STS support

FMK teknikermøde, 7/9-2011

Morten Kvistgaard
mkn@arosii.dk

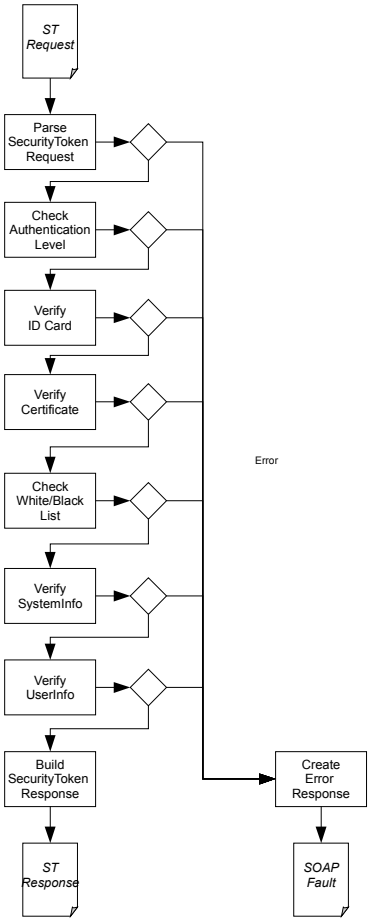
Hvem er vi?

- **Lille softwarehus på Katrinebjerg, Århus**
  - **Primært sundhed og energi**
- **Involveret i NSP**
  - **Support og integration**
- **Leverandør og support af STS**
  - **Involveret siden pilotfasen (2006)**

STS anvendelse

- **Web service udstillet på SDN**
  - **Test service alment tilg**
- **Direkte kald af STS service**
  - **Seal.Java/Seal.NET: NSI understøttede komponenter**
  - **Roll-your-own**
  - **Adgang til STS forespørgsel og svar**
- **Indirekte kald**
  - **Gennem DCC/Gateway**
  - ***Ikke* direkte adgang STS forespørgsel og svar**

Behandling af forespørgsel



1. Deserialiser forespørgsel
2. Check ID-kort
3. Check certifikat
4. Check ACL
5. Check systemoplysninger
6. Check brugeroplysninger
7. Signer ID-kort
8. Serialiser svar

STS fejlsvar

```
<?xml version="1.0" encoding="UTF-8" ?>
<soapenv:Envelope ...>
  <soapenv:Header>
    <wsse:Security id="">
      <wsu:Timestamp>
        <wsu:Created>2011-04-12T15:17:39</wsu:Created>
      </wsu:Timestamp>
    </wsse:Security>
  </soapenv:Header>
  <soapenv:Body>
    <soapenv:Fault>
      <faultcode>wst:InvalidRequest</faultcode>
      <faultstring>The request was invalid or malformed</faultstring>
      <faultactor>http://sosi.dk/sts</faultactor>
    </soapenv:Fault>
  </soapenv:Body>
</soapenv:Envelope>
```

- Timestamp
  - Servertid for svar
- faultcode
  - Klassifikation, angiver fejltypen
- faultactor
  - Klassifikation, angiver oprindelse af fejl
- faultstring
  - Detailinformation, primær information for support

Supporthenvendelser

- **Produktion eller testmiljø**
- **Tidspunkt for STS-kald**
- **Faultcode, -actor, -string**

- **Certifikatoplysninger**
- **Fejlende forespørgsel**
  - **STS forespørgsel**
  - **ID-kort ID (**<*saml:Attribute Name="sosi:IDCardID"*>**)**

Eksempel: Tidssynkronisering

STS svar	**faultcode** = wst:InvalidTimeRange **faultactor** = http://sosi.dk/sts **faultstring** = The requested time range is invalid or unsupported: IDCard is created after or expires before current system time
Årsag	Anvenderfejl, STS fejl
Forklaring	ID-kortet er udstedt på et system, der ikke er tidssynkroniseret med STS. Hvis tiden afviger signifikant (der tillades nogen tidsdrift), kan ID-kortet ikke udstedes.
Løsning	Undersøg om anvenderens IT-system anvender korrekt tid Check om NTP anvendes, evt. hyppighed og NTP server Synkroniser tid

Eksempel: Ugyldig føderation

STS svar	**faultcode** = wst:FailedAuthentication **faultactor** = http://sosi.dk/sts **faultstring** = Authentication failed: certificate issued by invalid party
Type	Anvenderfejl
Forklaring	Det underskrivende certifikat er ikke udstedt i føderationen og kan derfor ikke anvendes til udstedelse af ID-kort.
Løsning	Undersøg hvilken STS der er brugt, dvs. Test eller Produktion. Undersøg hvilken CA der har udstedt certifikatet

Eksempel: Forkert CPR-nummer relation

STS svar	**faultcode** = wst:FailedAuthentication **faultactor** = https://test.lra.certifikat.tdc.dk/sundhedsportalws/HandleSundhedsportalWS **faultstring** = Authentication failed: cvrrid-cpr mismatch [CVR:*-RID:*,*]
Type	
Forklaring	MOCES Certifikat og CPR-nummer fra ID-kort stemmer ikke overens, og identitet kan ikke bekræftes.
Løsning	Undersøg om CPR i ID-kort er som forventet Undersøg hvilket CPR er tilknyttet certifikatet (DanID)

Spørgsmål