Integrazione in SPID - Note e Modifiche necessarie per i SP

Legenda

GW	Gateway FedERa
SP	Service Provider appartenente alla federazione FedERa
IDP	Identity Provider appartenente alla federazione FedERa
IDP SPID	Identity Provider appartenente alla federazione SPID
Asserzione	Messaggio in formato SAML proveniente da un IDP che attesta l'avvenuta autenticazione da parte di un utente, e che trasposta gli attributi dell'utente

Riferimenti

[SPIDModalitàAttuative]	Modalità attuative SPID http://www.agid.gov.it/sites/default/files/circolari/spid-modalita_attuative_v1.pdf
[SPIDRegoleTecniche]	Regole tecniche SPID http://www.agid.gov.it/sites/default/files/circolari/spid-regole_tecniche_v1.pdf
[SAMLCore]	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
[SAMLAuthContext]	Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf

1 - Intermediazione del Gateway FedERa per SPID

Nota funzionale

Fin da prima dell’avvento di SPID, il GW si pone da intermediario tra i SP e gli IDP appartenenti alla federazione, fornendo primariamente i seguenti vantaggi:

1. Nessuna necessità per i SP/IDP di integrarsi applicativamente con gli altri IDP/SP della federazione: quando un SP/IDP entra nella federazione si integra esclusivamente con il GW, il quale gli da, automaticamente e senza necessità di modifiche di configurazione, visibilità degli altri IDP/SP con cui interagire.
2. Possibilità per i SP/IDP di interagire con IDP/SP che utilizzano una versione non compatibile di protocollo SAML.
   Il protocollo SAML infatti ha due versioni (SAML1.1 e SAML2.0) non compatibili tra loro. Grazie al GW viene resa comunque possibile la comunicazione, tramite la sua intermediazione.

Per fare questo, il GW si comporta come un IDP nei confronti dei SP, e come un SP nei confronti degli IDP:

- Riceve richieste di autenticazione dai SP utilizzando la versione del protocollo SAML utilizzata dal SP (si comporta quindi come un IDP nei contronti dei SP).
- Esegue un proxy della richiesta di autenticazione originaria verso l’IDP scelto dall’utente.
  La richiesta di autenticazione originaria prima dell’invio viene modificata affinchè sia compatibile con l’IDP scelto, ed in particolare con la versione del protocollo SAML utilizzata dall’IDP (si comporta quindi come un SP nei contronti degli IDP).
- Riceve l’asserzione dagli IDP utilizzando la versione del protocollo SAML utilizzata dall’IDP.
- Esegue un proxy dell’asserzione originaria verso il SP da cui è partita la richiesta di autenticazione.
  L’asserzione originaria prima dell’invio viene modificata affichè sia compatibile con l’SP richiedente, ed in particolare con la versione del protocollo SAML utilizzata dall’IDP.
  Inoltre, nell’asserzione rielaborata, il GW aggiunge degli attributi utente aggiuntivi utili al SP.

In questa maniera per i SP il GW funge sempre come l’unico IDP, mentre per gli IDP il GW funge sempre come l’unico SP appartenente alla federazione FedERa.

Un SP può venire comunque a conoscenza di quale sia l'IDP che effettivamente ha eseguito l'autenticazione, tramite l'attributo utente "authenticatingAuthority".
Inoltre, può venire a conoscenza di quale sia il metodo di autenticazione effettivamente utilizzato tramite l'attributo utente "authenticationMethod", che può essere valorizzato con "password", "otp" o "smartcard".

Con l'avvento di SPID, sono state fatte modifiche implementative sul GW affinchè i SP integrati in FedERa possano venire integrati in SPID (e quindi permettere l'accesso a utenti registrati su IDP SPID) in maniera tale da ridurre al minimo le modifiche implementative e di configurazione che questi devono eseguire.
L'obiettivo è quindi che, oltre a preservare il funzionamento del processo di autenticazione con IDP appartenenti alla federazione FedERa, i SP, già integrati o che si integreranno in FedERa, possano comunicare anche con gli IDP SPID, permettendo così l'accesso agli utenti registrati in tali entità.

