Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

spid

SPID – SISTEMA PUBBLICO PER L'IDENTITA' DIGITALE

Avviso nr 6
Data 29/07/2016

NOTE SUL DISPIEGAMENTO DI SPID PRESSO I GESTORI DEI SERVIZI

SOMMARIO

1 INTRODUZIONE

Il presente avviso ha lo scopo di fornire, attraverso un esempio rappresentativo, un riferimento per la configurazione dei sistemi afferenti ai gestori di servizi in ambito SPID, nel caso generale in cui questi siano enti il cui dispiegamento può essere distribuito geograficamente su vari siti di erogazione.

I formati previsti da SAML consentono di definire, nel file di configurazione (*metadata*) di un gestore di servizi (*service provider*), diversi punti di erogazione dei servizi (*assertionConsumerServer*). Questa flessibilità consentita dal SAML standard, recepita dal profilo di interoperabilità SPID, costituisce un elemento di strutturazione del file di configurazione che consente di evitare frammentazione nelle informazioni afferenti la stessa entità, con conseguente eliminazioni di ridondanze, semplificazione della manutenzione dei dati di configurazione e facilità nel dispiegamento dei sistemi.

2 ESEMPIO DI DISPIEGAMENTO DI UN GESTORE DI SERVIZI.

I siti di erogazione dei gestori dei servizi possono essere costituiti da nodi ospitanti singoli servizi oppure nodi dai quali vengono erogati una pluralità di servizi.

Un *nodo singolo* è un sistema finalizzato all'erogazione di un singolo servizio che integra al proprio interno componenti per la gestione dei profili utente e per la gestione degli accessi. Un esempio di nodo singolo potrebbe essere quello di un portale istituzionale o tematico.

Un *nodo cluster* è un sistema che mette a disposizione un insieme di servizi diversi. Il criterio di aggregazione di questi servizi può ad esempio essere basato sulla strutturazione interna dell'ente, esempio servizi erogati dallo stesso dipartimento oppure sulla responsabilità della gestione operativa dei servizi, esempio - nel caso di enti che si avvalgono di diversi fornitori – servizi erogati da uno stesso fornitore. La caratteristica di un *nodo cluster* è quella di avere un'infrastruttura condivisa per la gestione dei profili utente e per la gestione degli accessi, che operi come gateway unico verso i sistemi di autenticazione e di certificazione esterni.

