello regionale che a livello nazionale (Comuni, Province, ASL, Università, Comunità Montane, Enti regionali, ecc...) in modalità conforme a quanto previsto nelle linee guida e-government elaborate dal DigitPA.

La cooperazione applicativa in rete ha luogo quando ciò avviene in modo automatico. L'interoperabilità è, quindi, un prerequisito essenziale per la cooperazione applicativa. Le soluzioni per tali scopi mirano all'integrazione di nuove funzionalità, che mantengono comunque quelle autonomamente operanti nelle applicazioni già esistenti, con il pieno riuso dei relativi sistemi informativi. L'integrazione comporta l'attivazione di infrastrutture principalmente di tipo logico per l'interoperabilità, nonché l'estensione delle funzioni dell'applicazione esistente per il trattamento dei dati oggetto di scambio con le applicazioni operanti negli altri sistemi informativi, secondo le specifiche finalità della cooperazione applicativa.

Le soluzioni per tale integrazione devono ammettere altresì l'eterogeneità delle caratteristiche

tecniche e funzionali delle applicazioni già esistenti e dei relativi sistemi informativi.
L'integrazione di servizi eterogenei tra Enti distanti tra loro necessita della concertazione di *prot ocolli e standard*
fortemente condivisi e l'aderenza a strategie architetturali che garantiscano la interoperabilità tra i numerosi ed eterogenei soggetti coinvolti. Infatti, poiché ciascun Ente dispone di un proprio sistema informativo, le informazioni risultano fortemente frammentate e distribuite tra i differenti Enti ed anche all'interno di esse tra le diverse strutture. Inoltre, i documenti ed i dati sono strutturati, conservati e trasmessi secondo formati, modalità, sistemi di interconnessione e protocolli differenti nelle varie situazioni.

L'erogazione di servizi integrati, fra gli obiettivi del piano di azione di e-government, implica l'integrazione tra i servizi di diverse Amministrazioni mediante la realizzazione dell'interoperabilità dei sistemi informatici delle Amministrazioni stesse. Esiste un'estrema eterogeneità dei sistemi di cooperazione applicativa attualmente in uso nei progetti in essere presso le Regioni italiane. Tale eterogeneità, che deriva da necessità locali e da differenze nelle temporalità dei progetti, necessita di una standardizzazione che consenta la diffusione delle informazioni tra sistemi diversi in modo trasparente. L'infrastruttura di cooperazione ha come obiettivo la possibilità di far cooperare sistemi informativi diversi preservandone la propria indipendenza ed autonomia. Il modello è quello **federativo** dove, al contrario del modello gerarchico, tutti i sistemi sono paritetici e non vi sono sistemi centralizzati che ne accorpano le funzionalità, vi sono eventualmente servizi centralizzati di supporto alla cooperazione.

Questa soluzione si basa su principi quali la *non intrusività, la scalabilità, la flessibilità e la standardizzazione* . La non intrusività va intesa
come la possibilità di far dialogare tra di loro sistemi applicativi diversi, senza alterarne il funzionamento di base. Ciò è possibile se ciascun sistema continua a funzionare come in precedenza solo con l'aggiunta di funzionalità specifiche necessarie alla cooperazione applicativa. Tali funzionalità, sfruttando le funzioni proprie del sistema, siano queste trasversali o applicative, consentono di realizzare servizi erogabili verso l'esterno con modalità e standard predefiniti.

La libertà di interconnettere nuovi sistemi o di modificare il quadro globale delle interconnessioni deve essere supportata da un'estrema flessibilità dell'infrastruttura a livello gestionale. Per questo motivo, l'infrastruttura di cooperazione avrà strumenti di configurazione e monitoraggio tali da consentire una gestione semplice ed efficace dei servizi, dei sistemi e delle interconnessioni tra di essi. La flessibilità dell'infrastruttura ne consentirà una gestione dinamica, tale da garantire la continuità del servizio.

L'elemento che consente ai sistemi di interoperare è il processo di standardizzazione delle interazioni, standardizzazione rispetto alla quale tutti i sistemi si devono poter adeguare in modo indipendente. La standardizzazione riguarda più aspetti del sistema e deve essere definita in ogni sua componente. Nel caso dell'interoperabilità tramite servizi ed eventi, la standardizzazione riguarda, oltre i protocolli di comunicazione e invocazione remota, il messaggio ed il relativo processo di gestione in termini di: *struttura, formalizzazione, codifica, workflow e servizio applicativo* .

Un concetto importante, espresso dalle specifiche tecniche per la cooperazione applicativa sulla Rete Nazionale, è rappresentato dal *Dominio*. Esso è definito come l'insieme delle risorse (in particolare le procedure, i dati e i servizi) e delle politiche di una determinata organizzazione. Il Dominio è anche definito come il confine di responsabilità di un'organizzazione. Secondo questo modello, la comunicazione avviene tra entità omogenee (i domini appunto) e lo scopo dell'architettura cooperativa è abilitare l'integrazione degli oggetti informativi (procedure e dati) e delle politiche di domini diversi.

L'elemento fondamentale è rappresentato dalla definizione delle modalità in base alle quali un dominio servente esporta i propri servizi ed un dominio cliente vi accede. L'interoperabilità fra Amministrazioni dovrà svilupparsi sulla base di standard in modo tale che:

- siano identificati i servizi ed i dati che ogni amministrazione deciderà di rendere disponibili sulla rete;

- siano rispettati, per ogni servizio esposto, le politiche di sicurezza e di accesso e di controllo di qualità e correttezza dei servizi erogati.

In questo modo si ottiene uno schema estremamente preciso in termini di suddivisione tra aree e responsabilità connesse. L'elemento tecnologico centrale per la cooperazione applicativa è rappresentato dalla Porta di Dominio. Da un punto di vista fisico, essa può essere considerata un componente infrastrutturale della Rete, un "proxy" per l'accesso alle risorse applicative.

Dal punto di vista dell'architettura applicativa, può anche essere considerata come un *adattatore* , che consente a sistemi informatici esistenti, o comunque realizzati in base alle esigenze del dominio

specifico, di affacciarsi sulla Rete e partecipare all'interscambio telematico delle informazioni. In particolare, può trattarsi di:

- un sistema monolitico, o comunque operante su un singolo nodo presso una struttura di piccole dimensioni;

- un sistema distribuito su più nodi collegati in rete locale presso una struttura di dimensioni maggiori;

- una rete di area, alla quale sono collegati i sistemi informatici di strutture anche diverse o di una singola struttura.

