REGIONE MARCHE

Infrastrutture tecnologiche abilitanti della Regione Marche

Codice Versione:	def-4
Data emissione:	01/08/2011
Distribuzione:	interna, altri enti, fornitori

REDATTO DA				
< Amici Cinzia >	Firma		Data	18/01/2011
< Maggiulli Maria Laura >	Firma		Data	18/01/2011
< Sergiacomi Andrea >	Firma		Data	18/01/2011
< Settimi Donatella >	Firma		Data	18/01/2011
< Trojani Massimo >	Firma		Data	18/01/2011
EMESSO DA				
< Carota Serenella >	Firma		Data	01/08/2011
APPROVATO DA				
< Carota Serenella >	Firma		Data	01/08/2011

Note sulle MODIFICHE APPORTATE

BOZ-1	Bozza in condivisione per ciascun funzionario competente sui vari componenti dell'infrastruttura
DEF-1	Prima stesura definitiva condivisa
DEF-2	Seconda stesura allegata al progetto SIRA (Sistema Informativo Regionale Ambiente)
DEF-3	Terza stesura – aggiornamento sistema di autenticazione Cohesion Single Sign On in ottica federata SAML 2.0
DEF-4	Quarta stesura – generalizzazione standard di riferimento ad uso di ogni gara o progetto riferito a sistemi informativi che impiegano l'infrastruttura

REGIONE MARCHE

INDICE DELLE FIGURE

REGIONE MARCHE

INDICE GENERALE

1 LE INFRASTRUTTURE TECNOLOGICHE ABILITANTI

1.1 LA DIGITALIZZAZIONE NELLA REGIONE MARCHE

1.1.1 Introduzione

Nei paragrafi seguenti, verranno illustrati strumenti inerenti la cittadinanza digitale sviluppati nei progetti promossi dalla Regione Marche che nel tempo ha reso disponibili nel rispetto della normativa in materia di documentazione amministrativa in formato digitale per concretizzare l'obiettivo della società dell'informazione che verranno integrati in tutti i progetti futuri e quindi:

- framework Cohesion
- CNS-Carta Raffaello
- firma digitale
- PEC-Posta Elettronica Certificata
- protocollo informatico
- documento informatico
- Sistema Pubblico di Cooperazione

che diano rilevanza giuridica alle operazioni on-line.

Questo nuovo modello di interazione G2C richiede che all'utente fruitore dei servizi telematici (cittadino, impresa ente pubblico) sia fornita una "**cittadinanza digitale**" ovvero la possibilità per l'utente di disporre di una serie di fattori abilitanti e di strumenti, quali:

- **Identità digitale** tramite la dotazione delle credenziali SPID o della Carta Raffaello o TS-CNS per l'accesso sicuro ai servizi offerti via web attraverso un'autenticazione forte;
- **Diritti di accesso** ai servizi offerti via web secondo modalità valide per tutti i cittadini-utenti ed impiegando un catalogo dei servizi;
- **Firma digitale** dei documenti prodotti on line da sottomettere all'amministrazione;
- **Posta elettronica certificata (PEC) e sistema dei flussi documentali** per le comunicazioni a carattere ufficiale tra utente e PA;

La cittadinanza elettronica deve essere estesa, necessariamente, anche ai soggetti operanti all'interno della amministrazione che costituiscono il "back office" deputato alla effettiva erogazione dei servizi.

1.1.2 Il framework regionale Cohesion

Cohesion mette a disposizione una piattaforma infrastrutturale basata su di un sistema, organizzato ed aggregato, di diversi standard e diversi servizi telematici, fisicamente localizzabili presso la server farm della Regione Marche. Tale centro servizi ha lo scopo di supportare gli aspetti tecnici di gestione ed erogazione per via telematica di servizi amministrativi basati sul variegato patrimonio di contenuti, banche dati e servizi esposti dagli enti della Regione.
Il framework offre una serie di funzionalità chiave centralizzate quali servizi per la cooperazione applicativa, la sicurezza e l'autenticazione ed un sistema di SSO, l'automazione delle procedure e della documentazione e la gestione dei contenuti.

Il Single Sign On (SSO)

Quello che accade attualmente ad un generico utente Internet è che per avere la possibilità di usufruire di servizi resi disponibili on line deve possedere un vasto numero di account disseminati tra siti internet isolati. Questo modello comporta notevoli disagi agli utenti costretti a dover ricordare dozzine di coppie login e password e a ripetere le procedure di autenticazione ogni qualvolta passano da un sistema di erogazione ad un altro.
I disagi, peraltro, non si limitano solo agli utenti ma anche ai fornitori di servizi costretti a loro volta a implementare onerosi servizi di supporto agli utenti spesso quasi esclusivamente destinati alla gestione delle problematiche relative alla dimenticanza dei dati di autenticazione.

I sistemi di singola autenticazione (Single Sign On) consentono all'utente di autenticarsi una sola volta e di poter successivamente utilizzare i servizi erogati da tutti i sistemi che condividono lo strumento di Single Sign On senza dover ripetere l'autenticazione. In questo modo si possono costituire dei veri e propri circoli di fiducia all'interno dei quali l'utente non deve compiere autenticazioni ripetute.

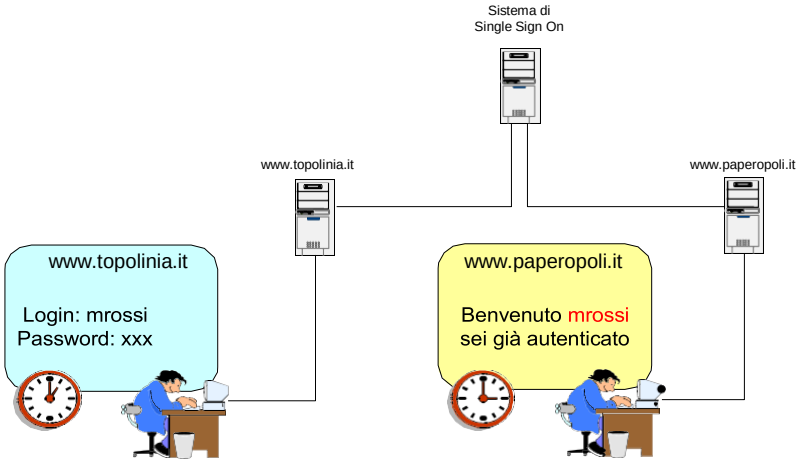

FIGURA 1 – PROCESSO DI SINGLE SIGN ON

L'identità digitale

Al fine di consentire l'accesso ai servizi solamente agli utenti che hanno il diritto, un sistema di erogazione dei servizi (ad es. un Portale dei Servizi) deve essere in grado di rilevare l'identità elettronica del richiedente, cioè quell'insieme di informazioni e dispositivi che consentono all'utente di essere correlato con il proprio profilo memorizzato all'interno dei sistemi informativi dell'amministrazione. Questa associazione avviene, solitamente, per mezzo di un codice univoco assegnato dall'amministrazione all'utente.
Si possono distinguere due tipologie di identità elettronica:

- *Identità elettronica interna*, costituita dal codice univoco presente all'interno dei sistemi informativi
- *Identità elettronica esterna*, costituita dalle procedure e dai dispositivi forniti all'utente per poter usufruire dei servizi erogati attraverso procedure telematiche.

Secondo questa classificazione, l'autenticazione dell'utente è quella procedura che consente l'associazione tra l'identità elettronica interna e quella esterna.
Considerato il fatto che ogni cittadino italiano è dotato, fin dalla sua nascita, del Codice Fiscale, che per sua natura è univoco, appare naturale utilizzarlo come la sua identità elettronica interna.
Un sistema di autenticazione, pertanto, deve essere sufficientemente "forte" da consentire una associazione certa dell'identità personale dell'utente con la sua identità elettronica interna, in questo caso il Codice Fiscale.

Il Processo di Autenticazione

La soluzione proposta si basa su quattro concetti fondamentali:

- Web Redirection
- Cookies
- Web Services
- Metadati XML

In Figura 2 illustrato lo schema di interazione tra l'utente, il sistema di erogazione dei servizi e il servizio di autenticazione che fa uso del meccanismo di ridirezionamento.

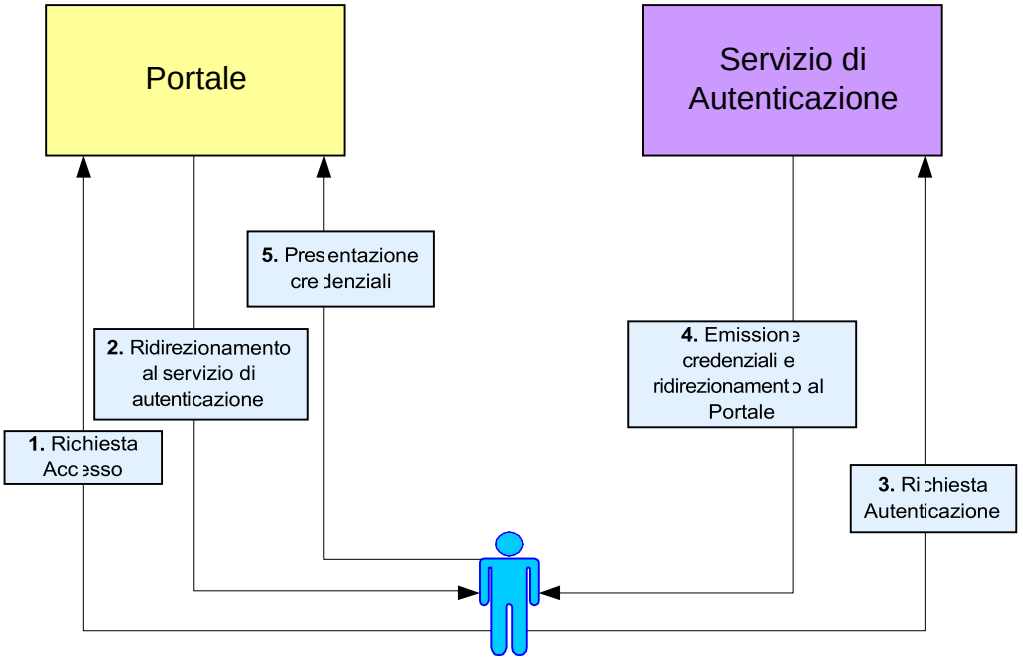

FIGURA 2 – SCHEMA DI INTERAZIONE

I passi sono dettagliati come segue:

1. **Richiesta di Accesso**: l'utente tenta l'accesso alla sezione autenticata di un portale. Dal punto di vista tecnico si può assumere, senza perdita di generalità, questa operazione come sostanziata in una HTTP Request presso il server.
2. **Ridirezionamento**: il browser utilizzato dall'utente viene ridirezionato al servizio di autenticazione. Dal punto di vista tecnico questa operazione viene realizzata tramite una HTTP Redirect Response (Codice 302) contenente vari parametri tra i quali l'URI di destinazione e l'URI mittente al quale ritornare una volta terminate le operazioni di autenticazione.
3. **Richiesta Autenticazione**: l'utente accede al servizio di autenticazione. Dal punto vista tecnico questa operazione consiste in una HTTP Request verso il server di autenticazione contenente tutti i parametri impostati nel punto precedente.
4. **Emissione Credeziali**: il sistema di autenticazione compie le operazioni necessarie all'autenticazione (dettagliate più avanti nel paragrafo) al termine delle quali emette le credenziali e ridireziona il browser dell'utente all'indirizzo mittente contenuto nei parametri.
5. **Presentazione Credenziali**: l'utente presenta le credenziali al portale ed accede ai servizi.

Le fasi indicate in precedenza sono maggiormente dettagliate nel Sequence Diagram illustrato in Figura 3 che schematizza il caso di autenticazione effettuata con successo.

