Differenze tra SPID e SAML 2.0

Mauro Molinari - mmolinari@dcssrl.it
DCS Software e Servizi – ottobre 2021
Per Gruppo di Lavoro SPID/eIDAS/CIE – CTS IDEM

Riferimenti

- Documentazione SAML 2.0
  http://saml.xml.org/saml-specifications
- Regole tecniche SPID
  https://www.agid.gov.it/it/piattaforme/spid
- Avvisi SPID (aggiornamenti alle regole tecniche)
  https://www.agid.gov.it/it/piattaforme/spid/avvisi-spid

Premesse da regole tecniche SPID

1 REGOLE TECNICHE PER IL GESTORE DELL'IDENTITÀ DIGITALE

Le modalità di funzionamento del *Gestore dell'identità digitale*, nel seguito indicato anche con il termine tecnico *Identity provider*, dovranno essere quelle previste da SAML v2 per il profilo "*Web Browser SSO*" (cfr. [SAML-TechOv] sez. 4.1)

1.2.1. CARATTERISTICHE DELLE ASSERZIONI

L'*asserzione* prodotta dall'*Identity Provider* deve essere conforme allo standard SAML v2.0 (cfr. [SAML-Core]) e rispettare le condizioni di seguito indicate.

Il protocollo *AuthnRequest* previsto per l'*Identity Provider* deve essere conforme allo standard SAML v2.0 (cfr. [SAML-Core]) e rispettare le condizioni di seguito indicate.

1.2.2.1. AUTHNREQUEST

1.2.2.4. IDP METADATA

Le caratteristiche dell'*Identity provider* devono essere definite attraverso *metadata* conformi allo standard SAMLv2.0.(cfr. [SAML-Metadata]), e rispettare le condizioni di seguito indicate:

1.3.2. SP METADATA

Le caratteristiche del *Service Provider* devono essere definite attraverso metadata conformi allo standard SAMLv2.0.(cfr. [SAML-Metadata]), e rispettare le condizioni di seguito indicate:

Tuttavia

- Le regole tecniche SPID introducono alcuni vincoli aggiuntivi laddove SAML 2.0 lascia discrezionalità
- Le regole tecniche SPID introducono alcuni vincoli *in contrasto* con le specifiche SAML 2.0
- Lo strumento di verifica della conformità con SPID spid-saml-check introduce ulteriori restrizioni non menzionate dalle regole tecniche SPID
- L'ambiente di test spid-testenv2 (ora deprecato) introduceva ulteriori restrizioni non menzionate dalle regole tecniche e non verificate da spid-saml-check

  => *Fortunatamente ora abbiamo spid-saml-check basato su spid-sp-test che funge anche da ambiente di test*

Conseguenze

- Assai difficilmente un'implementazione industry-standard di SAML 2.0 può essere usata as-is per implementare SPID
- In assenza di implementazioni "pronte" per SPID per la tecnologia in uso, occorre diventare esperti SAML 2.0 per poter preparare estensioni, fork ed adattamenti delle implementazioni SAML 2.0 per renderle conformi a SPID

  => Aumento di tempo e costi per poter implementare la funzionalità "Entra con SPID" sul proprio applicativo (richieste skill che vanno oltre gli obbiettivi di business)

Vincoli aggiuntivi: Response.Issuer obbligatorio

https://github.com/italia/spid-saml-check/issues/141 (correlato)

- SAML 2.0 Core, sez. 3.2.2 (StatusResponseType, da cui Response eredita)

1566 <saml:Issuer> [Optional]
1567 Identifies the entity that generated the response message. (For more information on this element, see
1568 Section 2.2.5.)

- Regole tecniche SPID, sez. 4.1.2.2 (Response)

- deve essere presente l'elemento <**Issuer**> a indicare l'*entityID* dell'entità emittente, cioè l'*Identity Provider* stesso; L'attributo format deve essere omesso o assumere valore "*urn:oasis:names:tc:SAML:2.0:nameid-format:entity*";

Vincoli aggiuntivi: Issuer.Format obbligatorio

https://github.com/italia/spid-regole-tecniche/issues/51

- SAML 2.0 Core, sez. 2.2.5 (Name Identifiers)

> 522 **2.2.5 Element <Issuer>**
>
> 523 The <Issuer> element, with complex type **NameIDType**, provides information about the issuer of a
> 524 SAML assertion or protocol message. The element requires the use of a string to carry the issuer's name,
> 525 but permits various pieces of descriptive data (see Section 2.2.2).
>
> 526 Overriding the usual rule for this element's type, if no `Format` value is provided with this element, then the
> 527 value `urn:oasis:names:tc:SAML:2.0:nameid-format:entity` is in effect (see Section 8.3.6).