Nell'ambito della definizione degli standard per la cooperazione applicativa, uno degli aspetti che deve essere normalizzato è quello dei profili di collaborazione, cioè degli schemi di interscambio di messaggi tra porte di dominio. Le collaborazioni principali prevedono l'adozione di modalità sincrone e asincrone di scambio dei messaggi. Le modalità sincrona e asincrona sono intese relativamente allo scambio di una coppia di messaggi, uno in andata e l'altro in ritorno. In uno scambio sincrono, la porta delegata che invia la richiesta di servizio, a seguito dell'invio del messaggio di andata, rimane in attesa del messaggio di ritorno. Viceversa, in uno scambio asincrono, i due messaggi di andata e di ritorno vengono scambiati senza che una delle due parti rimanga in attesa.

La scelta della modalità sincrona o asincrona può anche dipendere da aspetti legati alla latenza amministrativa delle procedure: ad esempio la necessità di intervento umano, ad esempio per l'apposizione della firma digitale di un pubblico ufficiale.

In generale, il servizio rappresenta la modalità più diretta di collaborazione tra due sistemi. Una richiesta, sottoposta da un sistema ad un altro, scatena in quest'ultimo l'esecuzione di un processo applicativo il cui risultato viene restituito sotto forma di risposta. Il servizio è tipicamente un tipo di collaborazione sincrona ma, se viene scomposto in due fasi differite nel tempo, vi è la sottomissione della richiesta e ricezione della risposta, che, dunque, può realizzare anche una collaborazione asincrona.

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

Fissato lo standard tecnologico che si basa sul **SOAP (Simple Object Access Protocol)**, l'elemento principale di un messaggio è rappresentato da una
struttura XML SOAP
composta da due parti:

- l'intestazione (*XML SOAP Header*) contiene i dati relativi al messaggio ed in particolare contiene l'identificativo del messaggio;

- la descrizione (*XML SOAP Body*) riporta l'indicazione del tipo di documenti informatici allegati e del relativo formato di codifica, in alternativa la ricevuta di ritorno nel caso di un servizio di notifica.

La struttura XML SOAP è inclusa in una *struttura MIME* allo scopo di allegare al messaggio uno o più documenti applicativi, in base allo standard XML SOAP with attachments. Una firma opzionale può essere inclusa nell'intestazione utilizzando gli standard XML SOAP Encryption e XML Signature. Nel caso di documenti informatici firmati, per la rilevanza legale si adotta il formato il PKCS#7 in base della circolare AIPA CR/24. Tali documenti saranno, fino a tale aggiornamento, inclusi sotto forma di allegato. La scelta delle strutture specifiche per la busta di e-government da utilizzare nello scambio dei messaggi costituisce una parte integrante della definizione preliminare dei servizi e non può costituire una variante da negoziarsi per ciascuno scambio.

La soluzione di adottare un'unica modalità, sia essa sincrona o asincrona, su tutto il territorio nazionale non è percorribile in virtù delle differenti realtà esistenti la cui conversione alla modalità prescelta comporterebbe degli impatti molto rilevanti in termini di tempi e di costi. D'altra parte, anche la soluzione che ogni Ente si doti delle strutture tecnico-organizzative per la realizzazione di entrambe le modalità di colloquio risulta onerosa e inutilmente ridondante. Di conseguenza è preferibile dotare il sistema di gestione del canale di interscambio e di cooperazione di un insieme di servizi di cooperazione applicativa che garantiscano il colloquio tra gli enti indipendentemente dalla modalità prescelta da ciascuno di essi.

L’adozione di un linguaggio comune prevede la scelta e l’utilizzo di standard per la rappresentazione dei dati (XML, SOAP, etc.) e dei servizi applicativi (LDAP, UDDI, WSDL, etc...), oltre alla loro definizione univoca in termini sintattici e semantici. Il formato di scambio dovrà essere quello definito dal bando dei progetti di e-Gov.

Lo strumento tecnologico per memorizzare i documenti che definiscono sintassi e semantica dei dati è individuabile in un Repository XML, mentre, per quelli che definiscono la sintassi e la semantica dei servizi, si individua un Registro dei Servizi (LDAP o UDDI). Il sistema di gestione del canale di interscambio e cooperazione mette a disposizione i servizi per l’accesso controllato alla consultazione e alla modifica, del Repository XML e del Registro dei Servizi, ferma restando la possibilità di avere una struttura federata di tali “contenitori” di informazioni.

La logica di business e le strutture dei registri dovranno essere sviluppati in accordo alle specifiche ebXML 3.0. Il modello informativo dei metadati dovrà essere aderente all’ebRIM, opportunamente verticalizzato per il dominio sanitario italiano. Il gestore eventi dovrà implementare l’interfaccia WS-BrokeredNotification, appartenente alla famiglia di specifiche WS-Notification, in modo che ogni peer od utente potrà interagire con uno qualsiasi di loro, garantendo, così, che l’intero sistema si comporti come un unico broker logico.

Standard per la sicurezza nell’interscambio delle informazioni

La sicurezza è l’insieme delle misure atte a garantire la disponibilità, la integrità e la riservatezza delle informazioni gestite. E’ un concetto fondamentale in un contesto di sistemi distribuiti che trattano dati sensibili come quelli presenti nelle basi dati delle Pubbliche Amministrazioni. Lo standard WS-Security è un protocollo di comunicazione che si applica ad architetture SOA che utilizzano il paradigma dei Web Services per l’interoperabilità applicativa. Esso stabilisce il grado di confidenzialità e le regole per verificare l’integrità delle informazioni scambiate attraverso web- services.

Uno degli aspetti fondamentali di WSS e l’uso del concetto di Security Token. Un SecurityToken è simile ad una carta d’identità o meglio ad un pass che deve essere mostrato per usufruire di un determinato WS. WS-Security è lo standard definito da OASIS che descrive gli enhancements introdotti in SOAP al fine di soddisfare i requisiti di integrità, riservatezza ed autenticazione dei messaggi. WS-Security utilizza XML-Signature per fornire l'integrità e

l'autenticazione del messaggio ed XML-Encryption per la riservatezza. La specifica offre una serie di meccanismi (profili) per associare security tokens all'interno dei messaggi. I token di sicurezza previsti sono di tipo Username (UsernameToken Profile), certificati digitali X.509v3 (X.509 Token Profile), asserzioni SAML 2.0 (SAML Token Profile) per lo scambio dei dati di autenticazione ed autorizzazione tra domini di sicurezza; per l'interscambio di tali certificati tra Web Services si deve tenere in considerazione lo standard Web Services Security X.509 Certificate Token Profile. La versione utilizzata dal framework corrisponde alla specifica Web Service Security - SOAP Message Security 1.0. Il tipo di token impiegato nell'ambito della cooperazione applicativa dovrà essere la SAML assertion ver. 2.0, dichiarazione di autorizzazione espressa mediante un particolare linguaggio utilizzato, SAML, appunto, che definisce le regole e la sintassi per lo scambio di informazioni e per l'autenticazione sicura tra applicazioni. Le asserzioni SAML sono allegate al messaggio SOAP usando lo standard WSSecurity all'interno di un header.