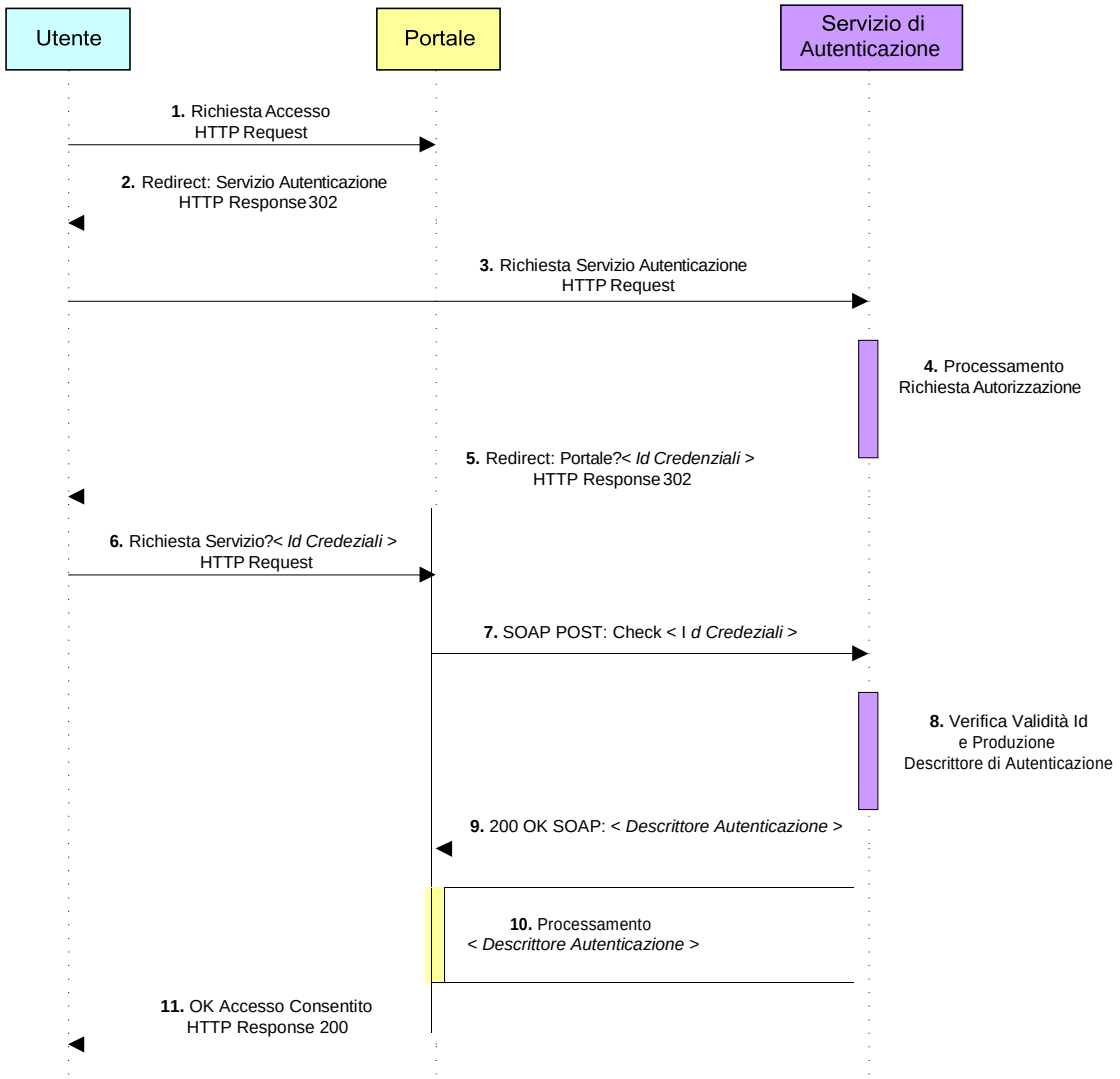

FIGURA 3 – SEQUENCE DIAGRAM DEL PROCESSO DI AUTENTICAZIONE

Le attività sono dettagliate come segue:

1. Il browser dell'utente tenta di accedere alla sezione autenticata di un portale inviando una HTTP Request al server del sistema di erogazione dei servizi
2. Il server del sistema di erogazione dei servizi risponde con una HTTP Redirect Response (code 302) ridirezionando il browser dell'utente presso il server del sistema di autenticazione. Tra i parametri saranno presenti:
    - L'indirizzo di destinazione corrispondente al server del sistema di autenticazione
    - L'indirizzo di ritorno al quale ridirezionare il browser una volta terminata la procedura di autenticazione
    - Una struttura dati codificata in XML contenente la richiesta di autenticazione

3. Il browser accede al servizio di autenticazione inviando una HTTP Request contenente tutti i parametri impostati nel punto precedente
4. Il sistema di autenticazione processa la richiesta di autorizzazione secondo la propria logica, ulteriori dettagli saranno forniti più avanti nel paragrafo
5. Il server del sistema di autenticazione risponde con una HTTP Redirect Response includendo tra i vari parametri una struttura dati codificata in XML denominata Id Credenziali contenente un estratto del risultato della procedura di autenticazione, in questa caso positiva
6. Il browser dell'utente accede all'indirizzo di ritorno precedentemente impostato come parametro nel punto 2 trasportando l'Id Credenziali inserito nel punto 5
7. Il sistema di erogazione dei servizi utilizza l'Id Credenziali come chiave per una interrogazione al sistema di autenticazione. Gli scopi di tale interrogazione sono la verifica della validità delle credenziali presentate dall'utente e l'ottenimento di una struttura dati denominata Descrittore Autenticazione contenente tutti i dati risultano dal processo di autenticazione codificati in XML. Il sistema utilizza il Descrittore di Autenticazione congiuntamente con gli altri strumenti quali il Descrittore di Sicurezza e il Descrittore di Profilo per la corretta erogazione del servizio. La chiamata al sistema di autenticazione avviene tramite un Web Service da questi esposto
8. Il sistema di autenticazione elabora opportunamente l'Id Credenziali e compone il Descrittore Autenticazione
9. Il sistema di autenticazione risponde alla chiamata al Web Service restituendo il Descrittore Autenticazione al server del sistema di erogazione dei servizi
10. Il sistema di erogazione processa il Descrittore di Autenticazione congiuntamente con gli altri strumenti quali il Descrittore di Sicurezza e il Descrittore di Profilo per la corretta erogazione del servizio
11. Il server del sistema di erogazione risponde al browser dell'utente con una HTTP Response di tipo 200 che autorizza l'accesso alla sezione autenticata del portale

In Figura 4 è illustrato il flusso delle attività compiute dal server di autenticazione per processare la richiesta di autenticazione.

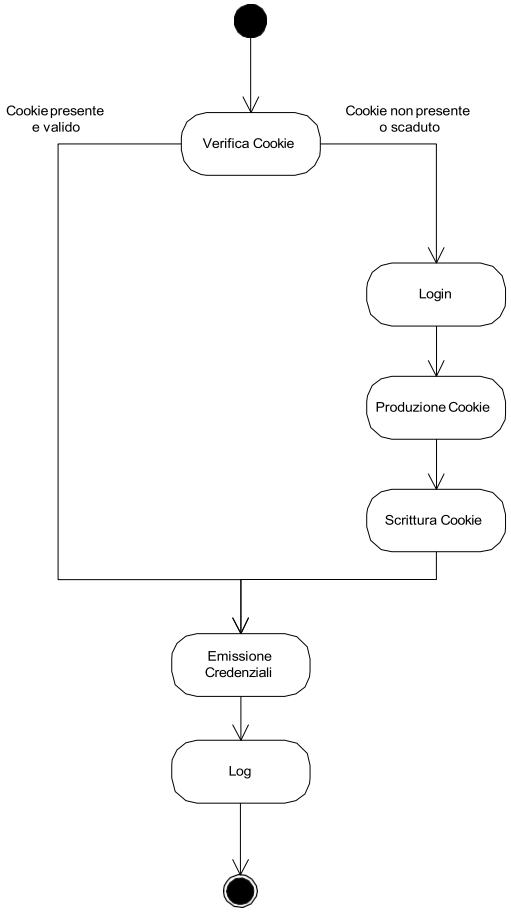

FIGURA 4 – PASSI DI ELABORAZIONE DEL PROCESSO DI AUTENTICAZIONE

Il processo di autenticazione si basa sull'utilizzo dei *cookies*. I *cookies* sono uno strumento utilizzato per gestire lo stato delle sessioni all'interno del protocollo HTTP, per sua natura senza stato, tramite la memorizzazione di informazioni sulla postazione client.
Il sistema di autenticazione, durante il passo 4 descritto nel Sequence Diagram precedente, verifica la presenza o meno di un *cookie* da esso stesso emesso precedentemente sul domino globale. Esistono due possibilità:

- il *cookie* è presente sul client ed è ancora in corso di validità. Ciò implica che l'utente (su quella determinata postazione) si è già autenticato con successo in precedenza pertanto il sistema di autenticazione può emettere delle nuove credenziali senza doverlo autenticare di nuovo
- il *cookie* non è presente sul client oppure è scaduto. Ciò implica che l'utente necessita di autenticarsi nuovamente secondo le modalità sulle quali saranno dati ulteriori dettagli nel seguito del paragrafo. Eseguita la fase di autenticazione il sistema produce un *cookie* da memorizzare sulla postazione client e emette le credenziali per consentire l'accesso al sistema di erogazione dei servizi.

Tutte queste attività vengano opportunamente registrate sul Log globale.

Dispositivi per l'autenticazione

L'utente potrà disporre di diversi tipi di autenticazione, l'utilizzo dei quali dipenderà da un lato dal livello di sicurezza del servizio erogato dall'altro dalle effettive disponibilità di tali dispositivi da parte dell'utente. In questa fase si possono identificare differenti tipologie di autenticazione.

- User e Password. Sistema di autenticazione basato su ciò che l'utente sa.
- Dispositivi a Microchip. Sistema di autenticazione basato su ciò che l'utente sa e su ciò che l'utente possiede. Dispositivi a Microchip utilizzabili nel presente contesto sono:
  - Carta d'Identità Elettronica
  - Carta Nazionale/Regionale dei Servizi
- User, Password e PIN sistema di autenticazione che prevede il riconoscimento dell'identità dell'utente.
- OTP. La modalità di autenticazione OTP Cohesion - One Time Password, a differenza delle terna Pin Raffaello, è una credenziale valida solo per una singola sessione di accesso. La OTP, al contrario delle credenziali statiche, non può essere memorizzata, pertanto richiede una tecnologia supplementare per poter essere generata ed usata ad ogni accesso. In particolare è richiesta l'installazione dell'APP Google Authenticator nel proprio smart phone

Sintetizzando concludiamo il sistema di autenticazione affermando che:
il Single Sign On (SSO) è utilizzato per il passaggio delle credenziali di utenti autenticati tra i portali di accesso; l'autenticazione sul framework è possibile mediante l'inserimento della coppia UserID/Password o la terna UserID/Password più PIN, oppure ancora mediante l'utilizzo di una CIE / CNS.
Il servizio consente agli utenti, in maniera del tutto trasparente, di navigare nelle aree riservate dei vari portali esposti sul framework senza doversi autenticare ogni volta, e soprattutto facendo in modo che le credenziali di autenticazione e il profilo dell'utente siano resi disponibili ai vari domini applicativi. Infatti, la verifica dell'autorizzazione per il dato utente ad usufruire del servizio è delegata al servizio stesso e alla possibilità per quest'ultimo di validare il profilo utente rispetto alle regole di accesso impostate sul catalogo regionale dei servizi, nucleo centrale del framework Cohesion.
Sistema di profiling: serve per la gestione coordinata di informazioni sull'utente accreditato, suddivise logicamente in un sottoinsieme statico (anagrafica estesa), che fa riferimento all'insieme degli attributi standard che vengono definiti e che costituiranno il profilo di base dell'utente, e in uno dinamico, contenente una serie di attributi in grado di indicare le preferenze dell'utente nell'accesso ai servizi piuttosto che a delle aree informative sui portali.
Gli utenti che si registreranno all'interno dell'infrastruttura della Regione Marche vengono memorizzati in un server LDAP. In tale repository verranno registrate le informazioni (attributi) che delineano l'identità di un utente. Una parte di questi saranno richiesti all'atto della registrazione ad uno dei portali appartenenti al framework, l'altra parte degli attributi potranno essere specificati su esplicita richiesta di un portale, all'atto di utilizzo di un determinato servizio.

Evoluzione verso un'architettura federata SAML 2.0

Attualmente la Regione Marche ha reingegnerizzando, dal punto di vista tecnologico ed organizzativo, il framework Cohesion SSO al fine di renderlo compatibile con lo standard emergente SAML 2.0. Infatti la versione 1.0 di Cohesion non si basava su questo standard di autenticazione, ma garantisce il Single Sign On mediante un flusso ad hoc.
L'implementazione dello standard SAML 2.0 consente la federazione del sistema con altri sistemi nazionali e locali aderenti alle specifiche GFID (Gestione Federata delle Identità Digitali) approvate a livello interregionale nell'ambito dal task infrastrutturale INF3 del progetto ICAR (Interoperabilità e Cooperazione Applicativa tra Regioni). Attualmente anche il sistema SPID adotta lo standard SAML 2.0.
Nella versione originale Cohesion si compone di due elementi: la SSO Libray, una DLL per l'integrazione dei servizi lato applicazione web chiamante (Services Provider), e l'Identity Provider (IdP), per garantire il processo di autenticazione comunicando con la SSO Library. In particolare, l'Identity Provider si compone di

due moduli: SSO, per la gestione delle credenziali contenute nell'LDAP di riferimento e persistenti nell'ambiente di Single Sign On, e SA, per la gestione delle modalità di autenticazione e delle funzionalità esposte dall'interfaccia di login.

La nuova versione del sistema, Cohesion 2.0, prevede l'introduzione di un modulo intermedio, l'SPmanager, per la gestione centralizzata dei flussi applicativi da/verso i Services Provider (che comunque integrano la precedente SSOLibrary) e implementa componenti software atte a supportare richieste e risposte in formato SAML 2.0.

