Det Danske Vaccinationsregister

IDWS - Snitfladebeskrivelse

Version 1.4.0

2015-11-08

Versionering

Version	Dato	Forfatter	Ændring
1.0	2015-11-08	MAL	Første udgave af dokumentet
1.1	2015-11-30	MAL	Rettelser om endpoint

Indhold

1 Indledning

Dette dokument indeholder en beskrivelse af hvilke tiltag der er nødvendige for at EPJ-systemer og lægepraksissystemer kan benytte de services som Det danske vacciantionsregister (DDV) stiller til rådighed via IDWS snitfladen.

IDWS snitfladen benytter i stedet for headers fra [dgws], headers defineret i Liberty Alliance Basic Profile Soap Binding [LIB-SOAP] specifikationen. Der er desuden beskrevet yderligere krav til den SAML Assertion der benyttes i [oioidws].

Forskellene mellem DGWS snitfladen og IDWS snitfladen er isoleret til Soap Header elementer og de deraf afledte forskelle. Dette dokument omhandler derfor kun disse forskelle og er derfor meget teknisk sammenlignet med [fmk14] dokumentet.

2 Soap Headers

Sikkerhedsmodellen for IDWS udstillingen af det fælles medicinkort er baseret på OIO Identity-based Web Services [oioidws] projektet, som grundlæggende er en specialisering af ID-WS basic profile lavet af Liberty Alliance [LIB-SOAP]. ID-WS Basic Profile benytter WS-Security [WSS] og WS-Addressing SOAP binding [WSAv1.0-SOAP] headers.

DDVs snitflade udstilles kun gennem sundhedsdatanettet, som er et nationalt netværk til brug ved udveksling af data mellem sundhedssektorens parter. Det kræver en aftale for at kunne tilgå sundhedsdatanettet. Se www.medcom.dk.

I de følgende sektioner listes de Soap Headers og attributter der kan indgå i IDWS kald.

Trust

For at LPS/EPJ systemets kald kan benytte DDV IDWS skal den nøgle der benyttes i kaldet trust'es via en af to metoder beskrevet i [LIB-SOAP] sektion 3.7.2.

1. Security headeren skal indeholde en SAML 2.0 holder-of-key assertion der er udstedt af en Secure Token Service (STS) som DDV IDWS er konfigureret til at stole på, og holder-of-key assertion skal indeholde en key der kan bruges til at verificere beskedens signatur. Assertionen selv skal være signeret af STS'en og nøglen til at verificere denne signature skal være udvekslet med DDV systemet i forvejen så DDV kan verificere signaturen.
2. Security headeren skal indeholde et X.509 certifikat i et BinarySecurityToken der er udstedt af en Certificate Authority (CA) som DDV IDWS er konfigureret til at stole på.
3. DDV skal have tilsendt public key som kan benyttes til at verificere signaturer lavet med LPS/EPJ systemets private key, så nøglen dermed er kendt og stoles på.

På sigt er det planen at der skal etableres en fællesoffentlig STS som FMK, DDV - og andre klientsystemer kan etablere trust til og dermed benytte metoden beskrevet i pkt 1). Denne er ikke klar endnu, men indtil den er klar (og evt. tilgængelig for systemer uden for sundhedsdatanettet) så er pkt 2 og pkt 3 fuldt gyldige måder at opnå adgang til FMK IDWS snitfladen.

2.1 WS:Security

Den centrale Soap Header i IDWS opslaget er ws:security elementet som bl.a. skal indeholde en SAML Assertion der identificerer personen der udfører opslaget via et Attribute element. Der findes gode eksempler på opbygningen af elemenet i [LIB-SOAP].

```
<saml2:Attribute FriendlyName="CprNumberIdentifier" Name="dk:gov:saml:attribute:CprNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml2:AttributeValue>2512484916</saml2:AttributeValue>
 </saml2:Attribute>
```

Security elementet skal desuden indeholde to signaturer, en for selve SAML Assertion og en for dokumentet som refererer alle de øvrige headers.
Wsu:Id attributten er påkrævet.
Bemærk at selvom man benytter en anden Trust metode end den beskrevet i pkt 1 i forrige afsnit bør man lave en SAML Assertion med holder-of-key – og så sørge for derudover at få etableret trust via en af de øvrige understøttede trust metoder.