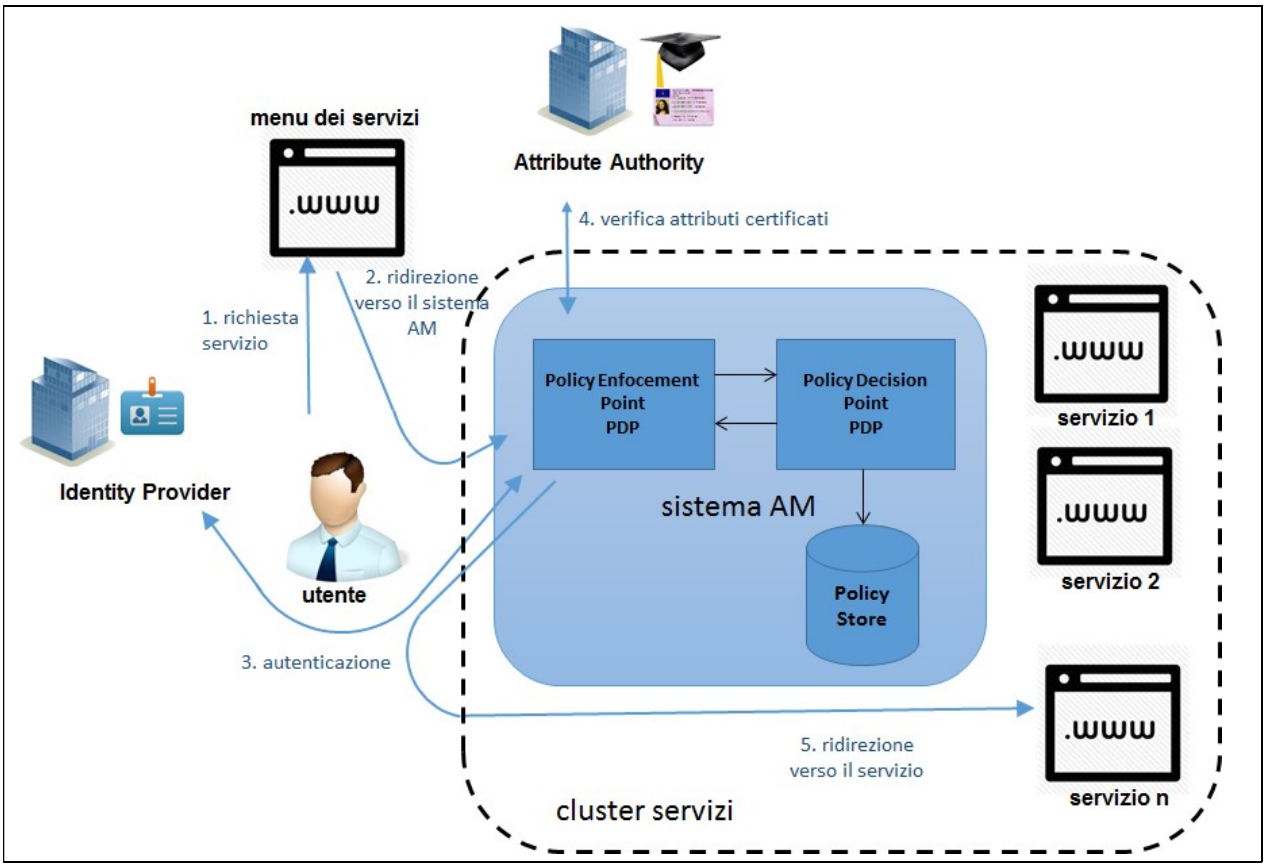

Figura 1 – Nodo cluster di servizi

In figura 1 è riportato una rappresentazione schematica auto esplicativa delle componenti di un nodo cluster, in cui sono riportati i passi relativi all'eccesso degli utenti ai servizi resi disponibili e le architetture classiche di riferimento relative ai sistemi di gestione degli accessi (access management)[1].

[1] la correlazione tra le risposte ed i relativi servizi di pertinenza potrà essere realizzata ad esempio mediante l'uso di identificatori univoci veicolati attraverso il parametro di *binding relaystate* oppure attraverso gli identificativi univoci dei messaggi SAML e dell'attributo inResposeTo.

In questo avviso si farà riferimento ad un ipotetico gestore dei servizi (*service provider*) il cui dispiegamento abbia le seguenti caratteristiche:

- presenza di tre diversi nodi di erogazione distribuiti geograficamente (siano essi nodi semplici o nodi cluster);
- servizi, orientati al cittadino, aggregati in due classi in base al set di attributi per i quali si chiede la certificazione contestualmente all'autenticazione dell'utente[2].

Classe di servizio	Elenco dei servizi	Attributi richiesti
Classe 1	servizio a, servizio b, …. servizio n	**family name;** **name;** **gender;** **dateOfBirth**
Classe 2	servizio k, servizio w, …. servizio z	**FiscalNumber;**

Tabella 1 – Ipotesi di dispiegamento

Per questo caso d'uso descriveremo contenuti e struttura dei file di configurazione (metadata).

La scelta di utilizzare un raggruppamento dei servizi per classi individuate dall'insieme di attributi richiesti, dando evidenza nel file di configurazione delle classi di servizi piuttosto che dei servizi stessi, consente di minimizzare la necessità di aggiornamento dei file di configurazione. Infatti, adottando questa modalità, la messa in produzione di un nuovo servizio afferente ad una classe e ad un nodo già specificati, non richiede alcun aggiornamento del file di configurazione.

2.1. METADATA INFOSET

Allo scopo di fornire autoconsistenza all'esposizione ed agevolare una rapida lettura del documento si riassumono in questo paragrafo i diversi parametri, previsti dallo standard SAML e recepiti dalle regole tecniche SPID, per la definizione dei file di configurazione delle entità operanti come *gestori di servizi*, quest'ultimi riferiti nella nomenclatura SAML con il termine *service provider*.

I file di configurazione sono indicati nella nomenclatura SAML con il termine *metadata*; ogni *service provider* secondo le regole tecniche SPID deve mettere a disposizione un solo *metadata*.

[2] con il criterio di classificazione adottato tutti i servizi appartenente ad una classe sono equivalenti ai fini della certificazione degli attributi operata dai gestori dell'identità a seguito dell'autenticazione dell'utente.