Un sistema di Single Sign On permette l'autenticazione unica dell'attore/utente al sistema per la fruizione di una moltitudine di risorse informatiche per le quali è autorizzato. Il concetto alla base è quello di consentire ad un utente di accedere ad un sistema software complesso e consistente di più applicazioni, attraverso una unica procedura di controllo dell'accesso. Nel caso di accesso al sistema via web, ci si interfaccia una sistema che ha il compito di verificare le credenziali degli attori che saranno, in tal modo, soggette a validazione e autenticazione prima che sia effettuato l'accesso e la fruizione dei servizi.

XACML (eXtensible Access Control Markup Language) è un altro standard, basato su XML e definito dal consorzio OASIS, che ha lo scopo di dichiarare e stabilire le politiche, le regole, le condizioni, gli attori cui essi si riferiscono la sintassi e la semantica di un linguaggio per regolare l'accesso ad un sistema informativo. Tra i principali linguaggi esistenti per la definizione di politiche di controllo di accesso, XACML si distingue per il fatto di essere stato definito come standard, versatile all'impiego in svariati campi applicativi e non è invece legato, come spesso

accade per altre soluzioni, ad uno specifico contesto. Il linguaggio XACML definisce, come SAML, un protocollo di richiesta/risposta, ove le richieste indicano la volontà di accedere a particolari servizi. A livello comunicativo le interconnessioni sicure sono realizzate in tecnologia VPN (Virtual private network), cioè attraverso collegamenti in rete con le stesse caratteristiche di una connessione diretta (sicurezza, velocità) ma effettuati su reti condivise (internet). Questo tipo di connessione si stabilisce grazie alla tecnica del tunneling che consiste nel creare un canale privato tra il pc client ed il server in una rete privata o pubblica il tutto attraverso l'uso di un protocollo di comunicazione apposito il PPTP (Point to Point Tunnelling Protocol). A loro volta le reti interne di un medesimo Ente sono organizzate in VLAN (Virtual LAN) e assegnate ai diversi servizi. La realizzazione delle varie sottoreti tramite VLAN separate garantisce il massimo livello di sicurezza e di separazione fra le LAN sicure e quella insicura, ed allo stesso

tempo da la possibilità di differenziare le prestazioni di rete a seconda delle esigenze dei diversi segmenti garantendo caratteristiche di scalabilità e costi ottimali.

Un ulteriore livello di sicurezza all'architettura è fornito dall'utilizzo del protocollo HTTPS, che consente di applicare al protocollo di trasferimento ipertesti (HTTP) l'algoritmo di autenticazione/crittografia asimmetrica Secure Sockets Layer (SSL): esso consente di creare un canale di interscambio cifrato tra client e server per mezzo dello scambio di certificati attraverso la rete Internet, che, una volta instaurato, consente di utilizzare al suo interno il protocollo HTTP per la comunicazione.

SPCoop, il Sistema Pubblico di Connettività

Il Sistema Pubblico di Connettività (SPC) ed il Sistema Pubblico di Cooperazione (SPCoop) forniscono l'infrastruttura comune per l'interconnessione, fino al livello applicativo, delle Amministrazioni Pubbliche, centrali e locali. Scopo dell'architettura cooperativa è di abilitare l'integrazione degli oggetti informativi (procedure e dati) e delle politiche di diversi domini, favorendo la comunicazione tra entità omogenee, garantendo autonomia alle singole amministrazioni e lasciando inalterato il loro patrimonio informativo.

Il principio di base è quello di sviluppare un'architettura organizzativa atta a garantire la natura federata, policentrica e non gerarchica del sistema. Fornire un insieme di servizi di connettività condivisi dalle Pubbliche Amministrazioni garantisce l'interazione della PA centrale e locale con tutti gli altri soggetti connessi a internet, nonché con le reti di altri enti, promuovendo l'erogazione di servizi di qualità per cittadini e imprese.

Alla base di tale architettura vi e la Porta di Dominio. Essa ha lo scopo di assicurare che lo scambio elettronico di informazioni tra le Pubbliche Amministrazioni abbia le stesse caratteristiche di quello tradizionale: l'Amministrazione che invia le informazioni in modo elettronico ad un'altra e garantita del fatto che la destinataria, e non altri, le abbia ricevute, così come la ricevente può trattare le informazioni elettroniche ottenute con pari dignità di quelle che oggi riceve con i metodi tradizionali, considerati fino ad ora gli unici probanti ai fini del procedimento amministrativo. Ciò e reso possibile indipendentemente da come viene realizzata la porta di dominio (fornitore, linguaggi, tecnologia,...) in quanto la sua interfaccia è stata definita e condivisa tra i diversi domini.

Le Porte devono interagire con i servizi applicativi esposti dalle singole Amministrazioni e colloquiare tra loro secondo gli standard definiti nell'ambito dell'SPCoop in maniera paritetica.

Per attuare tale disegno occorre che tutti gli attori (Amministrazioni centrali e locali, enti ed aziende) condividano le specifiche, gli standard e le modalità di realizzazione e gestione dei complessi elementi infrastrutturali comuni che disaccoppiano i sistemi (eventualmente legacy) delle amministrazioni ed implementano i servizi che abilitano la cooperazione applicativa tra sistemi.

Per scambiare messaggi applicativi fra Porte di Dominio si utilizza la busta di e-Government che è la definizione del formato di codifica e del contenuto dei messaggi SOAP utilizzati per implementare, sotto forma di Web services, i servizi esposti dalle Porte Applicative delle Amministrazioni Pubbliche. Lo strumento utilizzato per definire un formato dei dati condiviso tra tutte le Amministrazioni, a prescindere dai sistemi legacy e dalle basi dati, e XML. SOAP è invece utilizzato come standard per veicolare le informazioni codificate con XML sulla rete Internet mediante il protocollo HTTP. In generale, il tipo di struttura da utilizzarsi per busta e contenuto dipende dal tipo di messaggio e dalle esigenze di carattere normativo. In ambito sanitario si utilizzano esclusivamente messaggi che richiedono l'apposizione della firma digitale per garantire la fonte di provenienza delle informazioni.

