ATP WS Provider Profile

Author: Integration Expert Team (IET)
Owner: Integration Expert Team (IET)

1. Dokumenthistorik

1.1 Revisioner

Dato for denne version: 13.11.2014
Dato for næste version: *ukendt*

Version	Dato	Ændringer	Ændringer markeret
0.1	01.04.2014	Første version	Nej
0.2	13.11.2014	Afsnit 6. Ændring i beskrivelsen af hvilke typer af certifikater der kan anvendes i de forskellige miljøer.	Nej

Indholdsfortegnelse

2. Indledning

Dette dokument udgør ATP's Web Service Provider profil. Det er en simplificering (kravet om anvendelse af SAML2 er taget ud) af ATP's OIOIDWS Provider Profile, som igen er en præcisering og afgrænsning af IT&Telestyrelsen's profiler "Liberty Basic SOAP Binding" og "SAML Profile for Identity Tokens".

Profilen kan anvendes når anvender ikke kan eller ikke ønsker, at gøre brug af Identitetsbaseret Webservices.

Der kan kun udstilles services under denne profil når adgangen til servicen kan begrænses udelukkende på baggrund af det anvendte certifikat.

Profilen beskriver, hvorledes eksterne parter skal kommunikere for at tilgå sådanne web services, der udstilles af ATP.

3. Notationer og terminologi

Dette afsnit beskriver notationer og terminologi, der anvendes i dokumentet.

3.1 Referencer

Referencer til andre dokumenter eller standarder noteres i firkantede parenteser f.eks. "[LIB-Basic]".

3.2 Konventioner for notationer

Følgende tabel viser dokumentets oversættelse af de keywords, vi anvender fra RFC 2119:

Engelsk (RFC 2119)	Oversættes i dette dokument til
MAY	KAN
MUST	SKAL
MUST NOT	MÅ IKKE
REQUIRED	KRÆVET
SHOULD	BØR
SHOULD NOT	BØR IKKE

3.3 Namespaces

I profilen refereres til en række specifikke xml-elementer og attributter med forskellige namespace-prefixes. F.eks. *wsu:ID* og *wsa:RelatesTo*. For at undgå misforståelser vedrørende disse namespaces er de defineret her:

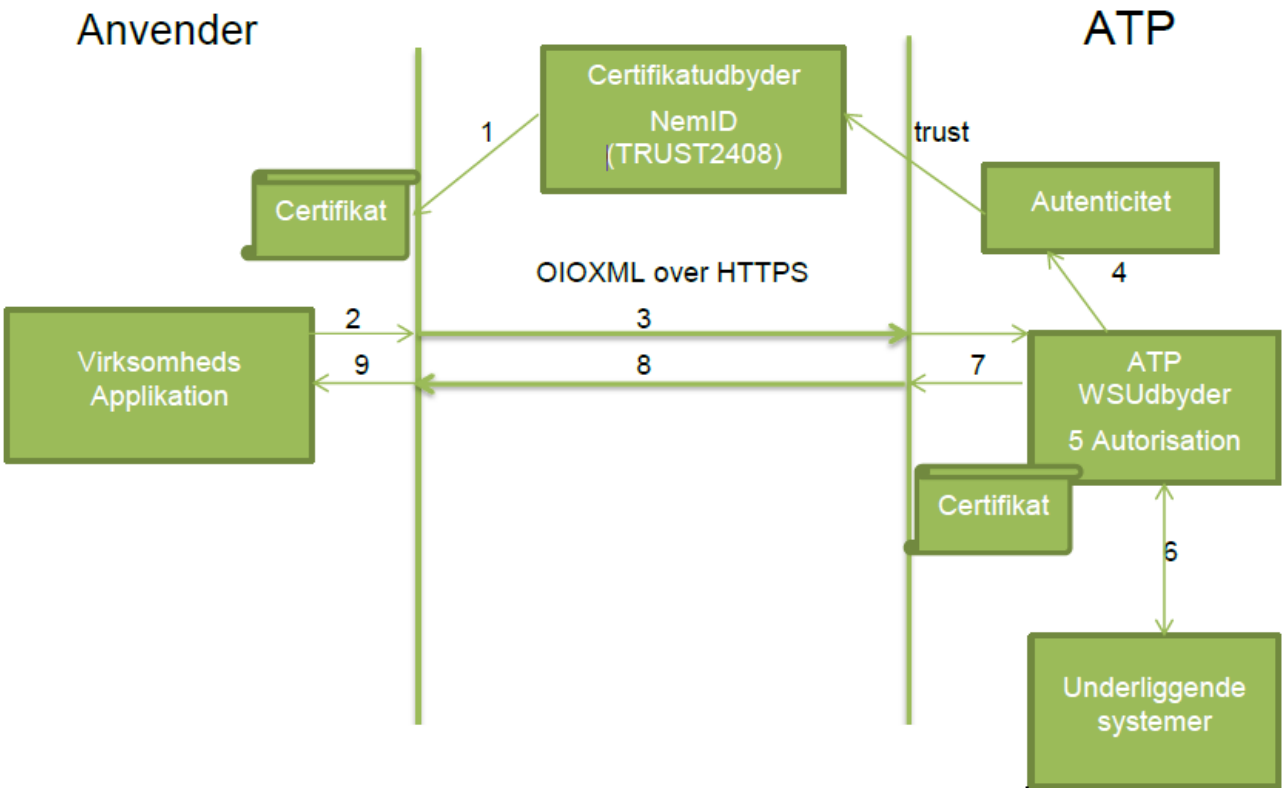
Prefix	Namespace
atp	http://www.atp.dk/oioidws/profile-1.1
s	http://schemas.xmlsoap.org/soap/envelope/
wsse	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
wsu	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd
wsa	http://www.w3.org/2005/08/addressing

