ASPETTI DI SICUREZZA NELLA COOPERAZIONE TRA I SERVIZI

Versione 1.0

INDICE

1. PREFAZIONE

1.1. Autori

Redatto da:	Andrea Carmignani	RTI IBM-SI
Verificato da:	Nazzareno Ticconi	RTI IBM-SI
Revisione a cura di:	Giovanni Olive	CNIPA
	Alfio Raia	CNIPA
	Alessandro Vinciarelli	CNIPA
Validato da:	Francesco Tortorelli	CNIPA

1.2. Modifiche Documento

Descrizione Modifica	Edizione	Data
Emissione 1^ bozza	0.1	19/01/2009

1.3. Riferimenti

Codice	Titolo

1.4. Acronimi e Definizioni

Sigla	Descrizione
SAML	Security Assertion Markup Language
WSDL	Web Service Description Language
AdS	Accordo di Servizio

2. OBIETTIVI E CONTESTO DI RIFERIMENTO

Il *Sistema Pubblico di Connettività e Cooperazione (SPC)* si colloca nel contesto definito dal Decreto legislativo n° 82 del 7 marzo 2005, pubblicato in G.U. del 16 maggio 2005, n. 112, recante il **"Codice dell'amministrazione digitale"** (C.A.D.) e successive modifiche ed integrazioni. Esso istituisce il SPC, definendone gli obiettivi, le funzionalità ed il modello di governance.

Il processo di regolamentazione normativa del SPC è proseguito nel tempo, arrivando alla pubblicazione del Decreto del Presidente del Consiglio dei Ministri n.1 del 1 aprile 2008, pubblicato in G.U. del 21 giugno 2008, n. 144, recante le **"Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettivita"**, previste dall'art. 71, comma 1-bis, del C.A.D, con il quale viene definito il quadro tecnico di riferimento per lo sviluppo dei servizi SPC e le regole per il funzionamento e l'adesione ai servizi SPC.

Parallelamente, come previsto dal modello condiviso di cooperazione applicativa per la P.A. italiana *SPCoop*, è stato avviato e portato a termine lo sviluppo dei *Servizi Infrastrutturali di interoperabilità, cooperazione ed accesso (SICA)* e del centro di gestione per l'erogazione di tali servizi (CG-SICA), infrastruttura condivisa a livello nazionale che abilita l'interoperabilità e la cooperazione applicativa fra le Amministrazioni pubbliche nonché l'accesso ai servizi applicativi da queste sviluppati e resi disponibili su SPC.

L'evoluzione dello scenario di riferimento e la disponibilità di servizi di infrastruttura per la cooperazione applicativa, hanno reso necessaria la definizione e publicazione di una serie di documenti che specificassero in dettaglio le modalità tecniche per l'interoperabilità e la cooperazione applicativa e l'utilizzo dei servizi SICA, come peraltro prevista dalle succitate regole tecniche.

Gli ultimi documenti tecnici relativi al SPCoop rilasciati alla fine del 2005, infatti, definivano un livello di condivisione che consentiva sia la stabilità del modello nel tempo rispetto al contesto organizzativo e tecnologico di riferimento, sia i necessari gradi di libertà per la sua implementazione; ciò a scapito del dettaglio tecnico necessario, invece, nel momento in cui si fa riferimento ad una specifica implementazione del modello ed a specifici servizi infrastrutturali.

I seguenti documenti sono stati redatti dal Raggruppamento Temporaneo di Imprese (IBM-Sistemi Informativi), incaricato dello sviluppo e dell'implementazione del Centro di Gestione dei servizi SICA, con la supervisione del CNIPA, ed hanno origine dalla documentazione sviluppata nel corso del progetto e nella fase di collaudo dei servizi stessi.

L'insieme di documenti prodotti specifica i modelli, le modalità, i dettagli tecnici di realizzazione, gestione ed utilizzo dei servizi SICA, le modalità di interfacciamento, le procedure qualificazione e gestione dei componenti infrastrutturali SPCoop, sulla base di quanto già previsto e definito nei documenti precedentemente condivisi e nel rispetto delle succitate regole tecniche.

