

# Haka SAML 2.0-profiililuonnos

Draftin Haka profiilin esittely  
Haka-Virtu päivillä 03.02.10

# Sisältö



- Me
- SAML Profiileista
- Haka 2.0 Profiili ehdotus ja sen vaikutukset jäseniin

# Me – Haka/Virtu Poppoo



- Manne Miettinen
- Mikael Linden
- Arto Tuomi
- Mika Suvanto
- Timo Mustonen
- Janne Lauros

# Mikä on profiili

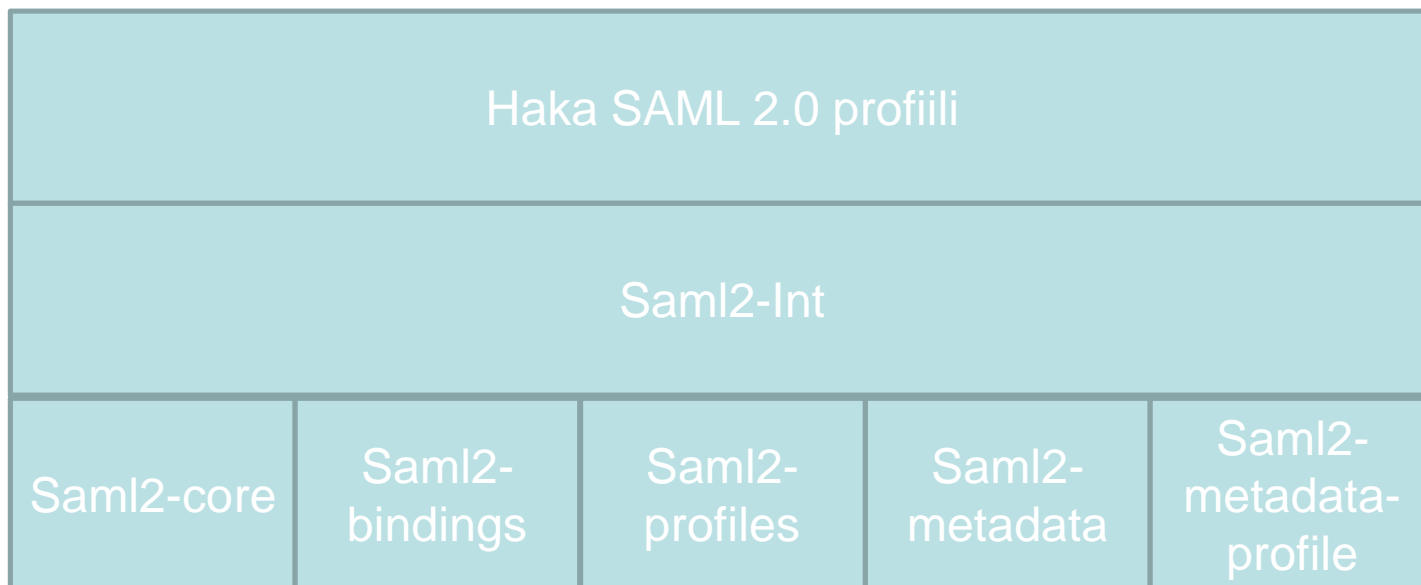


..SAML profile defines a set of constraints on the use of a general SAML protocol or assertion capability for a particular environment or context of use. Profiles of this nature may constrain optionality, require the use of specific SAML functionality (for example, attributes, conditions, or bindings), and in other respects define the processing rules to be followed by profile actors.[Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0]

# Mikä on profiili



Haka SAML 2.0 profiili dokumentti tarkoittaa olemassa olevia määritelmiä.



Motivation: Haka SAML 2.0 profiili mahdollistaa/helpottaa ei shibboleth Implementaatioiden tuomisen federaatioon.