- Regole Tecniche SPID , sez. 1.2.1 (Assertion)

> - deve essere presente l'elemento <**Issuer**> a indicare l'*entityID* dell'*Identity Provider* emittente (attualizzato come l'attributo ***entityID*** presente nei corrispondenti IdP *metadata*) con l'attributo ***Format*** riportante il valore "*urn:oasis:names:tc:SAML:2.0:nameid-format:entity*";

- Regole Tecniche SPID, sez. 1.2.2.1 (AuthnRequest)

> - deve essere presente l'elemento <**Issuer**> attualizzato come l'attributo ***entityID*** riportato nel corrispondente SP *metadata*, a indicare l'identificatore univoco del *Service Provider* emittente. L'elemento deve riportare gli attributi:
>   - ***Format*** fissato al valore "*urn:oasis:names:tc:SAML:2.0:nameid-format:entity*";

- Tuttavia (!!!), Regole Tecniche SPID, sez. 1.2.2.2 (Response)

> - deve essere presente l'elemento <**Issuer**> a indicare l'*entityID* dell'entità emittente, cioè l'*Identity Provider* stesso; L'attributo format deve essere omesso o assumere valore "*urn:oasis:names:tc:SAML:2.0:nameid-format:entity*";

Vincoli aggiuntivi: Issuer.Format obbligatorio (continua)

https://github.com/italia/spid-regole-tecniche/issues/51

- Avviso SPID 3, sez. 2.1 (LogoutRequest)

> - l'elemento <**Issuer**> attualizzato come l'attributo *entityID* riportato nel corrispondente *metadata*, a indicare l'identificatore univoco dell'entità (*gestore delle identità* o *fornitori di servizi*) emittente. L'elemento deve riportare gli attributi:
>   - ***Format f***issato al valore "*urn:oasis:names:tc:SAML:2.0:nameid-format:entity*";

- Avviso SPID 3, sez. 2.2 (LogoutResponse)

> - deve essere presente l'elemento <**Issuer**> a indicare l'*entityID* dell'entità emittente; L'elemento deve riportare gli attributi:
>   - ***Format*** fissato al valore "*urn:oasis:names:tc:SAML:2.0:nameid-format:entity*";

- Analoghi vincoli imposti dalle Regole Tecniche SPID nell'ambito delle Attribute Authority (per Assertion, sez. 2.2.1, AttributeQuery, sez. 2.2.2 e Response, sez. 2.2.2.2)

Vincoli aggiuntivi: Assertion.Subject.NameID.NameQualifier obbligatorio

- Regole Tecniche SPID, sez. 1.2.1 (Assertion)

> - deve essere presente l'elemento <**Subject**> a referenziare il soggetto che si è autenticato in cui devono comparire:
>   - l'elemento <**NameID**> atto a qualificare il soggetto dell'asserzione, in cui sono presenti i seguenti attributi:
>   - ***Format*** che deve assumere il valore "*urn:oasis:names:tc:SAML:2.0:nameid-format:transient*" (cfr. SAMLCore, sez. 8.3);
>   - ***NameQualifier*** che qualifica il dominio a cui afferisce tale valore (URI riconducibile all'*Identity Provider* stesso);

- SAML 2.0 Core, sez. 8.3.8 (Attribute Name Format Identifiers)

> 3357 **8.3.8 Transient Identifier**
>
> 3358 **URI:** `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`
>
> 3359 Indicates that the content of the element is an identifier with transient semantics and SHOULD be treated
> 3360 as an opaque and temporary value by the relying party. Transient identifier values MUST be generated in
> 3361 accordance with the rules for SAML identifiers (see Section 1.3.4), and MUST NOT exceed a length of
> 3362 256 characters.
>
> 3363 The `NameQualifier` and `SPNameQualifier` attributes MAY be used to signify that the identifier
> 3364 represents a transient and temporary pair-wise identifier. In such a case, they MAY be omitted in
> 3365 accordance with the rules specified in Section 8.3.7.

