

SOSI STS teknisk beskrivelse

Version 1.0.1

Status: offentliggjort

Indholdsfortegnelse

1	Introduktion.....	2
1.1	Baggrund.....	2
1.2	Formål.....	2
1.3	Baggrundsmateriale.....	2
1.4	Adgang.....	2
2	STS Webservice.....	2
2.1	SOSI STS Schema reference.....	3
2.2	IssueIDCard.....	3
2.2.1	Verifikation af ID-kort.....	8
2.3	Fejl og Fejlkoder.....	11
3	Appendix A – formelt skema (WSDL).....	14

1 Introduktion

1.1 Baggrund

SOSI har defineret et ID-kort aktører i sundhedssektoren kan benytte til sikker udveksling af akkreditiver. En mulig udsteder af disse ID-kort hedder STS tidligere kendt som IdP. Bevæggrunden for at udvikle STS'en kan man læse mere om på www.sosi.dk

1.2 Formål

Dette dokumentets formål er at dokumentere interfacet og opførelse af den webservice der er udstillet til at udstede ID-kort. Samt at opstille nogle testscenarier en klient skal kunne håndtere.

1.3 Baggrundsmateriale

Man kan nøjes med at læse dette dokument, men det kræver forståelse for SOSI og de standarder der bygges på. Denne liste af standarder er at finde på www.sosi.dk

- XML Schema (<http://www.w3.org/XML/Schema>)
- OIOXML (<http://www.oio.dk/dataudveksling/OIOXML>)
- SOAP (<http://www.w3.org/TR/SOAP/>)
- HTTP (<http://www.ietf.org/rfc/rfc2616.txt>)
- WS-Security (<http://www-106.ibm.com/developerworks/webservices/library/ws-secure/>)
- OCES (<https://www.signatursekretariatet.dk/certifikatpolitikker.html>)
- SHA-1, Md5 (<http://www.secure-hash-algorithm-md5-sha-1.co.uk/>)
- XMLSig (<http://www.w3.org/TR/xmlsig-core/>)
- SAML (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security)

1.4 Adgang

Der kræves adgang til sundhedsdatanettet for at kunne benytte STS webservicen.

Test Webservicen findes på URL: <http://pan.certifikat.dk/sts/services/SecurityTokenService>

2 STS Webservice

Der udstilles kun en operation i STS'en, dokumentation er skrevet så dette kan udvides uden at strukturen bliver anderledes.

2.1 SOSI STS Schema reference

Denne sektion har en udtømmende liste af de services der udstilles, der er initielt 1 service.

SOSI STS teknisk beskrivelse

Services understøttet:

- **IssueIDCard:** *IssueIDCardIn*, *IssueIDCardOut*

Check WSDL i appendix A for den formelle definition af in og out værdier.

2.2 IssueIDCard

Formålet med IssueIDCard er at:

1. Verificere det i *IssueIDCardRequest* vedlagte ID-kort
2. Udstede (signere) eller afvise at udstede et ID-kort

I de følgende underkapitler beskrives først normal tilfældet hvor alt går godt og i det efterfølgende de fejl man skal håndtere.

For at undgå yderligere forvirring er her en matrix over forskellige ID-kort og hvilke der udstedes af STS'en.

Autentifikation Level	Type	Lovlig	Udstedes af STS
1		Ja	Nej
2		Ja	Nej
3	system	Ja	Ja
3	user	Ja	Ja
4	system	Nej	Nej
4	user	Ja	Ja

- I et autentifikation level 3 request skal ID-kortet VOCES signeres.
- I et autentifikation level 4 request skal ID-kortet MOCES signeres.
- I et system kort skal der indgå en SystemLog, det er en fejl hvis der er en UserLog.
- I et user kort skal der indgå en SystemLog og en UserLog.

Dokumentation for indholdet af de forskellige felter og forskellen på strukturen af ID-kort i user og system ID-kort versionerne er udenfor scopet af dette dokument, man kan læse om dette i DGWS dokumentationen.