SOA e Web Service

Una SOA (Service Oriented Architecture), è un'architettura software, fortemente orientata al riuso e alla integrazione, che prevede la esposizione della logica applicativa sotto forma di servizi accoppiati tra loro in modo "debole". A livello implementativo la tecnologia utilizzata per lo sviluppo dei servizi non è determinante: l'idea di base è quella di racchiudere le funzionalità all'interno di interfacce che, nascondendo i dettagli tecnico/implementativi, sono esposte secondo modalità e forme documentate in modo standard e messe a disposizione su un apposito catalogo.

Si tratta di una filosofia progettuale particolarmente adatta a contesti applicativi distribuiti caratterizzati da marcata eterogeneità e complessità, forte dinamismo e elevato grado di interazione tra le diverse componenti, quale può essere il dominio applicativo sanitario. In esso infatti, è presente una molteplicità di attori che, a seconda delle specifiche situazioni, creano o utilizzano le informazioni, ed interagiscono tra loro secondo modalità non del tutto prevedibili a priori. Inoltre, molti Enti/strutture coinvolte dispongono già di un patrimonio informativo e

applicativo (legacy) che costituisce un bene rilevante, sia dal punto di vista economico (in quanto frutto di consistenti investimenti), sia da quello tecnologico: tale patrimonio richiede da un lato di essere preservato e dall'altro di essere messo in condizione di interagire con gli omologhi di altri enti, qualunque siano le piattaforme applicative sulle quali sono stati realizzati.

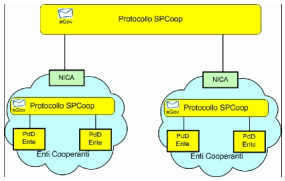
Una delle tecnologie maggiormente utilizzate per la realizzazione di architetture orientate ai servizi è quella dei Web Services, una specifica di protocolli e standard utilizzata per realizzare comunicazioni tra applicazioni di diversa natura interconnessi ad una medesima rete per garantirne l'interoperabilità. I Web Services sono pensati per realizzare dei blocchi funzionali indipendenti che, nel complesso, possano costituire un ambiente applicativo. Essi godono di alcune proprietà che li rendono particolarmente adatti per essere impiegati all'interno delle SOA. Una di queste proprietà è la completa autonomia che caratterizza ciascun servizio rispetto agli altri: ogni servizio è responsabile di un proprio dominio, con conseguente formazione di unità funzionali ben delineate e blandamente collegate tra loro mediante la aderenza ad uno standard di comunicazione. In virtù della indipendenza di cui i servizi godono, la logica applicativa che ciascun servizio incapsula non deve conformarsi a nessuna piattaforma particolare. Affinché essi possano offrire un'interfaccia software, sono descritti in un formato automaticamente elaborabile quale, ad esempio, il Web Services Description Language, utilizzando la quale altri sistemi possono interagire con il Web

Service stesso attivando le operazioni descritte nell'interfaccia tramite appositi "messaggi" inclusi in una "busta", in particolare la SOAP: tali messaggi sono, solitamente, trasportati tramite il protocollo HTTP e formattati secondo lo standard XML. Essi godono di alcune proprietà che li rendono particolarmente adatti per essere impiegati all'interno delle SOA. In virtù della indipendenza di cui i servizi godono, la logica applicativa che ciascun servizio incapsula, non deve conformarsi a nessuna piattaforma particolare. Proprio grazie all'utilizzo di standard basati su XML, tramite un'architettura SOA, applicazioni software scritte in diversi linguaggi di programmazione ed implementate su diverse piattaforme hardware possono, quindi, essere utilizzate tramite le interfacce che queste "espongono" pubblicamente e mediante l'utilizzo delle funzioni che sono in grado di effettuare (i "servizi" che mettono a disposizione) per lo scambio di informazioni e l'effettuazione di operazioni complesse sia su reti aziendali, come su Internet.

Tutti i dati scambiati sono formattati mediante tag XML in modo che gli stessi possano essere utilizzati ad entrambi i capi delle connessioni; il messaggio può essere codificato conformemente allo standard SOAP. L'interfaccia pubblica di un Web Service viene descritta tramite WSDL, un linguaggio basato su XML usato per la creazione di "documenti" descrittivi delle modalità di interfacciamento ed utilizzo del Web Service. La centralizzazione della descrizione e della localizzazione dei Web Service in un registro comune permette la ricerca ed il reperimento in maniera veloce dei Web Service disponibili in rete; a tale scopo viene attualmente utilizzato il protocollo UDDI.

I Web service hanno, inoltre, guadagnato consensi visto che, come protocollo di trasporto, possono utilizzare HTTP over TCP sulla porta 80; tale porta è, normalmente, una delle poche (se non l'unica) lasciata aperta dai sistemi firewall al traffico di entrata ed uscita dall'esterno verso i sistemi aziendali e ciò in quanto su tale porta transita il traffico HTTP dei web browser: ciò consente l'utilizzo dei Web Service senza modifiche sulle configurazioni di sicurezza dell'Amministrazione, un aspetto che, se da un lato è positivo, solleva preoccupazioni concernenti la sicurezza, motivo per cui si rendono necessari meccanismi di autenticazione dei Web Services stessi.

Come già anticipato, il sistema per la cooperazione applicativa a norma CNIPA-DigitPA – SPCoop richiede la realizzazione di sistemi per la integrazione (o l'abilitazione) del dominio applicativo dell'Ente/Amministrazione locale della Regione Abruzzo. In particolare, è necessario realizzare un insieme di componenti SPCoop, sottoinsieme del più vasto set di componenti detto "Nodo di Interconnessione per la Cooperazione Applicativa" (NICA nel seguito), che costituisce l'unico punto di ingresso/uscita della Rete Privata della Regione Abruzzo.



