IDEM METADATA PROFILE V1.0

Document:	IDEM Metadata Profile v1.0
Editor:	Maria Laura Mantovani
Identifier:	urn:mace:garr.it:idem:policy:metadataprofile
Version:	1.0
Last Modified:	2013-05-23
Status:	Final
License:	CC BY-NC-SA 3.0

1. Definizioni

Le parole[1] "DEVE" (in inglese "MUST" e "SHALL"), "NON DEVE" (in inglese "MUST NOT" e "SHALL NOT"), "RICHIESTO" (in inglese "REQUIRED"), "DOVREBBE" (in inglese "SHOULD"), "NON DOVREBBE" (in inglese "SHOULD NOT"), "RACCOMANDATO" (in inglese "RECOMMENDED"), "PUÒ" (in inglese "MAY") e "OPZIONALE" (in inglese "OPTIONAL"), usate in questo documento, devono essere interpretate secondo le definizioni presenti in RFC2119[2].

2. Introduzione

IDEM Metadata Profile definisce delle regole per coloro che, nella Federazione IDEM, producono metadati SAML (nei ruoli di registranti o aggregatori) e per i consumatori di metadati che partecipano alla Federazione IDEM.

L'adozione di questo profilo pone le basi per un interoperabilità scalabile ottenuta grazie al protocollo SAML.

Questo profilo è basato su "SAML V2.0 Metadata Interoperability Profile" [SAMLMetaIoP], su "Interoperable SAML 2.0 Web Browser SSO Deployment Profile" [SAML2int], su "Edugain Metadata Profile" [eduGMP] , su "SAML V2.0 Metadata Extensions for Login and Discovery User Interface" [SAMLMetaUI] e su "SAML 2 Profile for the Data Protection Code of Conduct" [SAML2MPDPCoC].

3. Autenticità e integrità dei metadati

I metadati DEVONO essere firmati digitalmente secondo le indicazioni di [SAMLMetaIoP] par 2.2.

[1] Se verbi, anche le relative coniugazioni delle stesso modo
[2] http://www.ietf.org/rfc/rfc2119.txt

4. Considerazioni sulla Sicurezza

Si riporta per maggiore chiarezza [SAMLMetaIoP] par 2.7.

I Metadati ottenuti tramite un trasporto insicuro DOVREBBERO essere firmati e DOVREBBERO scadere, in questo modo i consumatori sono obbligati a scaricarli nuovamente abbastanza frequentemente al fine di limitare i danni in caso di compromissione. Gli attributi `validUntil` e `cacheDuration` POSSONO essere appropriati per mitigare questa minaccia, a seconda del meccanismo di scambio.

In aggiunta, la distribuzione di metadati firmati senza una scadenza su un canale non fidato (ad es. pubblicati su un sito web pubblico) crea una esposizione. Un attaccante può corrompere il canale e sostituire un vecchio file di metadati contenente una chiave compromessa e procedere ad usare questa chiave insieme ad altri tipi di attacchi al fine di impersonare un sito. Fare ripetutamente scadere i Metadati (usando l'attributo `validUntil`) e ripubblicarli limita la finestra di esposizione allo stesso modo di una CRL.

Per queste ragioni si DEVE usare `validUntil` per limitare i danni da possibili compromissioni dei metadati.

Il Servizio IDEM GARR AAI, nel suo ruolo di aggregatore, aggiorna quotidianamente l'attributo `validUntil` con una finestra di validità di 5 giorni.

5. Requisiti per il produttore dei Metadati

Si riporta per maggiore chiarezza [SAMLMetaIoP] par 2.5.

Un frammento di metadati valido può iniziare con l'elemento `<md:EntityDescriptor>` oppure con l'elemento `<md:EntitiesDescriptor>`. Ogni elemento `<md:RoleDescriptor>` (od ogni elemento derivato ed ogni tipo derivato) che appare nel frammento di metadati DEVE essere conforme ai requisiti di questo profilo.

Tutte le chiavi crittografiche che il produttore riconosce come valide al tempo della produzione dei metadati DEVONO apparire all'interno dell'elemento "role", nella maniera descritta sotto nella sezione 4.1. Questo non include soltanto le chiavi di firma e di cifratura, ma anche tutte le chiavi usate per stabilire la mutua autenticazione con tecnologie quali TLS/SSL.

Le chiavi di firma ovvero per autenticare il trasporto, intese per usi futuri, POSSONO essere incluse come un modo per preparare la migrazione da una vecchia ad una nuova chiave (per esempio, key rollover). Una volta che sia passato il periodo di tempo necessario (tale periodo può essere dipendente da politiche specifiche della migrazione), la vecchia chiave può essere rimossa, al fine di completare il cambio. Chiavi scadute(che non vengono più usate da un'entità, per ragioni diverse dalla compromissione) DOVREBBERO essere rimosse una volta che il processo di migrazione ad una nuova chiave (o chiavi) è stato completato.