XML eksempel på Security element:

```
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:NS1="http://schemas.xmlsoap.org/soap/envelope/" xmlns="http://schemas.xmlsoap.org/soap/envelope/"
NS1:mustUnderstand="1">
    <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" wsu:Id="_b28b7d3e-ea8b-4151-b7f1-26a5c6d0c412">
      <wsu:Created>2014-09-21T19:52:16.125Z</wsu:Created>
      <wsu:Expires>2014-09-21T20:02:16.125Z</wsu:Expires>
    </wsu:Timestamp>
    <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" ID="_c191c238-041f-4976-8a5d-868f6f3ccf7e" IssueInstant="2014-
09-21T19:57:15.309Z" Version="2.0">
      <saml2:Issuer
Format="urn:oasis:names:tc:SAML:2.0:nameidformat:entity">https://sts.sundhed.dk</saml2:Issuer>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
          <ds:Reference URI="#_c191c238-041f-4976-8a5d-868f6f3ccf7e">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>OByI8xL+3DbmIoJPwfoLSZMFrxM=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>***BASE64 SignatureValue for Assertion element***</ds:SignatureValue>
        <ds:KeyInfo>
          <ds:KeyValue>
            <ds:RSAKeyValue>
              <ds:Modulus>***BASE64 Modulus***</ds:Modulus>
              <ds:Exponent>AQAB</ds:Exponent>
            </ds:RSAKeyValue>
          </ds:KeyValue>
        </ds:KeyInfo>
      </ds:Signature>
      <saml2:Subject>
        <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">C=DK,O=Ingen
organisatorisk tilknytning</saml2:NameID>
        <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
          <saml2:SubjectConfirmationData NotOnOrAfter="2014-09-22T03:57:15.309Z" Recipient="https://fmk">
            <ds:KeyInfo>
              <ds:X509Data>
                <ds:X509Certificate>***BASE64 CERT***</ds:X509Certificate>
              </ds:X509Data>
            </ds:KeyInfo>
          </saml2:SubjectConfirmationData>
        </saml2:SubjectConfirmation>
      </saml2:Subject>
      <saml2:Conditions NotBefore="2014-09-21T19:57:15.309Z" NotOnOrAfter="2014-09-22T03:57:15.309Z">
        <saml2:AudienceRestriction>
          <saml2:Audience>https://fmk</saml2:Audience>
        </saml2:AudienceRestriction>
      </saml2:Conditions>
      <saml2:AttributeStatement>
        <saml2:Attribute FriendlyName="SpecVer" Name="dk:gov:saml:attribute:SpecVer"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
          <saml2:AttributeValue>DK-SAML-2.0</saml2:AttributeValue>
        </saml2:Attribute>
```

```
        <saml2:Attribute FriendlyName="AssuranceLevel" Name="dk:gov:saml:attribute:AssuranceLevel"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
          <saml2:AttributeValue>3</saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute FriendlyName="CprNumberIdentifier" Name="dk:gov:saml:attribute:CprNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
          <saml2:AttributeValue>2512484916</saml2:AttributeValue>
        </saml2:Attribute>
      </saml2:AttributeStatement>
    </saml2:Assertion>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="_cad9fec6-d78c-4e93-971d-c298c80d1c52">
      <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <ds:Reference URI="#_90e86943-a8b9-4674-b1be-400f1f5fdb80">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
              <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xsd"/>
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <ds:DigestValue>NJooSjGnx4ch+bYD+raSFnJK3aM=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#_337c5d0d-a5bd-4e7b-9f3a-918a01f98c79">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
              <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xsd"/>
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <ds:DigestValue>/Acypl+frSy+wvS5QMhb4O+ScsI=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#_dad96bc7-7c82-4738-a3c4-78c58b502395">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
              <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xsd"/>
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <ds:DigestValue>BBebPUGVZOvEENrxdiIleuvpsLA=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#_d6ff9c04-b1c2-4622-b97f-98094cdf89ef">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
              <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xsd"/>
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <ds:DigestValue>efIb7T7jynPWgwz06aOOu1ltiyo=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#_6d46bd38-7d11-4f65-8a11-d79269edffdb">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
              <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xsd"/>
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <ds:DigestValue>Kj/WHDmy1wXAaQYgdSBw/ja0jEA=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#_7d7be81f-0812-4111-964d-14d9b2882c9c">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
```

```
            <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xsd"/>
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <ds:DigestValue>74hWBRQhvy9sLxAMHInvhXbtDOg=</ds:DigestValue>
      </ds:Reference>
      <ds:Reference URI="#_b28b7d3e-ea8b-4151-b7f1-26a5c6d0c412">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xsd"/>
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <ds:DigestValue>BmtLW4tqtUgT80Q1fi362sS2t0o=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>

<ds:SignatureValue>Nk7QvKND8E8cFtcj8re1MGwtAZrLCJvgw2ahKTgqLxcQUzT+0gVxBX2+/Ifu1zGlz2ne8LssP5EP
akOFSJX5qs06u/Vc5e+a1q+3o9mitQ66przWRz2KUkF8OTr3pUuuz3ThjkEqnueDBVx8kt9O26Oxc7QpmGEK9gH5s
Npb6Ld7PuryCbkWvdZf2gKpqSnI02oTuiicQtLZYKg5/IL2ICDJPwd1wIpVbCuyYtN6v/06iWwbLXesWiWwD3XeAt9ZD
EdvGY34KilWjCac8FY5S4EpSXrfLGTSwCax1EGKANdLZ+k+U+VnF9qhtklETrt/Rhf3zLY/0EBHTNTXeeOGrg==</ds:
SignatureValue>
    <ds:KeyInfo>
      <wsse:SecurityTokenReference xmlns:wsse11="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-
1.1.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
wsse11:TokenType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0" wsu:Id="_fcd711cf-
c396-4440-9bd9-3de674ad3247">
        <wsse:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLID">_c191c238-041f-4976-8a5d-868f6f3ccf7e</wsse:KeyIdentifier>
      </wsse:SecurityTokenReference>
    </ds:KeyInfo>
  </ds:Signature>
</wsse:Security>
```