Eksempel autentifikation level 4 request:

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope
  id="Envelope"
  xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:wssse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
  xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
```

SOSI STS teknisk beskrivelse

```
xmlns:medcom="http://www.medcom.dk/dgws/2006/04/dgws-1.0.xsd"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:sosi="http://www.sosi.dk/sosi/2006/04/sosi-1.0.xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<soap:Header>
  <wsse:Security>
    <wsu:Timestamp>
      <wsu:Created>
        2006-09-01T13:15:00Z
      </wsu:Created>
    </wsu:Timestamp>
  </wsse:Security>
</soap:Header>
<soap:Body>
  <wst:RequestSecurityToken Context="www.sosi.dk">
    <wst:TokenType>urn:oasis:names:tc:SAML:2.0:assertion</wst:TokenType>
    <wst:RequestType>http://schemas.xmlsoap.org/ws/2005/02/security/trust/I
ssue</wst:RequestType>
    <wst:Claims>
      <saml:Assertion
        IssueInstant="2006-08-31T15:29:53"
        Version="2.0"
        id="IDCard">
        <saml:Issuer>testissuer</saml:Issuer>
        <saml:Subject>
          <saml:NameID
Format="medcom:cprnumber">2601610143</saml:NameID>
          <saml:SubjectConfirmation>
            <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:2.0:cm:hol
der-of-key</saml:ConfirmationMethod>
            <saml:SubjectConfirmationData>
              <ds:KeyInfo>
                <ds:KeyName>OCESSignature</ds:KeyName>
              </ds:KeyInfo>
            </saml:SubjectConfirmationData>
          </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions>
          <NotBefore>2006-08-31T15:29:53</NotBefore>
          <NotOnOrAfter>2006-09-01T15:29:53</NotOnOrAfter>
        </saml:Conditions>
        <saml:AttributeStatement id="IDCardData">
          <saml:Attribute Name="sosi:IDCardID">
            <saml:AttributeValue>QFn9t9t01F/j78YqUiBWVA==</saml:Attribu
teValue>
          </saml:Attribute>
          <saml:Attribute Name="sosi:IDCardVersion">
            <saml:AttributeValue>1.0</saml:AttributeValue>
          </saml:Attribute>
          <saml:Attribute Name="sosi:IDCardType">
            <saml:AttributeValue>user</saml:AttributeValue>
          </saml:Attribute>
          <saml:Attribute Name="sosi:AuthenticationLevel">
            <saml:AttributeValue>4</saml:AttributeValue>
          </saml:Attribute>
        </saml:AttributeStatement>
      </saml:Assertion>
    </wst:Claims>
  </wst:RequestSecurityToken>
</soap:Body>
</soap:Envelope>
```

SOSI STS teknisk beskrivelse

```
<saml:AttributeStatement id="UserLog">
  <saml:Attribute Name="medcom:UserCivilRegistrationNumber">
    <saml:AttributeValue>0101340143</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="medcom:UserGivenName">
    <saml:AttributeValue>Anders</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="medcom:UserSurName">
    <saml:AttributeValue>And</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="medcom:UserEmailAddress">
    <saml:AttributeValue>aand@andeby.dk</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="medcom:UserRole">
    <saml:AttributeValue>nurse</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="medcom:UserAuthorizationCode">
    <saml:AttributeValue>19901</saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>
<saml:AttributeStatement id="SystemLog">
  <saml:Attribute Name="medcom:ITSystemName">
    <saml:AttributeValue>SOSITEST</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute
    Name="medcom:CareProviderID"
    NameFormat="medcom:cvrnumber">
    <saml:AttributeValue>orgCVR</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="medcom:CareProviderName">
    <saml:AttributeValue>orgName</saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>
<ds:Signature id="OCESSignature">
  <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="#IDCard">
      <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>RElHRVNU</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>U01HTkFUVVJF</ds:SignatureValue><!-- med
MOCES signatur-->
  <ds:KeyInfo>
    <ds:X509Data>
      <ds:X509Certificate>WDUwOQ==</ds:X509Certificate><!--
med MOCES signatur -->
    </ds:X509Data>
  </ds:KeyInfo>
```

SOSI STS teknisk beskrivelse