Per raggiungere lo scopo, il GW si fa carico di tutte le modifiche strutturali, implementative e funzionali necessarie al fine di ottemperare alle specifiche tecniche definite da AGID a cui si devono attenere in generale i SP integrati in SPID, senza che i SP integrati in FedERa rispettino queste specifiche.
In questa maniera, in analogia alla situazione antecedente a SPID, il GW si comporta sempre un IDP nei confronti dei SP, e come un SP nei confronti degli IDP SPID:

- Riceve richieste di autenticazione dai SP utilizzando la versione del protocollo SAML utilizzata dal SP (si comporta quindi come un IDP nei contronti dei SP).
- Esegue un proxy della richiesta di autenticazione originaria verso l'IDP SPID scelto dall'utente.
  La richiesta di autenticazione originaria prima dell'invio viene modificata affinchè vengano rispettate le specifiche tecniche definite da AGID a cui si devono attenere in generale i SP integrati in SPID.
  Nella richiesta di autenticazione rielaborata, il GW specifica per quale SP integrato in FedERa è richiesta l'autenticazione (il quale viene visto dagli IDP SPID come un servizio applicativo del GW, che è un SP nei confronti degli IDP SPID).
- Riceve l'asserzione dagli IDP SPID.
- Esegue un proxy dell'asserzione originaria verso il SP da cui è partita la richiesta di autenticazione.
  L'asserzione originaria prima dell'invio viene modificata affinchè sia compatibile con l'SP richiedente, ed in particolare con la versione del protocollo SAML utilizzata dall'IDP.
  Inoltre, nell'asserzione rielaborata, il GW aggiunge degli attributi utente aggiuntivi utili al SP.

In questa maniera per i SP il GW funge sempre come l'unico IDP, mentre per gli IDP SPID il GW funge sempre come l'unico SP appartenente alla federazione FedERa.

Le modifiche implementative operate sul GW sono state fatte al fine di ottemperare alle seguenti specifiche tecniche definite in [SPIDRegoleTecniche], senza che i SP integrati in FedERa se ne debbano preoccupare.

Le modifiche implementative operate sul GW di maggior importanza per rendere trasparente ai SP l'integrazione in SPID riguardano:

- La mappatura delle classi di autenticazione definite in ambito SPID con le corrispondenti (utilizzando la corrispondenza dei Level Of Assurance dell'ISO-IEC 29115) classi di autenticazione utilizzate in SAML.
  Ulteriori dettagli su questo argomento sono presentati nei successivi paragrafi.
- La mappatura degli attributi che in ambito SPID hanno una nomenclatura diversa rispetto alla federazione FedERa, negli attributi della federazione con lo stesso valore semantico.

Il GW quando esegue il proxy di questi attributi al SP, per mantenere il funzionalmento attuale li rinomina con il nome utilizzato all'interno della federazione FedERa.
Qui l'elenco degli attributi gestiti dalla federazione:
http://federazione.lepida.it/documentazione/documentazione-tecnica/attributi

- La modifica del valore dell'attributo CodiceFiscale proveniente dagli IDP SPID utilizzando la codifica che sta per essere standardizzata per i serialNumber dei certificati (Draft ETSI EN 319 412-1) che prevede che il codice fiscale italiano sia rappresentato con la stringa "TINIT-<codice_fiscale>".
  Il GW quando esegue il proxy di questo attributo al SP, per mantenere il funzionamento attuale rimuove il prefisso "TINIT-" dal valore dell'attributo che rappresenta il codice fiscale.
- Varie modifiche alla richiesta di autenticazione rielaborata che viene proxata agli IDP SPID, in modo che tutti i parametri del messaggio SAML siano conformi alle specifiche di AGID.

A livello funzionale i cambiamenti più rilevanti sono i seguenti:

1. Quando un SP integrato in FedERa e convenzionato SPID invia una richiesta di autenticazione al GW, quest'ultimo permetterà all'utente di autenticarsi, oltre che presso gli IDP integrati in FedERa, anche presso gli IDP SPID.
2. Se l'autenticazione avviene presso un IDP SPID tra gli attributi utente comparirà anche l'attributo "spidCode" valorizzato con la stringa che identifica univocamente l'utente in ambito SPID.
3. Se l'autenticazione avviene presso un IDP SPID, i possibili valori dell'attributo "authenticationMethod" (che informa circa il metodo di autenticazione effettivamente utilizzato) può assumere uno dei seguenti valori:
   a. "Primo Livello SPID"
   b. "Secondo Livello SPID"
   c. "Terzo Livello SPID"
4. Se l'autenticazione avviene presso un IDP SPID, l'attributo "policyLevel" (che informa circa la password policy utilizzata dell'utente autenticato) viene così gestito:
   a. è presente e valorizzato con "Medio" (ovverosia Dati Personali) se vengono utilizzati i livelli 1 e 2 SPID.
   b. non è presente se viene utilizzato il livello 3 SPID.