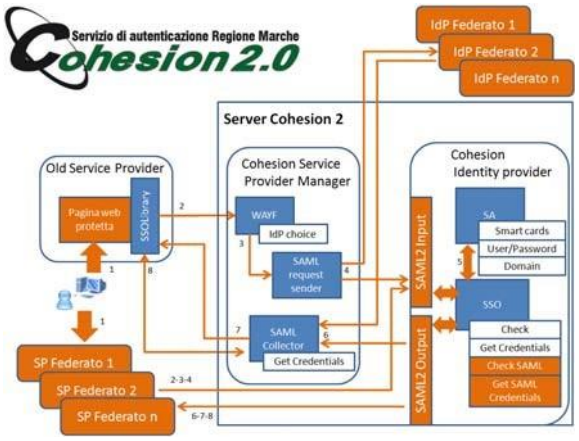

FIGURA 5 – FLUSSI DEL NUOVO SISTEMA DI AUTENTICAZIONE FEDERATA COHESION 2.0

Di seguito è fornita una breve descrizione dei flussi sviluppati (nel caso di accesso di un utente che scelta IdP Cohesion e una risorsa protetta da SP Cohesion).

1. L'utente richiede l'accesso a una risorsa protetta da Cohesion.
2. La SSOLibrary reindirizza alla pagina "Where Are You From?" (WAYF) dell'SPManager in cui è data la possibilità all'utente di scegliere con quale Identity Provider autenticarsi.
3. La WAYF passa il controllo al gestore SAML 2.0 che crea una richiesta di autenticazione SAML 2.0 e la invia all'IdP.
4. Se è stato scelto l'IdP di Cohesion l'utente viene reindirizzato alla pagina di controllo della richiesta SAML 2.0 in SSO che valuta se è già presente o meno una sessione per l'utente. Se è presente passa al punto 6.
5. Il controllo è reindirizzato a SA, dove l'utente può autenticarsi usando il metodo che preferisce.
6. SA passa il controllo a SSO che registra l'utente autenticato e restituisce la risposta SAML 2.0 contenente le credenziali, convertite in formato SAML 2.0, al modulo SAMLCollector dell'SPManager, che valuterà la correttezza della risposta e convertirà le credenziali ottenute nel formato compatibile per SSOLibrary.
7. SAMLCollector invia a SSOLibrary un indicatore di sessione a indicare che può richiamare la sua procedura GetCredential.
8. La SSOLibrary richiama il metodo GetCredential del SPManager mediante una richiesta SOAP protetta con Microsoft WSE e ottiene le credenziali. SSOLibrary autentica poi l'utente con le credenziali ottenute e fornisce accesso alla risorsa richiesta.

I flussi descritti, richiesti in ingresso dall'IDP, sono stati reingegnerizzati e dimezzati rispetto allo scenario iniziale oltre che resi compatibili con lo standard SAML 2.0. Sono stati poi sviluppati moduli specifici per gestire le nuove richieste in ingresso, convertendole nel formato riconosciuto dall'IdP Cohesion, e per trasformare il profilo in uscita in una risposta SAML 2.0 standard. Affinché la libreria SSOLibrary presente nel Service Provider continuasse a funzionare con la nuova struttura, si è reso necessario replicare, nel Service Provider Manager, alcune delle interfacce presenti nel vecchio IdP mediante le quali comunicava. Il Service Provider Manager contiene poi funzioni complementari alle nuove inserite nell'IdP, in altre parole fornisce un modulo di conversione della richiesta in arrivo dal SP in richiesta SAML 2.0 (SAML request sender) e un modulo di conversione della risposta in arrivo dall'IdP in formato compatibile alla vecchia SSOLibrary (SAML

collector). Ovviamente a supporto del corretto funzionamento sono stati creati i rispettivi metadati SAML 2.0 sia per l'IdP sia per il Service Provider Manager. Internamente è stato mantenuto un metadata dei sistemi federati comune all'IdP e al Service Provider Manager. La soluzione scelta, oltre ad essere retro compatibile permette la trasparenza dell'aggiornamento. Essendo la configurazione della gestione dei metadati SAML 2.0 centralizzata, tutti i fornitori di servizi che integravano Cohesion potranno usufruire delle nuove funzionalità di federazione continuando ad usare la vecchia SSOLibrary. Ne consegue che il Service Provider Manager gestisce i fornitori di servizio nei confronti della federazione Cohesion. Ogni Service Provider, che comunica con il SPManager, è perciò registrato ed autorizzato previa richiesta alla Regione Marche che si configura come intermediario tecnologico e gestore della governance del sistema di autenticazione.
Per completezza è stata, inoltre, sviluppata una nuova versione della SSOLibrary che opera direttamente con SAML 2.0 senza passare per l'SP manager Cohesion (se non per leggere la configurazione, ovvero i metadati che descrivono le entità presenti nella federazione), implementando il protocollo di binding HTTP-POST ed il Single Logout Protocol. Così facendo Il Service provider va a utilizzare la configurazione centralizzata nel Service Provider Manager della federazione, mantenendo un proprio metadata SAML 2.0 in modo da rendere il flusso più snello per le nuove implementazioni.
L'architettura logica descritta comprende anche i casi in cui un SP federato, in grado di generare autonomamente token SAML 2.0, gestisca in proprio accesso all'IdP Cohesion (senza utilizzare né SSO Library, né SP Manager).

1.2 LA CARTA RAFFAELLO

Normativa di riferimento

- DPR 2 marzo 2004, n.117 (GURI del 6 maggio 2004): Regolamento concernente la diffusione della carta nazionale dei servizi, a norma dell'articolo 27, comma 8, lettera b), della legge 16 gennaio 2003, n.3.
- Decreto interministeriale 9 dicembre 2004 (GURI del 18 dicembre 2004): Regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta Nazionale dei Servizi

Introduzione
La Carta Raffaello nasce con l'intento di essere la Carta Regionale dei Servizi e divenire uno strumento diffuso all'interno della cittadinanza e riconosciuto da tutte le amministrazioni per:

- L'autenticazione forte finalizzata ad una erogazione dei servizi in rete;
- La sottoscrizione digitale qualificata dei documenti;

Con la scelta del nome, ispirato a Raffaello Sanzio, pittore rinascimentale fortemente legato per origini ed opere alle Marche, si intende dare alla carta una chiara connotazione regionale.
L'ente emittente è la Regione Marche. La carta dovrà avere requisiti di sicurezza che permettono di utilizzare in rete le informazioni con la massima garanzia di sicurezza e tutela dei diritti personali.

Il Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa Art. 38 comma 2, sancisce che “Tutte le istanze e le dichiarazioni da presentare alla pubblica amministrazione o ai gestori o esercenti di pubblici servizi possono essere inviate anche per fax e via telematica:
a) se sottoscritte mediante la firma digitale, basata su di un certificato qualificato, rilasciato da un certificatore accreditato, e generata mediante un dispositivo per la creazione di una firma sicura;
b) ovvero quando l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi.”
La Carta Nazionale dei Servizi rappresenta quindi lo strumento principale che al pari della Carta di Identità Elettronica abilita il cittadino all’accesso ai servizi telematici di eGovernment e all’inoltro di istanze e dichiarazioni nell’ambito di tali servizi. Per tale motivo la Carta Raffaello aderisce allo standard Carta Nazionale dei Servizi e si conforma a tutti i requisiti tecnologici, organizzativi e di sicurezza previsti dalla normativa in termini di CNS e dispone di capacità di firma digitale qualificata.

1.2.1 Caratteristiche tecniche della carta CNS/CARTA RAFFAELLO

La Carta Raffaello è una carta a microprocessore che aderisce allo standard CNS e quindi, per quanto concerne la parte elettronica, presenta le stesse caratteristiche funzionali della CIE, ma mentre quest’ultima contiene gli elementi di sicurezza necessari per il riconoscimento a vista del titolare, la CNS-Carta Raffaello non contiene gli elementi “esterni” tipici di una carta d’identità.

La carta ha due funzionalità principali:

- è uno strumento di identificazione in rete. E’ dotata di un certificato di autenticazione rilasciato da un certificatore accreditato.
- ospita il servizio di firma digitale qualificata, fornendo al titolare la possibilità di sottoscrivere documenti elettronici.

La CNS-Carta Raffaello rispetta i vincoli imposti dagli standard internazionali sulle smart card, con particolare attenzione alle norme che regolamentano i documenti di identità (ISO/IEC 7816-1-2). Le dimensioni, lo spessore e le tolleranze sono conformi a quanto specificato dalla norma ISO/IEC 7810: 1995 per la carta di tipo ID-1.
E’ dotata di una memoria EEPROM di almeno 32 KB. Il microprocessore é conforme agli standard ISO/IEC 7816 parte 3, 4 e 8.
La struttura della memoria interna della carta è conforme al file system pubblicato sul sito del Centro nazionale per l’informatica nella pubblica amministrazione e aderente a quanto stabilito dalle regole tecniche per l’emissione della CNS.
La struttura del file system, concepita per consentire un uso flessibile della CNS, è suddivisa in:

- un’area necessaria per la gestione della carta (DF0, DF1, PIN, PUK, Id_carta, PIN_SO);
- un’area contenente le informazioni necessarie per l’autenticazione in rete (Kpri, c_carta, Dati_personali);
- un’area predisposta per le funzioni di firma digitale (Firma_digitale);
- un’area disponibile per eventuali servizi aggiuntivi (Memoria_residua).

La tabella 1 delle regole tecniche, di cui al Decreto Interministeriale 9 Dicembre 2004, riporta la descrizione dei campi elencati e, per ogni campo, le responsabilità in merito alla generazione, la predisposizione e la registrazione dell’informazione.
Il file elementare dei dati personali è codificato secondo le modalità previste per la Carta d’Identità Elettronica, riportate nella tabella 2 delle medesime regole tecniche.

Inoltre, in aggiunta a quanto prescritto dallo standard ISO/IEC 7816 parte 4 circa i comandi del sistema operativo, la carta rispetta le specifiche del sistema operativo (APDU) oggetto del protocollo d'intesa per la realizzazione dei progetti Carta d'identità elettronica e Carta nazionale dei servizi.

Sulla carta,in accordo alle regole tecniche è presente la scritta "Carta Nazionale dei Servizi" ed il logo dell'Ente emettitore Regione Marche.

Il layout della Carta Raffaello è riportato nella figura seguente.

FIGURA 6 - FRONTE E RETRO DELLA CNS- CARTA RAFFAELLO

L'immagine in semitrasparenza sullo sfondo è quella di Raffaello Sanzio a cui si ispira la carta.
I dati riportati sul fronte della CNS sono in Formato "Verdana True Type", stile normale dimensione 7 punti.
Le informazioni riportate sul fronte sono:

- codice fiscale 16 caratteri alfanumerici;
- cognome dimensionato per una lunghezza di 40 caratteri alfabetici;
- nome dimensionato per una lunghezza di 35 caratteri alfabetici;
- provincia di nascita per una lunghezza di 2 caratteri alfabetici;
- luogo di nascita, comune di nascita dimensionato per una lunghezza di 35 caratteri alfabetici;
- data di scadenza (GG/MM/AAAA) per una lunghezza di 10 caratteri alfanumerici;
- sesso, 1 carattere (M/F);
- data di nascita (GG/MM/AAAA) per una lunghezza di 10 caratteri alfanumerici;
- tre lettere in formato Braille standard a 6 punti riportanti la combinazione di 3 lettere del codice fiscale (le prime 2 che identificano il nome e il sedicesimo carattere del codice fiscale che ha la funzione di controllo dell'esatta trascrizione dei primi quindici caratteri;

Le informazioni riportate sul retro sono:

- banda magnetica ad ossidi rigidi e a tre tracce;
  la prima traccia è personalizzata all'atto dell'emissione e contiene: codice fiscale 16 caratteri, cognome e nome separati da 2 spazi per una lunghezza complessiva di 60 caratteri. Le informazioni registrate sono precedute da un carattere denominato «Start sentinel» e seguite da un carattere denominato «End sentinel».

Le informazioni sono registrate secondo la codifica IATA (International Air Transport Association) e il metodo di registrazione è AIKEN con densità 210 bpi.
la seconda traccia è personalizzata all'atto dell'emissione e contiene il codice fiscale convertito secondo tabella di conversione (caratteri numerici per una lunghezza complessiva di 34 caratteri comprensivi di start e end sentinel).
Le informazioni sono registrate secondo la codifica ABA (American Bankers Association) e il metodo di registrazione è AIKEM con densità 75 bpi.
la terza traccia è a disposizione per ulteriori sviluppi e non viene personalizzata all'atto dell'emissione.

- codice a barre del codice fiscale secondo lo standard di codifica 39 (oppure in modalità "128 code).