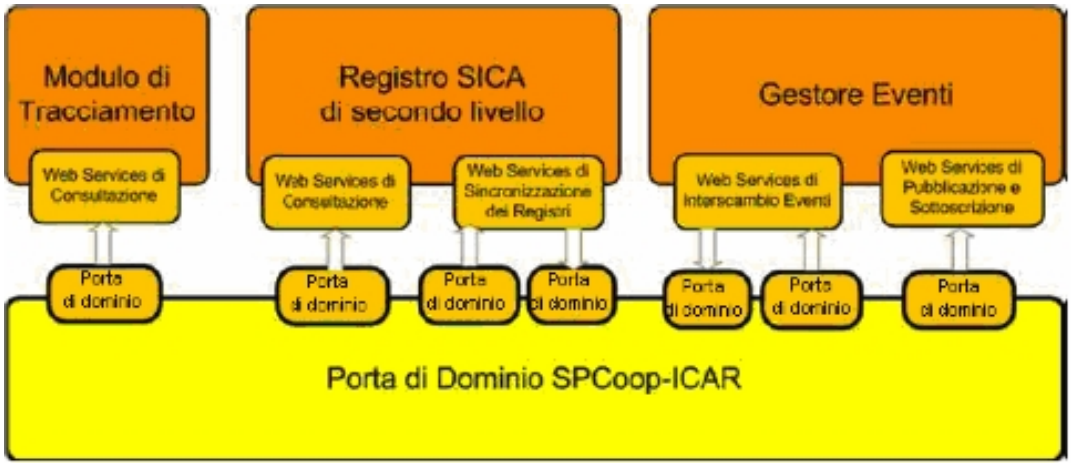
Generalmente il NICA è composto dai seguenti moduli:

- una Porta di Dominio

- un Gestore Eventi

- un Sistema di Tracciatura e Monitoraggio

- un Registro SICA secondario

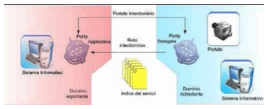


Dei suddetti moduli solo il primo è richiesto che venga messo in esercizio dall'Ente che decide di gestire autonomamente la propria Porta di Dominio anziché appoggiarsi alla struttura ARIT. Opzionali sono invece i moduli di Gestione Eventi e di Tracciatura e Monitoraggio perché disponibili nel NICA della Regione Abruzzo. Tuttavia, l'Ente che decida di gestire autonomamente anche tali moduli potrà farlo rispettando quelle che sono le specifiche tecniche del progetto ICAR. L'unico componente che non potrà essere realizzato dal singolo Ente regionale è il Registro SICA secondario perché, sempre secondo le specifiche del progetto ICAR nazionale, è previsto che venga realizzato uno ed un solo registro per Regione.

L'elemento tecnologico centrale per la cooperazione applicativa è rappresentato dalla Porta di

Dominio. Da un punto di vista fisico, essa può essere considerata un componente infrastrutturale della Rete, un “proxy” per l’accesso alle risorse applicative. Dal punto di vista dell’architettura applicativa, la Porta di Dominio può essere vista come un adattatore che consente a sistemi informatici esistenti, o comunque realizzati in base alle esigenze del dominio specifico, di affacciarsi sulla rete e partecipare all’interscambio telematico delle informazioni.

Nella figura successiva si evidenzia il modello di cooperazione applicativa, dove il termine “sistema informativo” deve essere inteso nella sua accezione più ampia.



In particolare, può trattarsi di:

- un sistema monolitico, o, comunque, operante su un singolo nodo presso una struttura di piccole dimensioni;

- un sistema distribuito su più nodi collegati in rete locale presso una struttura di dimensioni maggiori;

- una rete di area, alla quale sono collegati i sistemi informatici di strutture anche diverse, o di una singola struttura.

Risulta, quindi, chiaro che le porte di dominio, come componenti software di adattamento, possono essere chiamate a svolgere funzioni di integrazione diverse, a seconda del contesto nel quale si trovano ad operare. In particolare possiamo distinguere:

- la **Porta Applicativa** che è la Porta di Dominio atta all’erogazione dei servizi. Ogni dominio

esportante, in grado cioè di fornire servizi, lo fa attraverso la Porta Applicativa. La Porta Applicativa ha un riferimento sull'Indice dei Servizi in corrispondenza di tutti i servizi che esporta sia in modo diretto che indiretto. La Porta Applicativa è sempre in ascolto per accogliere le richieste fatte al dominio. Attraverso opportuni moduli denominati Wrapper, la Porta Applicativa interfaccia i sistemi informatici che sono alla base dell'erogazione di uno specifico servizio. Un servizio particolare della Porta di Dominio è quello di ricezione e gestione degli eventi come descritto in seguito.

- la **Porta Delegata** che è la Porta di Dominio attraverso cui si richiedono servizi o si notificano eventi ad un altro Dominio. La Porta Delegata è attivata dai Sistemi Informatici o dal Portale e sfrutta i servizi di Rete per realizzare la collaborazione.

Le collaborazioni principali prevedono l'adozione di modalità sincrone e asincrone di scambio dei messaggi. E' bene notare che le modalità sincrona e asincrona sono intese relativamente allo scambio di una coppia di messaggi, uno in andata e l'altro in ritorno. Il sincronismo è visto dal punto di vista della porta delegata. In uno scambio sincrono, la porta delegata, a seguito dell'invio del messaggio di andata, rimane in attesa del messaggio di ritorno. Viceversa, in uno scambio asincrono, i due messaggi di andata e di ritorno vengono scambiati senza che una delle due parti rimanga in attesa.

La scelta della modalità sincrona o asincrona può anche dipendere da aspetti legati alla latenza amministrativa delle procedure amministrative (es.: la necessità di intervento umano, ad esempio per l'apposizione della firma digitale di un pubblico ufficiale).

- **Collaborazione Sincrona**: è quella più semplice e tipicamente, è la modalità prevista per le richieste di informazioni. Presso il dominio richiedente il messaggio è formato dal sistema informativo, quindi trasmesso dalla porta delegata. La porta delegata rimane in attesa del messaggio di ritorno. Presso il dominio esportante il messaggio viene ricevuto ed immediatamente elaborato con la formazione e trasmissione del messaggio di ritorno. La collaborazione sincrona, una volta adottata, è da considerarsi come obbligatoria per le parti coinvolte. In altri termini, la porta applicativa deve restituire un messaggio di eccezione se l'elaborazione sincrona non è possibile, per esempio a causa di problemi tecnici temporanei.