Titolo Documento
1. Introduzione ai servizi SICA
2. Specifiche di nomenclatura in SPCoop
3. Specifiche di utilizzo del Servizio di Registro SICA
4. Modalità di funzionamento del Client SICA
5. Struttura dell'Accordo di Servizio e dell'Accordo di Cooperazione
6. Descrizione delle specifiche di sicurezza negli Accordi di Servizio
7. Aspetti di sicurezza applicativa nella cooperazione fra servizi
8. Modalità di funzionamento del Catalogo Schemi e Ontologie
9. Interfacce applicative tra Registro SICA generale e Registri SICA secondari
10. Modalità di Qualificazione del Registro SICA secondario
11. Modalità di Qualificazione della Porta di Dominio
12. Schema d'interoperabilità IndicePA
13. Guida ai servizi IndicePA
14. Modello di Gestione Federata delle Identità Digitali (GFID)
15. Modalità di accreditamento alla GFID
16. Modello di funzionamento dell'Indice dei Soggetti
17. Modello di funzionamento della Certification Authority

2.1. Scopi del documento

Obiettivo del presente documento è identificare quali informazioni è necessario veicolare a supporto della sicurezza applicativa in ambito SPCoop e mostrare una possibile modalità con cui descriverle e trasferirle a supporto delle interazioni in cooperazione applicativa.

Le principali tecnologie su cui si basano le specifiche di sicurezza oggetto del documento sono nel documento "*Descrizione delle specifiche di sicurezza negli accordi di servizio*".

2.2. Note di lettura del documento

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

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

2.3. Note sul Copyright

3. TRASFERIMENTO DI INFORMAZIONI DI SICUREZZA APPLICATIVA IN SPCOOP

Le principali tecnologie su cui si basano le specifiche di sicurezza oggetto del documento, SAML e WS-Security, sono introdotte al capitolo 3 del documento "*Descrizione delle specifiche di sicurezza negli accordi di servizio*".

3.1. Interazioni in cooperazioni applicativa e asserzioni SAML

In ambito di accesso federato F-SSO l'accesso da parte di un utente ai servizi e alle risorse offerte da un Service Provider può richiedere la raccolta di statement di autenticazione e di attributo relativi allo stesso soggetto che richiede il servizio di front-end (nel caso specifico descritte e veicolate secondo quanto previsto dalla specifica SAML 2.0).

Nel caso della cooperazione applicativa lo scenario di interazione cambia poiché si è in presenza di un'interazione puramente machine-to-machine tra due servizi applicativi offerti da due distinti Service Provider (fruitore ed erogatore). Non è prevista quindi un'interazione diretta con l'utente (per esempio via web browser, come avviene nel caso del Web Browser SSO Profile descritto dalla specifica SAML).

Tuttavia, un'interazione in cooperazione applicativa tra il Service Provider fruitore e il Service Provider erogatore può essere stata innescata da un precedente accesso via web di un utente a un servizio di front-end offerto dal Service Provider fruitore (per esempio un servizio al cittadino offerto tramite il portale di un'amministrazione comunale), accesso che potrebbe essere sottoposto a vincoli di autenticazione e autorizzazione utente.

In aggiunta, anche l'accesso a servizi applicativi in un contesto machine-to-machine potrebbe essere in realtà subordinato al trasferimento di opportune informazioni di autenticazione e autorizzazione utente, per esempio se si considera il caso in cui vi sia un soggetto che agisce per conto dell'ente che interagisce in cooperazione applicativa (per esempio un operatore o un funzionario).