4. Scenario

Scenariet for denne profil er, at et anvendersystem kalder en service udbudt af ATP. Der er tale om integration imellem to systemer.

Det er kun services hvortil adgangen (Autorisationen) kan gives på baggrund af det anvendende systems certifikat, der kan udbydes via dette scenario.

Services der kræver identitetsbaseret autorisation, skal anvende scenariet beskrevet i ATP OIOIDWS Provider Profile.



1. Anvender får udstedt virksomheds eller funktions certifikat
2. Anvender signerer request-besked
3. Beskeden sendes over HTTPS
4. ATP autentificerer beskeden på grundlag af trust til certifikatudbyderen.
5. Beskeden autoriseres
6. Servicen kaldes i de underliggende systemer
7. ATP signerer svarbeskeden med ATPs virksomhedscertifikat
8. Svarbeskeden sendes over HTTPS
9. Anvender autentificerer svarbeskeden

5. ATP WS Provider Profile for sikre web services

5.1 HTTP-fejl

I visse tilfælde vil ATP WS returnere HTTP-fejl:

Fejl	HTTP- status code
Web Servicen er forsøgt tilgået fra en ikke autoriseret IP adresse.	403 (Forbidden)
Klienten afsender flere kald end aftalt pr. tidsenhed.	503 (Service Unavailable) Retry-After <n sekunder>

5.2 Tidssætningspolitik

ATPs web service provider infrastruktur overholder tidssætningspolitikken, der er defineret i [TID].

5.3 SOAP Binding

Beskeder SKAL følge den SOAP binding, der er beskrevet i [LIB-Basic] kapitel 2 ”SOAP Binding”. Derudover SKAL følgende procesregler følges for SOAP Faults.

Rækkefølgen af elementer i SOAP-beskeder garanteres kun i det omfang, det specificeres af relevante skemaer.

5.3.1 SOAP Faults

Dette afsnit beskriver generel fejlhåndtering i henhold til SOAP 1.1, som definerer flg. elementer i fejlbeskeder:

<faultcode> – en maskinlæsbar fejl som et kvalificeret navn.

<faultstring> – en menneskelæsbar fejlbeskrivelse.

detail – applikationsspecifikke fejl (relateret til SOAP Body elementet). Må ikke indeholde information om fejl i SOAP headers (herunder sikkerhedsfejl).

5.3.2 Sikkerhedsfejl relateret til SOAP header

WS-Security 1.1 profilen fra OASIS definerer en række generelle fejl relateret til sikkerhedsvalidering - f.eks. ugyldig signatur m.fl.

Det er i OASIS profilen specificeret, at det er valgfrit for implementeringer at returnere sikkerhedsfejl, da dette kan give en angriber informationer at arbejde med. Vælges dette, defineres en række SOAP faults, som skal bruges. ATP returnerer følgende sikkerhedsfejl (i SOAP 1.1 format):

Nedenfor beskrives de definerede fejlkoder. Fejlkoder relateret til usupporterede elementer:

<faultcode>
wsse:UnsupportedSecurityToken
wsse:UnsupportedAlogrithm

Fejlkoder relateret til valideringsfejl:

<faultcode>
sbf:FrameworkVersionMismatch
wsa:MessageInformationHeaderRequired
wsse:InvalidSecurity
wsse:InvalidSecurityToken
wsse:FailedAuthentication
wsse:FailedCheck
wsse:SecurityTokenUnavailable
wsse:MessageExpired

ATP sender, hvor det giver mening, en faultstring, der beskriver den opståede fejl.

