- SIAU -
Specifiche di Interfaccia Applicativi Utente

Identity Provider Cittadini Regione Lombardia

Codice Documento: **CRS-ISAU-SIAU#76**

Revisione del Documento: **05.9**

Data revisione: **03/05/2012**

Stato: **EMESSO**

	Struttura	Nome	Data	Firma
Redatto da:	Area Architettura Generale	P.Valenti		
Verificato da:	Area Architettura Generale	P.Valenti		
	Governo Sistemi Informativi e Piattaforma CRS-SISS	J.Mason		
Approvato da:	Governo Sistemi Informativi e Piattaforma CRS-SISS	J.Mason		
Emesso da:	Strategia, Program Management e Bisiness	F.Sirtori		

Cronologia delle Revisioni

Revisione	Sintesi delle Modifiche
1	Prima versione
2	Seconda versione: introduzione canale SSL per riservatezza tra ITS e browser utente; introduzione chiusura sessione utente a carico dell'Ente Erogatore; precisazioni sulla validità dell'asserzione rilasciata da IdPC-RL
3	Terza versione: rivisitazione URL IdPC-RL e servizio WAYF (sezione 3.1 e 3.1.1); chiarimenti sul formato della SAML Response e sullo statusCode da essa veicolato (sezioni 2.2.2, 3.2 e 3.5); precisazione sulla verifica della catena di trust dei certificati veicolati dalla SAML Response (sezione 2.2.2)
4	Quarta versione: revisione della nomenclatura del componente "Interfaccia di accesso ai servizi" (sezioni 2.1 e successive)
5	Quinta versione: introdotto riferimento alla Postazione di Lavoro del Cittadino (punto 1. sezione 2.1)
6	Sesta versione: revisione della sezione 3.4.
7	Settima versione: apportata correzione al disegno in figura 2 (sezione 2.1), chiariti ambiente di esecuzione di AccessCheck e ResponseReceiver (sezione 2.1 e 2.2.3).
8	Ottava versione: l'asserzione utente può veicolare il numero di cellulare dell'utente (valore opzionale).
9	Nona versione: estensione ad IdPC per svincolarsi dal codice attivo entro il browser utente, recuperando i dati anagrafici dall'Archivio Carte di Regione Lombardia (sezioni 2.1 e 3.2.2), introduzione del parametro "profile" (sezione 3.2.2), introduzione pagina di manutenzione dei dati autocertificati da parte dell'utente (sezione 3.2.2).
10	Decima versione: introdotta precisazione inerente il campo eMailAddress entro l'asserzione predisposta da IdPC (sezione 3.2.2).
11	Undicesima versione: introdotta sezione 3.7 inerente il porting verso IdPC delle applicazioni integrate con Sirac/People.
12	Dodicesima versione: introdotta sezione 2.1 per l'inquadramento delle modalità di erogazione di servizi web.
13	Correzioni redazionali minori nella sezione 2.1.
14	Introdotto parametro friendlyName nella sezione 3.2.2
15	Aggiornamento al nuovo template documentale di Lombardia Informatica
16	Introdotto parametro idApplicazione nella sezione 3.2.2
17	Introdotto nuovo valore per il parametro "profile" nella sezione 3.2.2
18	Revisione completa del documento. Inserita sezione 2.2; introdotto chiarimento su esposizione della componente *AssertionConsumer* nella sezione 3.1; sezione 2.3.2: specificata durata dell'asserzione prodotta da IdPC; sezione 3.1.1: introdotto dettaglio su possibile errore notificato all'applicazione integrata; eliminata sezione relativa al servizio "Where Are You From?"; eliminati i riferimenti alla "reference implementation" in linguaggio .NET; modificata la nomenclatura "PdL Cittadino" in "Software CRS"; inserito in asserzione nuovo tag "*statoValidazioneProfiloUtente*".
19	Versione annullata
20	Versione annullata
21	Correzione indice delle revisioni
22	Introdotte precisazioni sulla modalità di trasferimento dei dati tra le componenti della "reference implementation".
23	Introdotte ulteriori precisazioni nel cap. 3.3 per chiarire le modalità di trasferimento delle asserzioni tra *Assertion Consumer* e a *Response Receiver*, con particolare riferimento alla "*reference implementation*", al fine di sensibilizzare l'integratore sulle problematiche di sicurezza inerenti tale meccanismo. Rimossi i riferimenti alla "*reference implementation*" per .NET in quanto le architetture non J2EE possono avvalersi della soluzione con Reverse Proxy e agente di sicurezza Shibboleth (cfr. CRS-ISAU-SIAU#97), come da cap. 2.3.
24	Introdotta informazione relativa alla residenza dell'utente nell'asserzione rilasciata da IdPC. Eliminati riferimenti alle root CA di cui effettuare il trust, in quanto già presenti nel documento CRS-ISAU-SIAU#77.

Limiti di utilizzo del documento
In base alla classificazione del documento.

Indice

1 INTRODUZIONE

1.1 Scopo e campo di applicazione

Questo documento ha lo scopo di illustrare le interfacce per la comunicazione tra gli attori coinvolti nello scenario per l'accesso ai servizi mediato dal componente denominato **IdPC-RL** (**Id**entity **P**rovider **C**ittadini di **R**egione **L**ombardia).

Tale componente regola la fase di autenticazione degli utenti (cittadini) che, utilizzando un web browser, richiedono i servizi online offerti dai diversi Enti che intendono avvalersi delle funzionalità di IdPC-RL.

Come già illustrato nel documento [1], l'accesso dei cittadini della Regione Lombardia avverrà mediante l'utilizzo della *Carta Regionale dei Servizi* (CRS).

Nel seguito, dopo una breve presentazione dell'architettura del sistema, verranno forniti i dettagli sulle interfacce *fornite* e *richieste* da parte di IdPC-RL nei confronti dei fornitori di servizi esterni con i quali avverrà lo scambio di informazioni, al fine di consentire o negare l'accesso agli utenti.

1.2 Riferimenti

[1] OASIS – "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1" - OASIS Standard, 2 September 2003

[2] OASIS – "Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML) V1.1" - OASIS Standard, 2 September 2003

[3] CRS-ISAU-SIAU#77-Reference_Implementation – descrive la procedura di installazione e configurazione della "Reference Implementation" di una web application in cui siano integrati i servizi di autenticazione forniti da IdPC di Regione Lombardia

1.3 Acronimi e definizioni

Le definizioni e gli acronimi utilizzati nel resto del documento sono:

CA	Certification Authority
CN	Common Name
CNS	Carta Nazionale dei Servizi
CRS	Carta Regionale dei Servizi
DN	Distinguished Name
HTTP	Hyper Text Transfer Protocol
IdP	Identity Provider
IdPC-RL	Identity Provider Cittadini di Regione Lombardia (Nuovo Gestore Cittadino)
I2A	Interfaccia di Accesso Alle Applicazioni
LI	Lombardia Informatica
PEOPLE	Progetto Enti Online PortaLi E-Government
RR	Response Receiver
SAML	Security Assertion Markup Language
SSL	Secure Socket Layer
TLS	Transport Layer Security
WAYF	Where Are You From
XML	Extensible Markup Language

2 ARCHITETTURA

2.1 Scenario di erogazione dei servizi al Cittadino

L'architettura dell'Identity Provider Cittadini di Regione Lombardia (nel seguito **IdPC-RL**) costituisce il mattone di partenza per la costruzione di servizi web al Cittadino.

L'IdPC supporta le applicazioni web nella fase di identificazione e autenticazione dell'utente mettendo a disposizione dell'applicazione un insieme di "attributi" (nome, cognome, codice fiscale, …) utilizzabili nell'erogazione del servizio.

L'IdPC supporta diverse piattaforme d'accesso (es. MS Windows, LINUX e Mac OS) e browser Internet (es. MS Internet Explorer, Firefox e Safari). Per una lista esaustiva delle compatibilità si consulti il sito di progetto http://www.crs.lombardia.it.

La componente di autenticazione IdPC, per le carte CRS lombarde, non fa uso di componenti attivi lato postazione utente mentre, nel caso dell'accesso con CNS non emesse da Regione Lombardia, le informazioni di "attributo" dell'utente possono essere ottenute solo facendo uso di componenti attivi (ActiveX, applet java) che limitano le piattaforme d'accesso ad Internet Explorer e Firefox su Microsoft Windows. In realtà questa limitazione sarà superata "federando" l'IdPC con i domini di emissione delle varie CNS i quali si fanno carico di produrre asserzioni di identità e di attributo riconosciute anche dall'IdPC di Regione Lombardia (e viceversa).

Tra i vantaggi di un'autenticazione CNS ricordiamo il riconoscimento forte dell'utente e la disponibilità di informazioni di "attributo" certificate dall'emettitore delle CNS, i cui processi devono rispondere a precisi obblighi di legge.

Effettuata l'autenticazione l'applicazione eroga i propri servizi web nelle consuete modalità anche se, per agevolare il Cittadino e rispettare le norme sull'accessibilità delle applicazioni, non devono essere trascurati i seguenti aspetti:

- In qualunque pagina dell'applicazione dovrebbe essere disponibile un "bottone" tramite cui fare il Logout dall'applicazione; ciò è necessario in quanto l'azione istintiva di rimozione della CRS/CNS dal lettore non ha alcun effetto sull'applicazione web che resta in sessione fino al Logout, alla chiusura del browser o allo scadere del timeout di sessione;
- Evitare l'impiego di componenti attive quali ActiveX o applet preferendo, dove possibile, l'utilizzo di tecniche di integrazione standard supportate da tutti i browser.

Relativamente al secondo punto, due aspetti che potrebbero interessare un'applicazione web sono la produzione di documenti per il Cittadino (es. un file PDF contenente il riscontro di un'operazione) o la necessità di far sottoscrivere al Cittadino un documento di richiesta o di autocertificazione.
Per lo scaricamento di documenti si raccomanda di utilizzare le direttive standard di download evitando l'impiego di componenti attive che nell'agevolare l'operatività dell'utente (ActiveX, applet, …) compromettono l'operatività multipiattaforma e violano le norme sull'accessibilità.

L'interazione con l'utente per la firma elettronica di istanze è invece più articolata in quanto, in base alle norme sull'accessibilità, non devono essere utilizzati componenti attivi quali, ad esempio, quelli nel passato realizzati e messi a disposizione dal CRS-SISS (cfr. CRS-ISAU-SIAU#33).

Il flusso di interazione con il Cittadino segue il seguente flusso logico:

- Il Cittadino identifica il procedimento di suo interesse e fornisce all'applicazione i dati richiesti per istruire l'istanza;
- L'applicazione produce il documento che deve essere sottoscritto dal Cittadino (es. un file PDF) pre-compilandolo quanto più possibile con i dati già in possesso o appena forniti dall'utente;
- Il Cittadino viene guidato al download del documento prodotto ed istruito in merito alla necessità della sua firma elettronica;
- Il Cittadino scarica il documento e lo sottoscrive utilizzando un'applicazione di firma elettronica a sua scelta; Regione Lombardia mette a disposizione gratuitamente un'applicazione per la firma elettronica con CRS denominata *CRS Manager* compatibile con diverse di piattaforme d'accesso (es. MS Windows, LINUX e Mac OS) - per una lista esaustiva delle compatibilità si consulti il sito di progetto http://www.crs.lombardia.it.

- La pagina offerta al cittadino deve prevedere la funzionalità di upload del documento firmato, al fine di portare a termine l'istruzione dell'istanza.

Si ricorda che l'applicazione web ha la necessità di verificare la coerenza del documento ottenuto dal Cittadino, cioè:

- La firma elettronica deve essere valida ed il certificato non revocato e non scaduto;
- Il titolare del certificato di sottoscrizione deve corrispondere al titolare dell'istanza che si sta istruendo;
- Il documento trasmesso deve corrispondere a quello scaricato per la firma e, se richiesta la compilazione da parte dell'utente di sue parti, che quanto compilato dall'utente sia conforme alle regole di validazione dei dati previste dall'applicazione esposta.

Quale condizione di miglior favore per l'utente potrebbe essere fornita la possibilità di eseguire lo scaricamento del documento ed il suo upload in due distinte sessioni di navigazione invece che contestualmente ad una sola sessione di navigazione.

Nel caso di erogazione di applicazioni web per cui sia prevista la fruizione sia da postazioni cittadino che da postazioni non presidiate (es. chioschi) possono emergere problematiche di navigazione (es. legate alla firma di documenti) che non consentono di far uso della medesima applicazione web in entrambi i contesti.
Poiché la fruizione da postazioni non presidiate potrebbe rendere necessario l'utilizzo di componenti attive si raccomanda la realizzazione di due alberi di navigazione distinti in cui l'uso di componenti attivi sia limitato alle sole stazioni non presidiate la cui integrità SW è sotto diretto il controllo del'erogatore del servizio applicativo.

2.2 Scenario di interazione

L'architettura logica alla base dello scenario di accesso ai servizi mediato dai componenti che fanno capo all'infrastruttura dell'Identity Provider Cittadini di Regione Lombardia (nel seguito **IdPC-RL**) è illustrata in Figura 1.

La figura individua il flusso di scambio di informazioni scambiate fra i diversi soggetti coinvolti (Regione Lombardia, Ente Erogatore di servizi di e-government) nel contesto di una richiesta di accesso ad un servizio da parte di un utente finale erogato da un ente (Regione Lombardia o ente esterno).

In particolare nella figura si evidenzia come l'utente finale tenti anzitutto un accesso al portale erogatore dei servizi (che può essere interno o esterno a Regione Lombardia) e come quest'ultimo lo rimandi presso l'IdPC-RL per l'autenticazione, ricevendo infine un "documento" firmato che attesta l'esito della procedura di autenticazione, sulla base del quale il portale erogatore dei servizi potrà autorizzare o meno l'accesso.