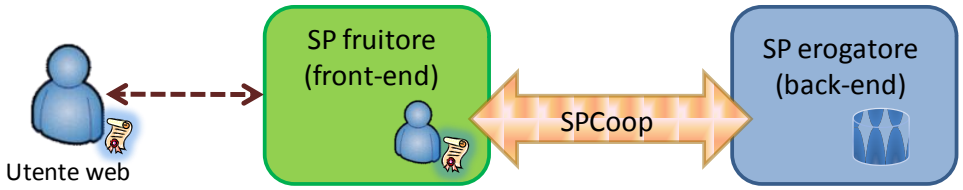

Figura 1. Interazione SPCoop e soggetti coinvolti

Alla luce di queste considerazioni si può delineare il quadro delle informazioni che può essere necessario trasferire nel caso delle interazioni in ambito SPCoop:

- statement di autenticazione che asseriscano l'identità del soggetto che agisce per conto dell'ente fruitore;
- statement di autenticazione che asseriscano l'identità dell'utente che ha innescato l'interazione in cooperazione applicativa accedendo a un servizio di front-end erogato dall'ente fruitore;
- statement di attributo inerenti il soggetto che agisce per conto dell'ente fruitore in base ai quali il dimostra di possedere le caratteristiche necessarie ad accedere al servizio applicativo offerto dall'ente erogatore (per esempio il ruolo di "funzionario di 1° livello");
- eventuali statement di attributo che caratterizzano l'utente che ha innescato l'interazione in cooperazione applicativa accedendo a un servizio di front-end erogato dall'ente fruitore.

La tipologia di informazioni da veicolare è analoga a quelle già illustrate nel modello del Servizio di Gestione delle Identità Digitali, dunque è possibile utilizzare anche nell'ambito delle interazioni in cooperazione applicativa gli stessi costrutti forniti dallo standard SAML descritti nel modello, vale a dire asserzioni contenenti statement di autenticazione e di attributo.

Il trasferimento di queste informazioni può avvenire secondo le modalità illustrate nella sezione seguente. Obiettivo delle sezioni che seguono è infatti proporre una modalità di trasferimento di queste informazioni nelle interazioni in cooperazione applicativa (tali modalità, insieme al contenuto stesso delle informazioni veicolate, dovranno di volta in volta essere coerenti con i requisiti di sicurezza pubblicati nell'Accordo di Servizio del servizio SPCoop che prende parte alla specifica interazione.

3.2. Trasferimento di asserzioni SAML

Come ricordato in precedenza, la cooperazione applicativa comporta interazioni machine-to-machine e non ammette una interazione diretta con l'utente. Il modello di cooperazione applicativa previsto da SPCoop prevede tra i suoi principi basilari l'erogazione e la fruizione di servizi attraverso le tecnologie e gli standard indicati genericamente come "Web service". Per poter adottare nell'ambito delle interazioni tra servizi in cooperazione applicativa un approccio basato su asserzioni SAML è necessario identificare le opportune modalità per veicolare statement di autenticazione e di attributo anche nel caso di interazioni machine-to-machine.

Un meccanismo idoneo è fornito dallo standard WS-Security il cui utilizzo è esplicitamente previsto in SPCoop: le specifiche SPCoop, infatti, prevedono già l'utilizzo di questo standard a diversi livelli (per esempio nei meccanismi di autenticazione, di controllo di integrità, di riservatezza ecc., sez. 4.2).

L'approccio proposto è di veicolare le asserzioni SAML mediante l'header WS-Security dei messaggi SOAP, secondo le modalità previste dal WS-Security SAML Token Profile definito da OASIS secondo quanto descritto nelle successivo sezioni.

3.2.1. WS-Security SAML Token Profile

Il WS-Security SAML Token Profile versione 1.1, descrive come utilizzare asserzioni SAML nel contesto dello standard WS-Security. In particolare, la specifica indica come includere e referenziare asserzioni SAML negli header WS-Security dei messaggi SOAP (sez. 3.3 e 3.4).

Le asserzioni SAML possono essere incluse integralmente (elemento `<saml:Assertion>`) all'interno dell'elemento `<wsse:Security>` (dove i prefissi `saml` e `wsse` indicano rispettivamente il namespace di SAML 2.0 e uno dei namespace utilizzati in WS-Security insieme a `wsse11`, `wsu` e altri ancora, citati nei rispettivi documenti di specifica).