- **Collaborazione Asincrona**: una forma lievemente più complessa di collaborazione è quella basata sulla modalità sincrona con possibilità di transizione ad una modalità asincrona. La prima fase di collaborazione e sostanzialmente eguale a quella descritta nel caso precedente

(collaborazione sincrona), con la formazione e la trasmissione di un messaggio presso il dominio richiedente. Anche in questo caso la porta delegata rimane in attesa del messaggio di ritorno. La differenza consiste nel fatto che il sistema esportante può eventualmente passare alla modalità asincrona, ad esempio per fare fronte a situazioni di carico eccessivo e/o di concomitanza con altre situazioni straordinarie. In caso di passaggio alla modalità asincrona, la porta applicativa si limita a restituire un messaggio di ritorno che conferma la ricezione del messaggio e attesta la presa in carico della richiesta in esso contenuta. In un tempo differito, successivo, la porta delegata, trasmette un messaggio con l'identificatore della richiesta e rimane in attesa del messaggio di ritorno. Se il sistema esportante ha la risposta, la restituisce e conclude la collaborazione, altrimenti risponde con un nulla di fatto e la transazione dovrà essere ripetuta.

In generale, il servizio rappresenta la modalità più diretta di collaborazione tra due sistemi. Una richiesta, sottoposta da un sistema ad un altro, scatena in quest'ultimo l'esecuzione di un processo applicativo il cui risultato viene restituito sotto forma di risposta. Il servizio è tipicamente un tipo di collaborazione sincrona ma è scomposto in due fasi differite nel tempo: sottomissione della richiesta e ricezione della risposta, può realizzare anche una collaborazione asincrona. Nei due casi, però, l'approccio dei sistemi informatici coinvolti nella collaborazione cambia sostanzialmente. Nel caso asincrono, chi effettua la richiesta deve essere in grado di iterare più volte il processo di richiesta, mentre il sistema che eroga il servizio deve essere in grado di gestire il sistema di code di richieste e di risposte.

La Porta di Dominio SPCoop-ICAR dovrà rispettare le specifiche SPCoop Ver. 1.1 e aggiunge anche le funzionalità di:

- relay SPCoop trasparente;

- tracciamento;

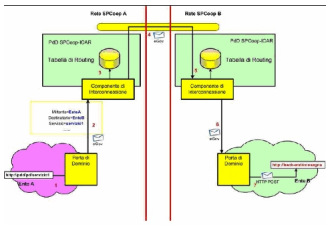
- sicurezza (Firewall XML).

Di seguito sono illustrate le funzionalita sopra citate.

Funzioni di relay SPCoop trasparente

Nella PdD SPCoop-ICAR dovrà essere presente una Componente di Interconnessione (CdI) che realizzerà la funzionalità di relay ossia ridirigerà le buste e-Gov verso i rispettivi destinatari. Il CdI si occupa quindi di ispezionare la busta e-Gov per identificare il servizio destinatario della busta. Se si tratta di un destinatario fuori dalla propria rete privata SPCoop, la busta sarà indirizzata alla PdD SPCoop-ICAR di ingresso della rete privata SPCoop di appartenenza, altrimenti alla rispettiva Porta di Dominio relativa al dominio di cooperazione destinatario.

L'ottimizzazione delle topologie di rete non modifica in alcun modo la logica punto punto della comunicazione tra la porta di dominio mittente e quella destinataria. L'esempio mostrato nella figura seguente evidenzia il dettaglio dei vari passaggi della busta e-Gov nell'interazione di una richiesta di servizio da un generico Ente A ad un generico Ente B appartenenti a reti SPCoop diverse.



In particolare, l'interazione si svolge tramite i seguenti passi: 1. invocazione della porta delegata da parte del Sistema Informativo interno al dominio di cooperazione dell'Ente A; 2. la porta di dominio mittente costruisce la busta e la spedisce alla PdD SPCoop-ICAR di ingresso/uscita nella sua Rete Privata SPCoop, 3. il CdI della PdD SPCoop-ICAR di ingresso/uscita, una volta effettuata la validazione della busta con successo, interroga la propria tabella di routing per individuare l'endpoint a cui inoltrare la busta. In questo esempio, dalle informazioni sulle proprie tabelle di routing, decide di inoltrarla al PdD SPCoop-ICAR della Rete Privata SPCoop B; 4. il CdI invia la busta alla PdD SPCoop-ICAR della Rete Privata SPCoop B; 5. la PdD SPCoop-ICAR della Rete Privata SPCoop B interroga la tabella di routing per capire dove spedire la busta. Si accorge che deve spedirla ad una porta di dominio locale alla propria Rete Privata SPCoop; 6. la busta viene inviata alla Porta di Dominio dell'Ente B; 7. la porta di dominio destinataria una volta ricevuta la busta ne effettua la validazione e in caso di successo la consegna al servizio locale abbinato alla porta applicativa riferita nella busta e-Gov.

E’ necessario, pertanto, gestire le seguenti situazioni:

- necessita di supportare dal punto di vista tecnico, organizzativo, gestionale i soggetti che parteciperanno alla comunità SPCoop;

- frequente necessità di aggiornamento delle PdD deployate;

- necessità di monitorare costantemente la rete SPCoop;

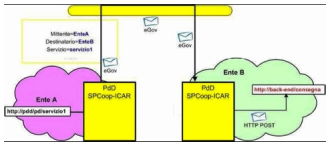
- necessità di intervenire in maniera coordinata sui Soggetti all’occorrenza di un problema.

Questi problemi dovrebbero disincentivare l’utilizzo di collegamenti punto punto tra PdD tendendo a strutturale la Rete SPCoop in un insieme di reti Private SPCoop. Comunque la PdD SPCoop- ICAR può essere utilizzata anche per realizzare comunicazioni punto punto. La figura che segue mostra un esempio in cui un Ente usa direttamente una PdD SPCoop-ICAR (ossia le buste generate dalla sua PdD non attraversano componenti della sua rete privata SPCoop configurate in modalità relay per raggiungere il destinatario) per richiedere un servizio.

Sarà anche possibile non utilizzare la funzione di relay della PdD SPCoop-ICAR utilizzando direttamente le PdD SPCoop-ICAR come indicato nella figura seguente. Quindi la PdD SPCoop- ICAR garantisce la massima flessibilità nel dispiegamento sul territorio. Nel caso in cui la PdD SPCoop-ICAR venga dispiegata in modalita “relay” risulteranno enormemente semplificati i compiti di monitoraggio e di sicurezza della Rete Privata SPCoop poiché potranno essere gestiti in un unico punto.

Funzioni di Tracciamento

La PdD SPCoop-ICAR tiene traccia delle Buste e-Gov inviate e delle Buste e-Gov ricevute in transito.



