SPID – Sistema Pubblico di Identità Digitale

Informazioni utili per Service Provider

Bozza

Metadata

Nelle more della messa in produzione del Registro SPID, AgID farà da tramite tra i Gestori delle identità ed i Fornitori di servizi per quel che riguarda la comunicazione delle URL dei metadata.

Di seguito si riportano le URL dei gestori delle identità:

Infocert: https://identity.infocert.it/metadata/metadata.xml

Poste Italiane: http://posteid.poste.it/jod-fs/metadata/metadata.xml

Telecom Italia Trust Technology: https://login.id.tim.it/spid-services/MetadataBrowser/idp

I *fornitori di servizi* dovranno pubblicare i *metadata* di competenza comunicando il loro indirizzo all'Agenzia tramite e-mail, mettendo in cc i *Gestori dell'identità*.

I *metadata* dovranno essere prodotti secondo le specifiche definite nelle regole tecniche sintetizzate per comodità di lettura nella tabella in calce. Se il formato dei *metadata* non risulta compatibile con tali specifiche, non potranno essere dispiegati presso i sistemi dei gestori.

I *fornitori di servizi* dovranno verificare e garantire la correttezza dei valori in essi riportati e la stabilità dei contenuti a partire dalla momento della segnalazione.

Il dispiegamento presso i sistemi dei *Gestori delle identità* avverrà secondo l'ordine di comunicazione delle URL.

Metadata

LEGENDA: In **neretto** gli elementi, in *corsivo* gli attributi
+ 1 o più elementi
• 0 o più elementi
? 0 o 1

EntityDescriptor					
entityID					Identificatore univoco in formato UUID
SPSSODescriptor	protocolSupportEnumeration				URI indicanti i protocolli supportati dall'entità urn:oasis:names:tc:SAML:2.0:protocol
	WantAuthnRequestSigned				Valore booleano che impone ai service provider che fanno uso di questo Identity provider l'obbligo della firma delle richieste di autenticazione;
	KeyDescriptor	KeyInfo	X509Data	VALORE	Certificato della chiave pubblica utilizzato per la verifica della firma dei messaggi prodotti. Alberatura come da specifiche SAML
	AttributeConsumingService +	Index			Indice posizionale dell'elemento relativo all'i-esimo servizio richiamato dalla authReq mediante l'attributo AttributeConsumingServiceIndex dell'elemento <AuthnRequest>;
		ServiceName		VALORE	Riportante l'identificatore dell'i-esimo set minimo di attributi necessari[1] per l'autorizzazione all'acceso
		RequestedAttribute+		Name	Nome dell'attributo come riportato nella tabella pubblicata sul sito dell'Agenzia
	AssertionConsumerService +	Index			Può assumere valori unsigned a partire da 0
		isDefault?			Obbligatorio e posto a true per index=0 false se presente negli altri casi
		Location			Url endpoint del servizio per la ricezione delle richieste
		Binding			Valori assunti: "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST";
	SingleLogoutService+	Location			Url endpoint del servizio per la ricezione delle richieste
		Binding			Valori assunti: "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST";
Signature					Firma dei metadata secondo standard XML Signature
Organization	OrganizationName*	VALORE			Indicante un identificatore language-qualified dell'organizzazione a cui l'entità afferisce
	OrganizationDisplayName*	VALORE			
	OrganizationURL*	VALORE			Riportante in modalità language-qualified la url istituzionale dell'organizzazione

Il nodo che l'IDP legge per mostrare l'ente di chiamata è il seguente:

Organization	OrganizationName*	VALORE	Indicante un identificatore language-qualified dell'organizzazione a cui l'entità afferisce
	OrganizationDisplayName*	VALORE	Indicante un identificatore language-qualified dell'organizzazione a cui l'entità afferisce
	OrganizationURL*	VALORE	Riportante in modalità language-qualified la url istituzionale dell'organizzazione

Esempio:

```
<md:Organization>
 <md:OrganizationName xml:lang="it">Nome entità</md:OrganizationName>
 <md:OrganizationDisplayName xml:lang="it">Nome che si vuole mostare sulla maschera di login</md:OrganizationDisplayName>
 <md:OrganizationURL xml:lang="it">https://www.xxx.xx<md:OrganizationURL>
</md:Organization>
```

Sarà compito dell'IDP mostrare il contenuto. Normalmente OrganizationName è un nome esteso, mentre OrganizationDisplayName è un nome breve tipo:

OrganizationName = Nome Pubblica Amministrazione – Luogo
OrganizationDisplayName = Nome PA

Comunicazione metadata

I metadata vanno comunicati a:

Agid:
Francesco Tortorelli (AgID): tortorelli@agid.gov.it
Alfio Raia (AgID): raia@agid.gov.it
Umberto Rosini (AgID): rosini@agid.gov

Per conoscenza ai 3 Idp:
Michele De Lazzari (Infocert): michele.delazzari@infocert.it
Roberto Palumbo (Poste): r.palumbo@posteitaliane.it
Gianluca Tovo (Tim): gianluca.tovo@telecomitalia.it

Toolkit layout IDP

I toolkit grafici (bottone di accesso e json stringhe) sono reperibili su github:

https://github.com/italia-it

Più specificatamente:

https://github.com/italia-it/spid-sp-access-button
https://github.com/italia-it/spid-i18n

Bisogna fare riferimento, inoltre al documento sulle interfacce SPID:
http://www.spid.gov.it/tecdoc/agid-spid-gestioneinterfacce.bozza.pdf

Link utili

Documentazione e regole tecniche
http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/spid

Avvisi
http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/spid/avvisi

Linee guida interfacce SPID
http://www.spid.gov.it/tecdoc/agid-spid-gestioneinterfacce.bozza.pdf

Repository toolkit SPID
https://github.com/italia-it

Il Paese che cambia passa da qui.

Agenzia per l'Italia Digitale

Presidenza del Consiglio dei Ministri

agid.gov.it