```
        </ds:Signature>
    </saml:Assertion>
</wst:Claims>
<wst:Issuer>
    <wsa:Address>http://www.ribeamt.dk/EPJ</wsa:Address>
</wst:Issuer>
</wst:RequestSecurityToken>
</soap:Body>
</soap:Envelope>
```

Eksempel autentifikation level 4 response:

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope
  id="Envelope"
  xmlns:soap="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:wst="http://schemas.xmlsoap.org/ws/2005/02/trust"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
  xmlns:medcom="http://www.medcom.dk/dgws/2006/04/dgws-1.0.xsd"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:sosi="http://www.sosi.dk/sosi/2006/04/sosi-1.0.xsd"
  xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soap:Header>
    <wsse:Security id="amRrMDk3d2doYXB2amY2cg==">
      <wsu:Timestamp>
        <wsu:Created>
          2006-09-01T13:15:00Z
        </wsu:Created>
      </wsu:Timestamp>
    </wsse:Security>
  </soap:Header>
  <soap:Body>
    <wst:RequestSecurityTokenResponse
      wsu:Id="uuiidfd874d3-0106-fa61-dce2-82f3df52fe18"
      Context="www.sosi.dk">
      <wst:TokenType>urn:oasis:names:tc:SAML:2.0:assertion</wst:TokenType>
      <wst:RequestedSecurityToken>
        <saml:Assertion
          IssueInstant="2006-08-31T15:29:53"
          Version="2.0"
          id="IDCard">
          <saml:Issuer>STS</saml:Issuer>
          <saml:Subject>
            <saml:NameID
              Format="medcom:cprnumber">2601610143</saml:NameID>
            <saml:SubjectConfirmation>
              <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:2.0:cm:hol
der-of-key</saml:ConfirmationMethod>
              <saml:SubjectConfirmationData>
                <ds:KeyInfo>
                  <ds:KeyName>OCESSignature</ds:KeyName>
                </ds:KeyInfo>
              </saml:SubjectConfirmationData>
```

SOSI STS teknisk beskrivelse

```
        </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions
        NotBefore="2006-08-31T15:29:53"
        NotOnOrAfter="2006-09-01T15:29:53"/>
    <saml:AttributeStatement id="IDCardData">
        <saml:Attribute Name="sosi:IDCardID">
            <saml:AttributeValue>QFn9t9t01F/j78YqUiBWVA==</saml:Attribu
teValue>

        </saml:Attribute>
        <saml:Attribute Name="sosi:IDCardVersion">
            <saml:AttributeValue>1.0</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="sosi:IDCardType">
            <saml:AttributeValue>user</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="sosi:AuthenticationLevel">
            <saml:AttributeValue>4</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="sosi:OCESCertHash">
            <saml:AttributeValue>3PqinWie9060qTDZFpbI7x4V75w=</saml:Att
tributeValue>

        </saml:Attribute>
    </saml:AttributeStatement>
    <saml:AttributeStatement id="UserLog">
        <saml:Attribute Name="medcom:UserCivilRegistrationNumber">
            <saml:AttributeValue>2601610143</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="medcom:UserGivenName">
            <saml:AttributeValue>Peter</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="medcom:UserSurName">
            <saml:AttributeValue>Buus</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="medcom:UserEmailAddress">
            <saml:AttributeValue>peter@signaturgruppen.dk</saml:Attribu
teValue>

        </saml:Attribute>
        <saml:Attribute Name="medcom:UserRole">
            <saml:AttributeValue>nurse</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="medcom:UserAuthorizationCode">
            <saml:AttributeValue>2101</saml:AttributeValue>
        </saml:Attribute>
    </saml:AttributeStatement>
    <saml:AttributeStatement id="SystemLog">
        <saml:Attribute Name="medcom:ITSystemName">
            <saml:AttributeValue>SOSITEST</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute
            Name="medcom:CareProviderID"
            NameFormat="medcom:cvrnumber">
            <saml:AttributeValue>orgCVR</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="medcom:CareProviderName">
            <saml:AttributeValue>orgName</saml:AttributeValue>
        </saml:Attribute>
    </saml:AttributeStatement>
    <ds:Signature id="OCESSignature">
```

