Suomi.fi e-Identification – Technical interface description

1 Suomi.fi e-Identification operating environment

Suomi.fi e-Identification offers a user authentication service for e-services across a SAML 2.0 compliant interface. For end users, Suomi.fi e-Identification offers a choice of their preferred method of identification and single sign-on to e-services connected to Suomi.fi e-Identification.

The e-service may limit the set of users’ tokens that are accepted in the identification. If a user has been identified with a strong authentication method, Suomi.fi e-Identification will complement the user’s data with Population Information System data.

The Figure below describes the operating environment of Suomi.fi e-Identification.

![Figure 1: Suomi.fi e-Identification operating environment](image)

1.1 General description of how Suomi.fi e-Identification operates

An e-service uses Suomi.fi e-Identification to authenticate a user. Suomi.fi e-Identification displays to the users a list of token providers accepted by the e-service, of which the users can select their preferred one for the identification process.
Suomi.fi e-Identification contacts the Population Information System to check that the personal identity code of an identified user is active and that its owner is alive, and complements the user’s data with Population Information System data. If successful, Suomi.fi e-Identification produces a SAML 2.0 compliant message, in which the required data is communicated to the e-service via the user’s browser.

In Suomi.fi e-Identification architecture, direct links are not needed between the e-service, Suomi.fi e-Identification and token provider services, as all traffic is communicated via the user’s browser in compliance with the SAML 2.0 standard.

The connection used for the identification process and the personal data transmitted during it are encrypted using a HTTPS protocol, and the parties’ identifies and message integrity are ascertained in compliance with the SAML 2.0 standard.

1.2. Single sign-on and single logout

Suomi.fi e-Identification creates a single sign-on (SSO) session for an authenticated end user, which gives the user access to all e-services connected to Suomi.fi e-Identification with a single login. A single sign-on session is valid for 32 minutes. An e-service is informed of the remaining duration of the session in connection with the login, and it has to initiate a re-login when the session times out.

An e-service connected to Suomi.fi e-Identification must support SAML 2.0 compliant single logout (SLO). As the user logs out, other sessions associated with the same single sign-on session are also terminated. The e-service must be capable of both initiating the logout process and processing logout requests received from Suomi.fi e-Identification.

1.3 Operating environment requirements for a Suomi.fi e-Identification end user

Suomi.fi e-Identification is intended for browser-based use. Its user interfaces, as well as the interfaces specific to the token providers services used in Suomi.fi e-Identification, are browser based.

Different language options are available in Suomi.fi e-Identification (Finnish, Swedish or English).

Users do not need to install any software on their workstations to use Suomi.fi e-Identification. The tokens used to identify a user may require additional components, including certificate card readers.

1.3.1 User’s browser software

Browser requirements set by Suomi.fi e-Identification:

- Suomi.fi e-Identification is HTML 5.0 compliant but also works with a more basic layout if the browser does not support HTML 5.0.
- In order to use the service, HTTP session cookies and JavaScript need to be enabled in the browser.
- The service uses TLS version 1.2 (versions 1.0. and 1.1 are supported to ensure compatibility between different environments). At minimum, 128-bit encryption is used.
1.3.2 Use of tokens

A user may be required to have specific equipment or software to use tokens:

- Banking IDs may, for example, be based on a list of key figures or a mobile application.
- For identification with a certificate card issued by the Population Register Centre (e.g. an electronic ID card, a health care smart card, a civil service card), a card reader and card software installed on the workstation are required.
- In identification based on a mobile certificate, the operator’s SIM card and a mobile phone are used.

1.3.3 Suomi.fi e-Identification on a mobile device

The user interface of Suomi.fi e-Identification runs in a browser. It is also available on mobile terminal devices, however with the browser restrictions described in section 1.2.1. Different tokens may set restrictions on mobile device use.