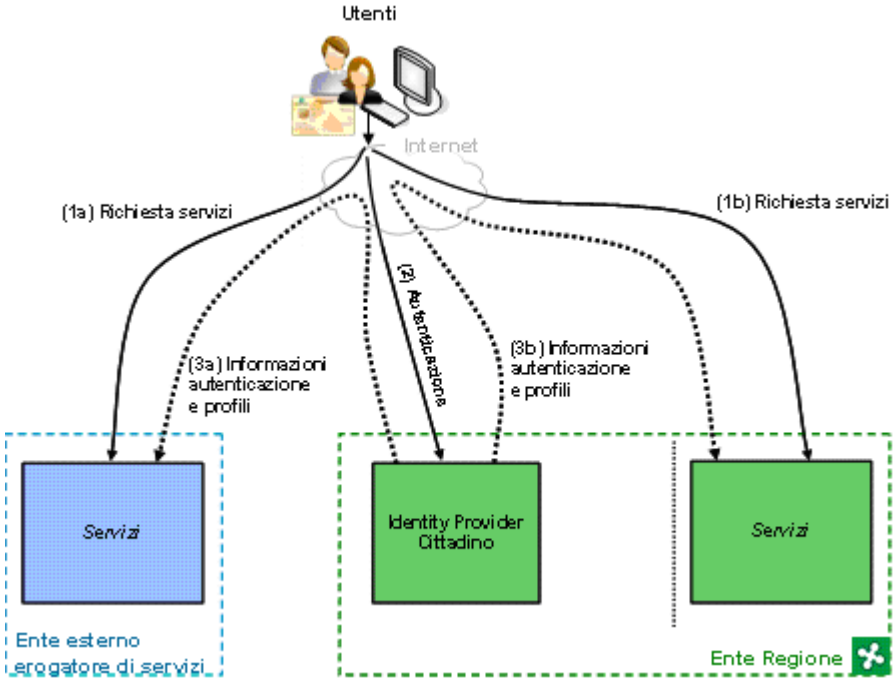

Figura 1 - Servizi e IdPC-RL comunicano tramite il browser del cittadino.

Nello scenario descritto in Figura 1 il protocollo utilizzato per rappresentare le informazioni di autenticazione che i soggetti coinvolti si scambiano (in particolare i fornitori di servizi finali e la Regione come identity provider) è quello definito dalla specifica SAML [1].

La versione di riferimento della specifica SAML che sarà inizialmente utilizzata è la 1.1, la stessa presente anche nel progetto PEOPLE con cui il sistema potrà così immediatamente interoperare. Seguendo la stessa linea di evoluzione di PEOPLE e per uniformarsi ad altri progetti nazionali in essere come ICAR, in futuro l'IdPC-RL potrebbe adottare una successiva versione di SAML, la 2.0, che completa la 1.1 in molti aspetti, arricchendo la potenza espressiva delle asserzioni ed introducendo svariati nuovi profili d'interazione.
In particolare nel seguito del documento verrà considerato come scenario di riferimento per l'autenticazione e l'accesso ai servizi da parte di un utente finale quello definito dal profilo di interazione SAML denominato "Browser POST Profile" nella modalità "Destination-Site-First", corrispondente all'opzione architetturale già presentata in Figura 1 (si vedano le specifiche SAML per maggiori dettagli).

Nella successiva Figura 2 viene illustrato il dettaglio delle interazioni con la sequenza di messaggi richiesti. Nello scenario illustrato in Figura 2 gli attori principali raffigurati sono il browser del cittadino, l'ente Regione Lombardia con il ruolo di Identity Provider e un generico Ente Erogatore di servizi. Quest'ultimo può coincidere con Regione Lombardia, nel caso in cui i servizi erogati siano quelli interni al relativo dominio, oppure essere un generico ente esterno.

Si noti inoltre che presso l'Ente Erogatore si ipotizza il dispiegamento di un componente denominato "Interfaccia di accesso alle applicazioni" (I2A) [1], che ha il compito di interfacciarsi da un lato con l'infrastruttura di autenticazione e dall'altro con il portale erogatore dei servizi finali per i cittadini.

Relativamente a tale componente, viene fornita da LI un'implementazione di riferimento, o "*reference implementation*" (per piattaforme J2EE), di cui gli Enti Erogatori potranno avvalersi per l'integrazione con la propria infrastruttura.
Questa implementazione non è prescrittiva e pertanto non esclude la possibilità da parte dei singoli Enti Erogatori dei servizi finali, di realizzare in modo autonomo componenti che realizzano le stesse funzionalità, ferme restando le interfacce esterne di interazione con IdPC-RL, descritte nelle sezioni successive di questo documento. Tali interfacce definiscono le modalità di trasmissione di una richiesta di autenticazione e della relativa risposta fornita dall'Identity Provider.

[1] Nel seguito anche indicato come "Interfaccia di accesso ai servizi".

In particolare l'Interfaccia di Accesso alle Applicazioni prevede al suo interno un componente denominato "*Access Check*" che ha il compito di filtrare tutte le richieste in arrivo destinate ai servizi applicativi erogati dall'Ente Erogatore e di verificare se l'utente richiedente deve essere o meno autenticato prima di consentire l'accesso alla risorsa finale richiesta dall'utente stesso.

Questo comporta il fatto che le richieste provenienti dal browser del cittadino non pervengono immediatamente ai servizi, ma devono obbligatoriamente transitare per questo componente che è in grado di innescare, se necessario, il processo di autenticazione. Come si vede dal dettaglio dei passi dell'interazione, al termine dell'autenticazione, l'interfaccia di accesso alle applicazioni deve trasferire i dati dell'utente al servizio applicativo. Per fare questo l'ente erogatore del servizio dovrà realizzare il componente denominato "*Response Receiver*" in grado di interpretare i dati del profilo e impostare un contesto applicativo idoneo al servizio.
Anche di tale componente viene fornita "*reference implementation*".

In particolare, il *Response Receiver* dovrà implementare un'interfaccia standard che verrà dettagliata in una sezione successiva del documento.

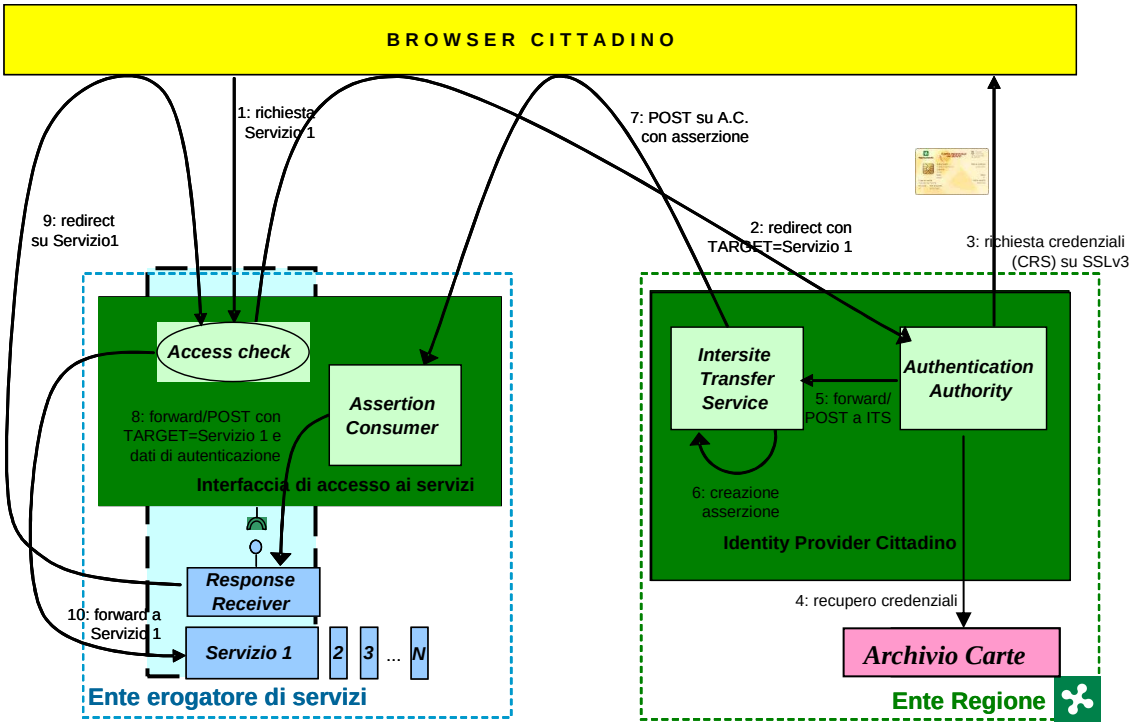

Figura 2 – Scenario generale di accesso ai servizi: dettaglio delle interazioni

La sequenza di messaggi scambiati è la seguente:

1. il cittadino utilizza il proprio browser per accedere ad un URL, che identifica l'entry-point del servizio richiesto (es. Servizio 1). Il browser è attestato su di una postazione Windows avente a bordo la "Postazione di Lavoro del Cittadino" di Regione Lombardia. [2]
2. La richiesta viene intercettata dall'interfaccia di accesso alle applicazioni dispiegata presso l'ente erogatore ("*Access check*") che verifica l'assenza di una sessione di autenticazione per l'utente richiedente. In conseguenza di ciò, *Access-Check* dirotta il browser dell'utente su IdPC-RL per iniziare la fase di autenticazione.
3. L'IdPC-RL riceve la richiesta di autenticazione proveniente dal browser utente come richiesta HTTP GET e, tramite il componente "*Authentication Authority*" crea un canale protetto con i protocolli TLS o SSL mediante il quale richiede all'utente di fornire le proprie credenziali, entro una sessione SSL v3 con client authentication. Per l'instaurazione di questa sessione, è quindi richiesto all'utente l'inserimento del PIN della CRS/CNS.

2 O analogo strumento (modulo CSP/PKCS#11) che consenta l'instaurazione di un canale SSLv3 con client authentication tramite token hardware (smartcard).

4. Le credenziali che contraddistinguono l'utente vengono recuperate contattando l'Archivio Carte di Regione Lombardia. Questo database contiene le informazioni anagrafiche utilizzate da Regione Lombardia per la produzione delle CRS/CNS. La prima release di IdPC-RL prevedeva la lettura della CRS/CNS per il recupero di queste informazioni, e ciò avveniva tramite l'esecuzione di codice attivo (ActiveX o applet) nel browser utente. La versione corrente di IdPC-RL elimina questa necessità di esecuzione di codice attivo, in accordo alle *best practices* in termini di accessibilità dei siti web, e recupera gli stessi dati utente dall'Archivio Carte. La lettura della smartcard viene eseguita solamente se la CRS/CNS in uso appartiene al circuito "demo", oppure se la smartcard in uso è una CNS emessa da altri Enti che non siano Regione Lombardia. A prescindere dalla "fonte" da cui vengono recuperate le credenziali utente, queste sono comunque composte dagli stessi dati elementari (nome, cognome, codice fiscale, eccetera), illustrati nel seguito di questo documento.

5. L'Authentication Authority inoltra le credenziali presentate al componente chiamato "*Inter-site Transfer Service*" (ITS). Tale interazione tra i componenti *Authentication Authority* e *Inter-site Transfer Service* potrà realizzarsi ove possibile mediante una interazione di tipo "forward" gestito interamente lato server, oppure, in alternativa, mediante una HTTP redirect che passa attraverso il browser del cittadino. In Figura 2 è rappresentata la prima modalità di interazione.

6. L'*Inter-site Transfer Service* utilizza i dati ricevuti per preparare una SAML Response contenente uno statement di autenticazione e uno statement di attributo. SAML Response è un documento XML con la struttura definita dalla specifica SAML 1.1 e firmato digitalmente dall'IdPC-RL. La struttura specifica del SAML Response prodotto dall'IdPc-RL è quella attualmente utilizzata anche nel progetto PEOPLE [3], al fine di permettere l'interoperabilità a livello di messaggi scambiati tra i servizi che necessitino di un riconoscimento del cittadino realizzati da diversi Enti/Pubbliche Amministrazioni, massimizzando il riuso e utilizzando uno standard già riconosciuto dagli Enti locali. Tale struttura è descritta in dettaglio nella sezione 3.2.

7. L'*Inter-site Transfer Service* produce come risposta per il browser del cittadino una pagina HTML contenente una form auto-post con le informazioni prodotte nella fase precedente [4]. Il target della form contenuta nella pagina è il componente "*Assertion Consumer*", dispiegato nell'interfaccia di accesso alle applicazioni, presso l'Ente Erogatore.

8. L'*Assertion Consumer* riceve la richiesta HTTP POST con le informazioni prodotte dall'*Inter-site Transfer Service* e verifica la correttezza e l'autenticità del Response ricevuto. Nel caso di verifica positiva, il componente *Assertion Consumer* estrae dal Response le informazioni che consentono di caratterizzare il profilo dell'utente autenticato operando una 'traduzione' del Response SAML in un formato interno XML 'non-SAML', più semplice e gestibile senza l'ausilio di librerie specifiche SAML e trasferisce le informazioni di autenticazione così elaborate al componente denominato "*Response Receiver*" con un'operazione di forward oppure passando per il browser del cittadino con una richiesta HTTP redirect sfruttando una form-auto-postante [5]. In figura è rappresentata la prima modalità, mentre nella sopracitata "*reference implementation*" è stata implementata la seconda modalità. Lo schema di tale formato interno XML è da considerarsi non normativo. Nella sezione 3.3 è fornito un esempio dettagliato di XML che è possibile utilizzare per la comunicazione tra *Assertion Consumer* e *Response Receiver* e utilizzato nella *reference implementation* fornita agli Enti Erogatori, ma qualunque altro formato che trasferisca le stesse informazioni è ammissibile. Si osserva che la comunicazione tra *Assertion Consumer* e *Response Receiver* deve preferibilmente avvenire in modalità *forward* (server-to-server). Qualora non risultasse tecnicamente percorribile tale modalità, è possibile passare tramite il browser dell'utente, mediante la produzione di una form auto-post in una pagina HTML. In questo secondo caso è indispensabile cifrare il contenuto della risposta, ad esempio utilizzando una chiave crittografica. Ulteriori dettagli sono forniti nella sezione 3.3.

[3] Con l'accezione "formato utilizzato nel progetto PEOPLE" relativo alle asserzioni, si fa riferimento unicamente al numero di informazioni trasferite, in termini di attributi del profilo (es. nome, cognome, ecc.) e non ad eventuali altre personalizzazioni del formato e nella struttura delle asserzioni SAML 1.1 che restano totalmente aderenti alla specifica del protocollo definito dalla specifica SAML 1.1 [1].