Il *metadata* dal punto di vista formale è un documento XML e nei contenuti riporta tutte le informazioni necessarie per l'interfacciamento dei sistemi di un *service provider* con quelli delle entità con essi interagenti (i gestori delle identità, nella nomenclatura SAML *Identity provider* e le autorità di attributo, nella nomenclatura SAML *attribute authority*). Si tratta dunque di un file di configurazione espresso in un linguaggio formale. Le informazioni necessarie per la configurazione dei sistemi sono contenute in determinati elementi e attributi previsti allo scopo dallo standard SAML. Si riportano di seguito, sinteticamente, tali elementi/attributi SAML con una breve illustrazione dei contenuti per essi previsti.

entityId — attributo SAML atto a definire una *uri* rappresentante l'identificatore univoco del *service provider*;

KeyDescriptor
Cardinalità: uno o più — elemento atto ad ospitare, nel sotto-elemento <*X509Certificate*>, il certificato da utilizzarsi per la verifica della firma del messaggio di richiesta di autenticazione; all'interno del *metadata* possono essere riportati uno o più elementi di questo tipo;

SingleLogoutService
Cardinalità: uno o più — elemento atto a riportare, attraverso gli attributi per esso previsti, le informazioni relative al servizio di *single logout* messo a disposizione dal *service provider*.

Attributi SAML previsti per l'elemento *SingleLogoutService*:

- *binding* — protocollo di trasporto da utilizzare;
- *location* — indirizzo *(url)* del servizio;

all'interno del *metadata* possono essere riportati uno o più elementi di questo tipo;

AssertionConsumerService
Cardinalità: uno o più — elemento atto a riportare, attraverso gli attributi per esso previsti, i riferimenti ad un nodo di erogazione dei servizi nel dominio dell'amministrazione, a cui i gestori delle identità (*identity provider*) devono far pervenire le risposte relative agli esisti dell'autenticazione (*SAMLResponse*). All'interno del *metadata* possono essere riportati uno o più elementi di questo tipo ad indicare l'unico o i diversi punti di erogazione dei servizi all'interno del dominio del gestore dei servizi (*service provider*). Ogni elemento presente è individuato da un indice che lo distingue dagli altri presenti; tale indice deve essere riportato nella richiesta di autenticazione (SAMLReq), mediante un attributo SAML (*AttributeConsumerServiceIndex*) appositamente previsto, al fine di selezionare l'indirizzo di risposta richiesto tra quelli elencati nel *metadata*.

attributi SAML previsti per l'elemento *AssertionConsumerService*:

index	indice associato all'i-esimo indirizzo di risposta;
isDefault	presente in un solo elemento atto ad evidenziare l'indirizzo di risposta nel caso non sia presente nella richiesta (*SAMLReq*) l' attributo SAML (*AssertionConsumerServiceIndex*) previsto per selezionarlo;
binding	protocollo di trasporto (*binding*) da utilizzare per il colloquio;
location	indirizzo *(url)* del punto di erogazione;

AttributeConsumingService
Cardinalità: uno o più

elemento atto a indicare, attraverso gli attributi per esso previsti, un set di attributi SPID di cui può essere richiesta la certificazione a seguito dell'avvenuta autenticazione. All'interno del *metadata* possono essere riportati uno o più elementi di questo tipo ad indicare l'unico o i diversi set di attributi SPID di cui si può chiedere la certificazione. Ogni elemento è caratterizzato da un indice che lo distingue dagli altri presenti; tale indice deve essere riportato nella richiesta di autenticazione (SAMLReq), mediante un attributo SAML (*AttributeConsumingServiceIndex*) appositamente previsto, al fine di selezionare tra quelli elencati nel metadata il set di attributi SPID richiesto; nel caso in cui il predetto attributo SAML fosse assente, a seguito della autenticazione non sarà certificato nessun attributo SPID

attributi/sottoelementi SAML previsti per l'elemento *AttributeConsumingService*:

index	indice associato all'i-esimo set di attributi SPID di cui si può fare richiesta;
ServiceName	elemento riportante l'identificatore associato al servizio che richiede lo specifico set di attributi SPID. Tale identificatore potrebbe, piuttosto che riferirsi ad un singolo servizio, corrispondente ad una categoria di servizi che richiedono tutti lo stesso set di attributi SPID;
RequestedAttribute *Cardinalità: uno o più*	elemento atto a indicare un attributo SPID appartenente al set. Possono essere riportati uno o più elementi di questo tipo uno per ogni attributo SPID appartenete all'insieme;

attributi SAML previsti per l'elemento *RequestedAttribute*:

Name identificatore dell'i-esimo attributo SPID richiesto (secondo la nomenclatura riportata nella tabella di attributi SPID pubblicata sul sito AgID);

Organization
Cardinalità: opzionale
Elemento opzionale riportante i riferimenti all'ente gestore dei servizi;

OrganizationName
Cardinalità: uno o più
denominazione ufficiale del gestore dei servizi;

OrganizationDisplayName
Cardinalità: uno o più
denominazione pubblica sul web del gestore dei servizi;

OrganizationURL
Cardinalità: uno o più
uri specificante una posizione in cui indirizzare un utente per ulteriori informazioni sul gestore dei servizi. Comunemente il sito istituzionale;

2.2. PARAMETRI DI CONFIGURAZIONE

Nella seguente tabella sono raccolte le informazioni necessarie per la configurazione del sistema in esame da riportare nel *metadata*.