Di Seguito un breve esempio di messaggio SOAP contenente una asserzione SAML (per semplicità sono stati omessi diversi dettagli non essenziali: il prefisso `soap` indica un namespace utilizzato dalla specifica SOAP):

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Header>
   <wsse:Security xmlns:wsse="..." xmlns:wsu="..." xmlns:wsse11="...">
      <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
[...]>
         [...]
         </saml:Assertion>
         [...]
   </wsse:Security>
   [...]
</soap:Header>
<soap:Body>
   [...]
</soap:Body>
</soap:Envelope>
[...SOAP ATTACHMENTS...]
```

Figura 2: Esempio di Asserzione SAML all'interno dell'Header WS-Security (evidenziato in grigio)

Una volta inclusa una asserzione SAML 2.0 in un header WS-Security, è possibile, se necessario, identificarla e referenziarla (per esempio per qualificarla, distinguendola da altre asserzioni eventualmente presenti).

Questo si può fare mediante un elemento **<wsse:SecurityTokenReference>** così strutturato:

- attributo **wsse11:TokenType** con valore http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0
- attributo opzionale **wsu:Id** che rappresenta un'etichetta di testo che caratterizza ulteriormente l'elemento (una possibile modalità di utilizzo di questo attributo verrà illustrata nei paragrafi successivi).

Il contenuto dell'elemento <wsse:SecurityTokenReference> può variare a seconda della modalità con cui si intende referenziare l'asserzione veicolata nell'header WS-Security, per esempio secondo una di queste alternative:

- **key identifier reference**: l'elemento <wsse:SecurityTokenReference> contiene un elemento <wsse:KeyIdentifier> che ha un attributo **wsse:ValueType** avente valore http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID; il valore dell'elemento <wsse:KeyIdentifier> rappresenta l'identificativo univoco dell'asserzione SAML veicolata nel messaggio SOAP;
- **direct or URI reference**: l'elemento <wsse:SecurityTokenReference> contiene un elemento **<wsse:Reference>** avente un attributo URI il cui valore referenzia l'identificativo dell'asserzione SAML veicolata nel messaggio (mediante un URI o un frammento di URI).

Gli esempi che seguono illustrano nell'ordine i due casi appena descritti (anche in questo caso sono stati omessi diversi dettagli non essenziali).

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Header>
 <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:wsse11="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-
1.1.xsd">
      <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
ID="s25b7d3cd258e50b3e5e53c49075118ea55d3e2a09" IssueInstant="2008-04-
07T18:30:55.640Z" Version="2.0">
       [...]
      </saml:Assertion>
 </wsse:Security>
 <wsse:SecurityTokenReference xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
```

```
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:wsse11="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd" wsu:Id="STR1" wsse11:TokenType="http://docs.oasis-open.org/wss/oasis-wss-saml-tokenprofile-1.1#SAMLV2.0">
            <wsse:KeyIdentifier wsu:Id="…" ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID">
     s25b7d3cd258e50b3e5e53c49075118ea55d3e2a09
            </wsse:KeyIdentifier>
      </wsse:SecurityTokenReference>
     </soap:Header>
     <soap:Body>
     [...]
     </soap:Body>
     </soap:Envelope>
```

Figura 3: Esempio relativo al caso in cui l'asserzione viene referenziata secondo la modalità key identifier reference

```
     <?xml version="1.0" encoding="UTF-8"?>
     <soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
     <soap:Header>
      <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:wsse11="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd">
            <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="s25b7d3cd258e50b3e5e53c49075118ea55d3e2a09" IssueInstant="2008-04-07T18:30:55.640Z" Version="2.0">
             [...]
            </saml:Assertion>
      </wsse:Security>
      <wsse:SecurityTokenReference
     xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:wsse11="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd" wsu:Id="…" wsse11:TokenType="http://docs.oasis-open.org/wss/oasis-wss-saml-tokenprofile-1.1#SAMLV2.0">
            <wsse:Reference wsu:Id="…" URI="#s25b7d3cd258e50b3e5e53c49075118ea55d3e2a09">
            </wsse:Reference>
```

```
    </wsse:SecurityTokenReference>
  </soap:Header>
  <soap:Body>
  [...]
  </soap:Body>
  </soap:Envelope>
```