4 IdPCRL informerà il cittadino che le informazioni relative al suo profilo stanno per essere trasferite ad un Ente Erogatore, chiedendo l'autorizzazione a procedere. Il cittadino avrà la possibilità di negare questa autorizzazione, ed in tal caso il servizio non dovrà essere erogato. Se invece il cittadino acconsente alla propagazione di queste informazioni, il flusso procede come descritto.

[5] Nel secondo caso, le informazioni veicolate dalla POST sono cifrate con una chiave simmetrica conosciuta da *AssertionConsumer* e *ResponseReceiver*. Nella reference implementation, tale chiave è memorizzata su di un file.

9. Il componente *Response Receiver* costituisce il punto di collegamento tra l'interfaccia di accesso alle applicazioni e il servizio vero e proprio erogato dal generico ente. Il compito di questo componente è di impostare un contesto idoneo all'operatività del servizio (e in particolare di creare una sessione di autenticazione per l'utente in accordo con le modalità specifiche utilizzate internamente dal portale erogatore dei servizi finali). Questo comporta il fatto che il *Response Receiver* vive **nello stesso contesto** o ambiente di erogazione **del servizio** (e di ***AccessCheck***), utilizzando la stessa tecnologia (in generale diversa da quella utilizzata dall'interfaccia di accesso alle applicazioni) ed essendo dipendente dalla sua logica applicativa per quanto riguarda la modalità di settaggio parametri e definizione del contesto citato. Dopo aver definito opportunamente il contesto, il Response Receiver dirotta il browser dell'utente nuovamente all'indirizzo del servizio richiesto (Servizio 1).
10. In conseguenza del punto 8, il browser dell'utente si trova in una condizione simile di quella al punto 1, con la differenza che ora esiste una sessione di autenticazione impostata. Questo comporta il fatto che il componente *Access Check* non attiva più alcuna procedura di autenticazione, bensì mette il browser in contatto con il servizio richiesto, consentendone così la fruizione.

2.3 COMPONENTI PER L'INTERFACCIAMENTO DEL PORTALE EROGATORE DEI SERVIZI CON IDPC-RL

Rispetto allo scenario illustrato alla sezione precedente, i due componenti principali che devono essere realizzati per interagire con l'IdPC-RL sono quelli denominati "*Access Check*" e "*Assertion Consumer*". Nel seguito il dettaglio di tali componenti.

Si noti che **per i servizi applicativi che non utilizzano piattaforme J2EE** le funzionalità demandate alle componenti "*Access Check*" e "*Assertion Consumer*" posso essere ottenute con una soluzione alternativa basata su Reverse Proxy Apache equipaggiato con l'agente di sicurezza Shibboleth; tale architettura, descritta nel documento CRS-ISAU-SIAU#97, non richiede dispiegamento di componenti applicative nel service provider e pertanto è totalmente indipendente dalla piattaforma applicativa.

2.3.1 Access check

Per rispettare il requisito di trasparenza e non invasività rispetto ai servizi finali erogati dai vari service provider, non è ovviamente possibile operare direttamente sui servizi applicativi.

L'unica possibilità consiste nell'operare direttamente sull'ambiente di esecuzione dei servizi esistente, utilizzando componenti specifici in grado di intercettare e manipolare le richieste prima che queste vengano elaborate dai componenti che implementano i servizi applicativi.

Questo è il motivo della collocazione del componente *Access-Check* all'inizio della sequenza di interazione, dove, come illustrato, intercetta le richieste di accesso a servizi generate dal browser web dell'utente.

Dal canto loro, i servizi non si rendono conto dell'esistenza di un'infrastruttura che filtra le richieste in ingresso. Così come descritto, il componente *Access-Check* può configurarsi come un *filtro web J2EE* la cui logica applicativa provvede a controllare le richieste in arrivo e decidere se propagarle direttamente agli erogatori di competenza, oppure se innescare prima il processo di autenticazione.

Si noti che, per completezza di trattazione, il componente *Access-Check* si configura in generale come una catena di filtri e non come un filtro unico. Infatti, per svolgere adeguatamente il suo compito, *Access-Check* dovrebbe conoscere qualche informazione in più relativamente al servizio richiesto, e sapere quindi se esso richiede o meno una autenticazione ed eventualmente di che tipo (forte, debole, ecc.) [6]. Questo tipo di informazioni può essere presente ad esempio qualora esista un "profilo" per i servizi disponibili. *Access-Check* potrebbe pertanto anzitutto leggere tale profilo e, in base al suo contenuto, attivare o meno la seconda fase (autenticazione) con diverse modalità. Da ultimo si sottolinea anche che a valle della fase di autenticazione, *Access-Check* potrebbe svolgere ulteriori controlli, legati ad esempio ad una fase di autorizzazione, sulla base di apposite ACL (access control list) definite per ciascun servizio, onde regolare in modo più fine l'accesso.
Nel seguito, tuttavia, si assumerà che Access-Check svolga solo la funzione di filtro di autenticazione, e questa sarà anche la sua prerogativa nella "*reference implementation*" fornita.

Per svolgere la propria funzione, "*Access-check*" recupera dalla sessione utente, o in altro modo, le informazioni relative allo stato di autenticazione dell'utente.

In particolare, "*Access-check*" verifica se nella sessione di tale utente è presente una "*Authentication Response*" SAML che certifica il completamento con successo di una precedente autenticazione.

Nel caso tale controllo risulti positivo, il filtro termina la propria attività inoltrando la richiesta all'indirizzo originario specificato nella richiesta HTTP pervenuta dal browser web. Viceversa, viene attivata la procedura di autenticazione che coinvolge le altre entità descritte nel modello architetturale. I dettagli relativi a questa fase sono descritti nel capitolo successivo, alla sezione 3.1.

[6] I servizi esposti tramite IdPC-RL restituiranno un'asserzione SAML ottenuta tramite autenticazione forte dell'utente.

Del componente "*Access-check*" viene fornita una "*reference implementation*" che potrà essere sostituita dall'Erogatore del servizio con implementazioni personalizzate, che aderiscano al comportamento descritto.

Si noti che questo componente non ha l'obiettivo di realizzare funzionalità di Single-Sign On in rete. In altri termini, se un cittadino, dopo aver interagito con un primo servizio web, dirige la propria navigazione su di un secondo servizio attestato su di un altro Ente Erogatore, verrà richiesta una nuova autenticazione all'IdPC-RL, in quanto l'*Access check* installato sul secondo Ente Erogatore viene contattato per la prima volta, e richiede un'autenticazione.

Questo comportamento è voluto, in quanto garantisce la visibilità al cittadino del fatto che sta avvenendo un trasferimento del proprio profilo a portali web differenti da quello originariamente interfacciato.

Si noti infine che in questo paragrafo, e nei successivi, si farà spesso riferimento all'IdPC-RL come Identity Provider di riferimento.

Ciò non esclude che l'Ente Erogatore che si dota delle componenti software *Access Check* e *Assertion Consumer* possa accettare asserzioni anche da Identity Provider al di fuori di IdPC-RL, che rimane comunque l'Identity Provider di riferimento per le web application erogate da Regione Lombardia.

2.3.2 Assertion Consumer

Il componente denominato "*Assertion Consumer*" svolge l'attività di ricezione dati inviati dall'IdPC-RL a valle della fase di autenticazione, effettuata in interazione diretta con l'utente. Esso riceve l'asserzione prodotta da IdPC-RL, ne verifica la correttezza e l'autenticità, ed estrae le informazioni relative al profilo dell'utente.

In particolare, Assertion Consumer deve effettuare i seguenti controlli di validità sull'asserzione ricevuta:

- verifica della validità dell'asserzione mediante consultazione dei relativi timestamp (tag <*Conditions*> nell'asserzione, con attributi *NotBefore* e *NotOnOrAfter*); a causa di tale controllo, è necessario che l'ora e data di sistema del nodo dove è installato il componente in esame siano sufficientemente attendibili [7];
- verifica sulla firma, allo scopo di rilevare un eventuale "tampering" delle informazioni trasmesse;
- verifica dello stato di validità del certificato utilizzato per la firma e di quelli presenti nella catena di certificati [8]: se il trust store dell'Assertion Consumer è configurato in modo da considerare attendibili anche le asserzioni relative a CRS virtuali, tali asserzioni vanno gestite in modo opportuno, in modo da evitare di erogare servizi quando non dovuto;
- verifica dello stato di revoca del certificato utilizzato per la firma e di quelli presenti nella catena di certificati, mediante consultazione delle relative CRL;
- verifica della validità dell'asserzione tramite ispezione del tag *StatusCode* entro la SAML Response: il servizio dell'Ente Erogatore può essere usufruito dall'utente se e solo se *StatusCode* è valorizzato a *Success*.

Nel caso in cui tutti i suddetti controlli abbiano dato esito positivo, *Assertion Consumer* estrae dall'asserzione i dati del profilo dell'utente pervenuti mediante l'asserzione ricevuta da IdPC-RL, crea una nuova struttura dati in formato XML non-SAML e li trasferisce al componente denominato "*Response Receiver*", preferibilmente con un'operazione di forward.

Nel caso almeno uno dei suddetti controlli abbia esito negativo, l'accesso al servizio esposto dall'Ente Erogatore non deve essere concesso.

I dettagli sul formato dei dati trasferiti sarà fornito nel capitolo successivo, alla sezione 3.3.

[7] La validità dell'asserzione non è in alcun modo correlata con la validità della sessione utente verso il servizio esposto dall'Ente Erogatore.

8 Per determinare la validità della catena di trust, l'eventuale certificato di CA presente nella SAML Response deve corrispondere ad uno dei certificati delle CA considerate attendibili, che devono essere presenti in un truststore (o db) locale all'Assertion Consumer.

2.3.3 Response Receiver

Il componente denominato "*Response Receiver*" non fa strettamente parte dell'Interfaccia di Accesso alle Applicazioni, in quanto è sviluppato e dispiegato in un ambiente che utilizza la medesima tecnologia del portale erogatore dei servizi.

Tale componente è sotto la diretta responsabilità dell'erogatore dei servizi e ha il compito di ricevere le informazioni di profilo dell'utente che ha completato la fase di autenticazione e *impostare* una sessione per tale utente che viene infine rimandato sulla pagina del servizio.

Analogamente, ha la responsabilità di *rimuovere* (o *invalidare*) tale sessione nel momento in cui l'utente sceglie di farlo, tramite azione esplicita sull'interfaccia grafica della web application esposta dall'Ente Erogatore.

Ciò potrà essere convenientemente implementato tramite un tasto dal nome significativo (es. "Chiudi sessione", oppure "Esci"), la cui selezione da parte dell'utente avrà come effetto la rimozione della sessione dell'utente stesso.

Si noti infine che, come già accennato, *Access-Check* e *Response Receiver* operano **nel medesimo ambiente o contesto**, dal momento che entrambi devono poter accedere alla sessione utente.

3 INTERFACCE

3.1 Interfaccia per il trasferimento della richiesta di autenticazione all'IdPC-RL

In caso di attivazione della procedura di autenticazione, il filtro *Access-Check* risponde al browser dell'utente con un comando di redirect verso **IdPC-RL**.

Tale accorgimento può essere realizzato tramite una response HTTP con la opportuna valorizzazione degli header *Status-Code* e *Location* o mediante tecnologie alternative quali l'uso di javascript o del tag HTML "meta refresh".

La "*reference implementation"* di *Access Check* fornita da LI farà utilizzo di javascript.

Per questo viene costruita una richiesta di tipo HTTP GET il cui URL è ottenuto componendo quello per l'accesso al servizio di login erogato da IdPC-RL, comprensivo di eventuali parametri, **con un parametro "TARGET"** che individua l'URL del servizio "Assertion Consumer" presente nel contesto dell'erogatore, all'interno dell'"interfaccia di accesso alle applicazioni".

L'URL del servizio "*Assertion Consumer*" contiene a sua volta un ulteriore parametro "target" (minuscolo) che specifica l'URL completo della pagina del servizio applicativo originariamente richiesta dall'utente. Il contenuto del parametro "TARGET" sarà quindi il seguente:

```
TARGET=https://host-erogatore:port/AssertionConsumer?target=http://host-
erogatore:port/servicePage?serviceParameters...
```

in cui:

- *host-erogatore:port* è la coppia hostname-porta del server presso cui è attivo l'ambiente per l'erogazione dei servizi comprensivo dell' "interfaccia di accesso alle applicazioni" ;
- *AssertionConsumer* è il puntatore alla risorsa web relativa alla interfaccia del componente *Assertion Consumer*; è libertà dell'erogatore decidere la struttura del nome usato; nella "*reference implementation*" fornita da LI, in accordo con le specifiche SAML, il nome della risorsa web è appunto *AssertionConsumer*; è **richiesto** di pubblicare questa risorsa web su SSL v3 con sola server authentication [9], in quanto tra IdPC ed *AssertionConsumer* transitano dati potenzialmente sensibili;
- *servicePage* è il puntatore alla risorsa web relativa al servizio richiesto dall'utente; ovviamente sta al singolo erogatore definire la struttura di questo nome così come quella per i suoi parametri applicativi ; è altresì responsabilità dell'Erogatore determinare se pubblicare questa risorsa web su SSL o meno (nell'esempio è indicato il protocollo http) ;
- *serviceParameters* è l'elenco dei parametri applicativi e relativi valori da passare alla risorsa web identificata al punto precedente; di nuovo, è responsabilità del singolo erogatore dei servizi definire quanti e quali parametri è necessario specificare.

L'URL del servizio di login erogato da IdPC-RL [10] è quindi il seguente [11]:

```
https://idpcrl.crs.lombardia.it/scauth/SSLAuthServlet?TARGET=https://host-
erogatore:port/AssertionConsumer?target=http://host-
erogatore:port/servicePage?serviceParameters...
```

9 In quanto è rilevante la cifratura del canale, e non la mutua autenticazione tra i soggetti in gioco. Si noti che *AssertionConsumer* instaurerà un canale SSL con il browser utente, dunque è consigliabile l'utilizzo di un certificato server rilasciato da una Certification Authority Omniroot. La reference implementation del componente *AssertionConsumer* sarà dotata di un certificato rilasciato da una Certification Authority non Omniroot.