Parametro di configurazione	Metadata infoset	Valore di attualizzazione element/attributi	Note
Identificatore ente	*entityId*	`https://denominazione.ente.it/sp`	Per garantire l'univocità si consiglia di usare il nome di dominio registrato dall'ente od un suo sottodominio
Denominazione	*OrganizationName*	`denominazione ente`	Denominazione dell'ente a che opera come gestore del servizio

Denominazione visibile sul web	*OrganizationDisplayName*	**denominazione ente**	Denominazione che l'ente che opera come gestore del servizio vuole rendere visibile in rete.
Indirizzo sito internet	*OrganizationURL*	**https://denominazione.ente.it**	
Indirizzo nodo di erogazione dei servizi nr1	*AssertionConsumerService* *index* *isDefault* *binding* *location*	*protocollo* **http-POST** *indirizzo* **https://denominazione.ente.it/nodo1/assertionConsumerService/POST** *protocollo* **http-redirect** *indirizzo* **https://denominazione.ente.it/nodo1/assertionConsumerService/redirect**	Ogni singolo nodo di servizi può supportare diversi binding (SAML). Nel caso di diversi tipi di binding supportati dallo stesso nodo saranno presenti nel *metadata* più elementi *AssertionConsumerService* ad esso corrispondenti (uno per ogni diverso tipo di binding)
Certificato verifica firma relativo al nodo 1	*KeyDescriptor* *KeyInfo* *X509Data* *X509Certificate*	**0kgUGll….. VBAs**	certificato X509 (codificato base64)
Indirizzo nodo di erogazione dei servizi nr2	*AssertionConsumerService* *index* *isDefault* *binding* *location*	*protocollo* **http-POST** *indirizzo* **https://denominazione.ente.it/nodo2/assertionConsumerService**	
Certificato verifica firma relativo al nodo 2	*KeyDescriptor* *KeyInfo* *X509Data* *X509Certificate*	**0kgUGll….. VBAs**	certificato X509 (codificato base64) nel caso specifico stesso del nodo 1

Indirizzo nodo di erogazione dei servizi nr3	*AssertionConsumerService* *index* *isDefault* *binding* *location*	*protocollo* **http-redirect** *indirizzo* **https://denominazione.ente.it/nodo3/assertionConsumerService**	
Certificato verifica firma relativo al nodo 3	*KeyDescriptor* *KeyInfo* *X509Data* *X509Certificate*	FZaz…….Mw8T	certificato X509 (codificato base64)
servizio di singleLogout		*protocollo* **SOAP** *indirizzo* **https://denominazione.ente.it/logoutService**	
Set di attributi classe 1	*AttributeConsumingService* *ServiceName* *RequestedAttribute*	**family name;** **name;** **gender;** **dateOfBirth;**	Corrispondenti a n servizi effettivi richiedenti lo stesso set di attributi, comunque dislocati nei nodi: servizio 1 servizio 2 ……. servizio n
Set di attributi classe 2	*AttributeConsumingService* *ServiceName* *RequestedAttribute*	**FiscalNumber;**	Corrispondenti a m servizi effettivi richiedenti lo stesso set di attributi, comunque dislocati nei nodi: servizio 1 servizio 2 ……. servizio m