SOSI STS teknisk beskrivelse

```

        <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="#IDCard">
            <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>RElHRVNU</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>U01HTkFUVVJF</ds:SignatureValue><!-- med
VOCES signatur-->
        <ds:KeyInfo>
          <ds:X509Data>
            <ds:X509Certificate>WDUwOQ==</ds:X509Certificate><!--
med VOCES signatur -->
          </ds:X509Data>
        </ds:KeyInfo>
      </ds:Signature>
    </saml:Assertion>
  </wst:RequestedSecurityToken>
  <wst:Status>
    <wst:Code>http://schemas.xmlsoap.org/ws/2005/02/security/trust/statu
s/valid</wst:Code>
  </wst:Status>
  <wst:Issuer>
    <wsa:Address>http://www.sosists.dk/STS</wsa:Address>
  </wst:Issuer>
</wst:RequestSecurityTokenResponse>
</soap:Body>
</soap:Envelope>
```

2.2.1 Verifikation af ID-kort

Autentifikation level og certifikat type afgør hvilke informationer i ID-kortet der kan valideres og verificeres. Det er vigtigt for en forbruger af ID-kort at vide hvilke felter i ID-kortet der er verificeret.

Bemærk at systemLog i xml'en svarer til SystemInfo i seal, og userLog i xml'en svarer til UserInfo i seal.

Første kolonne definerer et reference id til checkene, listen er ikke grupperet efter den rækkefølge checks bliver foretaget i.

ID	Verifikation/felt	Aktion
----	-------------------	--------

SOSI STS teknisk beskrivelse

Generelt		
c1	Xml verifikation	XML parses og i tilfælde af at requestet ikke overholder schemaet defineret i WSDL'en, returneres fejlkode wst:InvalidRequest
c2	Certifikat verifikation	Hvis certifikaterne ikke er defineret korrekt, returneres fejlkode wst:AuthenticationBadElements
c3	sosi:IDCardVersion	Verificeres til at have den version serveren har. Ved fejl returneres fejlkode wst:BadRequest
c4	sosi:IDCardType	Verificeres til at være system eller user, i begge tilfælde skal der være et systemcertifikat, men i user tilfældet skal der derudover være et medarbejdercertifikat. Ved fejl returneres fejlkode wst:BadRequest
c5	sosi:AuthenticationLevel	Verificeres til at være enten 3 eller 4, i tilfældet 3 skal der være signeret med et VOCES certifikat og kan være af type system eller bruger, i tilfældet 4 skal der være signeret med et MOCES certifikat, og typen skal være user. Ved fejl returneres fejlkode wst:BadRequest
c6	NotBefore, NotOnOrAfter	Verificeres at forskellen mellem de to tidsstempler ikke er over 24 timer og og er større end 0, notBefore skal være før ”nu”, dvs der kan ikke udstedes ID-kort der begynder i fremtiden. Ved fejl returneres fejlkode wst:InvalidTimeRange
Systemlog		
	medcom:ITSystemName*	Ingen verification
c7	Udløb	Virksomhedscertifikatets udløbsdato verificeres, hvis udløbet returneres fejlkode wst:FailedAuthentication
c8	Udsteder check	Virksomhedscertifikatets udsteder verificeres, hvis ukendt udsteder returneres fejlkode wst:FailedAuthentication
c9	Spærreliste	Virksomhedscertifikatet verificeres imod spærreliste, hvis spærret returneres fejlkode wst:FailedAuthentication
c10	SOSI-STs ACL	Virksomhedscertifikatet verificeres imod STS whiteliste, returnerer fejlkode wst:FailedAuthentication
c11	medcom:CareProviderID	CVR nummer, verificeres ved sammenligning med cvr i certifikatet, ved fejl returneres fejlkode wst:FailedAuthentication
Userlog		
	medcom:UserGivenName*	Ingen verification
	medcom:UserSurName*	Ingen verification
	medcom:UserEmailAddress*	Ingen verification
c12	Udløb	Medarbejdercertifikatets udløbsdato verificeres, hvis