1.2.2 Ruoli previsti nel circuito di emissione della Carta Raffaello

Il circuito di emissione della Carta Raffaello rispetta i requisiti previsti dalle regole tecniche per l'emissione della CNS.
I ruoli previsti nell'emissione della CNS sono:

- il **produttore**, ossia l'azienda che provvede alla fornitura delle carte a microprocessore con un chip compatibile con quello previsto dalla CNS, che predispone opportunamente lo spazio dedicato alla firma digitale, che applica al supporto fisico l'artwork e gli elementi costanti;
- il **certificatore**, cioè il soggetto, abilitato ai sensi dell' all'articolo 5 del Decreto Legislativo n.10 del 23 gennaio 2002, che presta servizi di certificazione delle informazioni necessarie per l'autenticazione o per la verifica delle firme elettroniche
- l'**ente emettitore** è la Regione Marche ed è responsabile:
  - della correttezza dei dati identificativi memorizzati nella carta e nel certificato di autenticazione;
  - della correttezza del codice fiscale memorizzato nella carta e riportato nel certificato di autenticazione;
  - della sicurezza delle fasi di produzione, inizializzazione, distribuzione.

Per la distribuzione delle carte sono stati abilitati appositi **Sportelli di registrazione locali –LRA** supportati da **Centri servizi** i quali verranno abilitati per la produzione della Carta Raffaello e la relativa personalizzazione. Ad un Centro servizi corrisponde più Sportelli di registrazione.

La Regione Marche ha istituito un **Centro tecnico regionale** di supporto al sistema di emissione con la finalità di rappresentare un centro di competenza per tutti gli aspetti tecnologici connessi con la produzione e l'utilizzo della Carta Raffaello. I compiti del centro sono:

- La consulenza e l'assistenza tecnica agli enti che fanno parte del circuito di distribuzione;
- La consulenza e l'assistenza tecnica a coloro che sviluppano o erogano servizi basati sulla Carta Raffaello;
- La definizione dei requisiti funzionali e di sicurezza del sistema di informativo di gestione della carta e di supporto all'intero processo di emissione, la supervisione alla sua implementazione e la successiva gestione e aggiornamento del sistema;
- L'adozione delle scelte tecnologiche per l'integrazione con il sistema regionale di autenticazione e SSO (Cohesion).

La Regione Marche provvede inoltre alla gestione delle carte emesse attraverso un **Call Center** all'interno del **Centro tecnico regionale** per l'assistenza agli utenti, la gestione dei malfunzionamenti e l'eventuale sostituzione o rinnovo delle carte in scadenza. I compiti del centro servizi sono:

- Gestione revoche, rinnovi, sospensioni;
- Contact center;

- Help desk.

1.2.3 Sistema informativo di gestione della CNS-Carta Raffaello

Il **Sistema Informativo di gestione della Carta Raffaello (SICR),** fornito dalla Regione Marche, ha lo scopo di supportare tutto il circuito di emissione delle carte e fornire le necessarie integrazioni con il resto dei sistemi informativi regionali collegati al concetto di cittadinanza elettronica.

Da punto di vista architetturale, il SICR è costituito da una procedura web ad accesso autenticato sicuro basato sui servizi del framework regionale Cohesion, e da una procedura WIN32 per interfacciare e gestire le periferiche necessarie per la produzione e personalizzazione della Carta Raffaello.

Gli attori umani del sistema sono:
- Operatori degli sportelli addetti alla registrazione e alla consegna delle carte
- Operatori dei Centri Servizi addetti alla personalizzazione delle carte
- Operatori del contact center per attività di help desk
- Addetti alla gestione dello stoccaggio e delle consegne dei lotti di carte.
- Amministratori del sistema

Gli attori non umani sono rappresentati dai sistemi che interagiscono con il SICR:
- Sistema di accesso al portale regionale dei servizi (Cohesion)
- Sistema di certificazione
- Sistema di gestione della posta certificata

Dotazione hardware e software dello sportello LRA di ritiro Carta Raffaello

Lo sportello di prenotazione/ritiro della Carta Raffaello è qualsiasi struttura che avendo sottoscritto una convenzione con la Regione Marche è dotata di:
- Personal Computer collegato alla rete internet per accedere all'applicativo web fornito dalla Regione Marche
- Stampante ad aghi per stampare e consegnare al cittadino la busta retinata contenete il codice PIN e PUK della Carta Raffaello come indicato di seguito.

Dotazione hardware e software Centro Servizi

Il Centro Servizi deve essere dotato di:
- Personal Computer collegato alla rete internet, e alla rete regionale
- Software win32 fornito dalla Regione per interfacciare le periferiche necessarie alla produzione della carta (stampante termografica, punzonatrice, lettore smart card)
- Stampante termografica per inserire i certificati di autenticazione e di firma nel chip, scrittura sulla banda magnetica e stampa della CNS

Nella Figura 7 vengono riportati e descritti i processi che vengono eseguiti nell'emissione di una Carta Raffaello.

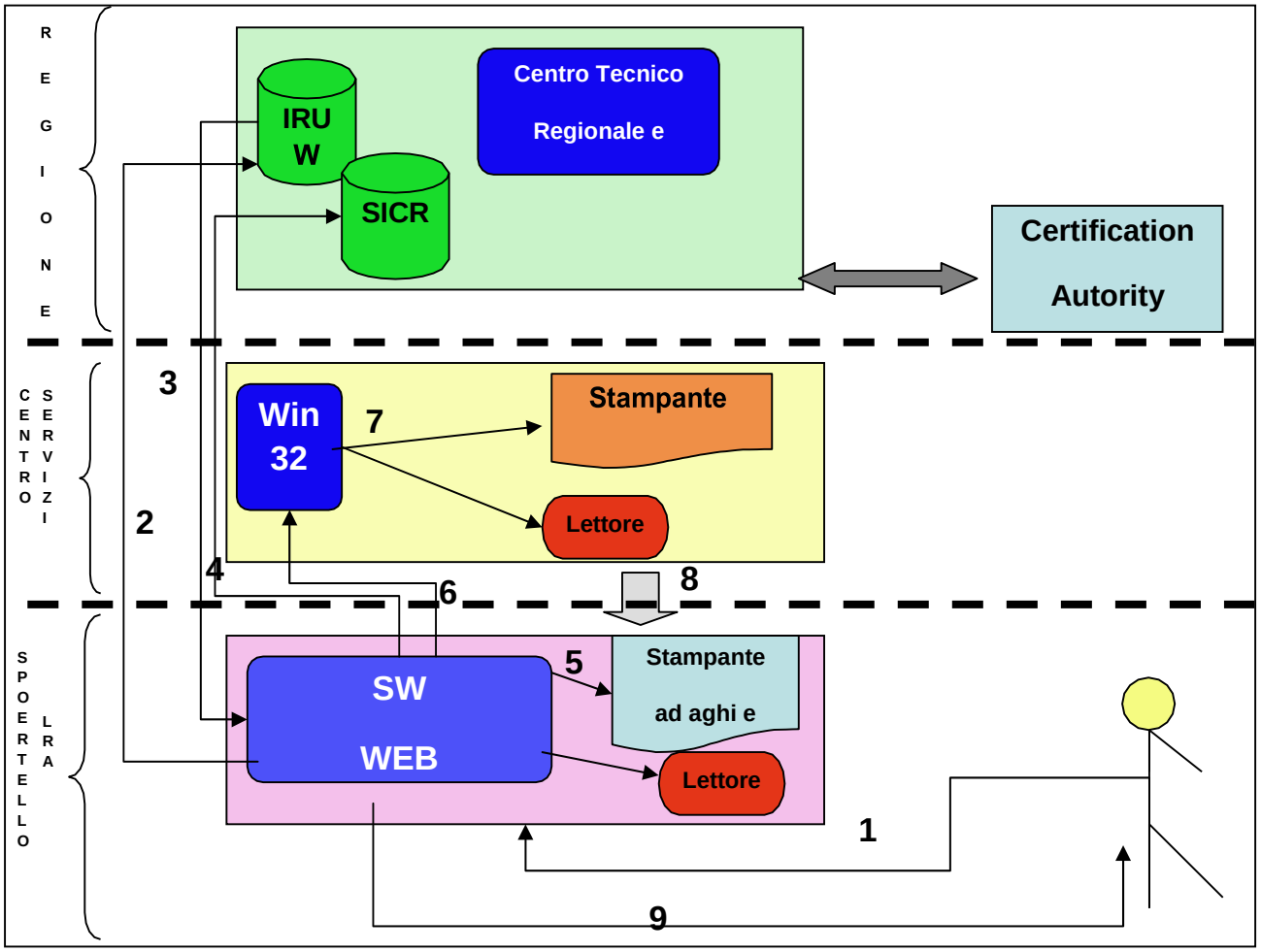

FIGURA 7 - PROCESSI DI DISTRIBUZIONE DELLA CARTA RAFFAELLO

Descrizione Step per la produzione/distribuzione della Carta Raffaello

1. Il Richiedente si reca allo sportello LRA con un documento di riconoscimento e il tesserino del codice fiscale
2. lo sportello attraverso l'applicativo web regionale ricerca nell'IRUW il cittadino
3. il software visualizza i dati anagrafici del cittadino e il relativo codice fiscale
4. l'operatore dello sportello inserisce i seguenti dati:
   - documento
   - numero di telefono
   - indirizzo di posta elettronica
   - il sistema effettua l'iscrizione al framework regionale Cohesion
   - creazione della casella di posta certificata utente@postaraffaello.it se richiesta dal richiedente
5. l'applicativo web allo sportello stampa il modulo precompilato da far sottoscrivere al richiedente ed invita lo stesso a ripresentarsi per il ritiro della Carta Raffaello.

6. Il sistema provvede automaticamente ad inviare la richiesta di generazione della CNS al proprio Centro Servizi
7. L'applicativo in dotazione presso il Centro Servizi, ad ogni richiesta di Carta Raffaello provvede:
   - all'inserimento dei dati personali del cittadino nel chip della CNS,
   - alla memorizzazione dei certificati di autenticazione e di firma
   - alla scrittura delle prime due tracce della banda magnetica
   - stampa termografica, fronte e retro della Carta Raffaello
   - cambia il PIN di fabbrica generandolo in maniera random e memorizza lo stesso criptato nel database di registrazione
8. Il Centro Servizi consegna il lotto di CNS prodotte allo sportello LRA.
9. Il cittadino si ripresenta allo sportello e lo sportello LRA provvede alla consegna della Carta Raffaello provvedendo:
   - Alla stampa della busta retinata contenete il PIN e PUK, utilizzando la stampante ad aghi
   - Alla sottoscrizione del modulo da parte del richiedente dell'avvenuta consegna
   - Ad informare il Richiedente delle proprie responsabilità.

1.3 LA FIRMA RAFFAELLO

La firma digitale costituisce uno dei dieci obiettivi per la digitalizzazione del Piano per l'e-Government. La firma digitale è uno strumento e come tale, deve essere utilizzato nei modi e nei casi appropriati. Ricordiamo che non è corretto il suo utilizzo come sistema di identificazione in rete, per il quale esistono strumenti quali la carta d'identità elettronica e le carte di accesso ai servizi. La firma digitale è utile nel momento in cui è necessario sottoscrivere una dichiarazione ottenendo la garanzia di integrità dei dati, oggetto della sottoscrizione e di autenticità delle informazioni relative al sottoscrittore.
Esempi tipici dell'utilizzo della firma digitale, possono essere ricercati in tutti gli adempimenti da effettuarsi verso le amministrazioni che richiedono appunto la sottoscrizione di una volontà: denunce, autorizzazioni, concessioni, richieste di contributi, di esenzioni a pagamenti a causa del reddito o di altre condizioni particolari, ricorsi, ecc. La legge la definisce il risultato di una procedura informatica che attraverso un procedimento crittografico a chiavi asimmetriche, permette di identificare il reale mittente di un documento informatico, verificandone l'autenticità. La Firma Digitale utilizza le potenzialità delle chiavi asimmetriche (crittografia a doppia chiave) e prevede che il titolare abbia due chiavi che gli vengono attribuite in modo univoco, una "privata", in possesso e conosciuta solo da lui, e una "pubblica", resa disponibile attraverso il certificato rilasciato dal certificatore emittente. Un documento elettronico firmato (cifrato) con una delle due chiavi, può essere reso "chiaro" (decifrato e verificato) esclusivamente utilizzando l'altra.
Ogni utente sarà fornito quindi di doppia chiave:

- la prima, privata e segreta
- la seconda, pubblica e disponibile per chiunque debba avere contatti con l'utente.

Le due chiavi sono correlate, ma del tutto diverse fra loro ed è impossibile sia ricavare l'una possedendo l'altra, sia decifrare il testo con la chiave utilizzata per cifrarlo. Sono legate bi-univocamente tra loro da una relazione matematica. Per il corretto funzionamento della tecnica di firma digitale, è di fondamentale

importanza che la chiave privata sia tenuta segreta dal suo legittimo proprietario. Esistono diversi schemi crittografici a chiave pubblica che consentono di realizzare la firma digitale (i più noti ed usati sono RSA, DSS) La firma digitale si basa su certificati elettronici rilasciati da soggetti definiti "certificatori".
L'applet di firma sviluppata internamente consente, all'interno si una procedimento informatizzato la generazione del documento in formato pdf/a e la relativa sottoscrizione digitale attraverso una CNS e l'invio al protocollo informatico PALEO della Regione.