# Haka 2.0 SAML profiili ehdotus



Page 4

- eduPersonScopedAffiliation (e.g. [student@example.org](#))

The Haka federation operator provides a list of the scope values permitted for each Identity Provider<sup>7</sup>. The list is provided using format(s) deemed currently appropriate.

Example (informative):

Suppose `idp.example.org` is the Example university's Identity Provider. Example university uses two scope values, "example.org" for employees and "student.example.org" for students. Following entry in the Shibboleth SAML2 metadata expresses the university's scopes

```
<EntityDescriptor entityId="https://idp.example.org/">
  <IDPSSODescriptor ...>
    <Extensions>
      <shibmd:Scope xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"
        regexp="false">example.org</shibmd:Scope>
      <shibmd:Scope xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"
        regexp="false">student.example.org</shibmd:Scope>
    </Extensions>
  </IDPSSODescriptor>
</EntityDescriptor>
```

When a Service Provider receives a scoped attribute from `idp.example.org`, it SHOULD ensure that scoped attributes, if any, carry either of the two scopes.

Examples of valid scoped attribute values from `idp.example.org`:

- `eduPersonPrincipalName="bobsmith@students.example.org"`
- `eduPersonScopedAffiliation="employee@example.org"`

Examples of invalid scoped attribute values from `idp.example.org`:

- `eduPersonPrincipalName="bobsmith@staff.example.org"`
- `eduPersonPrincipalName="johndoe@bad-example.org"`

### 3.3. Requested Attributes

One or several RequestedAttribute elements MAY be incorporated to SPSSODescriptor elements in the Haka federation metadata. Identity Provider SHOULD release to a Service Provider only attributes defined in metadata for each Service Provider entry.

### Bibliography

Cantor, S. (2009). *SAML v2.0 Metadata Interoperability Profile Version 1.0*. OASIS.

Cantor, S., Kemp, J., Philpott, R., & Maler, E. (2005). *Assertions and Protocols for the OASIS Secure Assertion Markup Language (SAML) V2.0*.

<sup>7</sup>Current list available in <http://www.csc.fi/haka/>

# Tausta dokumentteja..



## 2 Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0

4 OASIS Standard, 15 March 2005

6 Document Identifier:  
7 saml-core-2.0-os  
8 Location:  
9 <http://docs.oasis-open.org/security/saml/v2.0/>

10 Editors:  
11 Scott Cantor, Internet2  
12 John Kemp, Nokia  
13 Rob Philpott, RSA Security  
14 Eve Maler, Sun Microsystems  
15 SAML V2.0 Contributors:  
16 Conor P. Cahill, AOL  
17 John Hughes, Allos Origin  
18 Hal Lockhart, BEA Systems  
19 Michael Beach, Boeing  
20 Rebekah Metz, Booz Allen Hamilton  
21 Rick Randall, Booz Allen Hamilton  
22 Thomas Wisniewski, Entrust  
23 Irving Reid, Hewlett-Packard  
24 Paula Austel, IBM  
25 Mayann Hondo, IBM  
26 Nick Ragnozis, IBM  
27 Tony Nadalin, IBM  
28 RL 'Bob' Morgan, Internet2  
29 Peter C Davis, Neustar  
30 Jeff Hodges, Neustar  
31 Frederick Hirsch, Nokia  
32 John Kemp, Nokia  
33 Paul Madsen, NTT  
34 Steve Anderson, OpenNetwork  
35 Prateek Mishra, Principal Identity  
36 John Linn, RSA Security  
37 Rob Philpott, RSA Security  
38 Jahan Moweh, Sigaba  
39 Anne Anderson, Sun Microsystems

1 saml-core-2.0-os  
2 Copyright © OASIS Open 2005. All Rights Reserved.