SOSI STS teknisk beskrivelse

		udløbet returneres fejlkode wst:FailedAuthentication
c13	Udsteder check	Medarbejdercertifikatets udsteder verificeres, hvis ukendt udsteder returneres fejlkode wst:FailedAuthentication
c14	Spærreliste	Medarbejdercertifikat verificeres imod spærreliste, hvis spærret returneres fejlkode wst:FailedAuthentication
c15	SOSI-STs ACL	Medarbejdercertifikat verificeres imod STS blackliste, returnerer fejlkode wst:FailedAuthentication
c16	medcom:UserCivilRegistrationNumber **	Cpr nummer, verificeres ved opslag i pid/cpr, dette gøres kun hvis requestet er signeret med et MOCES certifikat, ved fejl returneres fejlkode wst:FailedAuthentication
c17	medcom:UserRole* ***	Rolle, verificeres ved opslag i autorisationsregisteret, dette gøres kun hvis requestet er signeret med et MOCES certifikat eller der er angivet et cprnummer, ved fejl returneres fejlkode wst:FailedAuthentication
c18	medcom:UserAuthorizationCode* ***	Rolle, verificeres ved opslag i autorisationsregisteret, dette gøres kun hvis requestet er signeret med et MOCES certifikat eller der er angivet et cprnummer, ved fejl returneres fejlkode wst:FailedAuthentication
c19	STS certifikat	Spærreliste og gyldighed checkes for STS certifikatet. Fejler checket returneres fejlkoden wst:RequestFailed

* Anbefalet at udfylde med mindst 1 karakter da seal ellers vil afvise ID-kortet, indholdet bliver ikke valideret

** Hvis værdien er blank og det er et MOCES certifikat vil det blive slået op i pid/cpr registret og tilføjet til ID-kortet

*** Check bliver ikke foretaget hvis blank, hvis autorisationregistreret ikke svarer slettes medcom:UserRole og medcom:UserAuthorizationCode fra id kortet før det signeres, og der returneres ingen fejl, med mindre det er en læge.

Et tip (hvis man ikke bruger seal):

Hvis man bruger seal vil ens ID-kort få skruet tiden 1 minut tilbage for at undgå tidssynkroniserings problemer. Hvis man ikke gør det bør man læse nedenstående.

Hvis man som klient f.eks skruer 1 minut baglæns i tid på NotBefore, NotOnOrAfter i stedet for at brug system tiden vil man miste 1 sekund i levetiden på sit ID-kort, men til gengæld slipper man uden om de værste tidssynkroniserings problemer på tværs af systemer. Selv moderne hardware som vi har i dag har ikke nødvendigvis særligt præcise ure.

Serveren laver et skarpt check på at NotBefore er efter system tiden på STS serveren, og i tilfælde af at klienten er hurtig til at lave et request og STS serveren modtager det hurtigt, risikerer man hvis klienten er bare en lille smule foran STS serveren i tid at få en fejl. Hvis dette skridt gik godt og relativt hurtigt, vil man kunne få et tilsvarende problem lidt senere imod en server man skal bruge ID kortet op imod.