Il tracciamento realizzato nell'implementazione di riferimento si attiene a quanto definito nel documento "Sistema pubblico di cooperazione: Porta di Dominio" del CNIPA-DigitPA. Viene quindi tracciato solo l'header e-Gov insieme all'ora di registrazione identificativo della porta di dominio tipo di Messaggio (Richiesta/Risposta)

La PdD esporrà le interfacce (web-services) attraverso cui sia possibile, in modo concorrente (on- line) recuperare le tracce.

Funzioni di sicurezza

La PdD SPCoop-ICAR implementa la funzionalità di Firewall-XML. Grazie alla funzionalità di Firewall-XML una PdD SPCoop-ICAR configurata in modalità relay potrà bloccare tutto il traffico in ingresso alla Rete SPCoop che non rispetta determinate regole. Le regole del firewall avranno come oggetto l'header delle buste di e.Gov. Qualora una busta di e- Gov non rispetti le regole stabilite la PdD SPCoop-ICAR ne terrà traccia.

La PdD SPCoop-ICAR, come da specifica SPCoop, identifica tutti i soggetti infrastrutturali e applicativi in gioco tramite certificati X.509 rilasciati da PKI riconosciute e l'uso di WS-Security tramite X509 Token Profile e SAML 2.0, compatibilità con SAML 1.1, per la gestione di autenticazione e autorizzazione da parte delle Porte di Dominio.

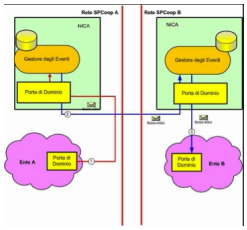
All'interno del NICA dovrà essere presente un modulo per la realizzazione di scambio di buste e-Gov secondo l'architettura **EDA (Event Driven Architecture)**, ovvero per la realizzazione di una politica di distribuzione in modalità pub-sub (publishing-subscribing). In questa modalità, un servizio che pubblica buste potrà essere associato ad una lista di servizi sottoscrittori che riceveranno tale busta all'atto della sua pubblicazione.

Il Gestore Eventi deve occuparsi di offrire un registro dei pubblicatori e relativi sottoscrittori e gestire la modalità di sottoscrizione, pubblicazione e distribuzione. Il Gestore Eventi SPCoop-ICAR è il primo dei servizi a valore aggiunto che sarà reso disponibile come deliverable di progetto. Il servizio, come accennato, permetterà lo scambio di buste egov secondo l'architettura EDA (Event Driven Architecture), permettendo agli iscritti di ricevere le buste inviate dai pubblicatori. Da questo punto di vista il Gestore Eventi SPCoop-ICAR può essere considerato un normale servizio SPCoop, accessibile come mostrato nella figura precedente.

Se si considerano eventi alla cui ricezione siano interessati un elevato numero di altri Enti, potenzialmente distribuiti su tutto il territorio nazionale, si può cogliere l'importanza di strutturare i Gestori di Eventi secondo una logica interregionale. In un caso del genere, si rende evidente l'utilità di scalare a livello interregionale lo smistamento degli eventi verso i potenziali fruitori.

Per questo motivo è previsto un Gestore Eventi in grado di dialogare per la ricezione e la consegna degli eventi non soltanto con le porte di dominio SPCoop ma anche con gli altri gestori di eventi SPCoop-ICAR. Nel seguito è illustrato un esempio di pubblicazione di un evento, da parte di un sistema informativo pubblicante (nell'esempio Ente A), e la sua ricezione da parte di un sistema informativo ricevente (nell'esempio Ente B), precedentemente registratosi presso il proprio Gestore Eventi. Il Gestore Eventi SPCoop-ICAR della Rete Privata SPCoop B si suppone iscritto alla ricezione di questo tipo di eventi presso il Gestore Eventi SPCoop-ICAR della Rete Privata SPCoop A.

La figura che segue mostra la fase di pubblicazione dell'evento da parte dell'Ente A sul Gestore Eventi SPCoop-ICAR della Rete Privata SPCoop A.



Come mostrato in figura, la pubblicazione di un evento da parte dell'Ente A si svolgerà attraverso i seguenti passi:

- la pubblicazione dell'evento sul Gestore Eventi SPCoop-ICAR della Rete Privata SPCoop A;

- la ricezione dell'Evento da parte del Gestore Eventi SPCoop-ICAR della Rete Privata SPCoop B, il cui Gestore Eventi si era precedentemente iscritto alla ricezione di questi tipo di eventi presso il Gestore della Rete Privata SPCoop A;

- la conseguente pubblicazione dell'evento sul Gestore Eventi SPCoop-ICAR della Rete Privata SPCoop B;

- la ricezione dell'Evento da parte dell'Ente B, la cui Porta di Dominio era precedentemente iscritta alla ricezione di questo tipo di eventi presso il Gestore Eventi SPCoop-ICAR della Rete Privata SPCoop B.

Le raccomandazioni reperibili dalla documentazione ICAR per quel che riguarda i componenti architetturali di pertinenza del **Task infrastrutturale INF-2** "*Gestione di Strumenti di Service*

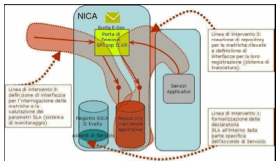
Level Agreement a livello interregionale SPECIFICHE TECNICHE DEL SISTEMA (INF2_SPE) ” si articolano lungo le seguenti tre linee di intervento:

- specifica dei livelli di servizio negli accordi di servizio;

- sistema di tracciatura;

- sistema di monitoraggio.

Il compito legato alla prima linea di intervento è, tuttavia, limitato all’individuazione del formalismo da utilizzare nella dichiarazione dei parametri SLA associati ai servizi applicativi cooperanti. Si può schematizzare l’architettura generale dell’intervento nel seguente modo.



La reference implementation del progetto ICAR comprende esempi di tracciatura e monitoraggio di parametri SLA. Questi esempi prevedono parametri derivanti da metriche di risorsa “di base”, utili, cioè, a fondare un sistema di gestione SLA semplice ma significativo ed in grado di evolvere verso forme di monitoraggio più sofisticate a seconda delle necessità che si potranno creare.

Per quanto riguarda invece la seconda e terza linea di intervento, si riporta di seguito un breve descrizione.