Le chiavi compromesse DEVONO essere rimosse dai metadati di una entità. Il produttore dei metadati NON DEVE fare affidamento sul fatto che il consumatore utilizzerà dei meccanismi online oppure offline per verificare la validità di una chiave (ad esempio una X.509 revocation lists, OCSP, etc.). Il momento esatto dal quale una compromissione si riflette nei metadati è lasciato ai requisiti delle parti coinvolte, al periodo di validità dei metadati (come dagli attributi a validUntil o cacheDuration) e dal meccanismo di scambio in uso.

5.1. Rappresentazione delle Chiavi

Si riporta per maggiore chiarezza [SAMLMetaIoP] par 2.5.1.

Ogni chiave inclusa nei metadati per un certo ruolo DEVE essere posta nel proprio elemento `<md:KeyDescriptor>`, con l'appropriato attributo "use" (si veda la sezione 2.4.1.1 di [SAML2MetaV2], come rivista da E62 in [SAML2Errata]) ed espressa usando l'elemento `<ds:KeyInfo>`.

Una o più delle seguenti rappresentazioni all'interno dell'elemento `<ds:KeyInfo>` DEVE essere presente:

- `<ds:KeyValue>`
- `<ds:X509Certificate>` (elemento figlio di `<ds:X509Data>`)

Nel secondo caso, è permesso solo un certificato. Se sono usate entrambe le forme, allora esse DEVONO rappresentare la stessa chiave.

Ogni altra rappresentazione nella forma di un elemento figlio di `<ds:KeyInfo>` (ad esempio `<ds:KeyName>`, `<ds:X509SubjectName>`, `<ds:X509IssuerSerial>`, etc.) PUÒ apparire, ma NON DEVE essere richiesto per identificare la chiave (sono solo suggerimenti).

Nel caso di un certificato X.509, non ci sono requisiti riguardo il contenuto del certificato tranne quello di contenere l'appropriata chiave pubblica. Specificamente, il certificato può essere scaduto, non ancora valido, trasportare estensioni critiche e non critiche, contrassegni d'uso, e contenere qualsiasi subject o emittente. L'uso di una struttura nel certificato è puramente una questione di convenienza di notazione nel comunicare una chiave e non ha significato semantico in questo profilo, a parte questo. Comunque è RACCOMANDATO che il certificato non sia scaduto.

5.2. Requisiti raccomandati da eduGAIN per la produzione dei Metadati

I requisiti raccomandati da eduGAIN [eduGMP] sono stati in alcuni casi resi più stringenti per la Federazione IDEM per aumentare la compatibilità tra le federazioni. Si riportano per maggiore chiarezza i paragrafi necessari.

Ogni file di metadati che fa uso di parti dei metadati pubblicati da eduGAIN DEVE includere un riferimento all'URL all'eduGAIN Metadata Terms of Use [ToU] oppure includere l'intero testo del ToU. Tale inclusione DEVE essere posta all'inizio del file di metadati e formattato come un commento XML.

Esempio:

```
<!—

Use of this metadata is subject to the Terms of Use at
http://www.edugain.org/policy/metadata-tou_1_0.txt

-->
```

L'elemento root dei metadata DEVE contenere

`<mdrpi:PublicationInfo>`, esso DEVE contenere

- `publisher`
- `<mdrpi:UsagePolicy>` con un link all'eduGAIN Metadata Terms of Use [ToU]

inoltre dovrebbe contenere uno tra gli attributi

- creationInstant o publicationID

Ogni elemento `<md:EntityDescriptor>` DEVE contenere

- `<mdrpi:RegistrationInfo>`, DEVE contenere
  - registrationAuthority

  che DOVREBBE contenere

  - registrationInstant
  - `<mdrpi:RegistrationPolicy>`.

registrationAuthority è l'identificativo univoco dell'autorità che ha registrato l'entità. È RACCOMANDATO che sia un URL che punta ad una pagina umanamente leggibile che descrive l'autorità registrante (ad es. la home page del registrante).

registrationInstant è l'istante in cui l'entità è stata registrata con l'autorità. Questo attributo DOVREBBE essere popolato per tutte le nuove entità. Tuttavia esso è opzionale perché l'istante di registrazione potrebbe non essere stato memorizzato dal registrante per le entità già esistenti.

`<mdrpi:RegistrationPolicy>` è la policy sotto la quale l'entità è stata registrata. La mancanza di questo elemento indica che il registrant non ha manifestato una policy di registrazione. Non indica che il registrante non possieda una policy di registrazione.