Vincoli aggiuntivi: Assertion.Subject.NameID.NameQualifier obbligatorio (continua)

- SAML 2.0 Core, sez. 8.3.7, richiamata dalla precedente

> 3326 The element's `NameQualifier` attribute, if present, MUST contain the unique identifier of the identity
> 3327 provider that generated the identifier (see Section 8.3.6). It MAY be omitted if the value can be derived
> 3328 from the context of the message containing the element, such as the issuer of a protocol message or an
> 3329 assertion containing the identifier in its subject. Note that a different system entity might later issue its own
> 3330 protocol message or assertion containing the identifier; the `NameQualifier` attribute does not change in
> 3331 this case, but MUST continue to identify the entity that originally created the identifier (and MUST NOT be
> 3332 omitted in such a case).

=> richiedere che l'identificatore sia transient è ragionevole, obbligare l'Identity Provider a specificare il NameQualifier è ridondante. Inoltre, se proprio dev'essere specificato, dovrebbe essere uguale all'entity ID dell'IdP (non un ad "URI riconducibile all'IdP").

Vincoli in contrasto: valore di AuthnRequest.Destination

https://github.com/italia/spid-regole-tecniche/issues/20

- SAML 2.0 Bindings, sez. 3.4.5.2 (HTTP Redirect Binding)

> 661 If the message is signed, the `Destination` XML attribute in the root SAML element of the protocol
> 662 message MUST contain the URL to which the sender has instructed the user agent to deliver the
> 663 message. The recipient MUST then verify that the value matches the location at which the message has
> 664 been received.

- SAML 2.0 Bindings, sez. 3.5.5.2 (HTTP POST Binding)

> 843 If the message is signed, the `Destination` XML attribute in the root SAML element of the protocol
> 844 message MUST contain the URL to which the sender has instructed the user agent to deliver the
> 845 message. The recipient MUST then verify that the value matches the location at which the message has
> 846 been received.

- l'attributo ***Destination***, a indicare l'indirizzo (URI reference) dell'*Identity provider* a cui è inviata la richiesta, come risultante nell'attributo ***entityID*** presente nel metadata IdP dell'*Identity Provider* a cui viene inviata la richiesta;

Per limitare l'impatto del conflitto sulle implementazioni, si richiede agli identity provider SPID di supportare l'attributo *Destination* come descritto in entrambe le definizioni.

Vincoli in contrasto: AuthnRequest.Issuer.NameQualifier obbligatorio

https://github.com/italia/spid-regole-tecniche/issues/15

- SAML 2.0 Core, sez. 8.3.6 (Attribute Name Format Identifiers)

> **8.3.6 Entity Identifier**
>
> **URI:** `urn:oasis:names:tc:SAML:2.0:nameid-format:entity`
>
> Indicates that the content of the element is the identifier of an entity that provides SAML-based services (such as a SAML authority, requester, or responder) or is a participant in SAML profiles (such as a service provider supporting the browser SSO profile). Such an identifier can be used in the `<Issuer>` element to identify the issuer of a SAML request, response, or assertion, or within the `<NameID>` element to make assertions about system entities that can issue SAML requests, responses, and assertions. It can also be used in other elements and attributes whose purpose is to identify a system entity in various protocol exchanges.
>
> The syntax of such an identifier is a URI of not more than 1024 characters in length. It is RECOMMENDED that a system entity use a URL containing its own domain name to identify itself.
>
> The `NameQualifier`, `SPNameQualifier`, and `SPProvidedID` attributes MUST be omitted.