2 General technical properties of Suomi.fi e-Identification

A SAML 2.0 interface is used for Suomi.fi e-Identification. The messages are transmitted in a UTF-8 format.

2.1 Technical connection

An e-service connects to Suomi.fi e-Identification by submitting its metadata to Suomi.fi e-Identification maintenance. For a description of the metadata file content, see the document E-service metadata.

Suomi.fi e-Identification and the e-service must sign the SAML 2.0 messages sent by them. To authenticate these messages, the recipient must have the sender’s public key (contained in a certificate). The certificate of Suomi.fi e-Identification is downloaded to the e-service’s server when the e-service is connected to the identification service. The e-service transmits its certificate to Suomi.fi e-Identification as part of its metadata.

2.2 SAML message exchanges

SAML messages between Suomi.fi e-Identification and an e-service are communicated through the user’s browser using the HTTP commands GET, REDIRECT and POST. The SAML 2.0 standard uses HTTP command bindings to define how each HTTP command transmits a SAML message.

- The e-service calls Suomi.fi e-Identification by sending an identification request message that includes a return address using the GET or POST command in the user’s browser.
- Suomi.fi e-Identification allows users to identify themselves with the method of their choice.
- Suomi.fi e-Identification sends a return message to the e-service with a POST command to the return address.

The connections are encrypted using TLS protocol; in other words, all call and response messages are sent using HTTPS connections.

- The e-service must ensure that all connections between the user's browser and the e-service are HTTPS-protected.
• Suomi.fi e-Identification is called using a HTTPS connection.
• The return address contained in the message of the e-service must use the HTTPS protocol.

All SAML messages are signed to authenticate the sender and to ensure the integrity and immutability of the messages. The parties must check the signatures of the messages they receive.

2.3 Testing

Connecting an e-service to Suomi.fi e-Identification is easier if one has a tool that decodes SAML messages. Extension packs for this purpose are available for browsers, including the ”SAML tracer” for Firefox and ”SAML Chrome Panel” and ”SAML Message Decoder” for Chrome.

3 Identification

Once Suomi.fi e-Identification has authenticated a user, a single sign-on session to all e-services connected to Suomi.fi e-Identification is created for him or her. While token provider may also offer single sign-on functionality, Suomi.fi e-Identification is unable to use it.
3.1 An example of an identification transaction

1. The user activates the login
2. The e-service detects that the user has not been identified
3. The e-service directs the user to Suomi.fi e-Identification and simultaneously sends a SAML identification request to the browser
4. The user’s browser communicates the SAML identification request to Suomi.fi e-Identification.
5. Suomi.fi e-Identification receives the SAML identification request and returns the token selection page to the browser.
6. The user selects his or her preferred token and identifies himself or herself.
7. The token provider redirects the browser to Suomi.fi e-Identification.
8. The browser transmits to Suomi.fi e-Identification the user’s unique identifier received from the token provider.
9. Suomi.fi e-Identification creates a single sign-on session and a SAML message that contains the user’s data, which it sends to the browser while directing the browser to the e-service.

Figure 2. An example of an identification transaction.
10. The browser sends the personal data contained in the SAML identification response to the e-service, which initiates a session for an identified user.
11. The e-service returns to the user the protected resource he or she requested originally.

For example, the e-service may send the identification request by submitting to the browser a HTML form which contains the SAML message in hidden fields. The form may be sent by a script that is executed automatically, or by the user who clicks on the Submit button on the form.

```html
...<form name="APRO" method="POST" action="https://testi.apro.tunnistus.fi/idp/profile/SAML2/POST/SSO">
    <input type="hidden" name="SAMLRequest" value="fZJBU8I..."/>
    <input type="hidden" name="RelayState" value="ss%3Amem%3Ac3"/>
    <input type="hidden" name="SigAlg" value="http%3A%2F%2Fwww.w3.org%2F2001%2F04%2Fxmldsig-more%23rsa-sha256"/>
    <input type="hidden" name="Signature" value="sO%2Fw.."/>
</form>
...
var form = document.APRO;
form.submit();
...
<input type="submit" value="Siirry tunnistautumaan">
```

The examples below use the following name specifications that have been included in full SAML 2.0 messages when transmitting them:

```xml
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
```

### 3.2 Identification request

The data that directs the identification transaction is defined in the metadata submitted by the e-service when connecting to Suomi.fi e-Identification.

