Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren
Conférence des directrices et directeurs cantonaux de la santé
Conferenza delle direttrici e dei direttori cantonali della sanità

eHealth Suisse

Harmonisation de l'interface pour le renouvellement des assertions IdP

Aide à la mise en œuvre à l'attention des communautés de référence

Berne, le 15. Mai 2020

ehealthsuisse
Kompetenz- und Koordinationsstelle von Bund und Kantonen
Centre de compétences et de coordination de la Confédération et des cantons
Centro di competenza e di coordinamento di Confederazione e Cantoni

Impressum

Informations complémentaires et diffusion :

www.e-health-suisse.ch

Objet et positionnement du document :
Le présent document décrit le consensus sur l'harmonisation de l'interface permettant de renouveler les assertions du fournisseur d'identification (*identification provider*, IdP). Cette interface est complétée par une signature dans le *web service security header* servant à authentifier la partie utilisatrice (*relying party*). Le consensus s'est formé et a été validé lors d'une série de concertations entre les éditeurs de moyens d'identification conformes au DEP et les fournisseurs de plateformes DEP. La présente aide à la mise en œuvre est accessible à l'adresse : www.e-health-suisse.ch.

Les aides à la mise en œuvre d'eHealth Suisse fournissent des informations sur la manière d'organiser certaines tâches dans le contexte du réseau numérique. Les acteurs concernés peuvent décider eux-mêmes s'ils souhaitent ou non s'en tenir aux suggestions et aux recommandations. La présente aide à la mise en œuvre n'a pas force obligatoire. L'évaluation finale de la conformité aux exigences légales incombe en tout état de cause aux organismes de certification.

À l'instar de l'annexe 8 de l'ODEP-DFI, le texte du document est rédigé en anglais.

Dans l'intérêt d'une meilleure lisibilité, il a été décidé de renoncer à l'utilisation des formes différenciées du masculin et du féminin. Sauf indication contraire, les deux sexes sont toujours concernés.

Content

Summary

This document summarizes the consensus reached be representatives of identity provider and EPR platform vendors on extending the renew transaction message with a signature authenticating the relying party to the web service security header. This consensus was reached during a series of conference calls with vendors of identity provider and EPR platforms.

1 Introduction

1.1 Motivation

The renew transaction is defined in Annex 8 EPRO-FDHA as mandatory but has not yet been tested at the projectathon. The requirements described in Annex 8 EPRO-FDHA define the renew transaction request to convey the initial assertion in the message body and the transport via a secured SOAP backchannel using TLS or IPsec. No additional requirements on the authentication of the relying party on the message level are specified in Annex 8 EPRO-FDHA.

ELCA proposed to enhance the requirements by adding a signature uniquely authenticating the relying party as an additional security requirement in their Trust ID implementation. ELCA Trust ID requires vendors of relying parties (vendors of EPR platforms and primary systems) to add a message signature to the SOAP Security Header as recommended by the Web Service Security specification of the OASIS group.

The proposal is justified by the fact that in common IT infrastructures TLS or IPsec transports typically do not terminate at the relying party application but on network infrastructure components like firewalls, reverse proxies or IPsec endpoints. Since Annex 8 specifies the minimal security requirements and the proposed solution increases the security, the proposed solution enhances the requirements specified in Annex 8. During proof of concept studies with ELCA Trust ID, Post CH and Swisscom implemented the solution as proposed by ELCA.

The harmonization of the renew transaction was initiated by Post CH and its vendor ITH icoserve. The intention was to reach an agreement between the stakeholder (vendors of relying party systems and certified identity provider) to avoid a situation where vendors need to implement identity provider specific implementations of the renew transaction.

In addition, questions on the time constraints for renew of an authentication assertion were raised by Swisscom Health during the calls. Annex 8 EPRO-FDHA defines the renew of an assertion to be allowed “before or just after the expiration of the defined session time in an EPR-System (RP)” and it was requested to reach an agreement for the detailed time constraints as well.

1.2 Mission and Approach

eHealth Suisse coordinated a series of calls to discuss the harmonization of the IdP renew transaction and find an agreement between the

vendors of certified identity provider and relying parties. Invitations were sent to the representatives of vendors of identity provider and EPR platforms, which are currently in the process of certification or claim to be certified in the near future.

During the calls the issue was discussed in detail, especially

1. The motivation for adding the signature to the security header and the related threat;
2. The structure of the security header, its elements and the attributes;
3. Conformance with Annex 8 and the OASIS Web Service Security specification.

The discussion can be summarized as follows:

1. The rating of the risk related to the thread differed between the participants;
2. Regardless of the different rating all participants agreed upon to implement a signature to the web service security header of the renew transaction;
3. The participants agreed upon the proposed structure of the security header, its elements and the attributes.