Tabella 2 – Elenco dei parametri di configurazione

2.3. METADATA ESEMPIO

Il *metadata* corrispondente ai dati di configurazione esposti nella tabella 2 è quello riportato nel seguente listato.

```
<md:EntityDescriptor entityID="https://denominazione.ente.it/sp"
ID="_c75b48d19e23e90be40c4ab5eb331e7c4f04f73fb5" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
        <ds:Signature>…… </ds:Signature>
        <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
WantAssertionsSigned="true">
                <md:KeyDescriptor use="signing">
                        <ds:KeyInfo>
                                <ds:X509Data>
                                <ds:X509Certificate> 0kgUGll….. VBAs</ds:X509Certificate>
                                </ds:X509Data>
                        </ds:KeyInfo>
                </md:KeyDescriptor>
                <md:KeyDescriptor use="signing">
                        <ds:KeyInfo>
                                <ds:X509Data>
                                        <ds:X509Certificate> FZaz…….Mw8T</ds:X509Certificate>
                                </ds:X509Data>
                        </ds:KeyInfo>
                </md:KeyDescriptor>
                <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://denominazione.ente.it/diparttimento1/singleLogoutService"/>
                <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
format:transient</md:NameIDFormat>
        <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://denominazione.ente.it/nodo1/assertionConsumerService/POST" index="0"/>
        <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://denominazione.ente.it/nodo1/assertionConsumerService/redirect" index="1"/>
        <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://denominazione.ente.it/nodo2/assertionConsumerService " index="2"/>
        <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings: HTTP-Redirect"
Location="https://denominazione.ente.it/nodo3/assertionConsumerService " index="3"/>
                <md:AttributeConsumingService index="0">
                        <md:ServiceName xml:lang="it">serviziClasse1</md:ServiceName>
                        <md:RequestedAttribute Name="familyName"/>
                        <md:RequestedAttribute Name="name"/>
                        <md:RequestedAttribute Name="gender"/>
                        <md:RequestedAttribute Name="dateOfBirth"/>
                </md:AttributeConsumingService>
                <md:AttributeConsumingService index="1">
                        <md:ServiceName xml:lang="it"> serviziClasse2</md:ServiceName>
                        <md:RequestedAttribute Name="fiscalNumber"/>
                </md:AttributeConsumingService>
```

```
        </md:SPSSODescriptor>
        <md:Organization>
                <md:OrganizationName xml:lang="it"> denominazione ente
                </md:OrganizationName>
                <md:OrganizationDisplayName xml:lang="it"> denominazione ente
                </md:OrganizationDisplayName>
                <md:OrganizationURL xml:lang="it"> https://nome.ente.it</md:OrganizationURL>
        </md:Organization>
</md:EntityDescriptor>
```

Listato 1 – metadata associato ai parametri di configurazione riportati in tabella 1

2.4. FORMATO RICHIESTE

La presenza presso il *service provider* di più nodi di erogazione del servizio comporta la necessità di riportare nella richiesta di autenticazione (*SAMLReq*) l'indicazione del nodo a cui afferisce il servizio per il quale si chiede l'autenticazione dell'utente. Questo può essere fatto utilizzando l'attributo *AssertionConsumerServiceIndex* (scelta consigliata), come riportato nell'esempio di richiesta seguente:

```
<samlp:AuthnRequest ID="_69aa0f5e9025aa57ac57fce83554e75c50b1a67230" Version="2.0"
IssueInstant="2016-07-05T10:03:17Z" Destination="https://identity.provider.it/idp/SSOService"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" AssertionConsumerServiceIndex="2"
AttributeConsumingServiceIndex="1">
        <ds:Signature> …</ds:Signature>
        <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"/>
        <samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/>
        <samlp:RequestedAuthnContext Comparison="minimum">
                <saml:AuthnContextClassRef>https://www.spid.gov.it/SpidL1</saml:AuthnContextClassRef>
        </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

Listato 2 – Formato richiesta – prima variante

In alternative è possibile utilizzare la coppia di attributi *AssertionConsumerServiceURL* e *ProtocolBinding* riportanti rispettivamente l'indirizzo (url) ed il binding (protocollo di trasporto tra quelli definiti dal SAML v2.0) da utilizzare per la trasmissione delle risposte. In questo caso, si ricorda, la coppia dei valori riportati nella richiesta deve necessariamente corrispondere ad una coppia già prevista nel *metadata* (in un elemento di tipo *AssertionConsumerService*).

```
<samlp:AuthnRequest ID="_69aa0f5e9025aa57ac57fce83554e75c50b1a67230" Version="2.0"
IssueInstant="2016-07-05T10:03:17Z" Destination="https://identity.provider.it/idp/SSOService"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" AssertionConsumerServiceURL="
https://denominazione.ente.it/nodo2/assertionConsumerService"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
AttributeConsumingServiceIndex="1">
        <ds:Signature> …</ds:Signature>
        <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"/>
        <samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/>
        <samlp:RequestedAuthnContext Comparison="maximum">
                <saml:AuthnContextClassRef>https://www.spid.gov.it/SpidL1</saml:AuthnContextClassRef>
        </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

Listato 3 – Formato richiesta – seconda variante

Si noti in entrambe le richieste la presenza dell'attributo *AttributeConsumingServiceIndex* ad indicare la classe a cui appartiene il servizio, associata all'insieme di attributi per i quali viene richiesta la certificazione nell'ambito dell'asserzione prodotta a seguito del buon esito dell'autenticazione.