1.3.1 Adobe per la firma

Tra le tecnologie esistenti per il supporto alla firma digitale, spicca il formato Adobe PDF (Portable Document Format) affermatosi non solo grazie alla disponibilità di un visualizzatore gratuito (Adobe Reader), ma soprattutto per un'ampia serie di caratteristiche e proprietà che ne fanno il formato ideale per la gestione elettronica dei documenti. Il PDF, nato oltre dieci anni fa come semplice formato documentale indipendente dalla piattaforma hardware e stampabile ad alta qualità, si è evoluto in un formato "intelligente" capace di rappresentare non solo testo e grafica ma anche dati, metadati e logica applicativa, con in più funzioni di sicurezza allo stato dell'arte che ne consentono il controllo e ne accrescono l'affidabilità. Inoltre, in Italia, il formato Adobe PDF è stato riconosciuto come standard di riferimento per la firma digitale in seguito alla sottoscrizione di un protocollo d'intesa tra il l'ex CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione) attuale DIGITPA e Adobe Systems Inc. , avvenuta il 16 febbraio 2006, che individua nel formato i requisiti richiesti dall'articolo 12, comma 9 della Deliberazione CNIPA n. 4/2005, in particolare per quanto concerne la disponibilità pubblica e gratuita sia delle specifiche del formato sia di un prodotto di verifica quale Adobe Reader, il diffuso visualizzatore di file Adobe PDF. Il quadro normativo della firma digitale in Italia è in realtà molto più ampio. In particolare, si segnalano le fonti seguenti:

- Il Codice dell'Amministrazione Digitale, entrato in vigore il 1° gennaio 2006, disciplina l'utilizzo dell'informazione digitale nelle PA: creazione, gestione e conservazione, trasmissione e disponibilità e del D.Lgvo 30 dicembre 2010 n°235 "modifiche ed integrazioni al D.Lgvo 82/05 CAD
- La Deliberazione n. 4/2005 stabilisce le regole per il riconoscimento e la verifica del documento informatico.
- Il DPCM 13/01/2004 stabilisce le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione anche temporale dei documenti informatici.

Il formato PDF ha introdotto nelle sue specifiche un supporto standard e documentato per funzionalità di firma digitale. Esso utilizza tecniche standard conformi anche a quanto previsto dalla vigente normativa europea ed italiana. La firma digitale nel formato PDF, in quanto funzionalità nativa, offre un'ampia serie di caratteristiche rispetto l'utilizzo generale della busta PKCS#7 di tipo "signed and enveloped data" (formato .P7M), un formato caratterizzato da numerose limitazioni d'uso.
Nell'ottica di favorire la diffusione di strumenti per la firma digitale non si può ignorare la difficoltà che molti utenti possono trovare nel reperire un'applicazione di verifica di file con firma digitale P7M. Malgrado gli sforzi operati dal CNIPA e dai Certificatori Accreditati, sono ancora poche in numero assoluto le persone in possesso dei programmi in grado di verificare e leggere file P7M. Al contrario la stragrande maggioranza degli utenti di personal computer (circa il 90% secondo le stime più recenti) sono in grado di riconoscere un file PDF e di utilizzare il visualizzatore Adobe Reader , ottenendo implicitamente la possibilità di verificare le eventuali firme digitali in esso contenute. Il documento PDF con firma digitale non subisce alcuna trasformazione in altro formato. Il formato P7M imbusta invece il documento firmato nascondendolo in un nuovo file e impedendo così l'accesso al documento a chi sia sprovvisto di un'applicazione compatibile. Per accedere al documento firmato P7M occorre inoltre "sbustarlo", con la conseguente duplicazione tra documento firmato e non firmato. Nel caso di documenti con più firme la duplicazione si moltiplica, essendo richiesti tanti sbustamenti quante sono le firme apposte al documento. È poi necessario considerare che sono di norma molte più le persone che necessitano di leggere e verificare documenti firmati da altri che non

quelle che devono crearli e firmarli. Il formato PDF offre in definitiva funzionalità di firma digitale trasparenti rispetto all'esigenza primaria di accedere con facilità ai documenti firmati.
Il formato PDF inoltre, consente di apporre firme digitali multiple come sigilli alle revisioni o alle nuove versioni di un documento. Vi è perciò la possibilità di apportare modifiche al documento successive alla firma senza invalidare quest'ultima. Questa funzionalità, non disponibile con il formato P7M, sfrutta la caratteristica del PDF di effettuare il salvataggio incrementale dei dati ed è fondamentale quando la firma è utilizzata inprocessi in cui più persone collaborano ad un unico documento modificandolo e apponendovi la propria firma digitale in tempi successivi. Un ambito in cui questa caratteristica è indispensabile è quello della modulistica elettronica, dove i processi tipicamente prevedono che più persone interagiscano con lo stesso documento aggiungendo e sottoscrivendo i propri dati in tempi successivi.
Con l'utilizzo del PDF è possibile gestire l'aspetto visivo della firma digitale nel documento firmato. Questa caratteristica consente di associare all'operazione di firma digitale una rappresentazione grafica di informazioni mediante "campi firma" liberamente posizionabili all'interno delle pagine del documento. I "campi firma" permettono inoltre di contestualizzare l'apposizione di una firma digitale nel contenuto del documento, così come è naturale fare con un autografo su un documento cartaceo. I campi firma consentono di contestualizzare la validità della firma a sezioni differenti di un documento. Più persone possono sottoscrivere parti diverse di un unico documento dando una chiara percezione di cosa ciascuno abbia sottoscritto, esattamente come avviene con la carta. Inoltre i "campi firma" consentono anche di controllare le tipologie di firma apponibili ad un documento PDF.
Grazie all'interoperabilità, a livello nazionale e internazionale, della firma digitale, favorisce l'utilizzo esteso, indipendentemente dal tipo di certificato, dal dispositivo di firma o dall'applicazione di firma. A tale scopo, in Italia, il CNIPA ha introdotto nella normativa dapprima il riconoscimento del solo formato P7M, consentendo un sostanziale allineamento dei servizi e delle applicazioni fornite dai Certificatori qualificati, e più recentemente con la Deliberazione n.4/2005 ha stabilito la possibilità di estendere ad altri il riconoscimento di "formato legale".

1.4 LA POSTA ELETTRONICA CERTIFICATA – POSTA RAFFAELLO

Nell'ambito delle iniziative significative sviluppate da Regione Marche per l'assegnazione della "Cittadinanza Digitale" ai marchigiani, si inquadra il progetto regionale per la messa in esercizio di un sistema di Posta Elettronica Certificata, chiamato PostaRaffaello, che ha l'obiettivo di mettere a disposizione del cittadino lo strumento per comunicare con modalità sicura con la Regione Marche in conformità al Codice delle Amministrazioni Digitali. In base all'art. 16 "Disposizioni per le pubbliche amministrazioni" comma 1 e comma 2 del DPR 68/2005, la Regione Marche, in qualità di Pubblica Amministrazione può svolgere autonomamente l'attività di gestione del servizio di posta elettronica certificata per i privati, rispettando le regole tecniche e di sicurezza previste dal regolamento, tuttavia limitatamente ai rapporti intrattenuti tra la Regione Marche ed i privati a cui sono rilasciate le caselle di posta elettronica certificata.
Pertanto, il sistema PostaRaffaello vincola il dominio PEC di postaraffaello.it usato dal cittadino digitale alla comunicazione con il solo dominio PEC *emarche.it* della Regione Marche. Il dominio *emarche.it* di PostaRaffaello, in base alle politiche definite dal gestore Regione Marche, dialoga esclusivamente con domini di posta elettronica certificata.

Le caselle di posta elettronica certificata, diversamente dalle usuali caselle di posta elettronica, consentono l'invio di posta elettronica con valore legale in conformità di quanto previsto dal "Codice dell'Amministrazione Digitale" (D.Lgs. n.82 del 7/03/2005 e D.Lgs. n.159 del 4/04/2006 e successive modificazioni).
Di seguito presentiamo una rappresentazione grafica che schematizza gli elementi caratteristici di un dominio di posta certificata e le sue interazioni con un altro dominio di posta certificata.

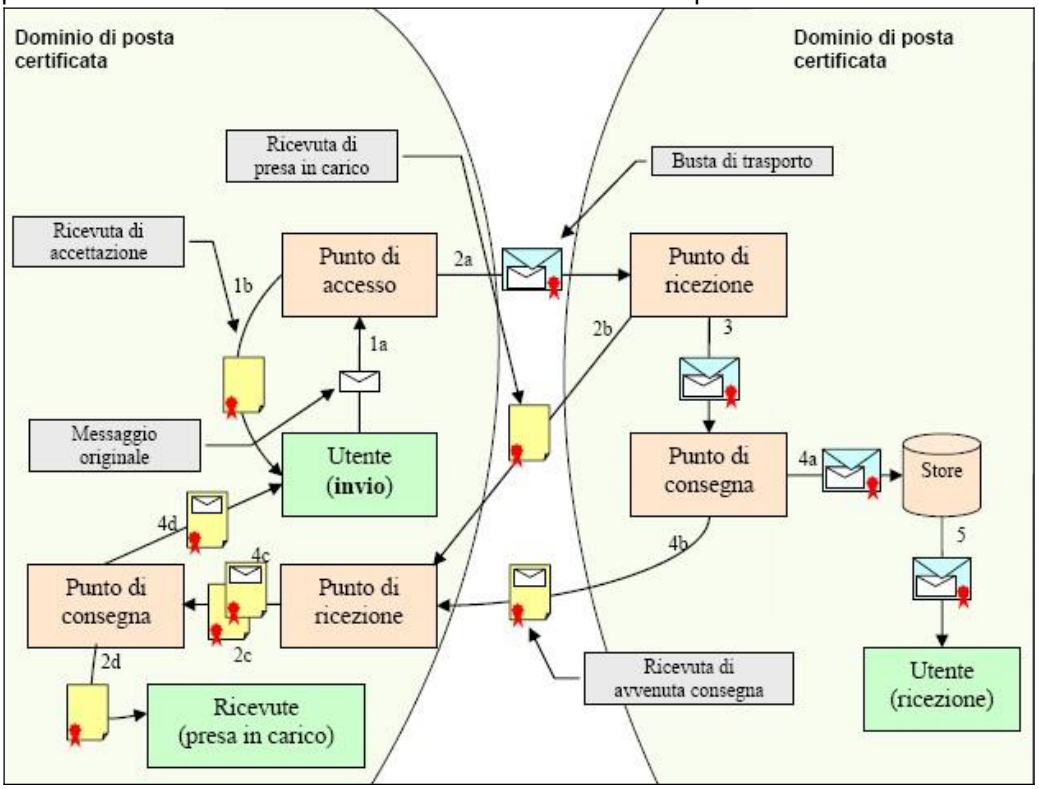

FIGURA 8 - BUSTA DI TRASPORTO CORRETTA E VALIDA CON CONSEGNA AVENTE ESITO POSITIVO

1a: l'utente invia una e-mail al Punto di accesso
1b: il Punto di accesso restituisce al mittente una Ricevuta di Accettazione
2a: il Punto di accesso crea una Busta di Trasporto e la inoltra al Punto di Ricezione del Gestore destinatario
2b: il Punto di Ricezione verifica la Busta di Trasporto e crea una Ricevuta di Presa di Carico che viene inoltrata al Punto di Ricezione del Gestore mittente
2c: il Punto di Ricezione verifica la validità della Ricevuta di Presa di Carico e la inoltra al Punto di Consegna
2d: il Punto di Ricezione salva la Ricevuta di Presa di Carico nello store delle ricevute del Gestore
3: il Punto di Ricezione inoltra la Busta di Trasporto al Punto di Consegna
4a: il Punto di Consegna verifica il contenuto della Busta di Trasporto e la salva nello store (mailbox del destinatario)
4b: il Punto di Consegna crea una Ricevuta di Avvenuta Consegna e la inoltra al Punto di Ricezione del Gestore mittente
4c: il Punto di Ricezione verifica la validità della Ricevuta di Avvenuta Consegna e la inoltra al Punto di Consegna
5: l'utente destinatario ha a disposizione la e-mail inviata.