- Regole Tecniche SPID, sez. 1.2.2.1 (AuthnRequest)

> - deve essere presente l'elemento **<Issuer>** attualizzato come l'attributo ***entityID*** riportato nel corrispondente SP *metadata*, a indicare l'identificatore univoco del *Service Provider* emittente. L'elemento deve riportare gli attributi:
>   - ***Format*** fissato al valore "*urn:oasis:names:tc:SAML:2.0:nameid-format:entity*";
>   - ***NameQualifier*** che qualifica il dominio a cui afferisce tale valore (URI riconducibile al *Service Provider* stesso);

- Tuttavia, NameQualifier non viene vincolato per Assertion.Issuer (sez. 1.2.1) e Response.Issuer (sez. 1.2.2.2)!!!

Vincoli in contrasto: LogoutResponse.Status.StatusCode.Value in caso di partial logout

https://github.com/italia/spid-regole-tecniche/issues/17

- Avviso SPID 3, sez. 2 (descrizione del processo di logout)

> Viceversa nel caso in cui si verificasse una condizione di *partial logout* il *gestore dell'identità,* se in condizione di poterlo fare, dovrà notificare tale esito al *fornitore di servizi* richiedente, riportando nella *response* (cfr par. 2.2) i seguenti *status code*:
>
> status code: *urn:oasis:names:tc:SAML:2.0:status:Requester*
>
> sub status: *urn:oasis:names:tc:SAML:2.0:PartialLogout*

- SAML 2.0 Core, sez. 3.7.3.2 (LogoutRequest processing rules)

> If the session authority successfully terminates the principal's session with respect to itself, then it MUST respond to the original requester, if any, with a `<LogoutResponse>` message containing a top-level status code of `urn:oasis:names:tc:SAML:2.0:status:Success`. If it cannot do so, then it MUST respond with a `<LogoutResponse>` message containing a top-level status code indicating the error. Thus, the top-level status indicates the state of the logout operation only with respect to the session authority itself.
>
> The session authority SHOULD attempt to contact each session participant using any applicable/usable protocol binding, even if one or more of these attempts fails or cannot be attempted (for example because the original request takes place using a protocol binding that does not enable the logout to be propagated to all participants).
>
> In the event that not all session participants successfully respond to these `<LogoutRequest>` messages (or if not all participants can be contacted), then the session authority MUST include in its `<LogoutResponse>` message a second-level status code of `urn:oasis:names:tc:SAML:2.0:status:PartialLogout` to indicate that not all other session participants successfully responded with confirmation of the logout.

=> 1. errore di battitura / 2. lo status code top level dovrebbe indicare se il logout è avvenuto con successo sull'IdP, indipendentemente da quanto accade agli altri partecipanti / 3. urn:oasis:names:tc:SAML:2.0:status:Requester indica un errore imputabile al richiedente

Vincoli in contrasto: risposta a logout con sessione scaduta

- Avviso SPID 3, sez. 2 (descrizione del processo di logout)

> Viceversa nel caso in cui si verificasse una condizione di *partial logout* il *gestore dell'identità,* se in condizione di poterlo fare, dovrà notificare tale esito al *fornitore di servizi* richiedente, riportando nella *response* (cfr par. 2.2) i seguenti *status code*:
>
> status code: *urn:oasis:names:tc:SAML:2.0:status:Requester*
>
> sub status: *urn:oasis:names:tc:SAML:2.0:PartialLogout*
>
> Quest'ultimo comportamento deve essere assunto dal *gestore dell'identità* anche nel caso di una richiesta di *single logout* operata presso un *fornitore di servizi* e presentata dopo la scadenza della *sessione globale,* a seguito del *timeout* della relativa *sessione di autenticazione* o della esplicita chiusura della stessa da parte dell'utente.

- SAML 2.0 Core, sez. 3.7.3.2 (LogoutRequest processing rules)

> When a session authority receives a `<LogoutRequest>` message, the session authority MUST authenticate the sender. If the sender is a session participant to which the session authority provided an assertion containing an authentication statement for the current session, then the session authority SHOULD do the following in the specified order:

- SAML 2.0 Core, sez. 3.4.1.4 (AuthnRequest processing rules)

> If the responder is unable to authenticate the presenter or does not recognize the requested subject, or if prevented from providing an assertion by policies in effect at the identity provider (for example the intended subject has prohibited the identity provider from providing assertions to the relying party), then it MUST return a `<Response>` with an error `<Status>`, and MAY return a second-level `<StatusCode>` of `urn:oasis:names:tc:SAML:2.0:status:AuthnFailed` or `urn:oasis:names:tc:SAML:2.0:status:UnknownPrincipal`.