Ulteriori dettagli sui cambiamenti di scenario sono presentati nei successivi paragrafi.

Un ulteriore modifica strutturale eseguita sul GW riguarda il registro delle transazioni: secondo le regole tecniche emanate da AGID, i SP devono provvedere a mantenere un registro delle transazioni contenente i tracciati delle richieste di autenticazione servite negli ultimi 24 mesi.
Il GW si fa carico di questo, mantenendo, oltre alle richieste di autenticazione e le asserzioni originali provenienti dai SP e dagli IDP, anche le versioni di queste che il GW stesso ha rielaborato per permettere una comunicazione compatibile tra le diverse entità.

2 - Classi di autenticazione

Nota funzionale - Nessuna modifica richiesta

Nella richiesta di autenticazione SAML che il SP invia al GW, non cambiano le classi di autenticazione (authentication context class, vedi [SAMLAuthContext] sez. 3) che il SP può definire tra quelli attesi:

- urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
  (LoA2 dell'ISO-IEC 29115)
- urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword
  (LoA3 dell'ISO-IEC 29115)
- urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard
  (LoA4 dell'ISO-IEC 29115)

In ambito SPID, queste classi di autenticazione sono mappate, rispettivamente, nelle seguenti, che sono le classi estese in ambito SPID corrispondenti allo stesso Level Of Assurance dell'ISO-IEC 29115:

- urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL1
  (LoA2 dell'ISO-IEC 29115)
- urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL2
  (LoA3 dell'ISO-IEC 29115)
- urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL3
  (LoA4 dell'ISO-IEC 29115)

Sarà il GW che autonomamente eseguirà questo mapping, rendendo l'operazione trasparente per il SP.

Si ha dunque che il SP definisce nella medesima maniera il grado di robustezza delle credenziali richieste, utilizzando le seguenti classi di autenticazione, referenziate dagli elementi <AuthnContextClassRef>:

- urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
  Se il SP richiede questa classe di autenticazione e l'utente decide di autenticarsi presso un IDP SPID, il risultato è che il SP permette l'accesso a utenze con un livello 1 SPID.
- urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword
  Se il SP richiede questa classe di autenticazione e l'utente decide di autenticarsi presso un IDP SPID, il risultato è che il SP permette l'accesso a utenze con un livello 2 SPID.
- urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard
  Se il SP richiede questa classe di autenticazione e l'utente decide di autenticarsi presso un IDP SPID, il risultato è che il SP permette l'accesso a utenze con un livello 3 SPID.

Ciascuna di queste classi, indica in ordine di preferenza il contesto di autenticazione (atteso o effettivo) secondo alcune dimensioni di riferimento, quali per esempio i meccanismi di autenticazione con cui l'IDP può identificare l'utente.
L'elemento <RequestedAuthnContext> prevede un attributo "Comparison" con il quale indicare il metodo per stabilire il rispetto del vincolo sul contesto di abilitazione: i valori ammessi per questo attributo sono "exact", "minimum", "better", "maximum".
Nel caso dell'elemento <RequestedAuthnContext>, questa informazione si riflette sulle tipologie di meccanismi utilizzabili dall'IDP ai fini dell'autenticazione dell'utente.
L'IDP ha facoltà di utilizzare per l'autenticazione una classe di autenticazione con robustezza più alta rispetto a quelle risultanti dall'indicazione del richiedente mediante l'attributo Comparison.

Analogamente, nel caso di autenticazione avvenuta con successo, nell'asserzione che riceve il SP proveniente dal GW, il nodo xml <AuthnContextClassRef> indicante la classe di autenticazione effettivamente utilizzata, sarà valorizzato dal GW in maniera tale che per il SP non cambierà nulla rispetto alla situazione pregressa.
Per quanto riguarda invece l'attributo utente "authenticationMethod", verrà popolato dal GW in maniera tale da far capire eventualmente se è stato utilizzato un IDP SPID, e quale metodo di autenticazione è stato utilizzato.
Se l'autenticazione avviene presso un IDP SPID, l'asserzione che arriverà al SP sarà così caratterizzata:

1. se viene utilizzato il livello 1 SPID:
    a. il nodo xml <AuthnContextClassRef> sarà valorizzato con "urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport"
    b. l'attributo utente "authenticationMethod" sarà valorizzato con "Primo Livello SPID"
2. se viene utilizzato il livello 2 SPID:
    a. il nodo xml <AuthnContextClassRef> sarà valorizzato con "urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword"
    b. l'attributo utente "authenticationMethod" sarà valorizzato con "Secondo Livello SPID"
3. se viene utilizzato il livello 3 SPID:
    a. il nodo xml <AuthnContextClassRef> sarà valorizzato con "urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard"
    b. l'attributo utente "authenticationMethod" sarà valorizzato con "Terzo Livello SPID"

Per ulteriori dettagli sui diversi livelli delle credenziali SPID, si rimanda al documento [SPIDModalitàAttuative].