Ogni elemento `<md:EntityDescriptor>` DEVE[3] inoltre contenere l'elemento:

- `<md:Organization>` con valori in inglese per gli elementi
  - `<md:OrganizationName>`
  - `<md:OrganizationDisplayName>`
  - `<md:OrganizationURL>`

  e con valori in italiano per gli elementi

  - `<md:OrganizationName>`
  - `<md:OrganizationDisplayName>`
  - `<md:OrganizationURL>`

Per gli IdP `<md:OrganizationDisplayName>` DOVREBBE essere valorizzato con il nome dell'unità organizzativa, se applicabile.

Per gli SP il valore di `<md:OrganizationDisplayName>` DEVE essere in italiano "*Service_Name* erogato da *Organization*" e in inglese "*Service_Name* provided by *Organization*", dove *Service_Name* è il nome della risorsa erogata dall'SP e *Organization* coincide con il valore di `<md:OrganizationName>`.

[3] eduGAIN richiedeva solo SHOULD

In ogni caso (IdP e SP) <md:OrganizationDisplayName> DEVE contenere un valore adatto ad essere mostrato all'utente finale del servizio.

Per <md:OrganizationURL> si intende uno o più URI, qualificati secondo la lingua, che specificano una locazione verso la quale dirigere l'utente per informazioni addizionali. Si noti che la lingua si riferisce al contenuto del materiale alla locazione specificata.

Nei moduli cartacei IdPRR e RRR, in vigore precedentemente la pubblicazione di questo documento, l'informazione richiesta alla voce "Organization Site URL" era equivalente a quanto viene ora richiesto con <md:OrganizationURL>.

Se <md:EntityDescriptor> contiene uno di questi elementi:

- <md:IDPSSODescriptor>
- <md:AttributeAuthorityDescriptor>
- <md:SPSSODescriptor>

ognuno di questi DOVREBBE contenere gli elementi:

- <mdui:DisplayName> con un valore in inglese,
- <mdui:DisplayName> con un valore nelle lingue, diverse dall'inglese, supportate dal servizio,
- <mdui:Description> con un valore in inglese,
- <mdui:Description> con un valore nelle lingue, diverse dall'inglese, supportate dal servizio.

Ogniqualvolta I contenuti di un file di metadati vengono aggregati da sorgenti diverse, DOVREBBE essere usato l'elemento <mdrpi:PublicationPath> dove appropriato.

Per firmare I propri metadati un produttore di metadati DEVE usare una chiave privata RSA di almeno 2048 bits.

5.3. Estensioni dei Metadati per l'interfaccia utente in fase di Login e di Discovery

5.3.1. Informazioni relative all'Interfaccia Utente

Si riportano per maggiore chiarezza i paragrafi necessari di [SAMLMetaUI].

Gli elementi di estensione dell'interfaccia utente sono orientati a soddisfare i requisiti di presentazione all'utente delle entità rappresentate dai metadati SAML, tipicamente nel processo di discovery dell'identity provider oppure per rappresentare il servizio che si vuole accedere sull'interfaccia utente dell'identity provider. Le specifiche di tale presentazione e l'uso degli elementi che seguono non è ambito di questa specifica, ma le comunità d'uso DOVREBBERO stabilire delle linee guida e anche i requisiti prescrittivi a favorire la coerenza e la comprensibilità per gli utenti.

L'elemento contenitore <mdui:UIInfo xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui">, definito sotto, DEVE apparire

dentro l'elemento <md:Extensions> di un elemento di ruolo[4] (uno il cui tipo è basato su **md:RoleDescriptorType**). L'uso dell'elemento <mdui:UIInfo>, o qualsiasi altro elemento definito in questa sezione, al di fuori di quel contesto non è definito da questa specifica.

Questo elemento DEVE essere presente.

Infine, questo elemento NON DEVE apparire più di una volta entro un dato elemento <md:Extensions>.

5.3.2.Elemento <mdui:UIInfo>

L'elemento <mdui:UIInfo> contiene informazioni pertinenti (ma non specificamente limitate) alla creazione di interfacce utente per le operazioni di discovery/selezione dell'identity provider, autenticazione dell'utente, consenso nel rilascio degli attributi, ecc.

Sebbene questo elemento possa contenere qualsiasi numero dei seguenti elementi, in qualsiasi ordine, nella Federazione IDEM i seguenti elementi DEVONO essere presenti.

<mdui:DisplayName>

Un nome, localizzato in lingua inglese e nelle lingue, diverse dall'inglese, supportate dal servizio, per l'entità che opera nel ruolo contenitore. Tali nomi servono per permettere all'utente di distinguere ed identificare l'entità che agisce in un ruolo particolare. Il contenuto di questo elemento dovrebbe essere adatto ad essere usato nella costruzione di interfacce utente accessibili ai disabili. Per gli SP sarà il nome con cui il servizio è conosciuto. Per gli IDP, coinciderà con il valore di "<md:OrganizationDisplayName>".