Sistema di tracciatura

Secondo le specifiche WS-Agreement, il sistema di tracciatura deve permettere ai servizi applicativi interdominio di tracciare lo stato del Servizio (“ServiceTerm”) e lo stato dei parametri SLA (“GuaranteeTerm”). Il sistema di tracciatura deve quindi prevedere i seguenti sotto componenti:

- DBWSA: un database in cui sono memorizzate le misurazioni delle metriche di risorsa associate ai parametri SLA contenuti nell’Accordo di Servizio e un dato indicatore dello stato del servizio;

- Interfaccia di scrittura sul Sistema di Tracciatura: un componente che espone dei metodi verso i servizi applicativi erogatori, utilizzabili per: o aggiornare lo stato del servizio; o inserire i dati necessari al sistema di tracciatura per generare gli SLA presenti nell’Accordo di Servizio.

- Interfaccia Operatore per consentire interattivamente di: o inserire nuovi servizi; o monitorare lo stato dei servizi; o monitorare lo stato degli SLA di ogni servizio.

La conformazione di questo database deve essere progettata per consentire di tener traccia di: - lo stato dei servizi messi a disposizione dall’Ente Erogatore; - le misure associate alle metriche di risorsa dichiarate negli Accordi di Servizio. Tali misure saranno realizzate in concomitanza con ogni erogazione del servizio relativo da parte dei servizi erogatori; gli algoritmi pubblicati nel repository degli Accordi di Servizio, per facilitare il calcolo dei parametri SLA da parte del sistema di monitoraggio.

Sistema di monitoraggio

Il Sistema di Monitoraggio espone tramite la Porta di Dominio i seguenti servizi (dei quali sarà specificato l’Accordo di Servizio completo):

- **ServiceTermState**: permetterà di ricavare lo stato di un servizio relativo ad un determinato Accordo di Servizio;

- **ServiceGuaranteeTerm**: permetterà di ricavare lo stato di uno o più parametri SLA ("ServiceLevelObject") per un servizio relativo ad un determinato Accordo di Servizio.

---

[1] ICAR-TaskINF1-D_ARCH-Linee_Architetturali.1.1.7.pdf

Task INF-1: Realizzazione dell'Infrastruttura di base per l'Interoperabilita e la Cooperazione Applicativa a livello interregionale: LINEE ARCHITETTURALI

[2] ICAR-INF-2-SpecificheTecniche3.0.pdf

Task INF-2: Gestione di Strumenti di Service Level Agreement a livello interregionale SPECIFICHE TECNICHE DEL SISTEMA (INF2_SPE)

[3] ICAR_Task_INF2_ParametriMonitoraggio2.1.pdf

Task INF-2: Gestione di Strumenti di Service Level Agreement a livello interregionale DEFINIZIONE DEI PARAMETRI SOGGETTI A MONITORAGGIO SLA

[4] ICAR_Task_INF2_Manuale1.0.pdf

Task INF-2: Gestione di Strumenti di Service Level Agreement a livello interregionale
MANUALE D'USO DI GESTIONE DEGLI STRUMENTI DI SLA A LIVELLO INTERREGIONALE

[5] ICAR-INF3-ModelloConcettuale_v1 0 2.pdf

Task INF-3: Sistema Federato Interregionale di Autenticazione: MODELLO CONCETTUALE DI RIFERIMENTO

[6] ICAR-INF-3-ModelloArchitetturale_v1.0.pdf

Task INF-3: Sistema Federato Interregionale di Autenticazione: MODELLO ARCHITETTURALE DI RIFERIMENTO

[7] ICAR-INF-3-ModelloOrganizzativo_v1.0.pdf

Task INF-3: Sistema Federato Interregionale di Autenticazione: ORGANIZZAZIONE

[8] ICAR - Task Ap1 - Modellazione organizzativa_v1.1.pdf

Task AP-1: Cooperazioni e compensazioni sanitarie: MODELLAZIONE ORGANIZZATIVA

[9] ICAR - Task Ap1 Modellazione Interfacce logiche e dati V1.4.pdf

Task AP-1: Cooperazioni e compensazioni sanitarie: MODELLAZIONE INTERFACCE

LOGICHE E DATI

[10] ICAR - Task Ap1 Documento Descrittivo Accordi di servizio.pdf

Task AP-1: Cooperazioni e compensazioni sanitarie: DOCUMENTO DESCRITTIVO DEGLI ACCORDI DI SERVIZIO

[11] ICAR – Task Ap2 cooperazione tra sistemi di anagrafe.pdf

Task AP-2: Cooperazione tra sistemi di anagrafe: ORGANIZZAZIONE

[12] ICAR - Task Ap3 - specificaADSv1.2.1.pdf

Task AP-3: Aree Organizzative Omogenee: SPECIFICHE DEGLI ACCORDI DI SERVIZIO

[13] ICAR - Task Ap3 - EstensioneSegnaturaInformatica.pdf

Task AP-3: Aree Organizzative Omogenee: ESTENSIONE DEL SISTEMA DI SEGNATURA INFORMA TICA

[14] ICAR - Task Ap3-Ontologia-v1.2.pdf

Task AP-3: Aree Organizzative Omogenee: ONTOLOGIA

[15] ICAR - Task Ap4 - Ontologia-v1.3.pdf

Task AP-4: Lavoro e specifiche per l'impiego: ONTOLOGIA

[16] ICAR - Task Ap4 - specificaADSv1.3.pdf

Task AP-4: Lavoro e specifiche per l'impiego: DOCUMENTO DESCRITTIVO DEGLI ACCORDI DI SERVIZIO

[17] ICAR- Task Ap4 - AnnotazioneSemanticaADS-ver1.0.pdf

Task AP-4: Lavoro e specifiche per l'impiego: ANNOTAZIONE SEMANTICA DEGLI ACCORDI DI SERVIZIO

[18] ICAR - Task Ap5 - Specifiche di cooperazione V1.1.pdf

Task AP-5: Tassa automobilistica regionale: SPECIFICHE DEL SISTEMA DI COOPERAZIONE

[19] ICAR_Task AP6 - SpecificaInterfacciaV2.5.1.pdf

Task AP-6: Osservatorio sulla rete distributiva dei carburanti: SPECIFICHE DI INTERFACCIA DEI SISTEMI REGIONALI

[20] ICAR - Task Ap7 - ModelloArchitetturale-InterfacceInterne-v095.pdf

Task AP-7: Sistema informativo di raccordo con CINSEDO: MODELLO ARCHITETTURALE – SPECIFICA DELLE INTERFACCE INTERNE E MODELLO DATI

[21] ICAR - Task Ap7 - SpecificaAccordodiServizio-v06.pdf

Task AP-7: Sistema informativo di raccordo con CINSEDO: ACCORDO DI SERVIZIO