3 - “spidCode” come attributo identificativo

Eventuale modifica richiesta

L’attributo identificativo utilizzato in SPID si chiama “spidCode”.
Di conseguenza, se un’autenticazione avviene presso un IDP SPID, tra gli attributi utente che saranno presenti nell’asserzione ricevuta dal SP, comparirà anche l’attributo “spidCode”, e sarà l’attributo che identifica univocamente l’utente in ambito SPID.

Il valore dell’attributo spidCode è definito dalla seguente regola:
spidCode = <cod_idp><numero_unico>

dove:

- <cod_idp> è un codice composto da 4 lettere
- <numero_unico> è un codice alfanumerico composto da 10 caratteri univoco nel dominio del gestore delle identità.

Il SP deve quindi gestire i due possibili casi:

1. L’utente per autenticarsi utilizza un IDP integrato in SPID:
   a. tra gli attributi presenti nell’asserzione compare l’attributo “spidCode”.
   b. deve trattare l’attributo “spidCode” come l’attributo identificativo dell’utente, ai fini di tracciatura e gestione dell’utenza stessa.
2. L’utente per autenticarsi utilizza un IDP non integrato in SPID:
   a. tra gli attributi presenti nell’asserzione non compare l’attributo “spidCode”.
   b. deve trattare come attributo identificativo dell’utente quello concordato in fase di integrazione in FedERa (di solito “CodiceFiscale” o “IdUtente”), ai fini di tracciatura e gestione dell’utenza stessa.

<u>Note tecniche ulteriori sul kit di integrazione J2EE:</u>
Se il SP utilizza il kit J2EE di integrazione fornito da Lepida, vanno fatte le seguenti considerazioni:

1 - Nelle versioni precedenti alla 2.x del toolkit, nel deployment descriptor dell’applicazione è presente il parametro di contesto “identifyingAttribute” (valorizzato in maniera predefinita con “CodiceFiscale”) il cui valore indica il nome dell’attributo che viene letto nell’asserzione quando viene invocato il metodo *it.cefriel.icar.inf3.web.beans.AuthenticationSessionBean.getUserID().*

2 - Nelle versioni del toolkit successive alla 2.x, nel deployment descriptor dell’applicazione è stato aggiunto un parametro di contesto chiamato “spidIdentifyingAttribute” (valorizzato in maniera predefinita con “spidCode”).
Con l’introduzione di questo parametro di contesto, cambia il comportamento del metodo *it.cefriel.icar.inf3.web.beans.AuthenticationSessionBean.getUserID()*, il quale restituisce:

- il valore dell’attributo chiamato come il parametro di contesto “spidIdentifyingAttribute”, se viene eseguita l’autenticazione tramite un IDP SPID (e se l’attributo definito è presente nell’asserzione)
- il valore dell’attributo chiamato come il parametro di contesto “identifyingAttribute”, se viene eseguita l’autenticazione tramite un IDP non SPID

Detto questo, va comunque rammentato che non è strettamente necessario l'utilizzo del metodo *it.cefriel.icar.inf3.web.beans.AuthenticationSessionBean.getUserID()*, in quanto è comunque a disposizione il metodo *it.cefriel.icar.inf3.web.beans.AuthenticationSessionBean.getAttributesMap()* che restituisce una Java.Util.Map contenente tutti gli attributi presenti nell'asserzione, da cui si possono estrarre applicativamente tutti gli attributi utente presenti, identificativi e non.

4 - Attributi identificativi dell'utente

Eventuale modifica richiesta

Le identità digitali rilasciate all'utente dagli IDP SPID contengono obbligatoriamente il codice identificativo, gli attributi identificativi e almeno un attributo secondario, funzionale alla comunicazione tra il gestore di identità digitale e l'utente.
Per attributi identificativi si intendono nome, cognome, luogo, data di nascita, sesso, codice fiscale e gli estremi del documento di identità utilizzato al fine dell'identificazione.
Per attributi secondari si intendono il numero di telefono fisso o mobile, l'indirizzo di posta elettronica, domicilio fisico e digitale.