1.5 I SISTEMI REGIONALI: IL PROTOCOLLO PALEO E ATTIWEB

Normativa di riferimento

- D.Lgs. 12 Aprile 2006, n.163 “Codice dei contratti pubblici relativi a lavori, servizi e forniture in attuazione alle direttive 2004/17/CE e 2004/18/CE”;
- Reg. Regionale n.1 del 12/01/2009 “Regolamento per l’acquisizione in economia di beni e servizi e funzionamento della cassa economale”.
- Decreto legislativo 7 marzo 2005, n. 82 “Codice dell’amministrazione digitale” aggiornato dal D.Lgs. n. 159 del 4 aprile 2006
- Decreto del Dirigente della P.F. Informatica nr 8/INF_02 del 23/11/2005 *“APQ SI-RM: Int. D03. Reg. reg. 8 del 28/10/04: Fornitura di servizi per lo sviluppo di estensioni software al sistema informativo Paleo – protocollo informatico e gestione documentale Regione Marche. Imp. a base di appalto € 25.540 IVA escl”*
- Decreto del Dirigente della P.F. Informatica nr.451/INF_02 del 11/12/2006, avente ad oggetto: “FDRM-PaLeO - Reg. reg. 8/04 - Indizione gara per la fornitura di servizi per la evoluzione e manutenzione del sistema informativo Paleo-protocollo informatico e gestione documentale Regione Marche. Imp. a base di appalto € 49.700 IVA escl”.
- DGR 62 del 29/01/2007 *“Progetto di e-Government FDRM-PaLeO (Flussi Documentali Regione Marche – Paperless Office System). Approvazione dello schema di convenzione per la promozione, la diffusione, l’utilizzo del sistema di protocollo informatico e gestione documentale basato sul software PaLeO”*
- Delibera di Giunta Regionale n.1759 del 01/12/2008 “Avvio della sperimentazione e dell’analisi finalizzata alla definizione del sistema di conservazione dei documenti cartacei e digitali della Regione Marche”.
- Decreto del Dirigente della P.F. Informatica nr.344/INF_02 del 04/12/2008 “DGR 1759 del 01/12/2008. Reg.R. 8/2004. Trattativa privata finalizzata alla realizzazione di un sistema software prototipale per la conservazione a norma dei documenti originali informatici”
- Delibera di Giunta Regionale n. 1287 del 03/08/2009 “Approvazione dello schema di convenzione per l’utilizzo in ASP del sistema di protocollo e gestione documentale PALEO nell’ambito del progetto PALEO-SALUTE”. Convezione sottoscritta dall’ASUR in data 05/10/2009 e dall’Azienda ospedaliera San Salvatore in data 01/04/2010.

Sistema attuale

L’introduzione delle tecnologie di crittografia e firma digitale, in conformità alla normativa vigente, permette di produrre documenti informatici e di trasmetterli con garanzia di riservatezza ed integrità. Il servizio di marcatura temporale, inoltre, consente di attribuire ai documenti informatici una data certa e verificabile. Il Piano di Azione di e-Government, approvato il 23 giugno 2000 dal Comitato dei Ministri per la Società dell’Informazione, ha come obbiettivo principale l’interoperabilità telematica tra tutte le Amministrazioni pubbliche. Componente fondamentale per questa evoluzione è stata l’adozione di un sistema di protocollo informatico, in quanto capace di attestare, con valenza giuridica, il momento dell’ingresso o dell’uscita di un documento, anche informatico.
Un sistema di protocollo informatico può essere visto come un insieme di moduli software integrati tra loro:

- Sistema di protocollo informatizzato senza scansione;

- Sistema di protocollo informatizzato con scansione;
- Sistema di protocollo informatico.

Il progetto della Regione Marche è volto a consentire agli Enti pubblici della regione di adottare un sistema interoperabile e cooperante di protocollo informatico e di gestione dei flussi documentali, coerente con le disposizioni di legge, nonché di offrire a cittadini, imprese e Amministrazioni la possibilità di sostituire lo scambio di documenti cartacei con lo scambio di documenti informatici, attraverso un sistema di posta elettronica certificata.
Il sistema di protocollo informatico Paleo comunica con l'esterno secondo due modalità: interoperabilità e web services. L'interoperabilità, così come previsto, dal DPR 445/2000 e successive integrazioni, permette a sistemi eterogenei di protocollazione informatica di amministrazioni, o meglio Area Organizzativa Omogenea - AOO, diverse di cooperare scambiandosi messaggi di protocollazione, tramite posta elettronica certificata. Il formato dei messaggi è stabilito all'interno della medesima normativa.
Il web service di Paleo espone funzionalità base di protocollazione utilizzabili da sistemi client appartenenti alla stessa amministrazione. In questo modo, diverse applicazioni possono integrare al loro interno funzionalità di protocollazione invocando il web service di Paleo.
E' importante sottolineare che, a differenza dell'interoperabilità, per utilizzare il web service occorre disporre di una utenza Paleo valida con cui autenticarsi ed effettuare le operazioni di protocollazione.
Il servizio permette di effettuare le seguenti operazioni:
Protocollazione in arrivo: registrazione di un protocollo in ingresso
Protocollazione in partenza: registrazione di un protocollo in uscita

Inoltre espone le seguenti funzionalità utili per comporre correttamente le richieste di protocollazione:

- Recupero degli operatori accreditati nel sistema
- Recupero delle ragioni di trasmissione
- Recupero dei registri
- Recupero del titolario di classificazione e fascicoli
- Recupero della rubrica mittenti/destinatari protocolli
- Inserimento/modifica nella rubrica mittenti/destinatari

Passiamo ora a descrivere il sistema Atti Web Decreti; questo è un sistema informativo per la gestione del ciclo di vita dei Decreti adottati dalle strutture Regionali.
Il sistema informativo integrato "attiweb - decreti" è un sistema autenticato, quindi dopo aver indicato l'indirizzo http://attiweb sul browser internet per accedere al sistema occorre inserire utente e password. Le funzionalità supportate sono quelle di inserimento, repertoriazione, e ricerca dei decreti.
Il sistema attiweb prevede, per la redazione dei decreti, l'utilizzo di template specifici, che consentano poi alla procedura la gestione automatica del decreto (inserimento numero e data, creazione della versione per estratto del decreto, etc.). Il sistema consente di scaricare sul proprio computer i suddetti modelli per compilarli. Dopo aver redatto il decreto, avendo necessità di stampare il decreto stesso per raccogliere le firme cartacee dei soggetti interessati, si procede all'inserimento del decreto nel sistema.

Scenari futuri
In relazione al sistema di gestione documentale e al sistema di conservazione, la Regione Marche ha aderito come capofila al progetto interregionale per la dematerializzazione ProDE – Progetto Dematerializzazione.
Nella realizzazione di sistemi informativi futuri si dovrà prendere in considerazione l'utilizzo dei deliverable di tale progetto e degli standard che definisce.
Nell'allegato *"PRODE - PROgetto interregionale DEmaterializzazione"* si descrive gli obiettivi e l'approccio complessivo che sarà adottato per la realizzazione del progetto interregionale per la dematerializzazione ProDE.

2 IL SISTEMA PUBBLICO DI COOPERAZIONE (SPCOOP)

2.1 PRINCIPI ORGANIZZATIVI

"Il Sistema Pubblico di Connettività e Cooperazione è un sistema di infrastrutture tecnologiche e regole comuni di interfaccia per interconnettere la PA e diffondere il suo patrimonio informativo, razionalizzando le soluzioni telematiche esistenti e introducendo un ambiente comune per integrare le applicazioni". D.Lgs. 42/2005.
Nell'individuare il modello di cooperazione applicativa, il Gruppo di lavoro per i Servizi di interoperabilità, cooperazione applicativa ed accesso del Sistema Pubblico di Connettività e di Cooperazione, ha tenuto conto dei seguenti principi organizzativi:

- il modello di cooperazione deve essere indipendente dagli assetti organizzativi e dai sistemi informatici interni dei soggetti cooperanti;
- ciascuna amministrazione cooperante mantiene la responsabilità dei propri servizi e dei propri dati;
- la cooperazione applicativa si attua sulla base degli accordi tra le parti ed ha un fondamento normativo o istituzionale.

2.2 ELEMENTI FONDAMENTALI DELL'ARCHITETTURA TECNICA ORGANIZZATIVA

Al fine di soddisfare i principi enunciati al punto precedente, l'architettura tecnica ed organizzativa del modello proposto, si basa sui seguenti elementi fondamentali:

- la cooperazione applicativa avviene attraverso lo scambio di “messaggi applicativi” e sulla base di accordi di servizio che esplicitano l’accordo stipulato sull’erogazione/fruizione delle prestazioni del servizio in questione;
- la metodologia adottata e quella della busta di e-government ed è tale da garantire la non intrusività tra sistemi che tra loro cooperano applicativamente;
- ogni amministrazione gestisce i flussi di cooperazione applicativa con le altre amministrazioni per il tramite di un unico punto (logico) del proprio sistema informativo, denominato Porta di Dominio dei Servizi Applicativi (PDSA);
- le amministrazioni che cooperano fra loro possono dar luogo a Domini di Cooperazione in cui siano stabiliti i servizi erogati, i relativi livelli di servizio e le responsabilità nel mantenimento di tali livelli;

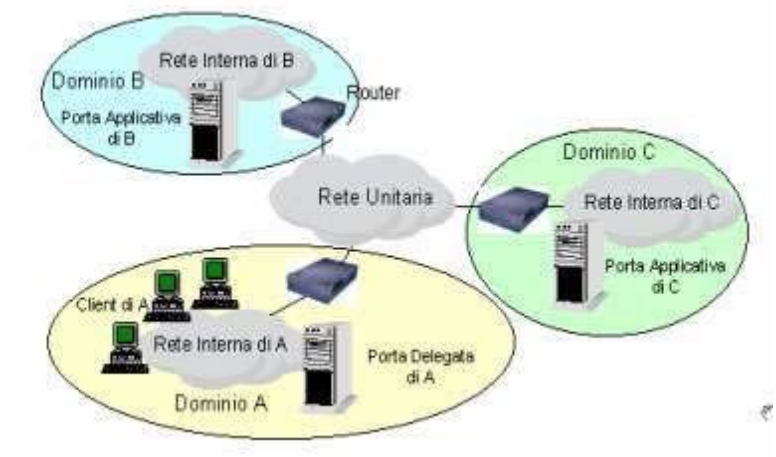

FIGURA 9 - SISTEMI COOPERANTI

- è definita una infrastruttura unitaria di servizi di interoperabilità e di cooperazione e accesso (SICA), che garantisce l’erogazione di servizi tecnologici di base, comuni a tutti i Domini di Cooperazione.

In questa architettura, il colloquio tra sistemi eterogenei cooperanti (Figura 9) è reso possibile dall’uso di elementi architetturali (porte) che disaccoppiano i contenuti tecnologici dei vari sistemi, da quelli applicativi. Ogni dominio della rete colloquia con gli altri attraverso un componente di interfaccia denominato “Porta di dominio” che svolge funzioni di barriera di ingresso per autorizzare l’accesso alle risorse applicative della rete e tradurre i messaggi provenienti da altri domini.
Questo componente può svolgere le funzioni di Porta Applicativa per mettere servizi e dati a disposizione degli altri domini, oppure la funzione di Porta Delegata per richiedere dati e servizi ad altri domini.
La comunicazione tra i domini, è realizzata attraverso un canale di interscambio basato su standard aperti (Web Services, XML, SOAP) che agevola il passaggio di messaggi tra i domini.

FIGURA 10 - DOMINI E PORTE DI DOMINIO

La Busta di e-Government e il modello logico e funzionale con cui si realizza la composizione di un messaggio mediante il quale si trasferiscono o richiedono informazioni e dati all'interno del Sistema Pubblico di Connettivita, secondo il paradigma della cooperazione applicativa.

2.3 ADOZIONE DI STANDARD

Per quanto riguarda le infrastrutture che dovranno essere create per garantire una gestione efficiente ed efficace del modello di cooperazione applicativa tra gli enti regionali, è importante sottolineare che le soluzioni adottabili dovranno essere basate su tecnologie standard.
Gli enti di standardizzazione di tecnologie di Web interoperability, le cui definizioni di specifiche e standard sono proposte come soluzioni ai requisiti tecnologici/ architetturali del modello di cooperazione CNIPA, sono:

- OASIS
- World Wide Web Consortium (W3C).

Gli standard dettati dall'OASIS (SOAP, UDDI e WSDL) e dal W3C (HTTP, HTTPS e XML), quindi, garantiscono un'alta interoperabilità tra diversi sistemi e linguaggi, specialmente se utilizzati rispettando le norme dettate dal WS-I (Web Service Interoperability).

2.4 MODELLO ARCHITETTURALE DI COOPERAZIONE APPLICATIVA

L'architettura tecnologica del Sistema Pubblico di Cooperazione a livello regionale, segue quella indicata dalle specifiche emanate dal CNIPA ed e composta da:

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

All'interno dell'infrastruttura di cooperazione applicativa saranno definiti gli elementi e utilizzati gli standard di seguito indicati:

- Accordo di servizio. (vedere documento CNIPA: Sistema pubblico di cooperazione: ACCORDO DI SERVIZIO V. 1.0 del 14/10/2005). Sono disponibili due proposte di specifica:
  - WSLA Web Services Level Agreement: si tratta di una proposta formalizzata tramite schema XML da IBM per la specifica, la creazione ed il monitoraggio di Service Level Agreement per Web Services.
  - WS-Agreement: si tratta di una serie di indicazioni proposte secondo schemi XML da Global Grid Forum.