2.3 Fejl og Fejlkoder

STS'en returnerer kun HTTP status koderne 200 og 500. Status kode 200 er forbeholdt tilfældet hvor service kaldet resulterer i et positivt svar, dvs et signeret ID-kort. Status kode 500 benyttes til alle fejltilfælde.

En klient skal dog også håndtere status kode 404 i tilfældet hvor STS'en ikke er i drift og derfor ikke svarer.

Kode 500 optræder hvis:

- Hvis forespørgslen ikke overholder strukturen defineret i WSDL'en
- Hvis indholdet ikke er korrekt (f.eks cpr-nummer der ikke findes)
- Hvis indholdet ikke er understøttet, f.eks autentifikation level 5
- Hvis et integrations punkt fejler eller er nede eller er blevet floodet
- Hvis STS'en fejler pga intern fejl

Der må ikke lækkes for mange informationer og fejlene er derfor med vilje sparsomme og ikke specielt uddybende. Men der er dog tilføjet (uspecificeret) ekstra information i forhold til WS-Trust specifikationen for at gøre fejlfinding nemmere.

Eksempel:

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope
  id="Envelope"
  xmlns:soap="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:wst="http://schemas.xmlsoap.org/ws/2005/02/trust"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:medcom="http://www.medcom.dk/dgws/2006/04/dgws-1.0.xsd"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:sosi="http://www.sosi.dk/sosi/2006/04/sosi-1.0.xsd"
  xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soap:Header>
    ...
  </soap:Header>
  <soap:Body>
    <soap:Fault>
      <faultcode>wst:InvalidRequest</faultcode>
      <faultstring>The request was invalid or malformed</faultstring>
      <faultactor>http://sosi.dk/sts</faultactor>
    </soap:Fault>
  </soap:Body>
</soap:Envelope>
```

SOSI STS teknisk beskrivelse

`Faultcode` indeholder fejlkoden se tabel nedenfor for mulige fejlkoder.

`Faultstring` indeholder en beskrivende fejltekst, første linje af denne fejltekst er i tabellen nedenfor, der kan være ekstra linjer der beskriver hvad der gik galt for at gøre det nemmere at debugge i tilfælde af fejl.

`Faultactor` indeholder URI til systemet der har afsløret fejlen.

System navn	System URI
STS	http://sosi.dk/sts
SEAL	http://sosi.dk/seal
Pid/cpr	https://pid.certifikat.dk/pidwsv2/pidwsdoc
Autoritationsregisteret	http://autorisation.sst.dk/webservices/Autorisation.asmx

Relevante fejl defineret i WS-trust som vi benytter (og vi benytter ikke andre):

medcom:FaultCode	wst:InvalidRequest
faultstring	The request was invalid or malformed
Forklaring	Forkert xml syntax, overholder ikke WSDL'en. Optræder typisk under udvikling eller hvis kontrakten er blevet ændret. En fejlkode der typisk skyldes en fejl i klienten. Eller en ældre version der rammer en nyere server med en ændret WSDL.

medcom:FaultCode	wst:FailedAuthentication
faultstring	Authentication failed
Forklaring	Skyldes at mindst 1 af verificeringerne har givet et negativt svar og betyder at brugeren/systemet ikke kan få et ID-kort.

medcom:FaultCode	wst:RequestFailed
faultstring	The specified request failed
Forklaring	Skyldes en fejl i et af STS's integrations punkter eller intern fejl i STS. Interne fejl dækker over kode fejl og system fejl. F.eks ingen adgang til

SOSI STS teknisk beskrivelse

database.

medcom:FaultCode	wst:AuthenticationBadElements
faultstring	Insufficient Digest Elements
Forklaring	Optræder hvis der er noget galt med indholdet af signaturen, så den ikke kan fortolkes. F.eks hvis encoding er foretaget forkert eller trunkeret. Dette er typisk en klient fejl.

medcom:FaultCode	wst:BadRequest
Faultstring	The specified RequestSecurityToken is not understood.
Forklaring	Optræder hvis klienten tilføjer et element eller værdi som er lovligt i WSDL'en men som STS'en ikke forstår. Det kunne f.eks være autentifikation level 2, eller hvis klienten har bygget et ID-kort med en ældre version end STS'en.

medcom:FaultCode	wst:InvalidTimeRange
Faultstring	The requested time range is invalid or unsupported
Forklaring	Optræder hvis klienten forespørger en varighed af ID-kortet der ikke er understøttet

3 Appendix A – formelt skema (WSDL)

Der er to forskellige skemaer, den ene er til test og den anden til produktion serveren.

Denne sektion indeholder den komplette WSDL for Test STS servicen, der er vedlagt for at gøre dette dokument selvindeholdt. Det er værd at bemærke at de importede xsd dokumenter ikke er standarderne men indskrænkede versioner der passer til den konkrete anvendelse.

Produktion STS servicen indeholder en selv indeholdt version med de officielle skemaer.

NOTE:

WSDL'en der er vist her er et snapshot af den korrekte WSDL taget på tidspunktet hvor dette dokument sidst blev redigeret.

Denne WSDL er derfor ikke nødvendigvis i den seneste version, og må derfor ikke benyttes til at lave en implementation af en klient til STS'en.

En URL til den korrekte WSDL står i det indledende kapitel.