- SAML 2.0 Core, sez. 3.2.2.2 (StatusCodes)

> `urn:oasis:names:tc:SAML:2.0:status:AuthnFailed`
>
> The responding provider was unable to successfully authenticate the principal.

Vincoli in contrasto: indicizzazione degli AssertionConsumerService

https://github.com/italia/spid-regole-tecniche/issues/53

- Regole Tecniche SPID, sez. 1.3.2 (SP metadata)

> - deve essere presente almeno un elemento **<AssertionConsumerService>** indicante il servizio (in termini di URL e relativo binding "HTTP-POST") a cui contattare il *Service Provider* per l'invio di risposte SAML, riportanti i seguenti attributi:
>   - ***index*** che può assumere valori unsigned;
>   - ***Binding*** posto al valore "*urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST*"
>   - ***Location*** url endpoint del servizio per la ricezione delle risposte;
>
> In particolare il primo di questi elementi (o l'unico elemento riportato) deve obbligatoriamente riportare:
>
> - l'attributo ***index*** posto al valore 0;
> - l'atrtibuto ***isDefault*** posto al valore true;

- SAML 2.0 Metadata, sez. 2.2. (IndexedEndpointType, tipo d AssertionConsumerService)

  => Perché il primo deve avere index = 0? Perché il primo dev'essere il default? Perché dev'esserci indicato un defaul esplicitamente?

2.2.3 Complex Type IndexedEndpointType

The complex type **IndexedEndpointType** extends **EndpointType** with a pair of attributes to permit the indexing of otherwise identical endpoints so that they can be referenced by protocol messages. It consists of the following additional attributes:

`index` [Required]

A required attribute that assigns a unique integer value to the endpoint so that it can be referenced in a protocol message. The index value need only be unique within a collection of like elements contained within the same parent element (i.e., they need not be unique across the entire instance).

`isDefault` [Optional]

An optional boolean attribute used to designate the default endpoint among an indexed set. If omitted, the value is assumed to be `false`.

In any such sequence of like endpoints based on this type, the default endpoint is the first such endpoint with the `isDefault` attribute set to `true`. If no such endpoints exist, the default endpoint is the first such endpoint without the `isDefault` attribute set to `false`. If no such endpoints exist, the default endpoint is the first element in the sequence.

Vincoli aggiunti da spid-saml-check: AuthnRequest.NameIDPolicy.AllowCreate

https://github.com/italia/spid-saml-check/issues/138

- Regole Tecniche SPID, sez. 1.2.2.1 (AuthnRe

  - deve essere presente l'elemento <**NameIDPolicy**> avente il relativo attributo ***AllowCreate***, se presente, valorizzato a "*true*" e l'attributo ***Format*** valorizzato come "*urn:oasis:names:tc:SAML:2.0:nameid-format:transient*";

- SAML 2.0 Core, sez. 3.4.1.1 (AuthnReq

  2123 `AllowCreate` [Optional]
  2124 A Boolean value used to indicate whether the identity provider is allowed, in the course of fulfilling the
  2125 request, to create a new identifier to represent the principal. Defaults to "false". When "false", the
  2126 requester constrains the identity provider to only issue an assertion to it if an acceptable identifier for
  2127 the principal has already been established. Note that this does not prevent the identity provider from
  2128 creating such identifiers outside the context of this specific request (for example, in advance for a
  2129 large number of principals).

  => la richiesta originale che sia AllowCreate="true" appare sensata per SPID

- Tuttavia, Avviso SPID 5, correzioni alle Regole Tecniche

Pagina/riga	errata	corrige
8/19	**<AttributeConsumingService>**	**<AssertionConsumerService>**
9/37	il relativo attributo ***AllowCreate***, se presente, valorizzato a "*true*" e	*eliminare*

- La frase dunque diventa: "dev'essere presente l'elemento <NameIDPolicy> avente l'attributo Format valorizzato come "urn:oasis:names:tc:SAML:2.0:nameid-format:transient""
  => l'avviso 5 stabilisce l'assenza di qualunque vincolo sull'attributo (opzionale) AllowCreate, tuttavia il validatore impone all'SP che AllowCreate venga omesso