6. Applikationsfejl (SOAP Body)

Dette afsnit beskriver fejlstrukturen, der generelt anvendes ved applikationsfejl fra backend systemer - eksempelvis ugyldige inputparametre. Disse fejl returneres kun, såfremt sikkerhedsvalideringen af beskeden går godt.

Alle fejl, som er relateret til SOAP <Body> elementet, skal som nævnt returneres i <detail> elementet.

Liberty Basic SOAP Binding 1.0 definerer en understruktur af <detail> elementet bestående af et <Status> element med flg. attributter:

- En obligatorisk `code` attribut, der angiver en overordnet fejlkode. Følgende værdier defineres i denne profil:
  - 1 = Fejl i kald – ATP vil kun anvende denne værdi.
  - 2 = Advarsel – ATP vil ikke anvende værdien.
  - 3 = Kun delvist resultat returneret – ATP vil ikke anvende værdien.
- En valgfri `ref` attribut som kan indeholde messageID på den indkomne besked
- En valgfri `comment` attribut med en menneskelæsbar forklaring / detaljering.

ATP ønsker i tillæg til ovenstående mulighed for at kunne returnere flere detaljer. Derfor defineres elementet <Reason>, som kan inkluderes i <detail> udover <Status> elementet. Elementet har flg. attributter:

- systemId – kodestreng der beskriver fejlen yderligere – altså en applikationsspecifik fejlkode.
- handle - som kan bruges til at slå op i ATP's logs for at se yderligere information, f.eks. et stack trace eller log-entry

Eksempel:

```
<detail>
      <Status code="1"/>
      <atp:Reason xmlns:atp="http://www.atp.dk/oioidws/profile-
                  1.1" systemId="419"
                  handle="INT328746832"/>
</detail>
```

6.1 SOAP-header

Dette afsnit beskriver brugen af WS-Addressing SOAP Binding [WSAv1.0-SOAP] og WS-Security [WSS] header-blokke.

Udover beskrivelsen af header-blokke beskrives også processerings-regler der skal overholdes af afsendersystemet.

Ved svar på en request anvendes samme header-blokke og processerings-regler, hvis ikke andet er beskrevet nedenfor.

6.1.1 Oversigt af Header-blokke

Følgende header-blokke SKAL være indeholdt I SOAP headeren:

- <wsa:MessageID>
- <wsa:RelatesTo> (mandatory on response)
- <wsa:Action>
- <wsse:Security

Følgende header-blok KAN være indeholdt I SOAP headeren:

- <wsa:To>

6.1.2 The <wsa:MessageID> Header-blokken

<wsa:MessageID> header-blokken er defineret i [WSAv1.0-SOAP].
Værdien af denne header-blok identificerer unikt den besked som indeholder den. Enhver besked SKAL indeholde præcist en sådan header-blok.

<wsa:MessageID> SKAL repræsenteres ved en Universally Unique Identifier som defineret i [UUID]. Et eksempel på en korrekt MessageID-header er:

<wsa:MessageID>urn:uuid:550e8400-e29b-41d4-a716-014466554400</wsa:MessageID>.

ATP tjekker mod replay attacks ved at kontrollere om et MessageID har været sendt før. ATP sender et MessageID i samme format tilbage i svarbeskeden.

6.1.3 <wsa:RelatesTo> Header-blokken

<wsa:RelatesTo> header-blokken er defineret i [WSAv1.0-SOAP].

Denne header-blok SKAL være indeholdt præcist en gang i svarbeskeder. Hvis Relationship Type attributten er anvendt SKAL den have værdien http://www.w3.org/2005/03/addressing/reply.

I svarbeskeder SKAL værdien af denne header-blok være sat til værdien af
<wsa:MessageID> header-blokken på den tilhørende request-besked.

6.1.4 <wsa:Action> Header-blokken

<wsa:Action> header-blokken er defineret i [WSAv1.0-SOAP].

Header-blokken SKAL være indeholdt præcist een gang i alle beskeder.