```
<?xml version="1.0"?>
<definitions name="sts"
targetNamespace="http://www.sosi.dk/webservices/sts/1.0/"
  xmlns:sts="http://www.sosi.dk/webservices/sts/1.0/"
  xmlns:medcom="http://www.medcom.dk/dgws/2006/04/dgws-1.0.xsd"
  xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
  xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns="http://schemas.xmlsoap.org/wsdl/">
<types>

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<xsd:import namespace="http://www.medcom.dk/dgws/2006/04/dgws-1.0.xsd"
schemaLocation="medcom.xsd"/>
</xsd:schema>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<xsd:import namespace="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" schemaLocation="wsse.xsd"/>
</xsd:schema>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<xsd:import namespace="http://schemas.xmlsoap.org/ws/2005/02/trust"
schemaLocation="ws-trust.xsd"/>
</xsd:schema>
</types>

<message name="issueIDCardIn">
<part name="header_wsse" element="wsse:Security"/>
<part name="parameters" element="wst:RequestSecurityToken"/>
</message>
<message name="issueIDCardOut">
<part name="header_wsse" element="wsse:Security"/>
<part name="parameters" element="wst:RequestSecurityTokenResponse"/>
</message>
```

SOSI STS teknisk beskrivelse

```
<portType name="stsServicePort">
  <operation name="issueIDCard">
    <input message="sts:issueIDCardIn"/>
    <output message="sts:issueIDCardOut"/>
  </operation>
</portType>

<binding name="stsServiceBinding" type="sts:stsServicePort">
  <soap:binding style="document"
  transport="http://schemas.xmlsoap.org/soap/http"/>

  <operation name="issueIDCard">
    <soap:operation soapAction="http://sosi.org/webservices/sts/1.0/stsService"
    style="document"/>

    <input>
      <soap:header message="issueIDCardIn" part="header_wsse" use="literal"/>
      <soap:body use="literal" parts="parameters"/>
    </input>

    <output>
      <soap:header message="issueIDCardOut" part="header_wsse" use="literal"/>
      <soap:body use="literal" parts="parameters"/>
    </output>

    <fault name="dgwsfault">
      <soap:fault name="sts:DgwsFaultMessage"/>
    </fault>
  </operation>
</binding>

<service name="stsService">
  <port name="sts:stsServicePort" binding="sts:stsServiceBinding">
    <soap:address
    location="http://pan.certifikat.dk/sts/services/securityTokenService"/>
  </port>
</service>

</definitions>
```