2.2 Framework

Framework headeren er defineret i [LIB-SOAP] - profile skal være ” urn:liberty:sb:profile:basic” og version skal være ”2.0”, ellers vil klienten få en FrameworkVersionMismatch fault returneret.
Wsu:Id attributten er påkrævet.

XML-Eksempel:

```
<sbf:Framework xmlns:sbf="urn:liberty:sb" xmlns:NS1="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:NS2="urn:liberty:sb:profile" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd" xmlns="http://schemas.xmlsoap.org/soap/envelope/" NS1:mustUnderstand="1"
NS2:profile="urn:liberty:sb:profile:basic" version="2.0" wsu:Id="_63dc044a-69de-4b83-b1e1-62b3921395af"/>
```

2.3 WS-Addressing headers

Action

I dette element udpeges den Action der skal udføres – værdien af Action bør være det samme som SOAPAction HTTP headeren – og de gyldige actions står defineret i WSDL filen for IDWS endpointet.
Wsu:Id attributten er påkrævet.

XML-Eksempel

<wsa:Action xmlns:wsa="http://www.w3.org/2005/08/addressing" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="_7b5a33d3-887e-4be4-8d79-f8bfcd3ffbe0">http://www.dkma.dk/medicinecard/xml.schema/2012/06/01#GetMedicineCardAsPDF</wsa:Action>

MessageID og RelatesTo

Der skal i hvert request medsendes et unikt message id – typisk et UUID – f.eks. 'urn:uuid:7a2e1f9a-91c9-4886-a7c3-1e8554f0dd74', eller en lignende unik streng. Denne er påkrævet og benyttes til at logge kaldet og sørge for at response logges sammen med.
Ligeledes vil der i response være en reference til dette message-id i RelatesTo headeren.
Wsu:Id attributten er påkrævet.