In an identification request, the e-service may change the actions defined in the metadata. For example, the language that Suomi.fi e-Identification should use in its user interface, or the tokens that the user may select for login, may be selected in the identification request.

The supported bindings are HTTP POST and HTTP REDIRECT.

#### E-service ID

**Explanation** E-service ID. Refers to the EntityID attribute specified in the e-service metadata.

**Based on this ID, Suomi.fi e-Identification service can find the e-service specifications, including the certificate that allows it to authenticate the origin of the message.**

**Location** saml2:issuer element in saml2p:AuthnRequest element

**Format** String, maximum length 1024 characters.

**Mandatory** Yes
Sample: `<saml2p:AuthnRequest ...>`

`...`<saml2:Issuer>https://kalastus.kunta.fi/lupa-asiat</saml2:Issuer>

**Suomi.fi e-Identification address**

**Explanation**: Target address of the message, or the address of Suomi.fi e-Identification. Specified in Suomi.fi e-Identification metadata for each binding.

**Location**: Destination attribute of element `saml2p:AuthnRequest`

**Format**: String

**Mandatory**: Yes

**Sample**: `<saml2p:AuthnRequest ... Destination="...">`

**Time stamp**

**Explanation**: Identification request generation time.

**Location**: `issueInstant` attribute of the `saml2p:AuthnRequest` element

**Format**: String, 20 characters.

Date/Time data type of W3C XML Schema specification in format: "YYYY-MM-DDThh:mm:ss"

in UTC format without time zone.

**Mandatory**: Yes

**Sample**: `<saml2p:AuthnRequest... IssueInstant="2015-09-28T16:27:36Z"...>`

**User interface language**

**Explanation**: User interface language

**Location**: `LG` element of the `vetuma xmlns="urn:vetuma:SAML:2.0:extensions"` element of the `saml2p:Extensions` element

**Format**: String, 2 characters.

ISO 639-1 standard language code.

The languages supported in Suomi.fi e-Identification are Finnish (fi), Swedish (sv) and English (en).

The language code can also be transmitted in the HTTP protocol as the value of the variable `locale` (similarly to the Transaction ID transmitted in the variable `RelayState`). This method should only be used if, for technical reasons, the language code cannot be included in the SAML message.

**Mandatory**: No

**Sample**: `<saml2p:AuthnRequest ...

...`
E-service return address or reference to return address

Explanation Return address or reference to return address to which the identification response is transmitted.

Location AssertionConsumerServiceURL or AssertionConsumerServiceIndex attribute of the saml2p:AuthnRequest element.

AssertionConsumerServiceURL attribute value must be equal to the return address specified in the e-service metadata.

Alternatively, reference can be made to the return address specified in the e-service metadata using the AssertionConsumerServiceIndex attribute.

Format: A URL having https protocol, or Suomi.fi e-Identification will reject the message (error code Requester).

Mandatory No

Sample
<saml2p:AuthnRequest ...>
    AssertionConsumerServiceURL="https://kalastus.kunta.fi/SAML2/POST"
</saml2p:AuthnRequest>

or

<saml2p:AuthnRequest ...>
    AssertionConsumerServiceIndex="1"
</saml2p:AuthnRequest>

Transaction ID

Explanation A transaction ID specified by the e-service that makes it possible to preserve the e-service status information throughout the identification transaction.

Based on the ID issued by it, the e-service can, for example, direct the user to the correct page after identification.

Rather than being included in the SAML message, the transaction ID is sent with the HTTP protocol.