10 Si veda a tal proposito anche il paragrafo 3.1.1.

11 Nella tabella è riportata la rappresentazione URL-encoded dell'indirizzo in oggetto.

E' necessario porre attenzione alla lunghezza massima dell'URL costruita e dipendente dal browser in uso dal cittadino; ad esempio, Internet Explorer consente l'uso di URL con la lunghezza massima di 2048 caratteri.

Con la HTTP request indicata termina il compito di *Access-Check* relativamente alla generazione della richiesta di autenticazione e il controllo viene passato a IdPC-RL.

3.1.1 Il servizio di "Where Are You From?"

La URL indicata nella sezione 3.1 indica la collocazione sulla rete Internet del servizio IdPC-RL.

Tuttavia, un generico Ente Erogatore di servizi potrebbe voler consentire l'accesso a tutti i cittadini dotati di uno strumento di autenticazione forte, quali la CNS, anche se questa CNS non è necessariamente quella rilasciata da Regione Lombardia e la cui autenticazione è gestita da IdPC-RL.

Per tale motivo, il Progetto metterà a disposizione anche una pagina di WAYF (*Where Are You From?*), che, se invocata, consentirà di redirigere la navigazione del browser verso l'Identity Provider di riferimento di quell'utente (in prima istanza verso il solo IdPC-RL).

La URL cui sarà attestato il servizio di WAYF messo a disposizione da Regione Lombardia sarà:

```
http://wayf.crs.lombardia.it/wayf/index.jsp?TARGET=https://host-
erogatore:port/AssertionConsumer?target=http://host-
erogatore:port/servicePage?serviceParameters...
```

3.1.2 La gestione degli errori di IdPC-RL

IdPC-RL può rilevare errori durante la presa in carico della chiamata (ad esempio a causa dell'assenza del parametro TARGET), oppure durante l'autenticazione dell'utente (ad esempio perché lo stesso non ha acconsentito alla lettura della propria smartcard da parte della pagina web di IdPC-RL).

In tutti i casi, viene generato un errore autoesplicativo che viene mostrato direttamente all'utente finale tramite web browser, senza notificare *Access Check* (operazione che risulterebbe tecnicamente impraticabile).

3.2 Interfaccia per il trasferimento della SAML Response di autenticazione dall'IdPC-RL al portale erogatore del servizio

IdPC-RL invia ad **Assertion Consumer** l'asserzione prodotta in fase di autenticazione, contenuta all'interno di una struttura SAML Response.

Tale operazione è fatta mediante submit di una form in modalità POST.

La form contiene tre campi nascosti: il primo, di nome "SAMLResponse" ha come valore la codifica in formato Base64 della SAML Response detta.

Il secondo, di nome "TARGET", riprende l'omonimo parametro inserito dal componente Access-Check e consente di determinare verso quale servizio rimandare la richiesta (mediante il sotto-parametro "target" minuscolo inserito nel precedente).

Il terzo è chiamato "authResponseStatus" e contiene uno Uniform Resource Name (URN) che sancisce l'esito (positivo o negativo) della fase di autenticazione. I possibili valori assunti da tale campo sono quelli riportati nella tabella seguente. Quest'ultimo campo non è normato dalla specifica SAML ma viene passato per mantenere l'interoperabilità con il progetto PEOPLE.

Response status	Significato
urn:people:names:authenticationstatus:success	l'autenticazione ha avuto successo
urn:people:names:authenticationstatus:failure	l'autenticazione non ha avuto successo

Tabella 3.1 - i valori possibili per lo status di autenticazione

Questo campo **non** è firmato da IdPC-RL e per tale motivo **non** si deve fare affidamento sul suo valore per determinare con certezza se l'autenticazione ha avuto successo o meno.

L'esito dell'autenticazione **deve** essere ricavato ispezionando il tag <*Status*>/<*StatusCode*> della SAML Response. Tale tag assume valore Success **se e solo se** l'autenticazione ha avuto successo.

Qui di seguito la sezione della SAML Response dove compare l'informazione descritta.

```
<Response xmlns="urn:oasis:names:tc:SAML:1.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol" IssueInstant="2006-11-07T13:59:20.922Z"
MajorVersion="1" MinorVersion="1" Recipient="http://host-erogatore:port/AssertionConsumer"
ResponseID="…">
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                …informazioni relative alla firma dell'intera SAML Response in accordo a XMLDS…
        </ds:Signature>

        <Status>
                <StatusCode Value="samlp:Success"/>
        </Status>

        <Assertion>
        … da zero ad N asserzioni firmate in accordo a XMLDS …
        </Assertion>

</Response>
```

I valori che possono essere assunti da StatusCode sono normati dalle specifiche SAML.

Il campo nascosto "authResponseStatus" viene comunque valorizzato da IdPC-RL con un valore coerente con il contenuto di <*Status*>/<*StatusCode*> della SAML Response per compatibilità con il progetto PEOPLE.

Nel box seguente viene riportato un esempio di codice HTML che realizza la form auto-post sopra descritta.

```
<html>
    <body onload="javascript:document.forms[0].submit()">
        <form method="post" action=" http://host-erogatore:port/AssertionConsumer">
            <input type="hidden" name="TARGET" value=" http://host-
erogatore:port/AssertionConsumer?target=http://host-
erogatore:port/servicePage?serviceParameters...">
            <input type="hidden" name="SAMLResponse" value="<codifica Base64 della SAML Response>">
            <input type="hidden" name="authResponseStatus" value="<status>">
        </form>
    </body>
</html>
```

Assertion Consumer, a valle delle verifiche svolte come descritto nella sezione 2.3.2, deve confrontare il parametro TARGET contenuto nella form ricevuta con il valore dell'attributo *Recipient* della SAML Response e con il proprio indirizzo locale. In questo modo verifica che la response stessa sia stata correttamente indirizzata.

Di seguito un esempio di intestazione della SAML Response:

```
<Response xmlns="urn:oasis:names:tc:SAML:1.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol" IssueInstant="2006-11-07T13:59:20.922Z"
MajorVersion="1" MinorVersion="1" Recipient="http://host-erogatore:port/AssertionConsumer"
ResponseID="f526b5f90d9e216e1227bcb77dde5390">
...
...
</Response >
```

La SAML Response è firmata da IdPC-RL e contiene un'asserzione al cui interno sono presenti uno *statement di autenticazione* e uno *statement di attributo* contenente i vari elementi del profilo trasferito.

Si noti che *authenticationstatus* (descritto in Tabella 3.1), ovvero *StatusCode* presente nella SAML Response, può essere *failure* nei seguenti casi:

a. l'utente ha negato l'autorizzazione al trasferimento dei dati del proprio profilo all'Ente Erogatore del servizio, oppure
b. IdPC-RL non è riuscito a firmare gli statement di autenticazione ed attributo dell'utente che ha richiesto il servizio.

In tutti questi casi, l'Ente Erogatore *non* deve concedere l'accesso al servizio esposto, segnalando altresì all'utente, tramite una pagina web, il motivo della mancata erogazione del servizio.

In entrambi i casi, l'*attribute statement* della SAML Response è nullo o non significativo.

In particolare alla sezione 3.5 viene riportato un esempio completo di SAML Response trasferita con successo. Nel seguito è descritta nel dettaglio la struttura di tali due statement.

3.2.1 Authentication statement

L'authentication statement dell'asserzione prodotta ha la seguente struttura (dove non diversamente specificato, tutti gli elementi e gli attributi riportati, al netto del valore assunto, devono essere considerati obbligatori):

```
<AuthenticationStatement AuthenticationInstant="2006-11-17T09:19:26.467Z" AuthenticationMethod="<meccanismo di
autenticazione>">
    <Subject>
        <NameIdentifier><identificativo utente></NameIdentifier>
        <SubjectConfirmation>
            <ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</ConfirmationMethod>
        </SubjectConfirmation>
    </Subject>
</AuthenticationStatement>
```

L'elemento *"AuthenticationStatement"* deve contenere gli attributi *"AuthenticationInstant"* e *"AuthenticationMethod"*.

Quest'ultimo ha come valore una stringa (parametro <*meccanismo di autenticazione*>) con cui è specificato il meccanismo utilizzato per effettuare l'autenticazione.

L'elenco dei possibili valori che può assumere tale attributo è il seguente:

Authentication method	**Significato**
urn:oasis:names:tc:SAML:1.0:am:HardwareToken	l'autenticazione è stata effettuata mediante dispositivo hardware (es. Smartcard) con certificato di autenticazione; IdPC-RL rilascia asserzioni firmate **esclusivamente** con **questa** modalità.
urn:people:names:pin	l'autenticazione è stata effettuata mediante inserimento di username e pin; IdPC-RL **non** rilascia asserzioni firmate con questa modalità, ma è possibile che altri Identity Provider utilizzino questo Authentication Method
urn:oasis:names:tc:SAML:1.0:am:password	l'autenticazione è stata effettuata mediante inserimento di username e password; IdPC-RL **non** rilascia asserzioni firmate con questa modalità, ma è possibile che altri Identity Provider utilizzino questo Authentication Method
urn:oasis:names:tc:SAML:1.0:am:X509-PKI	l'autenticazione è stata effettuata mediante un meccanismo basato su una chiave rilasciata da una PKI X.509; IdPC-RL **non** rilascia asserzioni firmate con questa modalità, ma è possibile che altri Identity Provider utilizzino questo Authentication Method
urn:ietf:rfc:2246	l'autenticazione è stata effettuata mediante protocollo SSL o TLS utilizzando un ceritifcato fornito dal client al server; IdPC-RL **non** rilascia asserzioni firmate con questa modalità, ma è possibile che altri Identity Provider utilizzino questo Authentication Method

Tabella 3.2 - I meccanismi di autenticazione supportati

L'elemento precedente deve contenere un elemento *"Subject"* contenente le informazioni relative all'utente (subject) autenticato.

Tali informazioni sono strutturate mediante un sotto-elemento *"NameIdentifier"* di *"Subject"* il cui valore è una stringa (parametro <*identificativo utente*>) con cui è possibile identificare univocamente l'utente che è stato autenticato.

Tale identificativo deve avere il formato <CODICEFISCALE>@idpc.crs.lombardia.it.

Inoltre, l'elemento *"Subject"* deve contenere il sotto-elemento *"SubjectConfirmation"* in cui il suo sotto-elemento *"ConfrmationMethod"* deve avere come valore la stringa standard "urn:oasis:names:tc:SAML:1.0:cm:bearer", come richiesto dalla specifica SAML 1.1 (cfr. [2], sez. 4.1.2).

3.2.2 Attribute statement

L'attribute statement dell'asserzione prodotta ha la seguente struttura (dove non diversamente specificato, tutti gli elementi e gli attributi riportati, al netto del valore assunto, devono essere considerati obbligatori):

```
<AttributeStatement>
   <Subject>
      <NameIdentifier><identificativo utente></NameIdentifier>
      <SubjectConfirmation>
         <ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</ConfirmationMethod>
      </SubjectConfirmation>
   </Subject>
   <Attribute AttributeName="<nome attributo>"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
      <AttributeValue><valore attributo></AttributeValue>
   </Attribute>
   <Attribute AttributeName="<nome attributo>"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
      <AttributeValue><valore attributo></AttributeValue>
   </Attribute>
```

```
   <Attribute AttributeName="<nome attributo>"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
      <AttributeValue><valore attributo></AttributeValue>
   </Attribute>
...
...
</AttributeStatement>
```

L'elemento *Subject* deve coincidere con quello presente nello statement di autenticazione, dal momento che lo statement di attributo contiene informazioni relative al profilo dell'utente che si è autenticato.

Le informazioni del profilo sono specificate mediante la ripetizione della struttura *Attribute* in cui è necessario specificare il nome del campo del profilo (parametro <*nome attributo*>), il namespace (costante fissata, come esempio, a "http://www.crs.lombardia.it/idpc") e il valore di tale campo (parametro <*valore attributo*>. Si noti che il valore dell'attributo *namespace* per i vari attributi è da considerarsi non normativo e non è previsto che le applicazioni che lo trattano facciano alcuna assunzione sul suo valore.

Nella tabella seguente sono elencati i campi del profilo tipicamente trasferiti [12], corredati di alcune note esplicative, dove necessario:

Nome campo	Note	Valorizzazione effettuata da IdPC-RL ? [13]
nome		sì
cognome		sì
codiceFiscale		sì
sesso		sì
luogoNascita		sì
provinciaNascita		sì
statoNascita		sì
dataNascita		sì
CNS_CARTA_REALE	Valori possibili: "true" (l'utente di è autenticato tramite una CRS) o "false" (l'utente si è autenticato tramite una CRS virtuale ["demo"], rilasciata da LI a fini di test)	sì
CNS_ISSUER	CA Issuer DN completo come presente sul certificato di autenticazione della carta	sì
CNS_SUBJECT	Subject DN completo come presente sul certificato di autenticazione della carta	sì
origineDatiUtente	Valori possibili: "ARCHIVIO CARTE" (i dati del profilo sono stati recuperati da Archivio Carte) o "SMARTCARD" (i dati del profilo sono stati recuperati dalla smartcard)	si
idComuneRegistrazione	Codice ISTAT dell'Ente di registrazione dell'utente	sì – valorizzato a '03' per autenticazioni tramite CRS per compatibilità con Progetto People

[12] Questa tabella è da considerarsi un superset delle informazioni potenzialmente collezionabili da un Identiy Provider.