Nei precedenti moduli cartacei IdPRR e RRR l'informazione ora recepita con <mdui:DisplayName> veniva richiesta alla voce "Service Name" .

<mdui:Description>

Una descrizione, localizzato in lingua inglese e nelle lingue, diverse dall'inglese, supportate dal servizio, per l'entità che opera nel ruolo contenitore lunga al massimo 100 caratteri. Sui sistemi che supportano un puntatore (ad esempio un mouse), il contenuto dell'elemento <mdui:Description> apparirà quando l'utente passa sopra il display name dell'SP o dell'IdP.

<mdui:InformationURL>

Una o più URL ad una locazione esterna di informazioni, localizzate nella lingua della pagina esterna (possibilmente in inglese e nella lingua supportata dal servizio), riguardanti l'entità che opera in un dato ruolo, adatte ad essere visualizzate dagli utenti. Il contenuto trovato a tale URL DOVREBBE fornire informazioni più complete rispetto a quelle fornite tramite l'elemento <mdui:Description>. In altre parole, l'URL di una pagina che descrive il servizio e il pubblico a cui esso è rivolto.

La pagina DEVE soddisfare quanto richiesto da NdP (Norme di Partecipazione) e specificato in ST (Specifiche Tecniche) nelle sezioni "Pagina associata all'IdP" e "Pagina associata alla risorsa".

[4] Nonostante la specifica generale, al momento attuale le Federazioni sono orientate ad utilizzare il tag <mdui:UIInfo solo per i ruoli di IDPSSODescriptor e SPSSODescriptor. In attesa di ulteriori precisazioni ci adeguiamo a questa convenzione.

Nel precedente modulo cartaceo IdPRR si utilizzava “IDP Web page URL” e nel RRR si utilizzava “Service URL” al posto di `<mdui:InformationURL>`.

`<mdui:PrivacyStatementURL>`

Una o più URL ad una locazione esterna di informazioni, localizzate nella lingua della pagina esterna (possibilmente in inglese e nella lingua supportata dal servizio), riguardante le pratiche relative alla privacy dell’entità che opera nel relativo ruolo. Tali dichiarazioni intendono fornire all’utente le informazioni riguardo a come verranno usati e gestiti i dati da parte dell’entità che agisce nel ruolo dato. In altre parole, l’URL della pagina web come richiesta da NdP (Norme di Partecipazione) e specificata in ST (Specifiche Tecniche) (ad es. user info, Privacy Policy).

Nei precedenti moduli cartacei IdPRR e RRR si utilizzava “Service Web page URL” al posto di `<mdui:PrivacyStatementURL>`.

Nella Federazione IDEM i seguenti elementi DOVREBBERO essere presenti:

`<mdui:Logo>`

Un’immagine logo, localizzato in lingua inglese e nelle lingue, diverse dall’inglese, supportate dal servizio, per l’entità che opera nel relativo ruolo[5].

Nella Federazione IDEM POSSONO essere presenti i seguenti elementi:

`<mdui:Keywords>`

Parole chiave, categorie ed etichette adatte per la ricerca e localizzate nelle diverse lingue per i relativi ruoli.

`<mdui:DiscoHints>`

Elemento contenitore, che deve essere posizionato nell’elemento `<md:Extensions>` di un elemento `<md:IDPSSODescriptor>`. Per maggiori info si veda [SAMLMetaUI].

5.4. Requisiti relativi agli Attributi

Per gli SP ogni elemento `<md:SPSSODescriptor>` PUÒ contenere:

[5] Requisiti riguardanti il logo:
– L’URL che individua il logo DEVE essere protetta con https.
– DOVREBBE essere fornito un logo di dimensioni approssimativamente 80px(larghezza) per 60px (altezza). Si PUÒ fornire anche un logo più grande, ma il rapporto tra le dimensioni DOVREBBE essere mantenuto (i loghi sono selezionati in base al rapporto tra le dimensioni).
– DOVREBBE essere fornito un logo di dimensioni 16px per 16px.
– I Loghi DOVREBBERO essere quadrati, per quanto possibile (1:1).
– I Loghi DOVREBBERO visualizzarsi bene anche se ridimensionati a 50×50 px. Ciò significa non usare troppi dettagli. Il testo dovrebbe essere grande quando la risoluzione è alta.
– I Loghi DOVREBBERO essere in formato PNG con sfondo trasparente.
– I Loghi DOVREBBERO apparire bene con sfondo bianco.
– I Loghi NON DOVREBBERO apparire male se ombreggiati con grigio al 20%.
– I Loghi DOVREBBERO riempire approssimativamente il 50% dell’immagine con del colore. Icone pesanti dovrebbero essere rese più leggere e loghi leggeri dovrebbero essere resi più pesanti. Ciò per avere un bilanciamento tra I loghi quando questi vengono mostrati in una lista.