Location RelayState variable.

Format Max 80 bytes

Mandatory No

Sample
<form method="post" action="...">
    <input type="hidden" name="RelayState" value="token" />
</form>
**Accepted tokens**

**Explanation** When making the identification request, the e-service may restrict the set of tokens specified in its basic data by listing the tokens that are accepted in the identification request. If the tokens have not been listed, all tokens specified in the e-service basic data are accepted.

**Location** saml2:AuthnContextClassRef element within the
saml2p:RequestedAuthnContext element

**Format:** String with the possible values of:

- urn:oaid:1.2.246.517.3002.110.1 = online banking ID
- urn:oaid:1.2.246.517.3002.110.2 = certificate card
- urn:oaid:1.2.246.517.3002.110.3 = mobile certificate
- urn:oaid:1.2.246.517.3002.110.5 = KatsoOTP (one-time password)
- urn:oaid:1.2.246.517.3002.110.6 = KatsoPWD (password)

In a customer testing environment also:

urn:oaid:1.2.246.517.3002.110.999 = test token only used in testing environments

**Mandatory** Not mandatory. If no tokens have been specified, the tokens listed in the e-service basic data are shown.

**Sample**

```xml
<saml2p:AuthnRequest
 ...
 <saml2p:RequestedAuthnContext
 xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
 Comparison="exact">
 <saml2:AuthnContextClassRef
 urn:oaid:1.2.246.517.3002.110.1
 </saml2:AuthnContextClassRef>
 </saml2p:RequestedAuthnContext>
</saml2p:AuthnRequest>
```

**Token processing**

**Explanation**

**Location** saml2p:NameIDPolicy element within the saml2p:AuthnRequest element

**Format:** Attributes AllowCreate and Format.

**Used in:** AllowCreate="true" and Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"

**Mandatory** Yes.

**Sample**

```xml
<saml2p:AuthnRequest
 ...
 <saml2p:NameIDPolicy AllowCreate="true"
 Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/>
```
3.3 Identification response

In the identification response, Suomi.fi e-Identification returns the data of an identified user and the used token. In addition to the user’s identify the e-service may, for example, receive the user’s name data and up-to-date address data from the Population Information System.

The supported binding is HTTP POST.

This section discusses data related to the session and the identification transaction. For the data transmitted on the user, see the page attributes transmitted on an identified user.

### Time stamp

**Explanation** Identification response generation time.

**Location**  
IssueInstant attribute of the saml2p:Response element

**Format:** String, 20 characters.

Date/Time data type of W3C XML Schema specification in format: "YYYY-MM-DDThh:mm:ss"

in UTC format without time zone.

**Mandatory** Yes

**Sample**

```xml
<saml2p:Response ...>
  IssueInstant="2015-09-28T16:27:36Z"
</saml2p:Response>
```

### Transaction ID

**Explanation** A transaction ID sent by the e-service in the identification call that makes it possible to preserve the e-service status information throughout the identification transaction. Based on the ID issued by it, the e-service can, for example, direct the user to the correct page after identification.

Rather than being included in the SAML message, the transaction ID is transmitted as a HTTP command parameter.

**Location** RelayState parameter

**Format** Max 80 bytes

**Mandatory** No

**Sample**

```html
<form method="post" action="...">
  <input type="hidden" name="RelayState" value="token" />
</form>
```

### Session ID

**Explanation** A single sign-on session ID created by Suomi.fi e-Identification.

The saml2:NameID element contains the attributes NameQualifier (Suomi.fi e-Identification ID) and SPNameQualifier (e-service ID) as well as Format (ID format
definition), which must be included unaltered in the logout request in addition to the ID.