Figura 4: Esempio relativo al caso in cui l'asserzione viene referenziata secondo la modalità direct or URI reference

Nel caso di asserzioni SAML 2.0, il WS-Security SAML Token Profile raccomanda l'uso della modalità *direct or URI reference* ("SHOULD") pur dando la possibilità di usare la modalità *key identifier reference* ("MAY")[1].

In aggiunta se necessario tramite opportuni metodi è' possibile oltre a referenziare anche provare la corrispondenza tra l'entità che emette il messaggio SOAP (detta Attesting Entity) e il subject dell'asserzione.

I metodi per farlo previsti dal WS-Security SAML Token Profile sono:

- "holder-of-key",
- "sender-vouches",
- "bearer".

Tali metodi sono legati alla metodologia di conferma del subject indicato nell'asserzione SAML.

In particolare, nel caso in cui il subject abbia un confirmation method di tipo "bearer" (come per esempio accade nel caso di asserzioni relative all'utente autenticato sul front-end) il WS-Security SAML Token Profile prevede che la prova della relazione esistente tra l'entità che emette il messaggio SOAP contenente l'asserzione e il subject di tale asserzione sia implicita e non debba essere verificata dall'entità ricevente.

Il WS-Security SAML Token Profile fornisce dunque modalità sufficientemente articolate per inserire asserzioni nell'header di un messaggio SOAP. Le sezioni che seguono discutono l'uso di questo profilo nel contesto SPCoop.

[1] Quella illustrata ("SAML assertion referenced from header or element") non è l'unica modalità prevista dal WS-Security SAML Token Profile con cui referenziare un'asserzione SAML: esistono anche le modalità "SAML assertion referenced from KeyInfo", "SAML assertion referenced from SignedInfo" e "SAML assertion referenced from encrypted data reference".

3.3. Uso della WS-Security SAML Token Profile in Ambito SPCoop

In ambito SPCoop si può ipotizzare la presenza di soggetti (reali o "virtuali") interni a ciascun ente (operatori, funzionari ecc.). Tali soggetti agiscono per conto del rispettivo ente (fruitore) nell'interazione SPCoop con altri enti (erogatori).

In aggiunta, può esistere un utente, non legato agli enti, che rappresenta la causa e l'oggetto dell'interazione tra gli enti stessi(per esempio il cittadino al centro di una procedura di cambio di residenza).

Le informazioni da trasferire a supporto della sicurezza applicativa in ambito di cooperazione applicativa si basano su ciò che ciascun servizio SPCoop descrive e pubblica nell'Accordo di Servizio sotto forma di vincoli in opportune policy. Tali informazioni possono essere strutturate sulla base dei costrutti messi a disposizione dallo standard SAML (statement di autenticazione e di attributo).

Un approccio ipotizzabile all'interno della cooperazione SPC può essere l'utilizzo di una singola asserzione SAML che veicola le informazioni necessarie all'ente fornitore di un servizio in cooperazione applicativa. L'asserzione può contenere:

- **uno statement di autenticazione**, che asserisce l'identità del soggetto che agisce per conto dell'ente richiedente;
- **zero o più statement di attributo**, in base ai quali il soggetto che agisce per conto dell'ente richiedente dimostra di possedere le caratteristiche necessarie ad accedere al servizio (per esempio il ruolo di "funzionario di 1° livello");
- **zero o più asserzioni di autenticazione e/o di attributo** poste nell'elemento `<Advice>` dell'asserzione, con i quali l'ente fruitore può se necessario veicolare e fornire all'ente erogatore le informazioni originariamente raccolte da terzi circa l'utente che ha innescato l'interazione..