- `<md:AttributeConsumingService>` nel quale si elencano tutti gli attributi richiesti da questo SP usando l'elemento `<md:RequestedAttribute>` con `isRequired="true"` per gli attributi obbligatori e `isRequired="false"` per gli attributi opzionali.

Se non si istanzia l'elemento `RequestedAttribute` è implicito che il servizio non richiede nessun attributo.

Gli SP DEVONO fornire gli elementi `RequestedAttribute` per descrivere gli attributi (e, opzionalmente, i valori richiesti) per tutti gli attributi che sono classificati come NECESSARI per poter avere accesso all'SP. Gli elementi `RequestedAttribute` DEVONO includere l'opzione `isRequired="true"` per indicare che l'attributo è NECESSARIO.

Se l'SP richiede solo uno, o alcuni, valore(i) particolare(i) per un certo attributo (ad es. eduPersonEntitlement="urn:mace:rediris.es:entitlement:wiki:tfemc2"), l'SP DEVE usare l'elemento `<saml:AttributeValue>` per indicare tale valore(i).

L'elemento `isRequired` viene usato per indicare se l'attributo è OBBLIGATORIO (NECESSARY) o OPZIONALE (CONSENT REQUIRED). `isRequired="true"` indica che l'attributo è OBBLIGATORIO. `isRequired="false"` o l'elemento `isRequired` non presente indica che l'attributo è OPZIONALE e pertanto deve essere richiesto il consenso.

Nel precedente modulo cartaceo RRR si utilizzava "URI1, …., URI6" al posto di `<md:RequestedAttribute>`.

5.5. Requisiti relativi ai Contatti

Ogni elemento `<md:EntityDescriptor>` DEVE contenere

- `<md:ContactPerson>` con `contactType="technical"`, il quale DEVE contenere
  - `<md:EmailAddress>` CHE DOVREBBE essere un indirizzo di un ruolo o di una lista e non un indirizzo personale.

In aggiunta PUÒ contenere una sequenza opzionale di elementi che identificano varie tipologie di contatti personali seguendo la sintassi definita in [SAMLMetaV2]. Le organizzazioni sono tenute considerare gli aspetti legati alla privacy, vista la natura pubblica dei Metadati.

6. Bibliografia

[SAMLMetaV2] Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf

[SAML2Errata] SAML Version 2.0 Errata 05 http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.html

[SAML2int] Interoperable SAML 2.0 Web Browser SSO Deployment Profile http://saml2int.org/profile/current

[SAMLMetaIoP] SAML V2.0 Metadata Interoperability Profile http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf

[eduGMP] Edugain Metadata Profile
http://www.geant.net/service/edugain/resources/Documents/eduGAIN%20Metadata %20profile.pdf

[SAMLMetaUI] SAML V2.0 Metadata Extensions for Login and Discovery User Interface http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/cs01/sstc-saml-metadata-ui-v1.0-cs01.pdf

[SAML2MPDPCoC] SAML 2 Profile for the Data Protection Code of Conduct
https://refeds.terena.org/index.php/SAML_2_Profile_for_the_Data_Protection_Code_of_Conduct

IDEM METADATA PROFILE V0.4

Document:	IDEM Metadata Profile v0.4
Editor:	Maria Laura Mantovani
Identifier:	urn:mace:garr.it:idem:policy:metadataprofile
Version:	0.4
Last Modified:	2013-02-15
Status:	Draft
License:	CC BY-NC-SA 3.0

1. Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT","SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119[6].

2. Introduction

The IDEM Metadata Profile defines rules for SAML metadata producers (acting in the role of a registrar or aggregator) and metadata consumers participating in the IDEM federation.

Adopting this profile lays the ground for scalable SAML interoperability.

This profile is based on SAML V2.0 Metadata Interoperability Profile [SAMLMetaIoP], on “Interoperable SAML 2.0 Web Browser SSO Deployment Profile” [SAML2int], on Edugain Metadata Profile [eduGMP] , on SAML V2.0 Metadata Extensions for Login and Discovery User Interface [SAMLMetaUI] and on SAML 2 Profile for the Data Protection Code of Conduct [SAML2MPDPCoC].

3. Metadata Genuine and Integrity

Metadata MUST be signed following instructions in [SAMLMetaIoP] par 2.2.

4. Security Considerations

The following text is shown for clarity ([SAMLMetaIoP] par 2.7).

Metadata obtained via an insecure transport should be both signed, and should expire, so that consumers are forced to refresh it often enough to limit the damage from compromised information. Either the `validUntil` or `cacheDuration` attribute may be appropriate to mitigate this threat, depending on the exchange mechanism.