**Location**  saml2:NameID element  
**Format**  String, maximum length 1,024 characters.  
**Mandatory**  Yes  
**Sample**  
<saml2p:Response ...  
  <saml2:Assertion ...  
  <saml2:Subject>  
    <saml2:NameID  
      Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" 
      NameQualifier="https://testi.apro.tunnistus.fi/idp1" 
      SPNameQualifier="https://kalastus.kunta.fi/lupa-asiat">  
      AAd ... dsUA==  
    </saml2:NameID>

**Level of authentication**

**Explanation**  The token selected by the user.  
**Location**  saml2:AuthnContextClassRef element of the saml2:AuthnContext element of the saml2:AuthnStatement element  
**Format**  An identifier in the format URN:OID is returned as the value.  
  urn:oid:1.2.246.517.3002.110.1  online banks  
  urn:oid:1.2.246.517.3002.110.2  certificate card  
  urn:oid:1.2.246.517.3002.110.3  mobile certificate  
  urn:oid:1.2.246.517.3002.110.5  KatsoOTP  
  urn:oid:1.2.246.517.3002.110.6  KatsoPWD  
  urn:oid:1.2.246.517.3002.110.999  test token only used in the customer testing environment  
**Mandatory**  Yes  
**Sample**  
<saml2p:Response ...  
  <saml2:Assertion ...  
  <saml2:AuthnStatement ...  
    <saml2:AuthnContext>  
      <saml2:AuthnContextClassRef>  
        urn:oid:1.2.246.517.3002.110.1  
      </saml2:AuthnContextClassRef>

**Return status**

**Explanation**  An indication of whether or not the identification transaction was successful is communicated to the e-service.  
**Location**  saml2p:Status element of the saml2p:Response element.  
**Format**  String. See status codes and explanations below.  
**Higher level status codes**

- **Success**  Identification was successful
- Requester = Error in identification request
- Responder = Processing of identification request failed
- VersionMismatch = Incorrect version in the identification request

Complementary status codes:

- AuthnFailed = Identification failed
- RequestDenied = Identification rejected by the token

The status element may include a StatusMessage element that contains more detailed information on the error.

**Mandatory** Yes

**Sample**

```xml
<saml2p:Response>
  <saml2p:Status>
  </saml2p:Status>
</saml2p:Response>
```

4 Logout

The figure below lists the SAML messages exchanged between e-services and Suomi.fi e-Identification when a user has been logged in to e-services connected to Suomi.fi e-Identification.

![Diagram](image)

*Figure 3. SAML messages exchanged by e-services and Suomi.fi e-Identification in the logout process. The messages are transmitted via the user’s browser.*
4.1 Logout request

An e-service can send a logout request to Suomi.fi e-Identification or vice versa (see Figure 3). The structure of the message is similar in both situations.

The e-service must terminate the local browser session before sending a logout request to Suomi.fi e-Identification.

The supported bindings are HTTP POST and HTTP REDIRECT.

**E-service ID**

**Explanation** E-service ID. Refers to the EntityID attribute specified in the e-service metadata.

Based on this ID, Suomi.fi e-Identification can find the e-service definitions, including the certificate that allows it to verify the origin of the message.

**Location** saml2:issuer element of the saml2p:LogoutRequest element

**Format** String, maximum length 1,024 characters.

**Mandatory** Yes

**Sample**

```xml
<saml2p:LogoutRequest...
  <saml2:Issuer>https://kalastus.kunta.fi/lupa-asiat </saml2:Issuer>
</saml2p:LogoutRequest>
```

**Time stamp**

**Explanation** Logout request creation time.

**Location** IssueInstant attribute of the saml2p:LogoutRequest element

**Format:** DateTime data type of W3C XML Schema specification in format: "YYYY-MM-DDThh:mm:ss"

in UTC format without time zone.

**Mandatory** Yes

**Sample**

```xml
<saml2p:LogoutRequest ... IssueInstant="2015-09-28T16:27:36Z"/>
```

**Session ID**

**Explanation** A single sign-on session ID created by Suomi.fi e-Identification that the e-service received in the identification response.