- Autenticazione federata. (standard XACML, SAML). Permette la gestione distribuita delle credenziali di accesso ai servizi. Lo standard SAML è quello adottato a livello regionale con il framework Cohesion per l'identità federata.
- Servizi di sicurezza. (vedasi documento CNIPA: SERVIZI DI SICUREZZA V. 1.0 del 14/10/2005).
- Registro SICA. (vedasi documento CNIPA: SERVIZI DI REGISTRO V. 1.0 del 14/10/2005).
- Porta di Dominio. (vedasi documento CNIPA: PORTA DI DOMINIO V. 1.0 del 14/10/2005). La porta di dominio e l'elemento meglio formalizzato (vedi requisiti funzionali) e tecnologicamente caratterizzato (vedi requisiti non funzionali) dal CNIPA. I requisiti descritti in tale documento sono dunque direttamente traducibili in una implementazione applicativa.

2.5 L'INFRASTRUTTURA DI COOPERAZIONE APPLICATIVA REGIONALE

Nel seguito vengono fornite linee guida orientate alle due classi principali di esigenze infrastrutturali di cooperazione applicativa:

- la corretta implementazione di infrastrutture di cooperazione applicativa tramite porte di dominio;
- la corretta integrazione di sistemi applicativi di fruizione o di erogazione dei servizi.

Tra i possibili scenari di cooperazione applicativa, viene fortemente sconsigliato quello che prevede potenziali connessioni punto-punto tra enti che comunichino semplicemente tramite tecnologie SOA. Risulta infatti evidente come sia assolutamente inefficiente e dispendioso uno schema in cui vi siano interconnessioni potenziali tra ogni attore, sia per la complessità che tale modello introduce, che per il costo eccessivo a carico dei singoli enti. Vengono di seguito fornite indicazioni che tendono ad un modello più efficiente di quello sopra rappresentato e basato sulle specifiche e regole tecniche fornite al livello nazionale dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione.

2.6 MODELLO DI INTERCONNESSIONE ENTI-PDD REGIONALE

Vengono illustrate, in questo paragrafo, le forme di interconnessione degli enti e PA appartenenti all'ambito regionale coinvolti nel sistema di cooperazione applicativa. A tal fine occorre distinguere due tipologie di ente. Il primo caso riguarda semplicemente enti dotati di sistema informativo ma che non sono dotati di porta di dominio: in questo caso, il canale d'accesso privilegiato ai servizi e quello basato sulla tecnologia dei Web Services.
Il secondo caso riguarda enti che possiedono al loro interno una infrastruttura di porta di dominio che consente l'erogazione e fruizione di servizi in uno scenario di cooperazione applicativa.

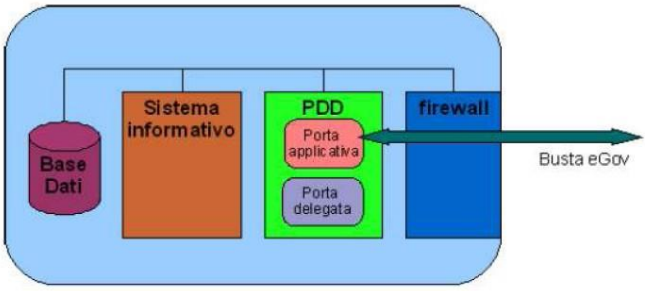

FIGURA 11 - ENTE DOTATO DI PDD ACCESSIBILE VIA CANALE E-GOV

In questo caso, infatti, il canale e-Gov rappresenta il punto di connessione verso l'esterno sia per l'erogazione dei servizi tramite porta applicativa (come visibile in Figura 11), sia per l'invocazione di servizi di altre porte di dominio, tramite porta delegata.
Il modello architetturale di cooperazione applicativa regionale, prevede che l'infrastruttura informatica regionale si ponga idealmente come strato intermedio di correlazione tra entità locali più piccole (per le quali funge da collettore) ed entità sia interne che esterne come enti di altre regioni (ma in generale qualsiasi sistema che possieda un'infrastruttura Porta di Dominio).
Assumendo che ogni entità (regione, provincia, comune, etc.) possa esporre una propria porta di dominio, quanto esposto si trova schematizzato nella seguente figura (Figura 12: Interconnessione Enti interni via e-Gov.).
In questo caso, un ente erogatore espone il proprio servizio tramite porta applicativa, servizio che viene invocato da un ente fruitore tramite porta delegata. Si nota, dunque, come l'apporto dato dall'infrastruttura SPCoop regionale riguardi essenzialmente il forwarding delle buste e-Gov tra i due enti. In pratica viene fornito il canale che permette la cooperazione applicativa tra i due enti.

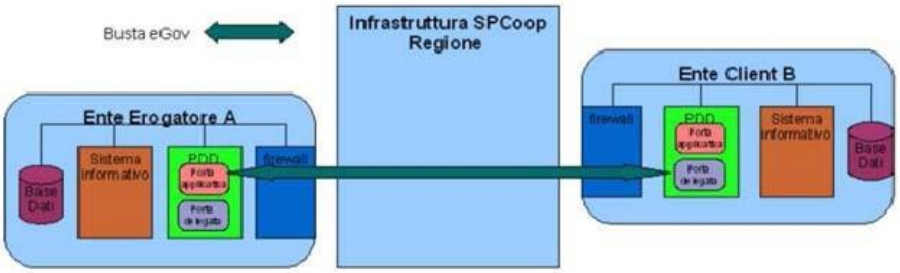

FIGURA 12 - INTERCONNESSIONE ENTI INTERNI VIA E-GOV

Per entità di piccole dimensioni si può realisticamente pensare che una infrastruttura PDD possa essere troppo onerosa e che queste debbano per via preferenziale interconnettersi con il nodo territoriale a loro più vicino appunto (che consenta ovviamente l'accesso ad ulteriori servizi esterni). In tale scenario, gli enti non dotati di porta di dominio possono realizzare un modello di comunicazione attraverso tecnologie standard, come quelle dei Web Services, ma senza l'onere del rispetto delle specifiche e-Gov che vengono comunque garantite dall'infrastruttura regionale.

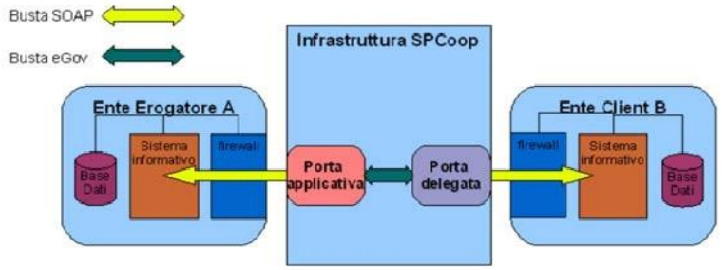

FIGURA 13 - INTERCONNESSIONE ENTI INTERNI VIA WS

Si noti come le funzionalità porta applicativa e delegata siano fornite in hosting dall'infrastruttura SPCoop regionale e di conseguenza tali enti sono virtualmente dotati di porta di dominio anche se erogano e richiamano il servizio applicativo mediante canale Web Services.
In questo modo gli enti interni sfrutterebbero le potenzialità della cooperazione applicativa appoggiandosi sull'infrastruttura regionale ed evitando di implementare soluzioni troppo onerose. Per contro, tale soluzione impedisce una gestione completamente indipendente quale sarebbe quella di dotare anche il piccolo ente interno di PdD.
Illustrati i due modelli di interconnessione basati sulla tipologia di enti che possiedono o no la porta di dominio, e facile ipotizzare scenari misti in cui enti non dotati di PdD richiamano enti che lo sono e viceversa.

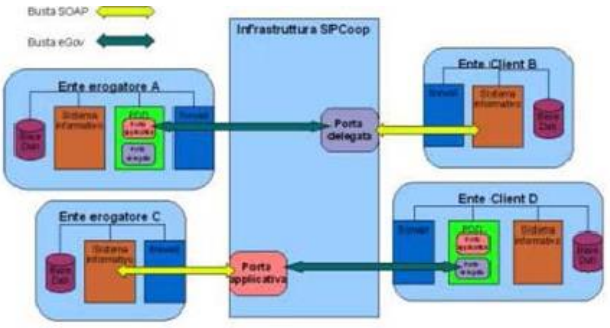

FIGURA 14 - SCENARIO MISTO DI COOPERAZIONE TRA ENTI DOTATI E NON, DI PDD

Dalla Figura 14 emerge chiaramente il ruolo fondamentale dell'infrastruttura di cooperazione applicativa regionale in quanto consente ad enti, eterogenei per dotazioni informatiche, di erogare ed invocare in maniera trasparente i servizi.

2.7 ARCHITETTURA INFRASTRUTTURA REGIONALE DI COOPERAZIONE

Con tale definizione si intende chiarire la struttura di cooperazione applicativa prevista per il nodo centralizzato regionale.

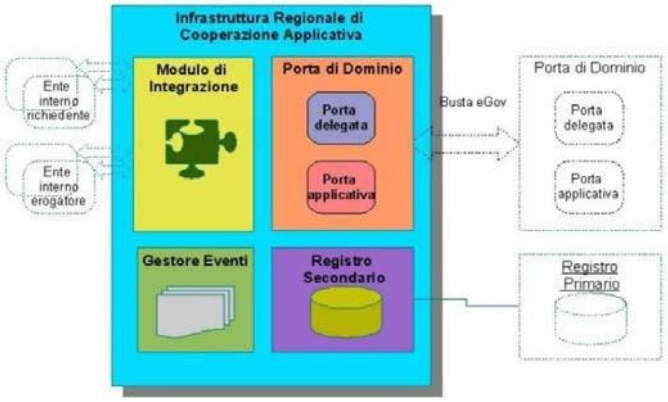

FIGURA 15 - SERVIZI DELL'INFRASTRUTTURA DI COOPERAZIONE APPLICATIVA REGIONALE

Per semplicità potrà essere chiamata Porta di Dominio Regionale, ma conterrà all'interno ulteriori servizi:

- Servizi di integrazione con Enti interni.
- Servizi di registro secondario.
- Gestione Eventi.

E' inoltre previsto che i singoli servizi applicativi espongano una consolle di amministrazione e monitoraggio per consentire un adeguato controllo sul funzionamento generale dell'infrastruttura. Ovviamente sono necessarie le più avanzate procedure al livello di sistema per le problematiche di:

- back up,
- disaster recovery,
- sicurezza,
- bilanciamento del carico applicativo,
- sorveglianza dei locali,
- ridondanza, etc..

2.8 SCENARIO DI COOPERAZIONE APPLICATIVA IN AMBITO INTERREGIONALE

Anche in ambito interregionale si può facilmente dimostrare la sconvenienza di uno scenario di cooperazione applicativa basato su connessioni punto-punto tra enti.

L'impiego del protocollo comune e-Gov tra nodi regionali permette invece di realizzare canali astratti di interoperabilità, indipendenti dalla logica applicativa, in cui sia già incluso il valore legale della comunicazione.
Uno scenario di cooperazione di questo tipo garantisce inoltre maggiore sicurezza applicativa in quanto sono facilmente individuati i canali fidati con cui comunicare:

- l'ente con la propria regione di pertinenza;
- le regioni tra di loro.

Infine, poichè i servizi infrastrutturali sono centralizzati al livello regionale, risulta minimizzata la complessità da gestire a carico degli attori partecipanti. Questi, infatti, dovranno esclusivamente limitarsi a risolvere le problematiche di collegamento con l'infrastruttura regionale.

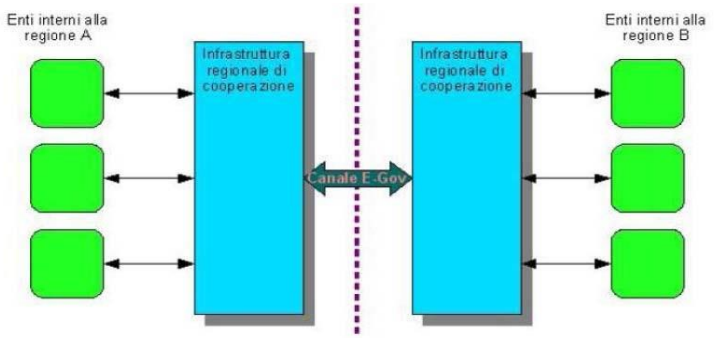

FIGURA 16 - CONNESSIONI ENTI ATTRAVERSO L'INFRASTRUTTURA REGIONALE DI COOPERAZIONE

2.9 SCHEMA DI INVOCAZIONE E INTEGRAZIONE DEI SERVIZI APPLICATIVI

Per questo aspetto occorre mettere in risalto due principali modelli implementativi:

- il primo prevede che vengano implementate ad hoc, rispetto al singolo servizio, le porte applicative e delegate;
- il secondo prevede che le funzionalità di porta applicativa e delegata siano fornite al livello di infrastruttura tecnologica, centralizzando di fatto il controllo sulla criticità di tali funzioni. In questo secondo caso si potrà accedere ai servizi di porta delegata e applicativa tramite opportuna configurazione e tramite client ad hoc che impiegano solamente il protocollo Web Services.

