Comments on the S212 SAML and S213 OIDC interface recommendations

1 Background

The Finnish Transport and Communications Agency (Traficom) published interface recommendations for the SAML and OpenID Connect protocols of identification services in 2018. When the TUPAS communications protocol was phased out by 2019, it was discovered that the interface recommendation needs to be specified.

During 2020, Traficom established an open mailing list focusing on technical issues related to strong electronic identification and trust services. The technical team, which mainly consisted of actors in the trust network and their experts, met several times in 2020 to consider the revision of the interface recommendation. Based on the feedback and suggestions of the technical team, Traficom asked for comments on changes related to the S212 (SAML) and S213 (OIDC) communication protocols in the lausuntopalvelu.fi service during the period 5 March – 6 April 2021.

Comments were received from the Digital and Population Data Services Agency (DVV), the OP Group, Danske Bank, Ubisecure and Aktia Bank. These comments are reviewed in the following sections.

1.1 Section 2.2.2 Is the table up to date?

Yes: 5

No: -

Comments:

- Fixed references to algorithms should be avoided in the specification. Instead, there should be a reference pointing to a list of algorithms specified and actively maintained by an established standardiser.
- We see no need for updates.

Assessment of the Finnish Transport and Communications Agency:
Based on the comments, there does not seem to be any need to change the recommendations.
Decision: No changes

1.2 Section 2.2.3/4.2.2 Should signing the authentication requests be specified as mandatory (it is currently optional)?

Yes: 5

No: -

Comments/Why :

- There would not be any room for interpretation, so to speak, in different use cases on whether using a signature is mandatory or not, and the safest method possible would always be used with regard to authentication requests. It would always be possible to check who the request came from.

- Reason: It is important to have the auth request as signed so that we know the source of the request. Also, signed has a expiry time, therefore it cannot be fraudulently invoked any number of times.
- The authentication request between Broker and IdP should be signed. The authentication request contains certain parameters, such as acr_values and ftn_spname, the integrity of which should be confirmed.
- Specifying the signature as mandatory categorically would reduce the need for individual configuration, which would make the implementation simpler.
- Mandatory would be good, because it would prevent forging or hijacking authentication requests.

Assessment of the Finnish Transport and Communications Agency: Based on the comments, changing the signature of the relying party's authentication requests from optional to mandatory is justified. Signing the authentication requests within the trust network can still be kept as optional. The same issue has been highlighted in the reform of Regulation M72, and the discussion will also continue in the preparation of the Regulation itself. Decision: To be changed to mandatory

1.3 Section 3.1.1.2/3.1.2.2 Is the list of optional attributes sufficient?

Yes: 4

No: -

Comments/What should be added:

- In our view, AuthCachingDisabled is new as a comment. The important thing is that these will remain as optional attributes in the future, too.

Assessment of the Finnish Transport and Communications Agency: Based on the comments, there does not seem to be any need to change the recommendations. AutoCachingDisabled has been included in the recommendation from the start. Decision: No changes

1.4 Section 4.2 Is the comment on ftn_spname, which was changed as mandatory in the parameters of an authentication request, clear enough?

Yes: 3

No: 2

Comments/How you would change the text:

- Reason: According to the description, they expect the Service Provider name to be displayed in the language selected by the user. Does it mean the Service provider has to send the SP name in all three languages? Please clarify.

- For the end user's user experience, the processing of the parameter should be specified.

  In addition to the application name, should e.g. the name of the broker service be displayed in the user interfaces or should there be an option to display it? In this context, the user interface often means two things: the user interface visible in the user's browser and the one shown in the identification means.

  It would be important to display the same information in the identification means as in the browser as accurately as possible.

  For example, if "You are logging in to the service of Example Shop Ltd" is shown in the browser, the mobile identification means should also display the same application name.

Assessment of the Finnish Transport and Communications Agency:

For the attribute ftn_spname, there seems to be a need to specify the interface recommendation. Making it mandatory to display the name of the service application in all of the situations and user interfaces that require actions by the user has been proposed in the work on reforming Regulation M72. The actual recommendation should specify what to do with browser settings in different languages.

Decision: The description related to language versions is specified based on the views of the technical working group as needed at a later stage. The text in the current recommendation could be sufficient: "The name is RECOMMENDED to be in the same language as user's preferred user interface language (parameter ui_locales)." The language versioning will be deleted from the published version and can be added later if the technical group decides it.

1.5 Section 4.2.1 Should the number of attributes transmitted in initial identification events (chaining) be increased?

Yes: -

No: 4

Comments/What should be added:

- Reason: A sufficient parameter "ftn_chain_level" already exists.
- There is no need to add attributes to the authentication request. Instead, the current FTN LOA levels could be specified with a vector describing the strength of the initial identification; it could be expressed as attributes handed over in the authentication response in connection with a chained authentication event.