In addition to the ID value, the saml2:NameID element must contain unaltered the attributes included in the identification response (NameQualifier, SPNameQualifier and Format).

**Location** saml2:NameID element

**Format** String

**Sample**

```xml
<saml2p:LogoutRequest...
  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
  Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
  <saml2:NameID
```
NameQualifier="https://testi.apro.tunnistus.fi/idp1"
SPNameQualifier="https://kalastus.kunta.fi/lupa-asiat">
AAE ... dsUA==
</saml2:NameID>

Mandatory Yes

User interface language

Explanation The e-service may specify the language in which the interfaces are displayed.
Location LG element of the vetuma xmlns="urn:vetuma:SAML:2.0:extensions" element of the saml2p:Extensions element
Format: String, 2 characters.
Language code compliant with the ISO 639-1 standard. The languages are Finnish (fi), Swedish (sv) and English (en).
Mandatory No
Sample

<saml2p:LogoutRequest ...>
<saml2p:Extensions>
<vetuma xmlns="urn:vetuma:SAML:2.0:extensions">
<LG>sv</LG>
</vetuma>
</saml2p:Extensions>

Transaction ID

Explanation A transaction ID issued by the e-service that makes it possible to preserve the e-service status information throughout the logout transaction.

For example, it can be used by the e-service to direct the user to a page specified by it after logout.

Rather than being included in the SAML message, the transaction ID is sent in the HTTP protocol.
Location RelayState parameter
Format Max 80 bytes
Mandatory No
Sample

<form method="post" action="....">
<input type="hidden" name="RelayState" value="token" />

4.2 Logout response

An e-service can send a logout response to Suomi.fi e-Identification or vice versa (see Figure 3). The structure of the logout response is similar in both situations. The supported bindings are HTTP POST and HTTP REDIRECT.

Time stamp

Explanation Logout response creation time.
Location IssueInstant attribute of the saml2p:LogoutResponse element
Format: String, 20 characters.
DateTime data type of W3C XML Schema specification in format: "YYYY-MM-DDThh:mm:ss"

in UTC format without time zone.

**Mandatory** Yes

**Sample** `<saml2p:LogoutResponse ... IssueInstant="2015-09-28T16:27:36Z" ...`

### E-service ID

**Explanation** E-service ID. Refers to the EntityID attribute specified in the e-service metadata.

**Location** `saml2:issuer` element in `saml2p:LogoutResponse` element

**Format** String, maximum length 1,024 characters.

**Mandatory** Yes

**Sample** `<saml2p:LogoutResponse ...`<saml2:Issuer>https://kalastus.kunta.fi/lupa-asiat</saml2:Issuer>`

### Transaction ID

**Explanation** A transaction ID issued by the e-service that makes it possible to preserve the e-service status information throughout the logout transaction.

For example, it can be used by the e-service to direct the user to a page specified by it after logout.

Rather than being included in the SAML message, the transaction ID is transmitted as a HTTP command parameter.

**Location** `RelayState` parameter

**Format** Max 80 bytes

**Mandatory** No

**Sample** `<form method="post" action="..."`<input type="hidden" name="RelayState" value="token" />

### Return status

**Explanation** An indication of whether or not the logout was successful is communicated to the e-service.

**Location** `saml2p:Status` element of the `saml2p:LogoutResponse` element.

**Format** String. See status codes and explanations below.

**Higher level status codes**

- **Success** = Logout succeeded
- **Requester** = Error in logout request
- **Responder** = Processing of logout request failed
- **VersionMismatch** = Incorrect version in the logout request

**Complementary status codes:**

- **AuthnFailed** = Logout failed
- RequestDenied = Logout request rejected by the service

The status element may include a StatusMessage element that contains more detailed information on the error.

```
<assertionResponse ...>
  <Status>
    <StatusCode
      Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
  </Status>
</assertionResponse>
```

**Mandatory** Yes