During the discussion, it turned out that the participants had no common understanding of the time constraints for renew of an authentication assertion. After discussion, an agreement was accepted by the participants as follows:

1. Outdated authentication assertions shall be renewable for a specified grace period;
2. The grace period shall match the idle time of the Identity Provider;
3. The idle time of identity provider shall be set to two hours.

1.3 Glossary

Term	Description
Grace Period	The duration an assertion can be renewed after expiration of its validity period.
Idle Time	The duration an identity provider keeps the session alive without user interaction.

1.4 References

1) Web Services Security: SOAP Message Security 1.1 (WS-Security 2004), OASIS Standard Specification, 1 February 2006.
2) XML- Signature Syntax and Processing, W3C Recommendation, 12 February 2002.
3) RFC 2119 “Key words for use in RFCs to Indicate Requirement Levels”. March 1997.

2 IdP renewal transaction

This section documents the requirements on the renew message request according to the consensus reached during the calls for the harmonization of the transaction.

2.1 Notational conventions

Keywords

The keywords "must", "must not", "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" in this document are to be interpreted as described in RFC 2119.

2.2 Requirements

2.2.1 Timestamp

Timestamp

The Web Service security header of the SOAP envelope shall contain a security timestamp element as described in chapter 10 of the Web Services Security specification.

The security timestamp element shall have a wsu:Id attribute which shall be used to reference the timestamp element in a XML signature (see below).

The security timestamp element shall contain a created element whose value must be the instant that the renew request is serialized for transmission as described in chapter 10 of the Web Services Security specification.

The security timestamp element shall contain an expires element named expires as described in chapter 10 of the Web Services Security specification. Identity provider shall discard any message whose security semantics have passed their expiration and shall respond with a fault code (wsu:MessageExpired).

2.2.2 Binary Security Token

Binary Security Token

The Web Service security header of the SOAP envelope shall contain a binary token element as described in chapter 6.3 of the Web Services Security specification.

The binary token element shall have an encoding type attribute set to EncodingType=”http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary”.

The binary token element shall have a value type attribute set to ValueType=”http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3”.

The binary token element may have a wsu:Id attribute.

2.2.3 Signature

The Web Service security header of the SOAP envelope shall contain a signature element conform to the XML signature specification and described in chapter 8 of the Web Service Security specification. The signed info element of the signature element shall contain two reference elements referencing the timestamp element of the security header and the SOAP body element by wsu:Id. The signature method element must reference a digest algorithm known to resist up to date attacks. Older digest algorithms, doubted to be insecure (for example SHA-1 digest) must neither be used by relying parties, nor accepted by the identity provider. The signature element must contain a key info element with one child element conveying a security token reference conformal to the XML signature specification and described in chapter 7 of the Web Service Security specification. The security token reference element conveys the issuer name and serial number to identify the certificate.	Signature

2.2.4 SOAP body element

The SOAP body element shall convey the assertion to renew as described in Annex 8 EPRO-FDHA. In addition, the body element shall have an wsu:Id attribute which is referenced in the key info element of the SOAP security header as described above.	Body Element

3 Renew time constraints

3.1 Requirements

Identity provider shall renew authentication assertions with a grace period equal the idle time of the identity provider.	Grace period
The idle time for certified identity provider shall be set to two hours (2h).	Idle Time