Altri attributi diversi da quelli identificativi e secondari attualmente rilasciati dagli IDP non sono più garantiti a seguito dell'autenticazione SPID.
E' necessario che il SP definisca il profilo del servizio, cioè l'elenco degli attributi necessari al servizio online.
Qui il manuale operatore per conoscere le modalità per gestire il profilo e i criteri secondo i quali permettere l'accesso al servizio online.
http://lepida.it/sites/default/files/u8/Contratti/federa/federa-manuale-operatore.pdf

5 - Gestione di una persona giuridica

Eventuale modifica richiesta

Gli IDP SPID possono gestire anche identità digitali associate ad un soggetto giuridico.
Le identità digitali associate a persone giuridiche rilasciate dagli IDP SPID contengono obbligatoriamente il codice identificativo, gli attributi identificativi e almeno un attributo secondario, funzionale alla comunicazione tra il gestore di identità digitale e l'utente.
Per attributi identificativi si intendono ragione sociale o denominazione sociale, sede legale, la partita iva.
Per attributi secondari si intende il numero di telefono fisso o mobile, l'indirizzo di posta elettronica, domicilio fisico e digitale.

6 - Gestione dei log

Eventuale modifica richiesta

I SP hanno l'obbligo di conservare per ventiquattro mesi le informazioni necessarie a imputare, alle singole identità digitali, identificate univocamente dal loro spidCode, le operazioni effettuate sui propri sistemi tramite SPID.

7 - SSO e gestione del Logout

Eventuale modifica richiesta

Il modello di gestione delle sessioni di autenticazione di differenzia a seconda del livello SPID con la quale viene instaurato un contesto di autenticazione.

Per il livello 1 SPID, per gli IDP SPID è ammessa l'instaurazione di una sessione di autenticazione ai fini di SSO (Single Sign On) della durata di mezz'ora.
Questo significa che se lo stesso utente si autentica presso un IDP SPID per accedere ad un SP integrato in SPID, se nell'arco di mezz'ora tenta di accedere ad un altro SP, e per farlo sceglierà di autenticarsi presso lo stesso IDP SPID con il quale si era autenticato precedentemente, quest'ultimo autenticherà automaticamente l'utente non chiedendo l'inserimento delle credenziali all'utente.

Per i livelli 2 e 3 SPID invece non è ammessa per gli IDP SPID l'instaurazione di una sessione di autenticazione ai fini di SSO.

Per quanto riguarda il logout, oltre a gestire autonomamente il termine della sessione applicativa all'interno del SP, nel caso in cui il SP prevede la possibilità di accesso per utenti con livello 1 SPID è obbligatoria l'implementazione della procedura di logout federa secondo le specifiche descritte all'url http://federazione.lepida.it/docs/federa-specifiche-logout.pdf.
Grazie a questa procedura il gateway fedERa si fa carico della riuscita del termine della sessione applicativa anche presso gli IDP (SPID e non), tramite il Single Logout Profile previsto dal protocollo SAML.

Se il SP invece prevede l'accesso solo per le utenze con livelli 2 e 3 SPID, il logout federato non è obbligatorio ma tuttavia consigliato.

8 - Gestione dei gateway locali

Modifica richiesta

Il gateway fedERa deve conoscere i metadata (livello di sicurezza, attributi, URL di Assertion Consumer Service, URL di accesso al servizio) di ogni servizio online ablitato ad utilizzare le interfacce di autenticazione SPID.
Qualora un Ente abbia predisposto un “servizio gateway” che permetta l’interfacciamento con fedERa e contestualmente comunichi con più applicazioni del proprio dominio, evitando l’interfacciamento diretto delle stesse con FedERa, è necessario modificare tale configurazione.

Nel caso di servizi SAML 2.0, esistono due possibilità:

- Interfacciare con fedERa i singoli servizi, comunicando a LepidaSpA i dati di integrazione degli stessi, compilando l’Allegato C previsto per l’attivazione di un servizio.
- Interfacciarsi come singolo Service Provider, prevedendo più servizi applicativi specificandoli sul file dei metadata, come nodi xml AttributeConsumingService. In questo caso, i singoli servizi dovranno inserire nella richiesta di autenticazione l’attributo "AttributeConsumingServiceIndex" specificato nel file metadata.
  (esempio: https://en.wikipedia.org/wiki/SAML_2.0#Authentication_Request_Protocol)

Nel caso di servizi People (SAML 1.1) non è più possibile prevedere questo scenario ed è necessario interfacciare con fedERa i singoli servizi distinti.