[6] See http://www.ietf.org/rfc/rfc2119.txt

In addition, distributing signed metadata without an expiration over an untrusted channel (e.g., posting it on a public web site) creates an exposure. An attacker can corrupt the channel and substitute an old metadata file containing a compromised key and proceed to use that key together with other attacks to impersonate a site. Repeatedly expiring (using a `validUntil` attribute) and reissuing the metadata limits the window of exposure, just as a CRL does.

For these reasons, you MUST use `validUntil` to limit the damage from possible compromised metadata.

The Service IDEM GARR AAI, as an aggregator, daily updates the `validUntil` attribute with value of five days.

5. Metadata Producer Requirements

The following text is shown for clarity ([SAMLMetaIoP] par 2.5).

A conforming metadata instance may be rooted by either an `<md:EntityDescriptor>` or `<md:EntitiesDescriptor>` element. Any `<md:RoleDescriptor>` element (or any derived element or type) appearing in the metadata instance MUST conform to this profile's requirements.

Any and all cryptographic keys that are known by the producer to be valid at the time of metadata production MUST appear within that role's element, in the manner described below in section 2.5.1. This includes not only signing and encryption keys, but also any keys used to establish mutual authentication with technologies such as TLS/SSL.

Signing or transport authentication keys intended for future use MAY be included as a means of preparing for migration from an older to a newer key (i.e., key rollover). Once an allowable period of time has elapsed (with this period dependent on deployment-specific policies), the older key can be removed, completing the change. Expired keys (those not in use anymore by an entity, for reasons other than compromise) SHOULD be removed once the rollover process to a new key (or keys) has been completed.

Compromised keys MUST be removed from an entity's metadata. The metadata producer MUST NOT rely on the metadata consumer utilizing online or offline mechanisms for verifying the validity of a key (e.g., X.509 revocation lists, OCSP, etc.). The exact time by which a compromise is reflected in metadata is left to the requirements of the parties involved, the metadata's validity period (as defined by a validUntil or cacheDuration attribute), and the exchange mechanism in use.

5.1. Key Representation

The following text is shown for clarity ([SAMLMetaIoP] par 2.5.1).

Each key included in a metadata role MUST be placed within its own `<md:KeyDescriptor>` element, with the appropriate use attribute (see section 2.4.1.1 of [SAML2MetaV2], as revised by E62 in [SAML2Errata]), and expressed using the `<ds:KeyInfo>` element.

One or more of the following representations within a `<ds:KeyInfo>` element MUST be present:

- `<ds:KeyValue>`
- `<ds:X509Certificate>` (child element of `<ds:X509Data>`)

In the case of the latter, only a single certificate is permitted. If both forms are used, then they MUST represent the same key.

Any other representation in the form of a `<ds:KeyInfo>` child element (such as `<ds:KeyName>`, `<ds:X509SubjectName>`, `<ds:X509IssuerSerial>`, etc.) MAY appear, but MUST NOT be required in order to identify the key (they are hints only).

In the case of an X.509 certificate, there are no requirements as to the content of the certificate apart from the requirement that it contain the appropriate public key. Specifically, the certificate may be expired, not yet valid, carry critical or non-critical extensions or usage flags, and contain any subject or issuer. The use of the certificate structure is merely a matter of notational convenience to communicate a key and has no semantics in this profile apart from that. However, it is RECOMMENDED that certificates be unexpired.

5.2. eduGAIN Metadata Producer Requirements

eduGAIN requirements [eduGMP] have been made in some cases more strict to increase compatibility between the federations. Here are shown for clarity the involved paragraphs.

Any metadata file which makes use of parts of metadata published by eduGAIN MUST include either a reference with a URL to the eduGAIN Metadata Terms of Use [ToU] or the entire ToU text. It MUST be placed at the top of the metadata file formatted as an XML comment.

Example:

```
<!—
Use of this metadata is subject to the Terms of Use at
http://www.edugain.org/policy/metadata-tou_1_0.txt
-->
```

The metadata root element MUST contain

`<mdrpi:PublicationInfo>`, it MUST contain

- `publisher`
- `<mdrpi:UsagePolicy>` with a link to the eduGAIN Metadata Terms of Use [ToU]

it SHOULD contain one of the attributes

- creationInstant or publicationID

Each `<md:EntityDescriptor>` element MUST contain

- `<mdrpi:RegistrationInfo>`, it MUST contain
  - registrationAuthority

  it SHOULD contain
  - registrationInstant
  - `<mdrpi:RegistrationPolicy>`.

registrationAuthority is the unique identifier of the authority that registered the entity. It is RECOMMENDED that this be a URL that resolves to a human readable page describing the registrar authority (e.g., the registrar's home page).

registrationInstant is The instant the entity was registered with the authority. This attribute SHOULD be populated for all newly registered entities but is optional because the registration instant may not have been tracked by the registrar for existing entities.