Assessment of the Finnish Transport and Communications Agency:

Based on the comments, there does not seem to be any need to add attributes to the initial identification.

Decision: No changes

1.6 Section 4.3.1/4.5.1 Is the new specification of errors at a sufficient level?

Yes:

No: 4

Comments:

- It would be good to have more than two specifications at the error level. The inference should not be transferred to the data content of the error_decscription section; instead, the recipient should get the right error=[value] with an unambiguous meaning directly. For example, 'user cancel' in particular should be brought to the error level to differentiate it from an actual access_denied situation.
- Reason: More error response are needed. For example, "invalid_grant", "invalid_grant_type", "invalid_state" which tells that the auth code is expired or the invalid code is sent.
- The condition of only returning an error response to an identified customer implementation, as discussed in the working groups, is missing from the section.
- A separate error code should be added for 'cancel'. Error = "cancel" that can then have an error_description additional field, or no additional field.

Assessment of the Finnish Transport and Communications Agency:

Error handling was discussed in the workshops of the technical team in 2020. Traficom requested a proposal for changing the recommendation from the members of the trust network. The proposal for a change was received and reviewed at a workshop of the technical team. Based on the comments, it can be understood that the text of the recommendation does not yet correspond to the wishes expressed. In Traficom's view, the mention of returning an error response can be added to the recommendation immediately. In error handling, it would be desirable for the actors in the trust network to reach an understanding of a standard method of handling errors or error situations. In Traficom's view, the best way to achieve this would be to arrange a separate workshop for harmonising error handling, where the actors could agree on the practices and standardised error messages.

Decision: A mention on returning an error response to the identified service application is added. A separate workshop meeting is arranged for error handling, based on which a harmonious view of the changes needed for the recommendation is established.

1.7 Free-form feedback on the OIDC recommendation Please give free-form feedback on the draft here (OIDC).

- Free OIDC feedback

  Mandate some basic requirements for the UI screen such as cancel button, display Service provider name, language selection, etc.

  It would be good to display the log/error ID so it can be used for investigation.

- Section 2.2.1 gives instructions to use the keys that have already been pinned in advance, but the key exchange process is not described. This has led to a wide variety of key exchange practices in networks. It would be better to act in the way established in the OIDC Core specification in the key exchange.

Assessment of the Finnish Transport and Communications Agency:

One of the issues discussed in the technical workshops in 2020 was harmonising the user interfaces and recording them in the recommendation. The Agency requested a proposal from the actors in the trust network, but no such proposal was submitted. Adding a harmonious graphic appearance or elements can be included in the recommendation, but this requires wider acceptance from the actors in the trust network. In addition, it is essential that the proposal to change the recommendation would come from the actors in the network as their harmonious view. In the reform of Regulation M72, carrying and displaying the name of the service application throughout the identification process has been highlighted. When the Regulation is completed, the texts of the recommendations will be changed to reflect the new regulation and its reasoning.

Pinned keys (certificate/key pinning) and key exchanges at both the telecommunications and application level are being clarified in connection with the reform of Regulation M72. When the Regulation has been completed, Traficom will also change the interface recommendations to reflect any changes in the Regulation or its reasoning.

The schedule for changes connected to the Regulation is early 2022.

Decision: No changes to the recommendation. The wish presented in connection with the user interface(s) will be discussed again by the technical team.

1.8 Comments on the SAML recommendation Give free-form feedback on the draft here (SAML).

- Free SAML feedback

  Standardize the auto key renewal in SAML flow.

Assessment of the Finnish Transport and Communications Agency:

The issue is discussed in the previous section (pinned keys/key exchange)

1.9 Other comments/Opinions

- Traficom has requested an opinion on the SAML and OIDC interface recommendations of the trust network from the Digital and Population Data Services Agency (DVV). DVV expresses its thanks for the opportunity to give its opinion on the issue and gives the following statement.

  In the view of DVV, it is good that the interface recommendation is updated and that the work on the updates has been done in cooperation with the trust network and other market operators. DVV also considers it a good thing that the interface descriptions are only published in English so that they can be widely used directly and that there will not be any differences in interpretation between the versions in different languages.

  Section 2.2.3 / 4.2.2

In the view of DVV, it is good that signing the authentication request would be specified as mandatory in the interface recommendation. Signing the authentication request is already a fairly common practice at the moment, but if it was specified as mandatory, there would not be any room for interpretation in different use cases with regard to the necessity of a signature, and the activity would always be as safe as possible. It would always be possible to check who the request came from.

Section 4.3.1 / 4.5.1

DVV suggests that the dictionary of the specification of error situations could be larger than two terms. The inference should not be transferred to the data content of the error_decscription section; instead, the recipient should get the right error=[value] with an unambiguous meaning directly. For example, 'user cancel' in particular should be brought to the error level to differentiate it from an actual access_denied situation.

Otherwise DVV has no comments on the interface recommendations.