In alternativa si può ipotizzare di veicolare più asserzioni distinte (ad esempio uno contenente uno statement di autenticazione e le altre contenenti uno o più statement di autenticazione e/o di attributo) nell'header del messaggio SOAP, referenziando ciascuna in modo opportuno.

Se l'header WS-Security contiene più asserzione ed è necessario identificare l'asserzione SAML rilevante in ambito SPCoop per l'autorizzazione di dovrà usare l'attributo `wsu:Id` dell'elemento `<wsse:SecurityTokenReference>` come descritto in precedenza. A tale scopo, è possibile per esempio assegnare all'attributo un valore convenzionale come "SPCoop".

3.4. Requisiti tecnologici sull'infrastruttura SPC

Veicolare asserzioni SAML nell'header di un messaggio SOAP pone nuove caratteristiche e requisiti sul comportamento e sulle funzionalità dei componenti software dell'infrastruttura SPCoop affinché sia possibile il trasferimento delle informazioni secondo le modalità descritte nelle sezioni precedenti.

Per esempio, nel caso della Porta di Dominio (e dei componenti software a essa legati) occorre valutare i seguenti aspetti:

- supporto allo standard WS-Security, e alle specifiche a esso correlate, almeno per quanto riguarda i costrutti citati nel presente documento;
- presenza di opportune API per l'inserimento e la gestione di header WS-Security formattati secondo quanto previsto dal WS-Security SAML Token Profile (questo vale sia lato richiedente, per iniettare le asserzioni SAML nel messaggio SOAP, sia lato fruitore, per la corrispondente estrazione a valle della ricezione del messaggio);
- il componente software deve fornire opportune garanzie di eventuale non sovrascrittura degli header WS-Security durante le fasi di preparazione e processing dei messaggi (ciò vale sia lato fruitore sia lato erogatore).

4. NON RIPUDIO FRA PORTE DI DOMINIO

Tra le regole per il non-ripudio dettate dal documento sui servizi di sicurezza SPCoop vi sono le seguenti:

- *L'allegato del messaggio PUO' contenere una richiesta, in tal caso questa DEVE essere un documento informatico sottoscritto con firma digitale.*
- *Le regole e gli standard della firma digitale fanno riferimento alla normativa seguente (DPR 29 dicembre 200 n.445 come modificato dal Decreto legislativo 29 gennaio 2002 n.10 e dal DPR 7 aprile 2003 n. 137, DPCM 13 gennaio 2004 [codice dell'amministrazione digitale][Decreto legislativo del 7 marzo 2005, n. 82 pubblicato su G.U. 16 maggio 2005, n.112 - S.O. n. 93]).*
- *La firma digitale PUO' essere apposta dall'utente che ha originato il processo che ha creato la busta, oppure PUO' essere apposta da altri utenti deputati a ricevere la richiesta, verificarla, e quindi apporre la propria firma.*
- *L'apposizione della firma sull'allegato rende possibile la memorizzazione del documento indipendentemente dal messaggio di trasporto (messaggio SPCoop), anche ai fini di dirimere possibili contenziosi.*
- *Gli allegati binari DEVONO essere codificati in formato BASE64 (RFC 3548).*
- *DEVE essere seguita la procedura seguente:*
    - *CASO A (collegamento diretto tra PD, connessione con protocollo HTTPS). Si PUO' utilizzare lo UserName Token profile:*
        - *creazione di un <wsse:Security> header;*
        - *inserimento dell' elemento <wsse:UsernameToken>, per specificare la username del fruitore del servizio;*
        - *inserimento, all'interno di <wsse:UsernameToken>, dell'elemento <wsse:Password> che contiene la password del richiedente il servizio. (la password può essere inviata all'interno del messaggio in un formato chiaro (wsse:PasswordText) oppure in un formato "digest" (wsse:PasswordDigest));*
    - *CASO B (non esiste un collegamento diretto tra PD). Si DEVE utilizzare X.509 security token profile:*
        - *creazione di un <wsse:Security> header;*
        - *inserimento dell' elemento <wsse:SecurityTokenReference>, per specificare il riferimento al fruitore del servizio;*
        - *inserimento, all'interno di <wsse:SecurityTokenReference>, di:*
            - *un subject Key Identifier (elemento <wsse:KeyIdentifier>);*