15 March 2005  
Page 1 of 66



## 2 Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0

4 OASIS Standard, 15 March 2005

6 Document Identifier:  
7 saml-profiles-2.0-os  
8 Location:  
9 <http://docs.oasis-open.org/security/saml/v2.0/>

10 Editors:  
11 John Hughes, Allos Origin  
12 Scott Cantor, Internet2  
13 Jeff Hodges, Neustar  
14 Frederick Hirsch, Nokia  
15 Prateek Mishra, Principal Identity  
16 Rob Philpott, RSA Security  
17 Eve Maler, Sun Microsystems  
18 SAML V2.0 Contributors:  
19 Conor P. Cahill, AOL  
20 John Hughes, Allos Origin  
21 Hal Lockhart, BEA Systems  
22 Michael Beach, Boeing  
23 Rebekah Metz, Booz Allen Hamilton  
24 Rick Randall, Booz Allen Hamilton  
25 Thomas Wisniewski, Entrust  
26 Irving Reid, Hewlett-Packard  
27 Paula Austel, IBM  
28 Mayann Hondo, IBM  
29 Michael Moinsson, IBM  
30 Tony Nadalin, IBM  
31 Nick Ragnozis, Individual  
32 Scott Cantor, Internet2  
33 RL 'Bob' Morgan, Internet2  
34 Peter C Davis, Neustar  
35 Jeff Hodges, Neustar  
36 Frederick Hirsch, Nokia  
37 John Kemp, Nokia  
38 Paul Madsen, NTT  
39 Steve Anderson, OpenNetwork  
40 Prateek Mishra, Principal Identity  
41 John Linn, RSA Security  
42 Rob Philpott, RSA Security  
43 Jahan Moweh, Sigaba  
44 Anne Anderson, Sun Microsystems

1 saml-profiles-2.0-os  
2 Copyright © OASIS Open 2005. All Rights Reserved.

15 March 2005  
Page 1 of 66

## 257 2.4 Implementation Constraints

### 258 2.4.1 Peer Authentication

259 An additional constraint is necessitated by the inability of SAML metadata to express the authentication requirements of back-channel communications between SAML-using entities, such as via the SAML SOAP binding [SAML2Bindg]. In lieu of extending metadata to capture such requirements, this profile assumes that such communications are secured by means of some combination of TLS/SSL and digital signing. If this assumption cannot be made, this profile might need to be supplemented in such scenarios.

### 264 2.5 Metadata Producer Requirements

265 A producer of metadata that adheres to this profile may be an actual participant in a SAML (or other) profile, or an aggregator of metadata describing many such participants. In either case, the content of the metadata (itself is independent of its source and MUST stand alone as a description of the requirements for securely communicating with the entity (or entities) described therein, to the extent that the constraints of the SAML V2.0 metadata specification [SAML2Meta] can express these requirements.

270 Subject to any constraints of the exchange mechanisms in use, a conforming metadata instance may be rooted by either an `<sd:RoleDescriptor>` or `<sd:EntityDescriptor>` element. Any `<sd:RoleDescriptor>` element (or any derived element or type) appearing in the metadata instance MUST conform to this profile's requirements.

274 Within the context of a particular role (and the protocols it supports, as expressed in its `processDerivationExpression` attribute), 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 2.6.1. This includes not only signing and encryption keys, but also any keys used to establish mutual authentication with technologies such as TLS/SSL.

279 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.

285 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 `validity` attribute of cacheDuration attribute), and the exchange mechanism in use.

### 290 2.5.1 Key Representation

291 Each key included in a metadata role MUST be placed within its own `<sd:KeyDescriptor>` element, with the appropriate `use` attribute (see section 2.4.1.1 of [SAML2Meta]), as revised by ESO in [SAML2Errata], and expressed using the `<sd:KeyInfo>` element.

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

- 296 • `<sd:KeyValue>`
- 296 • `<sd:X509Certificate>` (child element of `<sd:X509Data>`)

17 SAML-metadata-profile-1  
18 Copyright © OASIS Open 2005. All Rights Reserved.

4 August 2005  
Page 3 of 14

# Profiili – Kohta 2.1



## **Saml2Int – The Authentication Request – ”SingleSignOnService Binding”**

“The <samlp:AuthnRequest> issued by the Service Provider MUST be sent to the Identity Provider using the HTTP-REDIRECT binding.”