<mdrpi:RegistrationPolicy> is the policy under which the entity was registered. The lack of this element indicates that the registrar has not disclosed its registration policy. It does not indicate that the registrar lacks a registration policy.

It MUST[7] contain the element:

- <md:Organization> with values in English for the elements
  - <md:OrganizationName>
  - <md:OrganizationDisplayName>
  - <md:OrganizationURL>

  and with values Italian for the elements
  - <md:OrganizationName>
  - <md:OrganizationDisplayName>
  - <md:OrganizationURL>

For IdPs the value for the element <md:OrganizationDisplayName> SHOULD be the unit organization name, if applicable.

For SPs the value for the element <md:OrganizationDisplayName> MUST be "*Service_Name* erogato da *Organization*" in Italian, and "*Service_Name* provided by *Organization*" in English, where *Service_Name* is the name of the resource provided by the SP and *Organization* is the same value of <md:OrganizationName>.

In both cases (IdP and SP) <md:OrganizationDisplayName> MUST contain a value suitable to be shown to the end user of the service.

The element <md:OrganizationURL> means one or more language-qualified URIs that specify a location to which to direct a user for additional information. Note that the language qualifier refers to the content of the material at the specified location.

In the IdPRR and RRR paper forms, in force before the publication of this document, the information requested under "Organization Site URL" was equivalent to what is now required with <md:OrganizationURL>.

If the <md:EntityDescriptor> contains one of these elements:

- <md:IDPSSODescriptor>
- <md:AttributeAuthorityDescriptor>
- <md:SPSSODescriptor>

each one of them SHOULD contain the elements:

- <mdui:DisplayName> with a value in English

[7] eduGAIN required only SHOULD

- <mdui:DisplayName> with a value in the languages that the service supports, other than English
- <mdui:Description> with a value in English
- <mdui:Description> with a value in the languages that the service supports, other than English

Whenever contents of a metadata file gets aggregated from multiple sources, the <mdrpi:PublicationPath> element SHOULD be used where appropriate.

For signing its metadata, a metadata producer MUST use an RSA private key of at least 2048 bits.

5.3. Metadata Extensions for Login and Discovery User Interface

5.3.1. User Interface Information

Hereafter required paragraphs, related to [SAMLMetaUI], are shown for clarity.

The user interface extension elements are oriented towards the requirements of user agent presentation of entities represented by SAML metadata, typically as part of identity provider discovery or representing services requesting information from a user's identity provider. The specifics of such presentation and the use of the elements that follow is not in scope for this specification, but communities of use SHOULD establish guidelines and even prescriptive requirements to encourage consistency and understandability for users.

The <mdui:UIInfo xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui"> container element, defined below, MUST appear within the <md:Extensions> element of a role element[8] (one whose type is based on **md:RoleDescriptorType**). The use of the <mdui:UIInfo> element, or any other element defined in this section, outside of that context is not defined by this specification.

This element MUST appears.

Finally, this element MUST NOT appear more than once within a given <md:Extensions> element.

5.3.2. Element <mdui:UIInfo>

The <mdui:UIInfo> element contains information which pertains to (but is not specifically limited to) the creation of user interfaces for tasks such as identity provider selection/discovery, user authentication, attribute release consent, etc.

Although this element may contain any number of the following elements, in any order, in IDEM Federation the following elements MUST be present.

<mdui:DisplayName>
A localized name for the entity operating in the containing role. Such names are meant to allow a

[8] Despite of the general specification, currently Federations are directed to use the <mdui: UIInfo only for the IDPSSODescriptor and SPSSODescriptor roles. Pending further clarification we accept this convention.

user to distinguish and identify the entity acting in a particular role. The content of this element should be suitable for use in constructing accessible user interfaces for those with disabilities. For SPs, the name by which the service is known. For IDPs, <md:OrganizationDisplayName>.

In the previous paper forms, IdPRR and RRR, the information now implemented by <mdui:DisplayName> was required in the "Service Name" field.

<mdui:Description>

A localized description of the entity operating in the containing role, of 100 char maximum length. On systems that support a pointing device (such as a mouse), the content of the <mdui:Description> element will pop up when the user hovers over the IdP or the SP display name.

<mdui:InformationURL>

A URL to external location for localized information about the entity acting in a given role meant to be viewed by users. The content found at the URL SHOULD provide more complete information than what would be provided by the <mdui:Description> element. In other words, the URL of a page which describes the service and its intended audience.

The page MUST satisfy what requested by NdP (Norme di Partecipazione) and specified in ST (Specifiche Tecniche) in sections “Page associated with the IdP”and “Page associated with the resource”.