Bemærk:
Værdien af denne header-blok SKAL indeholde den same værdi som SOAPAction HTTP-headeren defineret i [SOAPv1.1]. SOAP specifikationen kræver HTTP-headeren på alle HTTP-baserede SOAP beskeder.

6.1.5 <wsa:To> Header-blokken

<wsa:To> header-blokken er defineret i [WSAv1.0-SOAP].

Den indeholder typisk WebServicens endpoint.

For synkrone request-response-beskeder kan dette felt udelades da ATP ikke bruger det.
Header-blokken er frivillig.

6.1.6 <wsse:Security>- Header-blokken

Der SKAL være præcist en forekomst af wsse:Security-blokken og den SKAL indeholde et `mustUnderstand`-attribut med værdien `true`.

I <wsse:Security>-headerblokken SKAL det optræde et <wsu:Timestamp>-element, der indeholder et <wsu:Created>-element. Udbyderen af servicen SKAL afvise beskeden, hvis tidsforskellen mellem værdien af <wsu:Created> og den lokale tid overstiger 5 minutter.

6.1.7 Beskedautentificering og integritet

Autentificering og integritet af beskeder etableres ved hjælp af digitale signaturer, der anvendes på SOAP beskeden. Fortrolighed SKAL etableres ved at bruge en sikker transport protokol (f.eks. ved brug af SSL 3.0 eller TLS 1.1 eller senere).

Afsenderen SKAL oprette og indsætte et og kun et <ds:Signature> element i <wsse:Security> header blokken og dette signature-element SKAL referere: SOAP <Body> elementet.

Alle SOAP header bloke i beskeden der er defineret i denne profil. Signaturen KAN referere andre elementer, herunder header-blokke der ikke er beskrevet i denne profil.

Afsenderens X.509 certifikat SKAL indeholdes i et <wsse:BinarySecurityToken> element i security-headeren. `ValueType` attributen i <wsse:BinarySecurityToken> SKAL have værdien `http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509- token-profile-1.0#X509v3`. I beskedsignaturen SKAL <ds:KeyInfo> elementet referere til denne token via en <wsse:SecurityTokenReference>.

ATP validerer beskedens signatur og security-token, herunder test af udløbsdato og tillid til udstederen af tokenet.

6.2 Eksempel

6.2.1 Request

```
<?xml version="1.0" encoding="UTF-8"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
            xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
            wss-wssecurity-
secext-1.0.xsd"
            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:wsa="http://www.w3.org/2005/08/addressing">
  <s:Header>
    <!-- MessageID skal være en UUID -->
    <wsa:MessageID  wsu:Id="mid">urn:uuid:550e8400-e29b-41d4-a716-446655440000</wsa:MessageID>

    <!-- wsa:To er optionel - ATP forventer den ikke og vi kigger ikke på dens værdi
                      det samme gælder for de optionelle elementer wsa:ReplyTo og
                      wsa:FaultTo--
>
```

```
    <wsa:To Id="to">http://atp.dk/ws/PingService</wsa:To>


       <!-- wsa:Action skal have samme værdi som HTTP action-headeren.

       ATP fortæller anvenderen hvad værdien skal være, når en specifik
operation kaldes, og vi fortæller hvad vi sætter i svarene. Vi prøver at følge
WS Adressing Core: det er RECOMMENDED at action er en IRI, der henviser til en
input, output eller fault-message fra WSDL -->

    <wsa:Action wsu:Id="action">urn:oio:atp:common:pingservice:wsdl:1.0.0:#Ping</wsa:Action>


    <!--Der skal være præcis én wsse:Security header med mustUnderstand="1" -->

    <wsse:Security mustUnderstand="1">

    <!-- Obligatorisk element ATP kontrollerer at tidsstemplet højst er 5 minutter gammelt.
    -->

      <wsu:Timestamp wsu:Id="ts">

        <!-- Created SKAL være tilstede -->

        <wsu:Created>2008-08-17T04:49:17Z</wsu:Created>

        <!-- Valgfrit element Hvis det er til stede vil

          ATP forkaste forespørgslen hvis lokal tid er

          senere end værdien Note til reply: ikke

          nødvendigt                          -->

         <wsu:Expires>2008-08-17T04:52:17Z</wsu:Expires>

      </wsu:Timestamp>

     <wsse:BinarySecurityToken EncodingType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401- wss-soap-message-security-1.0#Base64Binary"
ValueType="http://docs.oasis- open.org/wss/2004/01/oasis-200401-wss-x509-token-
profile-1.0#X509v3" wsu:Id="CertId-24550646" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">MIIE/jCCBGegAwIBAgIE... (X509 cert)

      </wsse:BinarySecurityToken>

      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

      <ds:SignedInfo>¨

            <!-- include the MessageID in the signature -->

           <ds:Reference URI="#mid">...</ds:Reference>

           <!-- include the To in the signature -->

          <ds:Reference URI="#to">...</ds:Reference>

          <!-- include the Action in the signature -->

         <ds:Reference URI="#action">...</ds:Reference>

         <!-- include the Timestamp in the signature -->

        <ds:Reference URI="#ts">...</ds:Reference>

         <!-- bind the body of the message -->

         <ds:Reference URI="#MsgBody">

           <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

           <ds:DigestValue>YgGfS0pi56pu...</ds:DigestValue>

         </ds:Reference>

       </ds:SignedInfo>
```

```
            <ds:KeyInfo>
              <wsse:SecurityTokenReference wsu:Id="STRId-837890545"
        xmlns:wsu="http://docs.oasis- open.org/wss/2004/01/oasis-200401-wss-
        wssecurity-utility-1.0.xsd">
              <wsse:Reference URI="#CertId-24550646"
        ValueType="http://docs.oasis- open.org/wss/2004/01/oasis-
        200401-wss-x509-token-profile-1.0#X509v3" />
            </wsse:SecurityTokenReference>
          </ds:KeyInfo>
          <ds:SignatureValue>
            HJJWbvqW9E84vJVQkjjLLA6nNvBX7mY00TZhwBdFNDElgs
            cSXZ5Ekw==
          </ds:SignatureValue>
</ds:Signatu
         re>
</wsse:Secu
      rity>
    </s:Header>
    <s:Body wsu:Id="MsgBody">
      <atp:Ping xmlns:atp="urn:oio:atp:common:pingservice:1.0.0">
        <atp:Tekst>Hej</atp:Tekst>
      </atp:Ping>
    </s:Body>
    </s:Envelope>
```