[13] Per utenti la cui autenticazione è effettuata con la Carta Regionale dei Servizi o altra Carta Nazionale dei Servizi. I dati relativi alla residenza sono valorizzati se l'accesso avviene con CRS non appartenenti al circuito reale, oppure con altra CNS.

emailAddress	E-mail address del cittadino, definito ed autocertificato dallo stesso alla prima interazione con l'Identity Provider; potrà essere utilizzato come contatto di riferimento per tutte le comunicazioni dall'Ente Erogatore verso il cittadino	sì verso Enti Erogatori **non** afferenti al dominio crs.lombardia.it; per servizi entro il dominio crs.lombardia.it, questo campo può essere assente o valorizzato in modo non significativo
cittaResidenza	Città di residenza dell'utente all'atto dell'emissione della CRS utilizzata in fase di autenticazione	Si - a partire da IdPC v4.0.00
provinciaResidenza	Provincia di residenza dell'utente all'atto dell'emissione della CRS utilizzata in fase di autenticazione	Si - a partire da IdPC v4.0.00
statoResidenza	Stato di residenza dell'utente all'atto dell'emissione della CRS utilizzata in fase di autenticazione	Si - a partire da IdPC v4.0.00
indirizzoResidenza		no
capResidenza		no
provinciaDomicilio		no
cellulare	Numero di telefono mobile del cittadino, definito ed autocertificato dallo stesso alla prima interazione con l'Identity Provider; è un valore opzionale (al cittadino è consentito di non valorizzarlo)	si – se inserito dall'utente (opzionale)
titolo		no
domicilioElettronico		no
cartaIdentita		no
cittaDomicilio		no
telefono		no
lavoro		no
capDomicilio		no
indirizzoDomicilio		no
statoDomicilio		no

Tabella 3.3 - I nomi degli attributi contenuti nello statement di attributo

Si noti che:

- tutti i campi partecipano alla composizione dell'asserzione, ma solo alcuni di essi hanno un valore significativo, mentre i restanti non sono valorizzati (cfr. Tabella 3.3.);
- i campi attualmente non valorizzati da IdPC-RL potrebbero esserlo in versioni successive;
- all'indirizzo https://idpcrl.crs.lombardia.it/AdminIdpc/ è resa disponibile all'utenza una pagina di amministrazione con cui modificare i dati sottoposti ad autocertificazione (e-mail e numero di cellulare), nonché di cancellare la lista dei siti considerati attendibili dall'utente e per i quali la pagina "riassuntiva" dei dati di asserzione viene mostrata solo al primo accesso;
- nella URL di chiamata ad IdPC-RL, oltre al parametro TARGET è possibile aggiungere un parametro "profile" che consente di specificare uno tra quattro possibili "profili" di dati utente cui si è interessati:

valore parametro "profile"	**campi valorizzati**
1	solo codice fiscale
2	codice fiscale, nome e cognome
3	codice fiscale, nome, cognome ed e-mail

4	tutti i dati
non valorizzato o valorizzato con valori non concessi	tutti i dati

Tale parametro, da specificare sulla URL di chiamata ad IdPC, è naturalmente facoltativo, dunque vi è compatibilità con le applicazioni già sviluppate. In caso di assenza del parametro, verranno restituiti tutti i dati.

L'URL del servizio di login erogato da IdPC-RL con l'aggiunta del parametro "profile" (nell'esempio uguale ad 1) è quindi il seguente:

```
https://idpcrl.crs.lombardia.it/scauth/SSLAuthServlet?profile=1&TARGET=https://
host-erogatore:port/AssertionConsumer?target=http://host-
erogatore:port/servicePage?serviceParameters...
```

- nella URL di chiamata ad IdPC-RL, oltre ai parametri sopra indicati, è possibile aggiungere un parametro "friendlyName" che consente di specificare un nome con cui identificare il servizio applicativo che chiede l'autenticazione. Tale nome, se specificato, verrà presentato all'utente nella pagina in cui si chiede l'autorizzazione alla propagazione del profilo. Il parametro "friendlyName" consente di essere maggiormente esplicativi verso l'utente finale, specificando il servizio applicativo con maggior chiarezza rispetto ad una URL [14]. La stringa che contiene il "friendlyName" deve essere priva di *blank*.

Una URL di esempio potrebbe dunque essere la seguente:

```
https://idpcrl.crs.lombardia.it/scauth/SSLAuthServlet?friendlyName=Applicazione
&TARGET=https://host-erogatore:port/AssertionConsumer?target=http://host-
erogatore:port/servicePage?serviceParameters...
```

[14] A partire dalla release di software IdPC-RL identificata come v2.4.04.

3.3 Interfaccia per il trasferimento della risposta XML (AuthDataHolder) con il profilo utente autenticato dall'I2A all'Ente Erogatore

Quanto contenuto nella presente sezione è da considerarsi non normativo. Di seguito è fornito un esempio di come i dati del profilo dell'utente autenticato possono essere trasferiti al portale erogatore, successivamente alla fase di estrazione dall'asserzione contenuta nella SAML Response prodotta da IdPC-RL e pervenuta ad Assertion Consumer. Il portale erogatore può definire una procedura alternativa che presenti un risultato analogo.

Dopo aver ricevuto l'asserzione prodotta da IdPC-RL, *Assertion Consumer* ne estrae i valori degli elementi rilevanti con i quali prepara un documento XML non-SAML, lo codifica in formato Base64 e lo trasmette quindi al portale erogatore, contattando il componente **Response Receiver** [15] all'URL:

```
http://host-erogatore:port/ResponseReceiver
```

dove *ResponseReceiver* è il puntatore alla interfaccia web del componente.

La struttura dati XML preparata prende il nome di "*AuthDataHolder*" ed è descritta in dettaglio nella sezione 3.3.1.

Questa trasmissione può avvenire in due modalità differenti:

- tramite forwarding (server-to-server), se la tecnologia con cui è sviluppato il componente *Response Receiver* è compatibile con quella dell'interfaccia di accesso alle applicazioni entro cui opera *Assertion Consumer* (es. se entrambi sono dispiegati nello stesso container J2EE). E' **la modalità di trasmissione consigliata**. In questo caso il documento XML sarà passato nella HTTP Request mediante un attributo di nome "authResponse" il cui valore è il contenuto in Base64 dell'XML da trasferire. *Response Receiver* inserisce nella Request anche un secondo attributo di nome "*expiresOn*" che riporta il timestamp oltre il quale il contenuto della risposta deve essere considerato scaduto e non più valido; nella "*reference implementation*" fornita da LI è implementata questa tecnica; oppure:
- tramite HTTP POST con una form. Si può ricorrere a tale modalità di trasmissione **solo** se non possibile diversamente, ovvero solo se il forwarding sopra illustrato risulta tecnicamente non percorribile (i.e. componenti *AssertionConsumer* e *ResponseReceiver* collocati su server differenti). In tal caso la form inviata via POST conterrà un campo nascosto con un parametro di nome "*authResponse*" il cui valore è il contenuto in Base64 dell'XML da trasferire. *Response Receiver* inserisce nella form anche un secondo attributo di nome "*expiresOn*" che riporta il timestamp oltre il quale il contenuto della risposta deve essere considerato scaduto e non più valido. Nel box seguente viene riportato il codice HTML che realizza la form auto-post descritta.

```
<html>
   <body onload="javascript:document.forms[0].submit()">
        <form method="post" action=" http://host-erogatore:port/ResponseReceiver">
            <input type="hidden" name="authResponse" value="<codifica Base64 di AuthDataHolder>"/>
            <input type="hidden" name="expiresOn" value=" 20061130T13:39:50.069CET"/>
        </form>
    </body>
</html>
```

E' **indispensabile** che il trasferimento dell'asserzione dall' *Assertion Consumer* al *Response Receiver* avvenga in modo cifrato allo scopo di impedire che i dati dell'asserzione vengano intercettati e/o modificati cioè, in generale, per evitare che il *Response Receiver* venga alimentato con asserzioni non prodotte dal proprio *Assertion Consumer.*

La cifratura dei dati può avvenire mediante utilizzo di una chiave simmetrica, nota ad *Assertion Consumer* e a *Response Receiver*. Nella "*reference implementation*" viene utilizzata una chiave simmetrica che non viene fornita con tale SW

[15] Al contrario di Access Check ed Assertion Consumer, questo componente non è normato dalle specifiche SAML.

allo scopo di costringere l'integratore del servizio a generare una propria chiave crittografica (cfr. CRS-ISAU-SIAU#77 per le modalità di generazione e configurazione della chiave e del corrispondente file).

Si noti che con cifratura dei dati di AuthDataHolder il valore del campo "*expiresOn"* sarà anch'esso cifrato con le stesse modalità adottate per AuthDataHolder.

Stante la possibilità di scegliere una qualsiasi delle suddette modalità di trasferimento, i componenti *Assertion Consumer* e *Response Receiver* devono poter essere configurabili per specificare quella prescelta.

Nell'implementazione di riferimento, ciò viene fatto inserendo nel deployment descriptor (es. file web.xml nel caso di ambiente J2EE) di tali componenti un parametro di contesto di nome "*authenticationResponseReceiverServiceTransferMode"* che può assumere i valori "*FORWARD*" (**consigliato**) o "*POST*", rispettivamente per le due opzioni riportate in precedenza.

3.3.1 La struttura "AuthDataHolder"

Un esempio di file XML trasferito tra *Assertion Consumer* e *Response Receiver* è riportato alla sezione 3.6.

Di seguito viene fornito lo schema che tale file può avere [16], in formato XML Schema.

La Figura 3 illustra la stessa struttura in forma grafica.

[16] L'esempio fa esplicito riferimento a quanto oggi implementato dai comuni aderenti al progetto People (ad esempio, il *targetNameSpace* di IdPC-RL non sarà quello riportato nell'esempio).

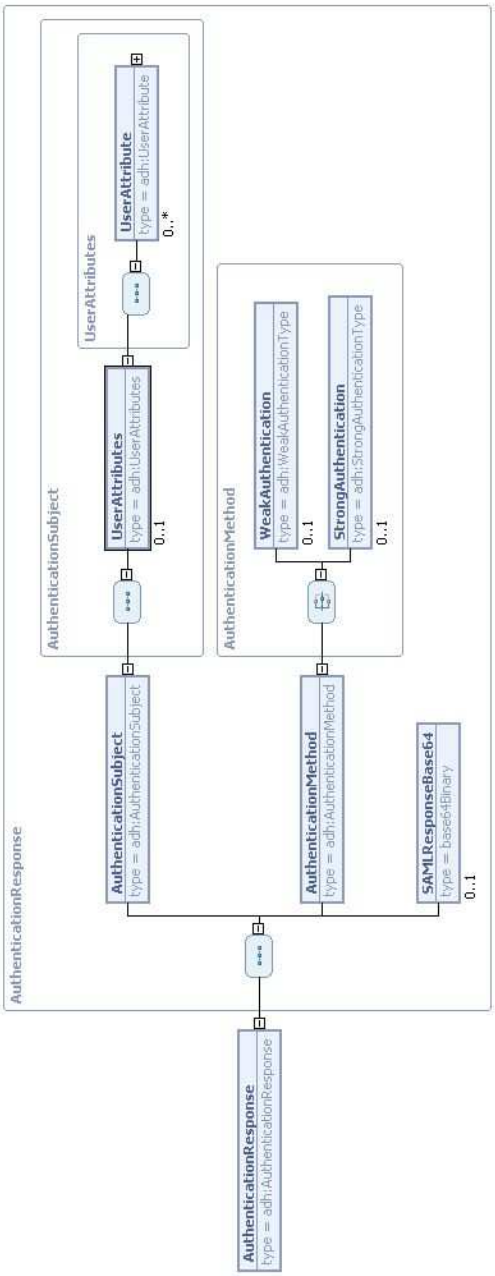

Figura 3 - Schema XML per AuthDataHolder

```
<?xml version="1.0" encoding="UTF-8"?>
<schema targetNamespace="http://www.progettopeople.it/sirac/peopleauthdataholder"
xmlns:adh="http://www.progettopeople.it/sirac/peopleauthdataholder"
xmlns="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">
   <element name="AuthenticationResponse" type="adh:AuthenticationResponse"/>
   <complexType name="AuthenticationResponse">
      <sequence>
         <element name="AuthenticationSubject" type="adh:AuthenticationSubject"/>
         <element name="AuthenticationMethod" type="adh:AuthenticationMethod"/>
         <element name="SAMLResponseBase64" type="base64Binary" minOccurs="0"/>
      </sequence>
      <attribute name="authenticationResponseStatus" type="adh:AuthenticationResponseStatus"
use="required"/>
      <attribute name="target" type="string" use="required"/>
      <attribute name="authenticationStatusMessage" type="string"/>
   </complexType>
   <simpleType name="AuthenticationResponseStatus">
```

```
      <restriction base="string">
         <enumeration value="urn:people:names:authenticationstatus:success"/>
         <enumeration value="urn:people:names:authenticationstatus:failure"/>
      </restriction>
   </simpleType>
   <complexType name="AuthenticationSubject">
      <sequence>
         <element name="UserAttributes" type="adh:UserAttributes" minOccurs="0"/>
      </sequence>
      <attribute name="userID" type="adh:UserIDType"/>
   </complexType>
   <complexType name="UserAttributes">
      <sequence>
         <element name="UserAttribute" type="adh:UserAttribute" minOccurs="0"
maxOccurs="unbounded"/>
      </sequence>
   </complexType>
   <complexType name="UserAttribute">
      <attribute name="name" type="string" use="required"/>
      <attribute name="value" type="string" use="required"/>
   </complexType>
   <simpleType name="StrongAuthenticationType">
      <annotation>
         <documentation>
           urn:people:names:authenticationmethod:pin - Autenticazione effettuata con inserimento del
PIN da parte dell'utente
            urn:oasis:names:tc:SAML:1.0:am:X509-PKI - Autenticazione effettuata mediante utilizzo
di un certificato software
            urn:oasis:names:tc:SAML:1.0:am:HardwareToken - Autenticazione effettuata utilizzando
un generico hardware token (ad esempio una smartcard)
            urn:ietf:rfc:2246 - Autenticazione effettuata utilizzando il protocollo SSL/TLS con
invio certificato da parte del client
          </documentation>
      </annotation>
      <restriction base="string">
         <whiteSpace value="collapse"/>
         <enumeration value="urn:people:names:authenticationmethod:pin"/>
         <enumeration value="urn:oasis:names:tc:SAML:1.0:am:HardwareToken"/>
         <enumeration value="urn:oasis:names:tc:SAML:1.0:am:X509-PKI"/>
         <enumeration value="urn:ietf:rfc:2246"/>
      </restriction>
   </simpleType>
   <complexType name="AuthenticationMethod">
      <choice>
         <element name="WeakAuthentication" type="adh:WeakAuthenticationType" minOccurs="0"/>
         <element name="StrongAuthentication" type="adh:StrongAuthenticationType" minOccurs="0"/>
      </choice>
   </complexType>
   <simpleType name="WeakAuthenticationType">
      <restriction base="string">
         <whiteSpace value="collapse"/>
         <enumeration value="urn:oasis:names:tc:SAML:1.0:am:password"/>
      </restriction>
   </simpleType>
   <simpleType name="UserIDType">
      <restriction base="string">
         <pattern value="[0-9a-zA-Z]+@([0-9a-zA-Z]+[_\.\-])*[0-9a-zA-Z]+"/>
      </restriction>
   </simpleType>
</schema>
```

L'attributo "*target*" dell'elemento "*AuthenticationResponse*" corrisponde all'URL del servizio finale sul portale erogatore, così come richiesto originariamente dall'utente via web browser (si veda anche la sezione 3.1).