Tällä hetkellä Haka metadassa suurimmalla osalla Idp:tä on sekä HTTP-POST että HTTP-REDIRECT binding käytössä. Muutama Idp on rekisteröinyt vain HTTP-POST bindingin. Aiheuttaa toimenpiteitä.

## **Saml2Int – The Response – ” AssertionConsumerService Binding”**

“The <samlp:Response> MUST be sent using the HTTP-POST binding saml2-bindings.”

Kaikki rekisteröidyt SAML2 SP:t ovat rekisteröineet vain ja ainoastaan HTTP-POST binding osoitteen. Ei aiheuta toimenpiteitä SP puolelle.

# Profiili – Kohta 2.2 – Single Logout



- Huom! Shibboleth Idp ei tue vielä SLO:ta!
- Logout requests and responses must be signed
- Idp:n pitää (MUST) huolehtia järkevästä käyttäkokemuksesta. Käyttäjän tulee nähdä mistä Sp:stä hän itseasiassa on kirjautumassa ulos ja mikä oli lopputulos. Jos ulos kirjautuminen epäonnistuu tästä pitää informoida selkeästi ja pyytää käyttäjää sulkemaan selain.
- Sp:n tulee (SHOULD) huolehtia myös applikaatiotason session hallinnasta. Jos tämän jättää tekemättä niin vaikutukset täytyy analysoida tarkkaan.

# Profiili – Kohta 3.1 – Metadata



Saml2 metadata interop. profilesta seuraa:

1. Metadataan tuottajan (Haka) rooli korostuu. Meistä tulee ikään kuin CA. Tästä seuraa myös validUntil attribuutin käyttöönotto.
2. Metadataassa olevan Idp/Sp sertifikaattien rooli pienenee. Idp/Sp ei saa tehdä mitään päätelmiä sertifikaatin oikeellisuudesta. Sertifikaatti on siis vain kääre julkiselle avaimelle.

Toisaalta me vaadimme että metadataan liitetty sertifikaatti on Soneran tai Comodon myöntämä.

# Profiili - Kohta 3.1 – Metadata - validUntil



- Tarkoituksena on suojata metadatan jakelu ulkopuolisia hyökkäyksiä vastaan. Aikaikkunan kulumisen jälkeen hyökkääjä ei pysty jakamaan vanhaa dataa.
- Kun aikaikkunaa aletaan pienentämään meidän täytyy pystyä varmistamaan että idp/sp päivittää metadatatietonsa tarpeeksi usein. Tähän riittää nykyinen 24h vaatimus.

# Profiili - Kohta 3.2 – Scoping of identities



- Skoopatut attribuutit nostetaan erityistarkasteluun
- Halutaan tarjota mekanismi jolla SP voi tarkistaa skoopin oikeellisuuden
- Tullee aiheuttamaan kahden erilaisen metadatan julkaisun: Metadatan jossa Extensions osassa kerrotaan validit skoopit kyseiselle entitylle ja Metadadan josta tämä puuttuu (kuten nykyinen). Tämä johtuu siitä että osa tuotteista ei tue Extensions osaa, näille tieto toimitetaan vielä määrittelemättömällä tavalla.

# Profiili - Kohta 3.3 – Requested Attributes



- Tällä hetkellä attribuutti filtteriä käytetään samaan toiminnallisuuteen. Tämä on tietenkin Shibboleth spesifinen ratkaisu
- "Idp SHOULD.." tällä hetkellä ainakaan Shib Idp ei toimi näin.

# Kommentit ehdotukseen



[haka-kehitys@postit.csc.fi](mailto:haka-kehitys@postit.csc.fi)

postilistalle ehdotuksia/ihmettelyjä  
profiilista.

19.2. Teknisen ryhmän kokous