Questo modello e rappresentato dal seguente schema:

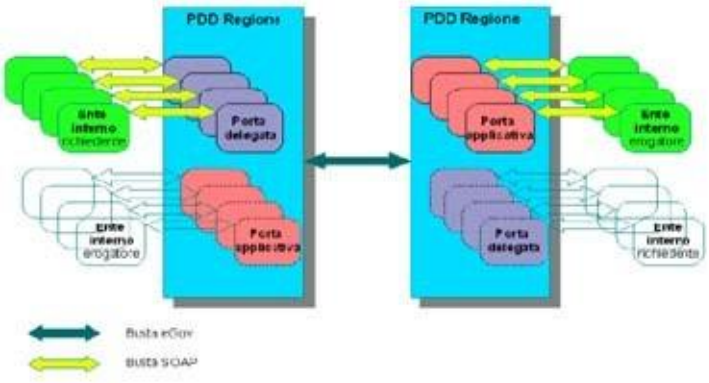

FIGURA 17 - SCHEMA INVOCAZIONE E INTEGRAZIONE SERVIZI APPLICATIVI IN STRUTTURA SPCOOP TRAMITE CANALE SOAP

Si nota come le funzionalità di porta applicativa e delegata siano implementate al livello strutturale e comunichino con i rispettivi servizi e client applicativi tramite un canale di minor complessità (SOAP) rispetto a quello costituito dalla busta eGov.

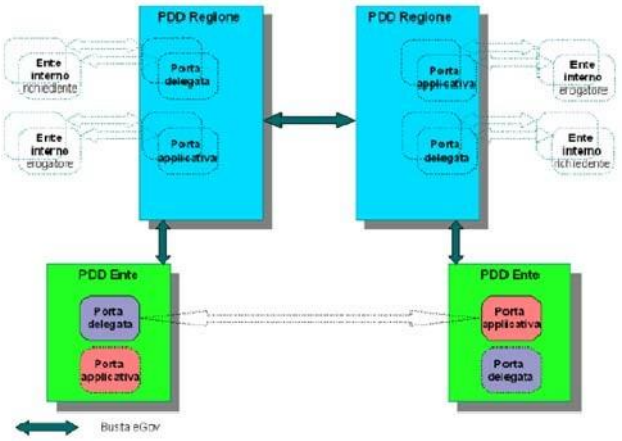

FIGURA 18 - SCHEMA INVOCAZIONE E INTEGRAZIONE SERVIZI APPLICATIVI IN STRUTTURA SPCOOP CON ENTI DOTATI DI PDD

Ciò garantisce la completa indipendenza della infrastruttura regionale dalle tecnologie utilizzate per servizi e client applicativi che risiedono negli enti. L'infrastruttura regionale funge quindi da relay di buste e-Gov. Il vantaggio, per gli enti, risulta essere la maggior semplicità dello schema di collegamento con altre porte di dominio ed il fatto di doversi fidare esclusivamente delle connessioni e-Gov da e verso le infrastrutture regionali che fungono da garanti delle comunicazioni interregionali.

2.10 SERVIZI PER IL CITTADINO

In genere i servizi applicativi non sono finalizzati ad un uso diretto da parte dei comuni cittadini per i quali le infrastrutture di cooperazione applicativa dovrebbero essere trasparenti. E' pero fondamentale sottolineare che un processo che coinvolge tale infrastruttura può essere indotto da un cittadino attraverso, per esempio, un sistema frontend messogli a disposizione dall'entità di servizi locali (previa autorizzazione). Quindi occorre ricordare, per i servizi che vedono come utente finale il cittadino, le seguenti indicazioni CNIPA:
I temi ritenuti prioritari dalla direttiva sono: l'adozione della Carta Nazionale dei Servizi (CNS) come strumento per accedere, in sicurezza, ai servizi in rete per i quali sia necessaria l'identificazione dell'utente. Le amministrazioni debbono pertanto provvedere a consentire l'accesso ai servizi ai titolari di tutte le CNS, indipendentemente dall'Ente di emissione delle stesse e come indicato nei precedenti paragrafi, verrà utilizzata la CNS regionale Carta Raffaello.

2.11 I POSSIBILI SCENARI DI COOPERAZIONE APPLICATIVA

E' di fondamentale importanza pensare che i servizi delle Pubbliche Amministrazioni siano indirizzati, in ultimo, ai cittadini i quali in qualche modo possono essere rappresentati come gli "starter" dei processi di interazione tra PA basati su cooperazione applicativa. E' quindi prevedibile l'impiego di uno strato d'interfaccia tra l'utente finale e le logiche di cooperazione fornite dai vari enti retrostanti. Ciò rappresenta uno scenario che ben rappresenta il caso dei servizi offerti da un Comune ad un cittadino/impresa tramite un portale web. Il portale rappresenta l'interfaccia attraverso cui il cittadino/impresa/ente può generare processi che coinvolgono uno o più enti (accesso ai servizi anagrafici, procedimenti autorizzativi in campo ambientale, pagamento tasse, etc.).
Inoltre, tutte le comunicazioni tra il backend del portale ed i servizi applicativi degli enti sono interazioni SPCoop.
Il modello architetturale per questo scenario, che riveste uno specifico interesse per il SIRA, prevede:

- una porta di dominio per ogni Ente coinvolto che può essere:
  - reale: la porta di dominio e in carico all'ente stesso.
  - virtuale: la porta di dominio fornita tramite il servizio di hosting a carico del Centro Controllo Reti (CCR) della Regione Marche che quindi non obbliga l'ente a dotarsi della relativa infrastruttura hw/sw.
- una porta di dominio davanti al backend del portale.

Quindi le interazioni sono:

utente -> portale -> PdD Ente Che Ospita Il Portale -> PdD Ente -> Servizio Applicativo Ente

Tale flusso di interazione può essere rappresentato dal seguente schema:

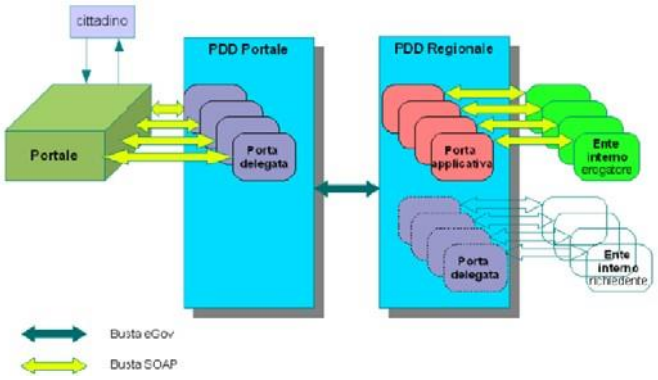

FIGURA 19 - SCHEMA DI INTERCONNESSIONE PORTALE CON SERVIZI ESTERNI TRAMITE PORTE DI DOMINIO

Nella figura soprastante, infatti, si nota quale sia il modello di interazione del portale verso i servizi applicativi erogati dai vari enti. Questi ultimi sono in generale erogati tramite una struttura centralizzata che offre le funzionalità di porta di dominio ed è in capo al Centro Controllo Reti Regionale. La figura mostra, dunque, come il portale acceda a tali servizi attraverso una PdD ad hoc. Il portale si serve di una serie di porte delegate (interne a tale porta di dominio) per richiamare i servizi. Ciò permette eventualmente ad un portale di fungere da strato di front-end per qualsiasi combinazione di ente pubblico o privato che esporti servizi eGov.
Nello scenario che comprende la presenza del Centro Controllo Reti Regionale, le funzionalità di PdD sono disponibili in un ambito orientato al territorio e sono rivolte tanto agli enti quanto al portale. Ciò permette ad entrambi di non doversi preoccupare di questo strato applicativo. Per cui l'architettura prevista e rappresentata dal seguente schema:

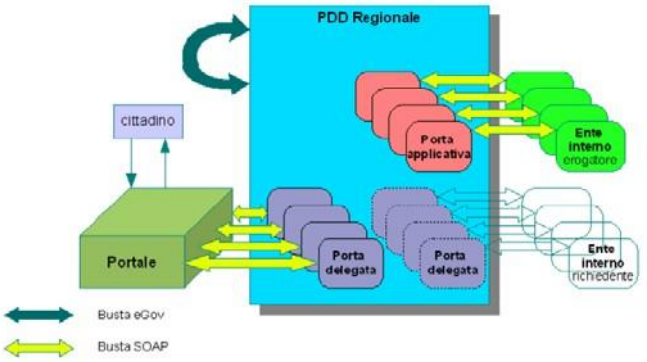

FIGURA 20 - SCHEMA DI INTERCONNESSIONE PORTALE CON SERVIZI ESTERNI TRAMITE INFRASTRUTTURA PDD REGIONALE

Si nota come i servizi legati alle specifiche SPCoop sono gestiti interamente dall'apposita infrastruttura regionale.
Tale infrastruttura offre i seguenti servizi:

- il servizio di Porta Delegata impiegato dal portale per l'invocazione dei servizi SPCoop;

- il servizio di Porta Applicativa impiegato dall'ente per erogare servizi in modalità SPCoop.

Il CCR promuove fortemente questa architettura per la sua aderenza alle normative in tema di interoperabilità/cooperazione applicativa e nel contempo per la sua flessibilità.
Tale caratteristica emerge infatti quasi spontaneamente dall'adozione delle specifiche SPCoop da parte degli enti erogatori. In pratica gli enti sono soggetti ad uno sforzo di identificazione e formalizzazione dei servizi che intendono esportare attraverso l'infrastruttura di e-Goverment. Proprio questo sforzo fa si che tali servizi possano essere facilmente pubblicati come servizi e-Gov ed essere infine potenzialmente richiamati da logiche di front end (come quelle dei portali-cittadino) e nello stesso tempo da altre pubbliche amministrazioni. Occorre sottolineare il forte vantaggio offerto dall'impiego dell'infrastruttura di PdD del CCR da parte degli enti. Infatti questi, non sono obbligati a dotarsi di funzionalità e-Gov ma devono concentrarsi sulla definizione ed implementazione dei servizi da esportare. Ciò rappresenta più un impegno dal punto di vista della definizione della logica legata al dominio di interesse che da quello prettamente tecnologico. Frutto di questa fase dovrebbe infatti essere una descrizione formale del servizio mediante, per esempio, diagrammi UML come:

- use case per la rappresentazione del contesto e dei requisiti funzionali,
- class diagram per la formalizzazione dei dati.

2.12 ARCHITETTURA GENERALE PORTALE/CCR/ENTI

Nella figura seguente è mostrato il caso generale, dell'architettura sopra descritta, che tiene conto della presenza di altri enti già dotati di Porta di Dominio e che si reggono sul CCR per il forwarding delle buste e-Gov. Tali soggetti possono essere:

- enti istituzionali che forniscono la schiera di servizi impiegati dal portale sia direttamente che attraverso processi di cooperazione;
- enti e aziende privati come per esempio Banche per la fornitura di servizi di pagamento richiamati dal portale stesso.

E' possibile riassumere lo scenario di più portali basato principalmente su servizi locali e non, erogati sia attraverso porte di dominio già esistenti, che tramite web services, con il seguente modello di riferimento (Figura 21). La posizione centrale del CCR (PDD Regionale) consente al portale di vedere tutti i servizi richiamati come raggiungibili direttamente, evitando connessioni con le altre porte di dominio coinvolte.

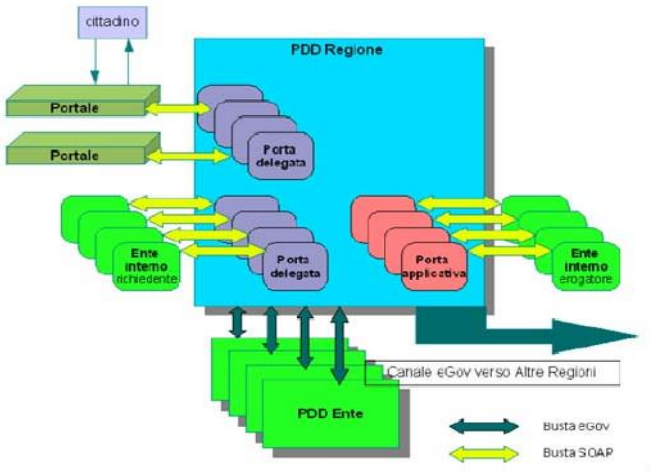

FIGURA 21 - SCENARIO SISTEMA GENERALE DI PORTALI BASATO SU INFRASTRUTTURA DI COOPERAZIONE APPLICATIVA A LIVELLO REGIONALE

3 STANDARD DI RIFERIMENTO

Si rimanda all'allegato "Standard di riferimento per lo sviluppo software", sempre in continua evoluzione e aggiornamento, in cui vengono elencati i principali standard di riferimento che debbono essere seguiti nella realizzazione di sistemi informativi regionali.
Altri standard di riferimento importanti sono quelli che riguardano il progetto interregionale per la dematerializzazione (Pro.De.) ed il piano regionale per gli interventi informatici nella sanità 2012-2014.