- *un binarySecurityToken, (certificato in formato X.509 v3, come elemento binario all'interno di un elemento <wsse:BinarySecurityToken> nel messaggio;*
- *un serial number per identificare il certificato digitale.*

Come si può vedere, la tutela del non-ripudio di un messaggio è legata essenzialmente a meccanismi di firma (anche se il documento SPCoop citato sembra riferirsi solo a interazioni tra Porte di Dominio). La specifica WS-SecurityPolicy mette a disposizione opportune policy assertion per porre il requisito che un determinato elemento del messaggio SOAP sia firmato, come visto in precedenza.

Inoltre, la specifica WS-SecurityPolicy definisce o cita diversi token di autenticazione da poter usare in una policy WS-Policy, quali per esempio:

- `<sp:BinarySecurityToken>` (definito da WS-Security);
- `<sp:UsernameToken>`;
- `<sp:X509Token>`.

Segue un esempio (frammento di policy) in cui si fa uso di alcune delle policy assertion appena citate.

```
[...]
<wsp:Policy>
 <sp:Wss10>
       <sp:MustSupportRefKeyIdentifier/>
       <sp:MustSupportRefEmbeddedToken/>
 </sp:Wss10>
 <sp:SignedParts>
       <sp:Attachments/>
       [...]
 </sp:SignedParts>
 <sp:AlgorithmSuite>
       <wsp:Policy>
             <sp:Basic256/>
       </wsp:Policy>
 </sp:AlgorithmSuite>
 <sp:SupportingTokens>
       <wsp:Policy>
                  <sp:UsernameToken>
                  <wsp:Policy>
                        <sp:HashPassword/>
```

```
                    </wsp:Policy>
                </sp:UsernameToken>
            </wsp:Policy>
        </sp:SupportingTokens>
        [...]
    </wsp:Policy>
    [...]
```

5. TRASPORTO

Il documento sui servizi di sicurezza SPCoop si occupa di requisiti a livello di trasporto in ambito SPCoop solo in alcuni casi, per esempio quelli che riguardano la comunicazione tra Porte di Dominio a supporto di altri requisiti di sicurezza, per esempio la riservatezza:

- *I meccanismi di riservatezza riguardanti lo scambio tra PD DOVREBBERO essere implementati attraverso i protocolli SSL v 3.0 o TLS v 1.0. e basati su chiavi crittografiche certificate a tale scopo da una o più infrastrutture a chiave pubblica accreditate e i cui certificati radice sono presenti nella TCL della Bridge CA.*

Le principali policy assertion che la specifica WS-SecurityPolicy mette a disposizione per porre requisiti circa il trasporto del messaggio SOAP sono:

- `<sp:TransportBinding>`: contiene una nested policy in cui poter precisare mediante opportuni sotto-elementi i requisiti di trasporto, tra cui:
  - `<sp:TransportToken>`: contiene una nested policy in cui poter precisare mediante opportuni sotto-elementi i requisiti sullo specifico token di trasporto da utilizzare (per esempio `<sp:HttpsToken>`);
  - `<sp:AlgorithmSuite>`: (descritto nel documento SPCoop – Specifiche di sicurezza negli ADS);
  - `<sp:IncludeTimestamp>`: richiede che venga inclusa la proprietà `wsu:Timestamp` nell'header `wsse:Security`;
- `<sp:SymmetricBinding>`: precisa i requisiti che valgono in caso di interazioni multiple tra le parti "initiator" e "recipient" con protezione dei messaggi mediante chiavi simmetriche (lo stesso token di firma viene usato nelle interazioni nelle due direzioni, e lo stesso accade per quello di encryption); contiene una nested policy in cui poter precisare mediante opportuni sotto-elementi altri requisiti, tra cui:
  - `<sp:AlgorithmSuite>`;

- <sp:EncryptBeforeSigning>;
- <sp:EncryptSignature>;
- <sp:OnlySignEntireHeadersAndBody>;

- <sp:AsymmetricBinding> : precisa i requisiti che valgono in caso di interazioni multiple tra le parti "initiator" e "recipient" con protezione dei messaggi mediante chiavi asimmetriche (sia per il token di firma che per quello di encryption).