L'attributo "*userID*" dell'elemento "*AuthenticationSubject*" contiene l'identificativo utente, così come presente nell'asserzione prodotta da IdPC-RL e definito nella sezione 3.2.1.

Lo stesso elemento deve contenere tanti sotto-elementi "*UserAttribute*" quanti sono gli attributi contenuti nello statement di attributo dell'asserzione di cui sopra.

Infine, l'elemento "*AuthenticationMethod*" specificherà un sotto-elemento che, secondo lo schema può essere "*WeakAuthentication*" oppure "*StrongAuthentication*" il quale ha come valore l'URN che specifica il meccanismo di

autenticazione utilizzato durante la fase di autenticazione, anch'esso riportato nell'asserzione prodotta da IdPC-RL. Si noti che, dal momento che IdPC-RL effettua autenticazioni di tipo "forte" (cioè escludendo il meccanismo che prevede l'inserimento di username e password), nelle asserzioni prodotte da tale IdP, l'elemento *"AuthenticationMethod"* conterrà sempre il sotto-elemento *"StrongAuthentication"*, i cui valori possibili sono riportati nella Tabella 3.1 (si veda anche la sezione 3.2.1).

3.4 SOFTWARE DI BASE E TECNOLOGIA WEB UTILIZZATA DAGLI ENTI EROGATORI

Come già evidenziato, LI mette a disposizione una "*reference implementation*" dei componenti *Access Check*, *Assertion Consumer* e *Response Receiver*.

Conseguentemente, gli Enti Erogatori che volessero utilizzare (tutta od in parte) questa implementazione, dovranno dotare il proprio sistema informativo di un adeguato software di base (ad esempio, Web container J2EE v1.4 o successive per la "*reference implementation*" in tecnologia J2EE).

Per ulteriori approfondimenti in merito, si rimanda il lettore al documento [3].

3.5 ESEMPIO DI SAML RESPONSE PRODOTTA DA IDPC-RL

Di seguito viene riportato un esempio di SAML Response trasferita dall'IdPC-RL all'interfaccia di accesso alle applicazioni, in particolare al componente *Assertion Consumer* [17].

La SAML Response riportata rispetta lo schema generale previsto dallo standard OASIS, ovvero:

```
<Response xmlns="urn:oasis:names:tc:SAML:1.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol" IssueInstant="2006-11-07T13:59:20.922Z"
MajorVersion="1" MinorVersion="1" Recipient="http://host-erogatore:port/AssertionConsumer"
ResponseID="f526b5f90d9e216e1227bcb77dde5390">

        <!-- informazioni relative alla firma della SAML Response in accordo con XMLDS -->
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                . . .
        </ds:Signature>

        <!-- stato dell'autenticazione in accordo a specifiche SAML 1.1 -->
        <Status>
                <StatusCode Value="samlp:Success"/>
        </Status>

        <!-- asserzioni relative all'utente autenticato -->
        <!-- sono consentite da zero ad N occorrenze firmate  singolarmente -->
        <Assertion xmlns="urn:oasis:names:tc:SAML:1.0:assertion"
AssertionID="d47cb436f930f71d900cb0ad3f2047e9" IssueInstant="2006-11-07T13:59:20.921Z"
Issuer="http://www.crs.lombardia.it/idpc" MajorVersion="1" MinorVersion="1">
                                . . .
        </Assertion>

</Response>
```

Prima di presentare l'esempio oggetto della presente sezione, si ricorda che le URL ed i namespace sotto riportati sono a titolo di esempio.

```
<Response xmlns="urn:oasis:names:tc:SAML:1.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol" IssueInstant="2006-11-07T13:59:20.922Z"
MajorVersion="1" MinorVersion="1" Recipient="http://host-erogatore:port/AssertionConsumer"
ResponseID="f526b5f90d9e216e1227bcb77dde5390">

        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:SignedInfo>
                        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
                        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                        <ds:Reference URI="#f526b5f90d9e216e1227bcb77dde5390">
                                <ds:Transforms>
                                        <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                                        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#">
                                                <ec:InclusiveNamespaces
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="code ds kind rw saml samlp typens
#default"/>
                                        </ds:Transform>
                                </ds:Transforms>
                                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                                <ds:DigestValue>bOUjypUHni6Qfb48Dy5mNe6LDwM=</ds:DigestValue>
                        </ds:Reference>
                </ds:SignedInfo>
                <ds:SignatureValue>
gau5DU0R4KRy6cbwX+8tKNxWMeatZpFRloSx0/2BTQvdHtRYfcFGIt+jLt7Lx3RDNg2teFQp70lE
```

[17] L'esempio si riferisce ad un'asserzione prodotta da IdPC-RL in versione 1. Nella versione corrente, IdPC-RL veicola un'asserzione più ricca, come illustrato nelle sezioni precedenti. Si noti che quanto riportato è ovviamente al netto della codifica base64 e della cifratura di canale ottenuta tramite SSL v3 con sola server authentication.

```
QNgzd+TRp91FYd0uKkOSzqTQeHRdsa/rMk+aOdc2M6icHojWR+CGbCK0fy7V2FZSOpGIGuE6z3gf
VuQRYp6DDQAk2a/suyeIfniDAR3Pp7nloyd3WDqXI+anmRilh9esYsYX5BysyMF+ld5hl2tqRbBb
zQO+Hk05sT/HYKZgyL1ZsQJ3lCHyl/St8zFcKhaMdY8RA6BgkrXaFFbRgrxZ9t5kvHSVlhlhUmm8
E1VhAg9MokSrfSq9zHQDfD4Y6vze+w7jvBPhww==
</ds:SignatureValue>
                <ds:KeyInfo>
                        <ds:X509Data>
                                <ds:X509Certificate>
MIIDNDCCAp2gAwIBAgICApYwDQYJKoZIhvcNAQEEBQAwgakxCzAJBgNVBAYTAlVTMRIwEAYDVQQI
EwlXaXNjb25zaW4xEDAOBgNVBAcTB01hZGlzb24xIDAeBgNVBAoTF1VuaXZlcnNpdHkgb2YgV2lz
Y29uc2luMSswKQYDVQQLEyJEaXZpc2lvbiBvZiBJbmZvcm1hdGlvbiBUZWNobm9sb2d5MSUwIwYD
VQQDExxIRVBLSSBTZXJ2ZXIgQ0EgLS0gMjAwMjA3MDFBMB4XDTAzMDEyMTAwMTk1NFoXDTA3MDMw
MjAwMTk1NFowcjELMAkGA1UEBhMCVVMxETAPBgNVBAgTCE1pY2hpZ2FuMRIwEAYDVQQHEwlBbm4g
QXJib3IxEjAQBgNVBAoTCUludGVybmV0MjENMAsGA1UECxMETUFDRTEZMBcGA1UEAxMQd3d3Lm9w
ZW5zYW1sLm9yZzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKd4L+13N4YIoBSSPDhb
OwStLLq7qaM0gYSeARQA6b32jhPL/+x5t4S5zbasX+CMb36Ds6N2kEmBjwdw2HdF2wlsBx0KpMBR
mqA9FgpkhxCxRHc3716I2ScsgGuBzZRHR6vc/oCuH15Ea4Kz+a1bj58UXb5EG6pL3L30EZrw0+9C
XkqY835QITbbyGMNG5Cu5sr6iH0dHMCeTneYZQXw61yk+AyW4cvGKRFeTBVNH8Rml+DnaysyXzPH
yYU9G7/PCf84mNidixNOojTmsGn7dbu2jCpj7ZpbBuoUgcIEyTd2ruAVGHE0oszlJ6i34uQYH3rS
TiEKSbm3712GENXyuAECAwEAAaMdMBswDAYDVR0TAQH/BAIwADALBgNVHQ8EBAMCBaAwDQYJKoZI
hvcNAQEEBQADgYEAg4QdCd5wWwxsZ13RrB6vvVyoKYkaq3wNg4tF4VdEFpw4vH/nkte69Dsp5A2Q
DP/2L9QOfrAZrKgegL80DigGQl/Goer2rBY33dYAxMjoACv3MQSIwfMuxvPxMrkrnPbal6tPmyCc
aB1i9mr9QCA/CDFhmkYZ1dwYKQx6Tw4QpFQ=
</ds:X509Certificate>
                                <ds:X509Certificate>
MIIC6zCCAlSgAwIBAgICAlYwDQYJKoZIhvcNAQEEBQAwgakxCzAJBgNVBAYTAlVTMRIwEAYDVQQI
EwlXaXNjb25zaW4xEDAOBgNVBAcTB01hZGlzb24xIDAeBgNVBAoTF1VuaXZlcnNpdHkgb2YgV2lz
Y29uc2luMSswKQYDVQQLEyJEaXZpc2lvbiBvZiBJbmZvcm1hdGlvbiBUZWNobm9sb2d5MSUwIwYD
VQQDExxIRVBLSSBNYXN0ZXIgQ0EgLS0gMjAwMjA3MDFBMB4XDTAyMDYzMDIyMzIxNFoXDTI3MDIy
MDIyMzIxNFowgakxCzAJBgNVBAYTAlVTMRIwEAYDVQQIEwlXaXNjb25zaW4xEDAOBgNVBAcTB01h
ZGlzb24xIDAeBgNVBAoTF1VuaXZlcnNpdHkgb2YgV2lzY29uc2luMSswKQYDVQQLEyJEaXZpc2lv
biBvZiBJbmZvcm1hdGlvbiBUZWNobm9sb2d5MSUwIwYDVQQDExxIRVBLSSBTZXJ2ZXIgQ0EgLS0g
MjAwMjA3MDFBMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCvImusW7uaRS7xLsi2ZzZuUz6g
bfATwxwvtQ+8cuyDpRlhvr1qnghC9EnjRH9qpq/Z5FVZ5bqyGziCy0kEPt+2WiZMGRiQEzloi5HN
Etz1Nlc7FCJ0HATxtkEUhQ96v2DmoIEogPINqLICIqfiraPWFHOp6qDritrdj/fwLptQawIDAQAB
oyAwHjAPBgNVHRMBAf8EBTADAQH/MAsGA1UdDwQEAwIBpjANBgkqhkiG9w0BAQQFAAOBgQAttxlP
3fTyIVMAIm8ddE8Bvk0/5Bhn5KvMAOMtnlCEArcFd4/m+pU4vEDwK6JSIoKfN/ySLXlu5ItApeJM
Whcqvrczq5BF4/WQZukC1ha6FS2cAmjy35jYWMfVWcdBi9YiM4SJ6gjGf83y9axPpuHcjwxQ5fLq
ZfnvrWH+1owJhQ==
</ds:X509Certificate>
                        </ds:X509Data>
                </ds:KeyInfo>
        </ds:Signature>

        <Status>
                <StatusCode Value="samlp:Success"/>
        </Status>

        <Assertion xmlns="urn:oasis:names:tc:SAML:1.0:assertion"
AssertionID="d47cb436f930f71d900cb0ad3f2047e9" IssueInstant="2006-11-07T13:59:20.921Z"
Issuer="http://www.crs.lombardia.it/idpc" MajorVersion="1" MinorVersion="1">
                <Conditions NotBefore="2006-11-07T13:59:20.921Z" NotOnOrAfter="2006-11-
07T14:04:20.921Z"/>
                <AuthenticationStatement AuthenticationInstant="2006-11-07T13:59:20.921Z"
AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:HardwareToken">
                        <Subject>
                                <NameIdentifier> RSSMRA50A01F205R@crs.lombardia.it</NameIdentifier>
                                <SubjectConfirmation>

        <ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</ConfirmationMethod>
                                </SubjectConfirmation>
                        </Subject>
                </AuthenticationStatement>
                <AttributeStatement>
                        <Subject>
                                <NameIdentifier>
RSSMRA50A01F205R@idpc.crs.lombardia.it</NameIdentifier>
                                <SubjectConfirmation>

        <ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</ConfirmationMethod>
                                </SubjectConfirmation>
                        </Subject>
                        <Attribute AttributeName="provinciaResidenza"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue>MI</AttributeValue>
                        </Attribute>
```

```
                        <Attribute AttributeName="luogoNascita"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue>MILANO</AttributeValue>
                        </Attribute>
                        <Attribute AttributeName="CNS_CARTA_REALE"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue>true</AttributeValue>
                        </Attribute>
                        <Attribute AttributeName="indirizzoResidenza"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue/>
                        </Attribute>
                        <Attribute AttributeName="capResidenza"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue>20100</AttributeValue>
                        </Attribute>
                        <Attribute AttributeName="provinciaDomicilio"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue/>
                        </Attribute>
                        <Attribute AttributeName="provinciaNascita"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue>MI</AttributeValue>
                        </Attribute>
                        <Attribute AttributeName="cellulare"
AttributeNamespace="http://www.crs..lombardia.it/idpc">
                                <AttributeValue/>
                        </Attribute>
                        <Attribute AttributeName="titolo"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue/>
                        </Attribute>
                        <Attribute AttributeName="cittaResidenza"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue>MILANO</AttributeValue>
                        </Attribute>
                        <Attribute AttributeName="emailAddress"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue>mario.rossi@regione.lombardia.it</AttributeValue>
                        </Attribute>
                        <Attribute AttributeName="statoResidenza"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue/>
                        </Attribute>
                        <Attribute AttributeName="CNS_ISSUER"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue>CN=Regione Lombardia Certification Authority
Cittadini, OU=Servizi di certificazione, O=I.T. Telecom S.R.L., C=IT</AttributeValue>
                        </Attribute>
                        <Attribute AttributeName="cartaIdentita"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue/>
                        </Attribute>
                        <Attribute AttributeName="cittaDomicilio"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue/>
                        </Attribute>
                        <Attribute AttributeName="sesso"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue>M</AttributeValue>
                        </Attribute>
                        <Attribute AttributeName="telefono"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue/>
                        </Attribute>
                        <Attribute AttributeName="nome"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue>MARIO</AttributeValue>
                        </Attribute>
                        <Attribute AttributeName="dataNascita"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue>06/07/1972</AttributeValue>
                        </Attribute>
                        <Attribute AttributeName="statoNascita"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue>ITALIA</AttributeValue>
```

```
                        </Attribute>
                        <Attribute AttributeName="cognome"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue>ROSSI</AttributeValue>
                        </Attribute>
                        <Attribute AttributeName="CNS_SUBJECT"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue>CN="
RSSMRA50A01F205R/6030106561250008.ZoAOnld210kyWOFT1AqpQQb3/Zo=", OU=Regione Lombardia, O=CRS-SISS,
C=IT</AttributeValue>
                        </Attribute>
                        <Attribute AttributeName="statoDomicilio"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue/>
                        </Attribute>
                        <Attribute AttributeName="codiceFiscale"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue> RSSMRA50A01F205R</AttributeValue>
                        </Attribute>
                        <Attribute AttributeName="lavoro"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue/>
                        </Attribute>
                        <Attribute AttributeName="capDomicilio"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue/>
                        </Attribute>
                        <Attribute AttributeName="indirizzoDomicilio"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue/>
                        </Attribute>
                        <Attribute AttributeName="idComuneRegistrazione"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue>03</AttributeValue>
                        </Attribute>
                        <Attribute AttributeName="domicilioElettronico"
AttributeNamespace="http://www.crs.lombardia.it/idpc">
                                <AttributeValue/>
                        </Attribute>
                </AttributeStatement>
                <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <ds:SignedInfo>
                                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#"/>
                                <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1"/>
                                <ds:Reference URI="#d47cb436f930f71d900cb0ad3f2047e9">
                                        <ds:Transforms>
                                                <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                                                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#">
                                                        <ec:InclusiveNamespaces
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="code ds kind rw saml samlp typens
#default"/>
                                                </ds:Transform>
                                        </ds:Transforms>
                                        <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                                        <ds:DigestValue>KehC3Lrbhz4sP548iI7oyqA6QvA=</ds:DigestValue>
                                </ds:Reference>
                        </ds:SignedInfo>
                        <ds:SignatureValue>
Du4c0ffosizy+GMvOnbZua/Xa5LUoiutuAKCZxd4rTt5y4n4HFENBXZX20rOfm5wBByeIYFIFeBS
s+gscYpbnWTfXiG59oYu7FHZ7w8C6UgdVQ+5wxvG3RDf0U+wgwr3vTltY5bG4FniGjCW2Bcc+lU3
0jKhLHSf3YjXKo28kbIylTV6qiPm5jTtMKIvRPvjB8wI7FFYIm/NTCoejBuxj0X4cYp2odz+n3S9
9zXiv10Z3AQPo5KXLoxOxCP3kwcFlMrVtXVmwoFXd6SeZBXOOGLXL7JNTZDhepIFvh3dtdOXwgze
PD+nWN+zv6pqrF+j27q9YS3liJKersEXv3AQnw==
</ds:SignatureValue>
                        <ds:KeyInfo>
                                <ds:X509Data>
                                        <ds:X509Certificate>
MIIDNDCCAp2gAwIBAgICApYwDQYJKoZIhvcNAQEEBQAwgakxCzAJBgNVBAYTAlVTMRIwEAYDVQQI
EwlXaXNjb25zaW4xEDAOBgNVBAcTB01hZGlzb24xIDAeBgNVBAoTF1VuaXZlcnNpdHkgb2YgV2lz
Y29uc2luMSswKQYDVQQLEyJEaXZpc2lvbiBvZiBJbmZvcm1hdGlvbiBUZWNobm9sb2d5MSUwIwYD
VQQDExxIRVBLSSBTZXJ2ZXIgQ0EgLS0gMjAwMjA3MDFBMB4XDTAzMDEyMTAwMTk1NFoXDTA3MDMw
```

```
MjAwMTk1NFowcjELMAkGA1UEBhMCVVMxETAPBgNVBAgTCE1pY2hpZ2FuMRIwEAYDVQQHEwlBbm4g
QXJib3IxEjAQBgNVBAoTCUludGVybmV0MjENMAsGA1UECxMETUFDRTEZMBcGA1UEAxMQd3d3Lm9w
ZW5zYW1sLm9yZzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKd4L+13N4YIoBSSPDhb
OwStLLq7qaM0gYSeARQA6b32jhPL/+x5t4S5zbasX+CMb36Ds6N2kEmBjwdw2HdF2wlsBx0KpMBR
mqA9FgpkhxCxRHc3716I2ScsgGuBzZRHR6vc/oCuH15Ea4Kz+a1bj58UXb5EG6pL3L30EZrw0+9C
XkqY835QITbbyGMNG5Cu5sr6iH0dHMCeTneYZQXw61yk+AyW4cvGKRFeTBVNH8Rml+DnaysyXzPH
yYU9G7/PCf84mNidixNOojTmsGn7dbu2jCpj7ZpbBuoUgcIEyTd2ruAVGHE0oszlJ6i34uQYH3rS
TiEKSbm3712GENXyuAECAwEAAaMdMBswDAYDVR0TAQH/BAIwADALBgNVHQ8EBAMCBaAwDQYJKoZI
hvcNAQEEBQADgYEAg4QdCd5wWwxsZ13RrB6vvVyoKYkaq3wNg4tF4VdEFpw4vH/nkte69Dsp5A2Q
DP/2L9QOfrAZrKgegL80DigGQl/Goer2rBY33dYAxMjoACv3MQSIwfMuxvPxMrkrnPbal6tPmyCc
aB1i9mr9QCA/CDFhmkYZ1dwYKQx6Tw4QpFQ=
</ds:X509Certificate>
                                    <ds:X509Certificate>
MIIC6zCCAlSgAwIBAgICAlYwDQYJKoZIhvcNAQEEBQAwgakxCzAJBgNVBAYTAlVTMRIwEAYDVQQI
EwlXaXNjb25zaW4xEDAOBgNVBAcTB01hZGlzb24xIDAeBgNVBAoTF1VuaXZlcnNpdHkgb2YgV2lz
Y29uc2luMSswKQYDVQQLEyJEaXZpc2lvbiBvZiBJbmZvcm1hdGlvbiBUZWNobm9sb2d5MSUwIwYD
VQQDExxIRVBLSSBNYXN0ZXIgQ0EgLS0gMjAwMjA3MDFBMB4XDTAyMDYzMDIyMzIxNFoXDTI3MDIy
MDIyMzIxNFowgakxCzAJBgNVBAYTAlVTMRIwEAYDVQQIEwlXaXNjb25zaW4xEDAOBgNVBAcTB01h
ZGlzb24xIDAeBgNVBAoTF1VuaXZlcnNpdHkgb2YgV2lzY29uc2luMSswKQYDVQQLEyJEaXZpc2lv
biBvZiBJbmZvcm1hdGlvbiBUZWNobm9sb2d5MSUwIwYDVQQDExxIRVBLSSBTZXJ2ZXIgQ0EgLS0g
MjAwMjA3MDFBMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCvImusW7uaRS7xLsi2ZzZuUz6g
bfATwxwvtQ+8cuyDpRlhvr1qnghC9EnjRH9qpq/Z5FVZ5bqyGziCy0kEPt+2WiZMGRiQEzloi5HN
Etz1Nlc7FCJ0HATxtkEUhQ96v2DmoIEogPINqLICIqfiraPWFHOp6qDritrdj/fwLptQawIDAQAB
oyAwHjAPBgNVHRMBAf8EBTADAQH/MAsGA1UdDwQEAwIBpjANBgkqhkiG9w0BAQQFAAOBgQAttxlP
3fTyIVMAIm8ddE8Bvk0/5Bhn5KvMAOMtnlCEArcFd4/m+pU4vEDwK6JSIoKfN/ySLXlu5ItApeJM
Whcqvrczq5BF4/WQZukC1ha6FS2cAmjy35jYWMfVWcdBi9YiM4SJ6gjGf83y9axPpuHcjwxQ5fLq
ZfnvrWH+1owJhQ==
</ds:X509Certificate>
                            </ds:X509Data>
                        </ds:KeyInfo>
                </ds:Signature>
        </Assertion>

</Response>
```