Appendix 1: Renew request example

The following lines list a message example (not normative) with abbreviated binary encoded values of certificates and signatures for better readability.

```
0 <soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
1   <soap:Header xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
2     <wsse:Security
3       xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
4       xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
5       soap:mustUnderstand="1"
6       xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
7       <wsu:Timestamp wsu:Id="TS-15277e04-85e0-4b9c-9692-76c3e7be17bc" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
8         <wsu:Created xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">2019-03-26T15:13:15.144Z</wsu:Created>
9         <wsu:Expires xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">2019-
03-26T15:18:15.144Z</wsu:Expires>
10      </wsu:Timestamp>
11      <wsse:BinarySecurityToken
12        EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Bi-
nary"
13        ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"
14        wsu:Id="X509-6dfe58da-6804-48ba-ad52-e871c63455df"
15        xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
16        xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
17        MIIDPTCCAiWgAwIBAgIEPVbC1zANBgkqhkiG9w0BAQUFADBPMQswCQYDVQQGEwJjaDELMAkGA1UECBMCdmQxD-
DAKBgNVBAc
18        ...qSqEb/3VB3ITUav3DIo2o2mRCKyfHV471QUNt4qNFmEwRxpsoGst/UYoTqW8/buv4A=
19      </wsse:BinarySecurityToken>
20      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="SIG-98f468bf-4022-4e31-9886-6f30f1c676bc">
21        <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
22          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
23            <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="soap"/>
24          </ds:CanonicalizationMethod>
25          <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
26          <ds:Reference URI="#TS-15277e04-85e0-4b9c-9692-76c3e7be17bc" xmlns:ds="http://www.w3.org/2000/09/xmld-
sig#">
27            <ds:Transforms xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
28              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
29                <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="soap wsse"/>
30              </ds:Transform>
31            </ds:Transforms>
32            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
33            <ds:DigestValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">LCxW9EORpAp-
npju2Q17b0MB1LGt8CMCuvoOqCtlhFx0=</ds:DigestValue>
34          </ds:Reference>
35          <ds:Reference URI="#_33c9f0c5-c7d2-4d53-ad2f-944320637754" xmlns:ds="http://www.w3.org/2000/09/xmld-
sig#">
36            <ds:Transforms xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
37              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
38            </ds:Transforms>
39            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
```

```
40          <ds:DigestValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">TwKUz3SxOx1NaFVvy55AbbpWXbU-
Jmfn+mreDpkNa/pg=</ds:DigestValue>
41        </ds:Reference>
42       </ds:SignedInfo>
43       <ds:SignatureValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
44        MXd0WKOSV/1p8U630+CrSu/1vLBbefqtpUI6HSyjfA68+ULGkdMNi5D++wJjB/j0sCdEs6g9tiWqiQoa5kk/tUXCeDIKjv
45        ...oodmB+gly/1lYmFez4sapcBg7ZGEMwCLTQcuMKw9y+jrYghSc2fCOeLQw9EQ==
46       </ds:SignatureValue>
47       <ds:KeyInfo Id="KI-2c6438fa-738a-4ffb-aa52-379bd9380b1a" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
48        <wsse:SecurityTokenReference
49          wsu:Id="STR-76ccd654-581d-446e-a00b-8ed529bcc4ab"
50          xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
51          xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
52          <ds:X509Data xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
53            <ds:X509IssuerSerial xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
54              <ds:X509IssuerName xmlns:ds="http://www.w3.org/2000/09/xmld-
sig#">CN=lk,OU=lk,O=lk,L=lsn,ST=vd,C=ch</ds:X509IssuerName>
55              <ds:X509SerialNumber xmlns:ds="http://www.w3.org/2000/09/xmldsig#">1029096151</ds:X509SerialNumber>
56            </ds:X509IssuerSerial>
57          </ds:X509Data>
58        </wsse:SecurityTokenReference>
59       </ds:KeyInfo>
60     </ds:Signature>
61   </wsse:Security>
62  </soap:Header>
63  <soap:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
64   wsu:Id="_33c9f0c5-c7d2-4d53-ad2f-944320637754" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
65    <wst:RequestSecurityToken xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
66     <wst:RequestType xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512">http://docs.oasis-open.org/ws-
sx/ws-trust/200512/Renew</wst:RequestType>
67     <wst:TokenType xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512">http://docs.oasis-open.org/wss/oa-
sis-wss-saml-token-profile-1.1#SAMLV2.0</wst:TokenType>
68     <wst:RenewTarget xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
69      <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
ID="ID_6ff2590e-8df8-4f04-9ae0-cfd16d816c49" IssueInstant="2019-03-26T15:12:13.246Z" Version="2.0">
          <!-- SAML Assertion omitted -->
130       </saml:Assertion>
131     </wst:RenewTarget>
132     <wst:Renewing xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512"/>
133    </wst:RequestSecurityToken>
134  </soap:Body>
135 </soap:Envelope>
```

Appendix 1: Renew response example

The following lines list a response message example (not normative):

```
0 <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
1  <SOAP-ENV:Header xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"/>
2  <SOAP-ENV:Body xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
3   <wst:RequestSecurityTokenResponse
4     xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512" Context="">
5    <wst:TokenType
6     xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
7     http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0
8    </wst:TokenType>
9    <wst:Lifetime
10     xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
```

```
11      <wsu:Created
12        xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
13        2019-03-26T15:13:13.378Z
14       </wsu:Created>
15      <wsu:Expires
16        xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
17        2019-03-26T15:18:13.378Z
18       </wsu:Expires>
19     </wst:Lifetime>
20     <wst:RequestedSecurityToken xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
21      <!-- include Assertion returned by the IdP here -->
22     </wst:RequestedSecurityToken>
23     <wst:RequestedAttachedReference
24       xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
25       <wsse:SecurityTokenReference
26         xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
27         xmlns:NS1="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd"
28         xmlns="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd"
29         NS1:TokenType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0">
30         <wsse:KeyIdentifier
31           ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID"
32           xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
33           #ID_cf6f7da6-c670-4c35-b413-39182b5672f2
34          </wsse:KeyIdentifier>
35       </wsse:SecurityTokenReference>
36      </wst:RequestedAttachedReference>
37    </wst:RequestSecurityTokenResponse>
38  </SOAP-ENV:Body>
39 </SOAP-ENV:Envelope>
```