XML-Eksempel (request og response):

<wsa:MessageID xmlns:wsa="http://www.w3.org/2005/08/addressing" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="_90e86943-a8b9-4674-b1be-400f1f5fdb80">urn:uuid:8b410a98-764c-4bf4-9e7f-cc67b46a235c</wsa:MessageID>

XML-Eksempel (kun response):

<wsa:RelatesTo xmlns:wsa="http://www.w3.org/2005/08/addressing" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" RelationshipType="http://www.w3.org/2005/08/addressing/reply" wsu:Id="_cfee7063-6ba4-4b2f-9cfc-2817afe525a9">urn:uuid:8b410a98-764c-4bf4-9e7f-cc67b46a235c</wsa:RelatesTo>

To og ReplyTo(optional)

Wsu:Id attributten er påkrævet når elementerne findes.
XML-Eksempel

<wsa:To xmlns:wsa="http://www.w3.org/2005/08/addressing" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="_f85a30d3-8d7e-4971-b1c0-923b661a4c19">http://localhost:8080/fmk12/idws/MedicineCardIdwsEndpoint</wsa:To>
<wsa:ReplyTo xmlns:wsa="http://www.w3.org/2005/08/addressing" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="_ad769333-4211-435e-8e79-66a0f44e306f">
<wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
</wsa:ReplyTo>

2.4 WhitelistingHeader

WhitelistingHeader er beskrevet i [ddv14] og strukturen og kravene til indholdet er identiske for IDWS.

Om elementet gælder, at er det borgerens egne data skal rollen være ”Borger”, men er det data om en person som borgeren er værge for skal RequestedRole sættes til ”Værge”, og endelig kan man også slå data op om sine børn hvis man sætter RequestedRole til ”Forældermyndighed”. DDV IDWS verificerer derefter om personen i SAML Assertion har rettigheden til at lave et Forældermyndighed/Værge opslag på personnummeret i Soap Body.
Har man ikke rettighed til at lave den pågældende type opslag på personen returneres i stedet en fault.

Denne header skal ikke have wsu:Id attributten sat.

3 Versionering af services

Foregår på præcis samme måde og med de samme namespaces- og Actions beskrevet i [ddv14]. DDV Idws servicen udstilles dog på separate endpoints.

IDWS End-point

Hver kommende version af snitfladen udstilles som et særskilt end-point. DDV 1.4 IDWS vil få end-point:

https://<server>/ddv/idws/VaccinationsServiceIDWS_2013_12_01

WSDL-filen er udstillet på

https://<server>/ddv/idws/VaccinationsServiceIDWS_2013_12_01.wsdl

4 Faults

I IDWS DDV returneres fejl i en IDWS fault i stedet for en DGWS fault. med et Status element fra urn:liberty:sbf namespacet (fra Liberty Alliance).
IDWS fault benytter de samme fejltekster som de tekster der er beskrevet i [ddv14].

XML-Eksempel:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <soapenv:Fault>
      <faultcode>soapenv:Server</faultcode>
      <faultstring xml:lang="en">Cpr-nr 2105595088 (PersonIdentifier) findes ikke</faultstring>
      <detail>
        <sbf:Status xmlns:sbf="urn:liberty:sb" code="TODO" comment="TODO">Cpr-nr 2105595088 (PersonIdentifier)
findes ikke</sbf:Status>
      </detail>
    </soapenv:Fault>
  </soapenv:Body>
</soapenv:Envelope>
```

5 Referenceliste

Reference	Dokument
ddv14	DDV - Snitfladebeskrivelse - 1.4.0.pdf
LIB-SOAP	Liberty Basic SOAP Binding - http://www.projectliberty.org/liberty/content/download/4712/32213/file/Liberty-Basic-SOAP-Binding-1.0_Final.pdf
WSAv1.0-SOAP	WS-Addressing SOAP Binding
WSS	WS-Security
oioidws	OIO Identity-based Web Services v1.0.1a - http://digitaliser.dk/resource/526486
borgeradgang	Borgeradgang til Nationale Services – TODO: mangler url