3.6 ESEMPIO DI XML TRASFERITO AL PORTALE EROGATORE

Si ricorda che le URL ed i namespace sotto riportati sono a titolo di esempio [18].

```
<?xml version="1.0" encoding="UTF-8"?>
<peop:AuthenticationResponse target="http://domain1.com:8090/people-
dummy/AssertionConsumerService?target=http://domain1.com:8090/people-
dummy/initProcess.do?processName=it.people.fsl.servizi.test.dummyservice.servizio2"
authenticationResponseStatus="urn:people:names:authenticationstatus:success"
authenticationStatusMessage="" xmlns:peop="http://www.progettopeople.it/sirac/peopleauthdataholder">

<peop:AuthenticationSubject userID="RSSMRA50A01F205R@idpc.crs.lombardia.it">
    <peop:UserAttributes>
      <peop:UserAttribute value="MI" name="provinciaResidenza"/>
      <peop:UserAttribute value="MILANO" name="luogoNascita"/>
      <peop:UserAttribute value="true" name="CNS_CARTA_REALE"/>
      <peop:UserAttribute value="" name="indirizzoResidenza"/>
      <peop:UserAttribute value="10100" name="capResidenza"/>
      <peop:UserAttribute value="" name="provinciaDomicilio"/>
      <peop:UserAttribute value="MI" name="provinciaNascita"/>
      <peop:UserAttribute value="" name="cellulare"/>
      <peop:UserAttribute value="Milano" name="cittaResidenza"/>
      <peop:UserAttribute value="" name="titolo"/>
      <peop:UserAttribute value="mario.rossi@regione.lombardia.it" name="emailAddress"/>
      <peop:UserAttribute value="" name="statoResidenza"/>
      <peop:UserAttribute value="CN=Regione Lombardia Certification Authority Cittadini, OU=Servizi
di certificazione, O=I.T. Telecom S.R.L., C=IT" name="CNS_ISSUER"/>
      <peop:UserAttribute value="" name="cartaIdentita"/>
      <peop:UserAttribute value="" name="cittaDomicilio"/>
      <peop:UserAttribute value="M" name="sesso"/>
      <peop:UserAttribute value="" name="telefono"/>
      <peop:UserAttribute value="MARIO" name="nome"/>
      <peop:UserAttribute value="01/01/1950" name="dataNascita"/>
      <peop:UserAttribute value="ITALIA" name="statoNascita"/>
      <peop:UserAttribute value="ROSSI" name="cognome"/>
      <peop:UserAttribute value="CN= RSSMRA50A01F205R/6030106561250008.ZoAOnld210kyWOFT1AqpQQb3/Zo=,
OU=Regione Lombardia, O=CRS-SISS, C=IT" name="CNS_SUBJECT"/>
      <peop:UserAttribute value=" RSSMRA50A01F205R" name="codiceFiscale"/>
      <peop:UserAttribute value="" name="statoDomicilio"/>
      <peop:UserAttribute value="" name="lavoro"/>
      <peop:UserAttribute value="" name="capDomicilio"/>
      <peop:UserAttribute value="" name="indirizzoDomicilio"/>
      <peop:UserAttribute value="03" name="idComuneRegistrazione"/>
      <peop:UserAttribute value="" name="domicilioElettronico"/>
    </peop:UserAttributes>
  </peop:AuthenticationSubject>

  <peop:AuthenticationMethod>
<peop:StrongAuthentication>urn:oasis:names:tc:SAML:1.0:am:HardwareToken</peop:StrongAuthentication>
  </peop:AuthenticationMethod>

</peop:AuthenticationResponse>
```

[18] L'esempio si riferisce ad un'asserzione prodotta da IdPC-RL in versione 1. Nella versione corrente, IdPC-RL veicola un'asserzione più ricca, come illustrato nelle sezioni precedenti.

3.7 INTEGRAZIONE DI UN SERVICE PROVIDER PEOPLE NELL'INFRASTRUTTURA IDPC

Questa sezione descrive le modalità di integrazione di un Service Provider People che utilizza l'infrastruttura SiRAC con il servizio di autenticazione IdPc di Regione Lombardia.

3.7.1 Integrazione di un Service Provider People sino alla versione 2.0.1

L'integrazione con IdPC per un portale erogatore di servizi People è particolarmente semplice, poichè IdPc utilizza le stesse interfacce e protocolli definiti nell'ambito per l'infrastruttura di autenticazione SiRAC (Servizio Infrastrutturale di Registrazione e Autenticazione di Comunità) presente in ogni installazione People.
Per realizzare l'integrazione con il servizio IdPc di Regione Lombardia di un portale che utilizza la versione base SiRAc: è quindi sufficiente intervenire a livello di parametri di configurazione di alcune web application.

3.7.1.1 Configurazione dell'Assertion Consumer Service

Il componente SiRAc Assertion Comsumer Service è il bridge del SIRAC dal mondo SAML verso la people web application. Tale componente riceve la `SAMLResponse` prodotta dall'Identity Provider (l'IdPc in questo caso), verifica l'XML signature e passa (con un forward o con un HTTP POST) il suo contenuto (userID dell'utente autenticato, gli attributi del profilo di registrazione dell'utente, etc.) alla servlet AuthResponseReceiverService per l'impostazione delle variabili di sessione.