6.2.2 Response

```
    <s:Envelope
        xmlns:s="http://schemas.xmlsoap.org/s
        oap/envelope/"
        xmlns:sec="urn:liberty:security:2006-
        08"
        xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
    wssecurity-secext- 1.0.xsd"
        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:wsa="http://www.w3.org/2005/08/addressing">
      <s:Header>
        <!--  MessageID skal være en UUID. Vi sender et nyt tilbage i svarbeskeden.
    Vi logger MessageID i svarbeskeder.
        -->
        <wsa:MessageID  wsu:Id="mid">urn:uuid:550e8400-e29b-41d4-a716-487329473223</wsa:MessageID>

        <!-- Værdien af RelatesTo er den samme som værdien af messageid-feltet i requestet.-->
        <wsa:RelatesTo wsu:Id="relatesTo">urn:uuid:550e8400-e29b-41d4-a716-
```

```
446655440000</wsa:RelatesTo>


<!-- wsa:Action Det samme som i Requesten + Response eller Fault (hvis vi returnerer en
fejl)
<wsa:Action wsu:Id="action">urn:oio:atp:pdk:pingservice:wsdl:1.0.0:#PingResponse</wsa:Action>
    <!-- Der skal være præcis en wsse:Security header med mustUnderstand="1" -->
    <wsse:Security mustUnderstand="1">
      <!-- Obligatorisk element ATP sætter tidsstemplet. -->
      <wsu:Timestamp wsu:Id="ts">
        <!-- Liberty SOAP 3.7 Created SKAL være tilstede -->
        <wsu:Created>2008-08-17T04:49:17Z</wsu:Created >
      </wsu:Timestamp>
     <wsse:BinarySecurityToken EncodingType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401- wss-soap-message-security-1.0#Base64Binary"
                               ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401- wss-x509-token-profile-1.0#X509v3"
                               wsu:Id="CertId-24550646"
xmlns:wsu="http://docs.oasis- open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">
                MIIE/jCCBGegAwIBAgIE... (X509 cert)
     </wsse:BinarySecurityToken>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <!-- in general include a ds:Reference for each wsa: header added
according to SOAP binding -->
          <!-- include the MessageID in the signature -->
          <ds:Reference URI="#mid">...</ds:Reference>
          <!-- include the To in the signature -->
          <ds:Reference URI="#relatesTo">...</ds:Reference>
          <!-- include the Action in the signature -->
          <ds:Reference URI="#action">...</ds:Reference>
          <!-- include the Timestamp in the signature -->
          <ds:Reference URI="#ts">...</ds:Reference>
          <!-- bind the body of the message -->
          <ds:Reference URI="#MsgBody">
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>YgGfS0pi56pu...</ds:DigestValue>
  </ds:Reference>
</ds:SignedInfo>
          <ds:KeyInfo>
                    <wsse:SecurityTokenReference wsu:Id="STRId-837890545"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd">
```

```
                <wsse:Reference URI="#CertId-24550646"
        ValueType="http://docs.oasis- open.org/wss/2004/01/oasis-
        200401-wss-x509-token-profile-1.0#X509v3" />

                        </wsse:SecurityTokenReference>

              </ds:KeyInfo>

              <ds:SignatureValue>

                HJJWbvqW9E84vJVQkjjLLA6nNvBX7mY00TZhwBdFNDElgscSXZ5Ekw==

              </ds:SignatureValue>

</ds:Signature
             >

</wsse:Securi
          ty>

       </s:Header>

         <s:Body wsu:Id="MsgBody">

           <atp:PingResponse xmlns:atp="urn:oio:atp:common:pingservice:1.0.0">

             <atp:Tekst>Hej</atp:Tekst>

             <atp:Dato>Hej</atp:Dato>

             <atp:Klokken>Hej</atp:Klokken>

           </atp:PingResponse>

         </s:Body>

           </s:Envelope>
```