In the previous paper form, IdPRR, the information now implemented by <mdui:InformationURL> was required in the “IDP Web page URL” field.

<mdui:PrivacyStatementURL>

A URL to localized information about the privacy practices of the entity operating in the containing role. Such statements are meant to provide a user with information about how information will be used and managed by the entity acting in a given role. In other words, the URL of the web page as requested by NdP (Norme di Partecipazione) and specified in ST (Specifiche Tecniche) (eg. user info, Privacy Policy).

In the previous paper forms, IdPRR and RRR, the information now implemented by <mdui:PrivacyStatementURL> was required in the “Service Web page URL” field.

IDEM Federation metadata SHOULD contain the following elements:

<mdui:Logo>

A localized logo image for the entity operating in the containing role[9].

[9] Logo requirements:
Shibboleth - The URL specifying the logo must be https protected.
Shibboleth - One logo should be provided of size approximately 80px(width) by 60px (height). A larger logo may be provided but the aspect ratio should be maintained (logos are selected based on apsect ration).
Shibboleth - One logo should be provided of size 16px by 16px.
Shibboleth - Logo backgrounds should be transparent.
DiscoJuice - Logos SHOULD be as square as possible (1:1).
DiscoJuice - Logos SHOULD look nice when resized down to 50×50 px. This means, do not use to much details. Text much be large when the resolution is high.
DiscoJuice - Logos SHOULD be in PNG format with transparent background.
DiscoJuice - Logos SHOULD look good on white background.
DiscoJuice - Logos SHOULD NOT look bad on 20% grey.

IDEM Federation metadata MAY contain the following elements:

`<mdui:Keywords>`
: Localized search keywords, tags, categories, or labels for the containing role.

`<mdui:DiscoHints>`
: Container element, to be placed in `<md:Extensions>` element of an `<md:IDPSSODescriptor>` element. More info: [SAMLMetaUI].

5.4. Attribute-related Requirements

For SPs each `<md:SPSSODescriptor>` element MAY contain:

- `<md:AttributeConsumingService>` that lists all attributes requested by this SP as `<md:RequestedAttribute>` element with `isRequired="true"` for required attributes and `isRequired="false"` for just useful attributes.

Having no `RequestedAttributes` element in place implies the service does not require any attributes.

SPs MUST provide `RequestedAttribute` elements describing attributes (and, optionally, requested values) for all attributes it is categorizing as NECESSARY in order to access the SP. The `RequestedAttribute` elements MUST include the optional `isRequired="true"` to indicate that the attribute is NECESSARY.

If the SP requires just one or some particular value(s) of an attribute (such as, eduPersonEntitlement="urn:mace:rediris.es:entitlement:wiki:tfemc2"), the SP MUST use the `<saml:AttributeValue>` element to indicate that value(s).

The `isRequired` element is used to indicate the attribute is NECESSARY or CONSENT REQUIRED. `isRequired="true"` indicates the attribute is NECESSARY. `isRequired="false"` or missing `isRequired` attribute indicates the attribute is CONSENT REQUIRED.

In the previous paper form, RRR, the information now implemented by `<md:RequestedAttribute>` was required in the “URI1, …., URI6” fields.

5.5. Contacts Requirements

Each `<md:EntityDescriptor>` element MUST contain

- `<md:ContactPerson>` with `contactType="technical"`, it MUST contain
  - `<md:EmailAddress>` which SHOULD be a role address and not a personal address.

In addition it MAY contain an optional sequence of elements identifying various kinds of contact personnel following the syntax stated in [SAMLMetaV2]. Organizations are required to consider issues related to privacy, given the public nature of metadata.

DiscoJuice - Logos SHOULD fill approx 50% of the image with color. Heavy icons should be made lighter, and lighter logos made heavier. This is to have balance between logos when shown on a list.

6. Bibliografy

[SAMLMetaV2] Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf

[SAML2Errata] SAML Version 2.0 Errata 05 http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.html

[SAML2int] Interoperable SAML 2.0 Web Browser SSO Deployment Profile http://saml2int.org/profile/current

[SAMLMetaIoP] SAML V2.0 Metadata Interoperability Profile http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf

[eduGMP] Edugain Metadata Profile http://www.geant.net/service/edugain/resources/Documents/eduGAIN%20Metadata%20profile.pdf

[SAMLMetaUI] SAML V2.0 Metadata Extensions for Login and Discovery User Interface http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/cs01/sstc-saml-metadata-ui-v1.0-cs01.pdf

[SAML2MPDPCoC] SAML 2 Profile for the Data Protection Code of Conduct https://refeds.terena.org/index.php/SAML_2_Profile_for_the_Data_Protection_Code_of_Conduct