Vincoli aggiunti da spid-saml-check: attributi senza valore

https://github.com/italia/spid-saml-check/issues/137

- Le Regole Tecniche SPID non indicano in alcun modo come, all'interno di un AttributeStatement, un attributo senza valore debba essere indicato (es.: digitalAddress se l'utente non ha la PEC, ivaCode se la persona giuridica non ha la partita IVA, ecc.)
- SAML 2.0 Core distingue i tre tipici casi:
  - valore vuoto (sez. 2.7.3.1.1)
  - valore null (sez. 2.7.3.1.1)
  - attributo esistente, ma assenza di v
    (sez. 2.7.3.1)

1246 If a SAML attribute includes an empty value, such as the empty string, the corresponding
1247 `<AttributeValue>` element MUST be empty (generally this is serialized as `<AttributeValue/>`).
1248 This overrides the requirement in Section 1.3.1 that string values in SAML content contain at least one
1249 non-whitespace character.

1250 If a SAML attribute includes a "null" value, the corresponding `<AttributeValue>` element MUST be
1251 empty and MUST contain the reserved `xsi:nil` XML attribute with a value of "`true`" or "`1`".

1218 The meaning of an `<Attribute>` element that contains no `<AttributeValue>` elements depends on
1219 its context. Within an `<AttributeStatement>`, if the SAML attribute exists but has no values, then the
1220 `<AttributeValue>` element MUST be omitted. Within a `<samlp:AttributeQuery>`, the absence of
1221 values indicates that the requester is interested in any or all of the named attribute's values (see also
1222 Section 3.3.2.3).

1223 Any other uses of the `<Attribute>` element by profiles or other specifications MUST define the
1224 semantics of specifying or omitting `<AttributeValue>` elements.

- => negli esempi sopra indicati,
  in quale caso ricadiamo? In ogr
  caso, all'atto pratico, ha verame
  senso distinguere tra i tre casi,
  assenza di regole distinte di
  elaborazione di valore vuoto/null/assente?
- Il validatore vieta l'uso della rappresentazione per "assenza di valore" e ne impone il rifiuto da parte dell'SP

Vincoli aggiunti da spid-testenv2: AuthnRequest.ProviderName

https://github.com/italia/spid-testenv2/issues/341

- SAML 2.0 Core, sez. 3.4.1 (AuthnRequest

2080 `ProviderName` [Optional]
2081 Specifies the human-readable name of the requester for use by the presenter's user agent or the
2082 identity provider.

- Le Regole Tecniche SPID non fanno menzione alcuna di questo attributo, suggerendo che venga semplicemente ignorato

- Avviso 19 v4 (metadati per soggetti aggregatori)

  - `OrganizationDisplayName` (1 o più occorrenze nel caso multilingua) — Contiene la denominazione del soggetto riportato nel tag `OrganizationName`, eventualmente abbreviata e senza esplicitazione di acronimi (dal primo esempio soprastante, per la Società Nazionale S.p.A., "SAN").

    Durante la fase di autenticazione, gli IDP avvisano l'utente dell'invio degli attributi al soggetto indicato nel tag `OrganizationDisplayName`.

- Avviso 29 v3 (metadati per SP pubblici e privati)

  - `OrganizationDisplayName` (1 o più occorrenze) — Denominazione del SP – eventualmente in forma abbreviata (ad esempio senza esplicitare gli eventuali acronimi) e con il corretto utilizzo delle minuscole e maiuscole – così come riportata nell'estensione `commonName` del certificato elettronico del SP (esempio: "AgID").

    Durante la fase di autenticazione, gli IDP avvisano l'utente dell'invio degli attributi al SP, visualizzando il valore di questo tag per indicare il soggetto richiedente.

=> SPID impone agli IdP l'uso delle informazioni presenti nei metadati, piuttosto che quanto specificato in AuthnRequest.ProviderName, che sembra dunque essere semplicemente ignorato

=> tuttavia l'ambiente di test spid-testenv2 rifiutava richieste contenenti l'attributo AuthnRequest.ProviderName

GRAZIE
PER L'ATTENZIONE