7. Miljøer hos ATP

ATP opererer med 4 miljøer, som skal anvendes til udviklings-, test- og produktionsformål.

Miljø	CA For certifikater	Data
Udviklingsmiljø	TDC OCES Systemtest CA II (er under udfasning) eller TRUST2408 Systemtest VIII CA eller TRUST2408 Systemtest XIX CA	Indeholder ikke data Services er stubbet af
Integrationstestmiljø	TDC OCES Systemtest CA II (er under udfasning) eller TRUST2408 Systemtest VIII CA eller TRUST2408 Systemtest XIX CA	Indeholder anonymiserede data

Miljø	CA For certifikater	Data
Pilotmiljø (Pre-Produktion)	TDC OCES Systemtest CA II (er under udfasning) eller TRUST2408 Systemtest VIII CA eller TRUST2408 Systemtest XIX CA	Indeholder anonymiserede data
Produktionsmiljø	TDC OCES CA (er under udfasning) eller TRUST2408 OCES CA 1	Produktionsdata

I ATP's WS implementation i udviklingsmiljøet eksisterer en PingService, der af anvender kan benyttes til at afprøve, at tilslutningen til ATP fungerer, og at den i dette dokument beskrevne standard overholdes.

8. Source IP Filtrering

For at sikre testmiljøerne og i nogle tilfælde også produktionsmiljøet tilføjer ATP source IP address filtrering på de forskellige endpoints. Dette medfører, at kunden skal levere en liste af IP net - evt. en enkelt IP adresse som SOAP kald vil komme fra - til de forskellige miljøer.

9. Referencer

[IDWS-Scenarios] OIO IDWS Scenarios, Version 1.1“, Danish IT and Telecom Agency

[LIB-Basic] Liberty Basic SOAP Binding 1.0”, Liberty Alliance Project.

[OIO-BOOT] OIO Bootstrap Token Profile Version 1.0.1”, Danish IT and Telecom Agency

[OIO-IDT] OIO SAML Profile for Identity Tokens V1.0”, Danish IT and Telecom Agency

[OIO-Priv] OIOSAML Basic Privilege Profile 0.9.doc

[OIO-SSO] OIO Web SSO Profile V2.0.7

[OIO-WST] OIO WS-Trust Profile V1.0.1”, Danish IT and Telecom Agency.

[OIO-WST-DEP] OIO WS-Trust Deployment Profile Version 1.0”, Danish IT and Telecom Agency

[SAMLCoreV2] Oasis Standard, S. Cantor, J. Kemp, R. Philpott, E. Maler (Editors), Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005

[UUID] A Universally Unique IDentifier (UUID) URN Namespace
http://www.ietf.org/rfc/rfc4122.txt

[WST] WS-Trust 1.3, OASIS Standard, 19 March 2007

[TID] "Politik for tidssætning", Økonomistyrelsen
http://www.skat.dk/SKAT.aspx?oId=1790376&vId=0