Seguono tre esempi, uno per ciascuna delle policy assertion appena citate.

Esempio d'uso della policy assertion <sp:TransportBinding> (frammento di policy):

```
[...]
<sp:TransportBinding>
 <wsp:Policy>
  <sp:TransportToken>
     <wsp:Policy>
       <sp:HttpsToken>
       <wsp:Policy>
         <sp:RequireClientCertificate>
        </wsp:Policy>
        </sp:HttpsToken>
       </wsp:Policy>
   </sp:TransportToken>
    <sp:AlgorithmSuite>
     <wsp:Policy>
          <sp:Basic256 />
     </wsp:Policy>
    </sp:AlgorithmSuite>
       <sp:Layout>
        <wsp:Policy>
          <sp:Strict />
        </wsp:Policy>
      </sp:Layout>
      <sp:IncludeTimestamp />
    </wsp:Policy>
</sp:TransportBinding>
[...]
```

Esempio d'uso della policy assertion <sp:SymmetricBinding> (frammento di policy):

```
[...]
<sp:SymmetricBinding>
 <wsp:Policy>
      <sp:ProtectionToken>
            <wsp:Policy>
                  <sp:X509Token sp:IncludeToken="http://docs.oasis-
open.org/ws-sx/ws-securitypolicy/200512/IncludeToken/Never">
                        <wsp:Policy>
                              <sp:RequireThumbprintReference/>
                              <sp:WssX509V3Token11/>
                        </wsp:Policy>
                  </sp:X509Token>
            </wsp:Policy>
      </sp:ProtectionToken>
      <sp:AlgorithmSuite>
            <wsp:Policy>
                  <sp:Basic256/>
            </wsp:Policy>
      </sp:AlgorithmSuite>
      <sp:Layout>
            <wsp:Policy>
                  <sp:Strict/>
            </wsp:Policy>
      </sp:Layout>
      <sp:IncludeTimestamp/>
      <sp:OnlySignEntireHeadersAndBody/>
 </wsp:Policy>
</sp:SymmetricBinding>
[...]
```

Esempio d'uso della policy assertion <sp:AsymmetricBinding> (frammento di policy):

```
[...]
<sp:AsymmetricBinding>
 <wsp:Policy>
      <sp:InitiatorToken>
```

```
                  <wsp:Policy>
                        <sp:X509Token sp:IncludeToken="http://docs.oasis-
open.org/ws-sx/ws-securitypolicy/200512/IncludeToken/AlwaysToRecipient">
                              <wsp:Policy>
                                    <sp:WssX509V3Token10/>
                              </wsp:Policy>
                        </sp:X509Token>
                  </wsp:Policy>
            </sp:InitiatorToken>
            <sp:RecipientToken>
                  <wsp:Policy>
                        <sp:X509Token sp:IncludeToken="http://docs.oasis-
open.org/ws-sx/ws-securitypolicy/200512/IncludeToken/Never">
                              <wsp:Policy>
                                    <sp:WssX509V3Token10/>
                              </wsp:Policy>
                        </sp:X509Token>
                  </wsp:Policy>
            </sp:RecipientToken>
            <sp:AlgorithmSuite>
                  <wsp:Policy>
                        <sp:Basic256/>
                  </wsp:Policy>
            </sp:AlgorithmSuite>
            <sp:Layout>
                  <wsp:Policy>
                        <sp:Strict/>
                  </wsp:Policy>
            </sp:Layout>
            <sp:IncludeTimestamp/>
            <sp:ProtectTokens/>
            <sp:OnlySignEntireHeadersAndBody/>
      </wsp:Policy>
     </sp:AsymmetricBinding>
     [...]
```