L'*Assertion Consumer* è implementato mediante una servlet la cui definizione è contenuta in `WEB-INF/web.xml` della web application `people o sirac` (a seconda della modalità di deployment prescelta):

```
<servlet>
        <servlet-name>AssertionConsumerService</servlet-name>
        <display-name>Sirac Assertion Consumer Service</display-name>
        <description>Sirac Assertion Consumer Service</description>
        <servlet-class>
            it.people.sirac.web.AssertionConsumerServlet
        </servlet-class>
       …
```

I parametri di inizializzazione **`(<init-param>)`** ai fini dell'integrazione con l'IdPc sono i seguenti (per un elenco esaustivi dei parametri di configurazione si rimanda alla documentazione SiRAC inclusa nella distribuzione People):

param-name	param-value
keystorePath	Percorso del trust store contenente i certificati di CA
keystorePassword	Password per l'accesso al trust store
certificateAlias	Nome dell'alias del certificato nel trust store da utilizzare per la verifica della firma della SAML Response

Un esempio di configurazione dei parametri sopra indicati è il seguente:

```
<servlet>
      <servlet-name>AssertionConsumerService</servlet-name>
      <display-name>Sirac Assertion Consumer Service</display-name>
      <description>Sirac Assertion Consumer Service</description>
      <servlet-class>it.people.sirac.web.AssertionConsumerServlet</servlet-class>
      <init-param>
            <param-name>keystorePath</param-name>
            <!--  path relativo alla webapp -->
            <param-value>/keystore/test.jks</param-value>
      </init-param>
      <init-param>
            <param-name>certificateAlias</param-name>
            <param-value>mykey</param-value>
      </init-param>
```

```
            <init-param>
                  <param-name>keystorePassword</param-name>
                  <param-value>testpwd</param-value>
            </init-param>
      …
```

Per poter verificare l'asserzione veicolata dall'IdPc è necessario che il certificato utilizzato per la firma della Response SAML sia stato emesso da una CA 'trusted'. Ulteriori dettagli a tal proposito sono disponibili nel documento [3].

3.7.1.2 Configurazione SiRAC Gateway

L'integrazione viene completata attraverso l'indicazione delle impostazioni per la redirezione della richiesta di autenticazione verso il servizio IdPc, intervenendo sui parametri di configurazione specificati nel deployment descriptor della web application `'sirac'` nel modo seguente:

```
<servlet>
  <servlet-name>AuthGatewayServlet</servlet-name>
  <display-name>SIRAC Authentication Gateway Servlet</display-name>
  <description>SIRAC Authentication Gateway Servlet</description>
  <servlet-class>it.people.sirac.web.AuthGatewayServlet</servlet-class>
  <init-param>
    <param-name>weakLoginRedirect</param-name>
    <param-value>http://wayf.crs.lombardia.it/wayf/</param-value>
  </init-param>
  <init-param>
    <param-name>strongLoginRedirect</param-name>
    <param-value>http://wayf.crs.lombardia.it/wayf/</param-value>
  </init-param>
</servlet>
```

Come si vede, la configurazione consiste semplicemente nell'indicazione dell'URL del servizio WAYF dell'IdPC sia nel caso di autenticazione debole, sia nel caso di autenticazione forte. Questo significa che si utilizzerà il servizio di autenticazione forte offerto dall'IdPc indipendentemente dai requisiti di autenticazione (debole o forte) indicati da uno specifico servizio People.

3.7.2 Integrazione di un Service Provider People integrato con SiRAC-SSO (SiRAC v2.0.2)

Con il rilascio della versione 2.0.2 del portale People l'infrastruttura SiRAC nella sua versione base per l'autenticazione all'accesso ai servizi è stata estesa per offrire funzionalità di Single-Sign-On (SSO) e interfacciamento verso più Identity Provider. Ciò ha migliorato il supporto ad una gestione integrata ed unitaria del processo di autenticazione, qualunque sia il servizio acceduto dall'utente su uno qualunque dei portali integrati con l'infrastruttura SiRAC. In questo modo non si richiede più all'utente di effettuare una nuova autenticazione nel momento in cui vuole passare dai servizi di un portale a quelli di un altro, realizzando così la funzionalità di SSO tra essi. L'infrastruttura SiRAC-SSO presenta inoltre il vantaggio di consentire agli utenti di scegliere su quale tra gli IdP disponibili e compatibili con l'infrastruttura, effettuare l'autenticazione. In questo modo sia gli utenti che già usufruivano dell'accesso al portale precedentemente integrato con SiRAC (es. un portale PEOPLE), sia altri utenti afferenti a sistemi diversi, vengono abilitati all'accesso a tutti i servizi integrati.

L'integrazione con l'IdPc nel caso di utilizzo dei componenti SiRAC-SSO si riduce alla definizione di una opportuna entry nel file di configurazione *sirac-config.xml* utilizzato dalla web application *sirac-sso* avente la struttura sotto riportata:

```
<?xml version="1.0" encoding="UTF-8"?>
<sir:SiracConfiguration
xmlns:sir="http://www.progettopeople.it/b003/ServiziInfrastrutturali/Sirac">
  <FederationConfig>
    <IdPConfig>
     <IdP trustLevel="TRUSTED">
            <Name>IdPC-RL</Name>
            <Description>Identity Provider Cittardini - Regione Lombardia</Description>
   ...
```

```
   ...
   ...
      </IdP>
      <IdP trustLevel="TRUSTED">
       <Name>CA-People1</Name>
       <Description>CA-People demo</Description>
   ...
   ...
      </IdP>
  <SSOConfig SSOEnabled="true">
    <AuthenticationTargetConfig>
      <AuthenticationTarget>
        <Name>People8000</Name>
        <Description>Portale People (port 8000)</Description>
   ...
      </AuthenticationTarget>
      <AuthenticationTarget>
        <Name>PeopleTest8002</Name>
        <Description>Portale People Test port 8002</Description>
   ...
      </AuthenticationTarget>
    </AuthenticationTargetConfig>
  </SSOConfig>
</sir:SiracConfiguration>
```

In particolare, per l'integrazione con l'IdPc occorre definire un elemento IdP che referenzi l'URL del servizio di autenticazione IdPc e specifichi i certificati da utilizzare per la verifica della firma della Response SAML e per la verifica di trust, come sotto indicato:

```
…
<IdP trustLevel="TRUSTED">
      <Name>IdPC-RL</Name>
      <Description>Identity Provider Cittardini - Regione Lombardia</Description>
      <AssertionIssuer>https://idpcrl.crs.lombardia.it//scauth</AssertionIssuer>
      <AuthenticationServices>
            <AuthenticationService>
        <Method>WEAK</Method>
        <Location>http://wayf.crs.lombardia.it/wayf/</Location>
</AuthenticationService>
            <AuthenticationService>
                  <Method>STRONG</Method>
            <Location>http://wayf.crs.lombardia.it/wayf/</Location>
            </AuthenticationService>
      </AuthenticationServices>
      <SigningInfo trustVerification="enabled">
            <X509Certificate subject="CN=LISIT S.P.A./168637, OU=U.O. Sviluppo, O=Altri Certificati, C=IT" issuer="CN=LISIT CA di
Servizio, OU=Servizio di certificazione, O=LISIT S.p.A., C=IT" alias="idpcrl-signer">
<X509Data>MIIENTCCAx2gAwIBAgICefAwDQYJKoZIhvcNAQEFBQAwaDELMAkGA1UEBhMCSVQxFTATBgNVBAoTDExJU0lU
IFMucC5BLjEjMCEGA1UECxMaU2Vydml6aW8gZGkgY2VydGlmaWNhemlvbmUxHTAbBgNVBAMTFExJU0lUIENBIGRpIFNlcnZpe
mlvMB4XDTA3MDEwOTEwMjIzNFoXDTEwMDEwOTEwMjIyOFowXzELMAkGA1UEBhMCSVQxGjAYBgNVBAoTEUFsdHJpIENl
cnRpZmljYXRpMRYwFAYDVQQLEw1VLk8uIFN2aWx1cHBvMRwwGgYDVQQDExNMSVNJVCBTLlAuQS4vMTY4NjM3MIGfMA
0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCqZHw3M9EipZZSsNH848hfp+qcn0B1Viv+rb6C5lQ0phz9sWgrm3+E3I6hoI2a5LltYaO
BLE8LaHlFu5osTg3G7sNBXzEFwugTNnadDORwTxMlcS8xtWP6URty1tbYjggcJVTJeIzeLAj/QMrdCXxFVukqfVXBF+LwwQxamQ7h
PwIDAQABo4IBdDCCAXAwDAYDVR0TAQH/BAIwADBIBgNVHSAEQTA/MD0GCisGAQQBvG4TAh0wLzAtBggrBgEFBQcCARY
haHR0cDovL3d3dy5saXNpdC5pdC9maXJtYWRpZ2l0YWxlMA4GA1UdDwEB/wQEAwIDuDATBgNVHSUEDDAKBggrBgEFBQcDAz
AfBgNVHSMEGDAWgBSEzbEvHKvQi896/sG8V7CKHQ6FCzCBsAYDVR0fBIGoMIGlMIGioIGfoIGchoGZbGRhcDovL2xkYXAuY3J
zLmxvbWJhcmRpYS5pdC9jbiUzZENEUDEsb3UlM2RDUkwlMjBDQSUyMFNlcnZpemlvLG8lM2RMSVNJVCUyMFMucC5BLixjJTNk
SVQ/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MB0GA1UdD
gQWBBSfESc5Tjs7A0mBgK4E/sEhiBlgSDANBgkqhkiG9w0BAQUFAAOCAQEAeI4irlc/5oUORm/T3LGk0PW5YfFrC6urvrjRx2iZAly
Mgxuy3mVwlWM5QiYkSaikdObcUv0d4Guh5oVN/srd4L9vpa+0PhLvSKtykuY0sz56fmV1wlIJJlGTm0Dvs7HDKEb2jxPJ9O0MHqc8IxW
OY+HRco8HVY2iU/nFTS9Mwjlq2MwelASAnUwaPtJlXDGShLk7rFwz4nZbbrdj8uQNWn48btGLSpkIaqXJoml6QToocPCZaK3nc7orxyp
k0OwLm/vxgbNLqePCUTIBvfKSEXpjtQ4E7gAKadN0JStY4nyUFHnpEbasJll+xUWxxXKXRMJNq/b4xtPw/7pBq7H78A==</X509Data
>
            </X509Certificate>
            <X509Certificate subject="CN=LISIT CA di Servizio, OU=Servizio di certificazione, O=LISIT S.p.A., C=IT" issuer="CN=LISIT
CA di Servizio, OU=Servizio di certificazione, O=LISIT S.p.A., C=IT" alias="idpcrl-root">
<X509Data>MIIEkDCCA3igAwIBAgIBATANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJJVDEVMBMGA1UEChMMTElTSV
QgUy5wLkEuMSMwIQYDVQQLExpTZXJ2aXppbyBkaSBjZXJ0aWZpY2F6aW9uZTEdMBsGA1UEAxMUTElTSVQgQ0EgZGkgU2Vy
dml6aW8wHhcNMDQwOTAyMTQ1OTQ4WhcNMTYwOTAyMTQ1ODA0WjBoMQswCQYDVQQGEwJJVDEVMBMGA1UEChMMT
```

ElTSVQgUy5wLkEuMSMwIQYDVQQLExpTZXJ2aXppbyBkaSBjZXJ0aWZpY2F6aW9uZTEdMBsGA1UEAxMUTElTSVQgQ0EgZGk
gU2Vydml6aW8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC/vb2Sb3EiCu7TQO26R+SUM7IHTREJMUMqy148mc
dEe9aZ9kY7M6ZtcZ4zsc3mGT13ZWB5OPQsL7+1yyK5/BnIen0imUlZzhYBbUqLTkvOKyJYSORJlrKZ4Be6Sm1N99LxPr/G5ckkZq5H2
yvFt8XBaQkUNNAJBksJbu7NP7kWBRfbvicdr+2QCe4HjUiMLEUqHxq/X8d1whFBHRGltcfEfX76/LJpMwa1DUR8rJfFD4bVKjIZFG9H
ugN9YAnYnzP2lVrEcuRecuySefirvSmEkWMAQVy+Xn/DwOr/bdPsrJatqyyHusHlep6FPNVmfbboEF/3eqRnMbRrT0R8rOpBAgMBAAG
jggFDMIIBPzASBgNVHRMBAf8ECDAGAQH/AgEAMEcGA1UdIARAMD4wPAYJKwYBBAG8bhMCMC8wLQYIKwYBBQUHAgE
WIWh0dHA6Ly93d3cubGlzaXQuaXQvZmlybWFkaWdpdGFsZTCBsAYDVR0fBIGoMIGlMIGioIGfoIGchoGZbGRhcDovL2xkYXAuY3
JzLmxvbWJhcmRpYS5pdC9jbiUzZExJU0lUJTIwQ0ElMjBkaSUyMFNlcnZpemlvLG91JTNkU2Vydml6aW8lMjBkaSUyMGNlcnRpZmlj
YXppb25lLG8lM2RMSVNJVCUyMFMucC5BLixjJTNkSVQ/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdD9iYXNlMA4GA1UdDwE
B/wQEAwIBBjAdBgNVHQ4EFgQUhM2xLxyr0IvPev7BvFewih0OhQswDQYJKoZIhvcNAQEFBQADggEBAG+nIGrRPLttAA3tB9Hk5
X3OfAjmFJPkd1Ggm2cXOTqEPsxB7gXxuVNtRCh8z/D+83onq1Nx3YQNrbMqEdPgmkc5qGu5XFJewHuZanJJtjpFauHVovIuV+GcMzB
Pl/iu268LBzb+9AWO/GxE8M7Ay0XfMWwjtStk6Xg/lDFO8TOBrMutpw8TUU2aC1GbXQmIaLoySfLQbo7kopT56GvPwt+45JzuumnK+
ZZZd1euDWPcXhcgY3xsyvzHFM0bvf9ON3HIEIJhowpePNewqbvT3KirS0dxMUQLkl7TacOKRomWbskBqFWOFzC9SRWjb7vPkU0R5
NsEsYRLyvekQS5+K9g=</X509Data>
            </X509Certificate>
        </SigningInfo>
</IdP>
…

La configurazione sopra mostrata consente ad una applicazione integrata con SiRAC-SSO di ricevere Response SAML prodotte dalla CA “reale” descritta nelle sezioni precedenti. Qualora si desideri supportare, in aggiunta, la ricezione di Response SAML prodotte attraverso la CA “demo” di Lombardia Informatica occorre aggiungere all’elemento *SigningInfo* il certificato root della CA “demo” (per la verifica di trust) e il certificato foglia da utilizzare come riferimento per la verifica della firma della Response SAML.

Segnalibro FineDoc – Non Cancellare