



SWAMID

Swedish Academic Identity Federation



SWAMID

SWAMID byter signerings- nyckel för SAML-metadata

SWAMID Webinar 5 2016

Fredrik Domeij

SWAMID Operations, Umeå universitet

fredrik.domeij@umu.se



SWAMID

Varför byts SWAMIDs signeringsnyckel

- När signeringsnyckeln för SAML-metadata skapades i början av maj 2007 valdes en giltighetstid på 10 år
- Nu har 10 år passerat och signeringsnyckeln blir ogiltig 1 maj 2017



SWAMID

Vad betyder detta?

- SWAMID signerar federationens metadata med en asynkron krypteringsnyckel med tillhörande signeringscertifikat
- Signeringen garanterar att den metadata som du laddar ner till din IdP eller din SP kommer från SWAMID
- Du behöver uppdatera signeringsnyckel och metadataflöde i din IdP eller din SP



SWAMID

- **Gammal signeringsnyckel för SWAMID**
 - <http://md.swamid.se/md/md-signer.crt>
 - Subject: CN=SWAMID metadata signer v1.1
 - Giltigt från **4 maj 2007** till **1 maj 2017**
 - <http://md.swamid.se/md/swamid-2.0.xml> för IdP:er
 - <http://md.swamid.se/md/swamid-idp.xml> för SP:s (bara SWAMID)
 - <http://md.swamid.se/md/swamid-idp-transitive.xml> för SP:s (SWAMID+eduGAIN)

- **Ny signeringsnyckel för SWAMID**
 - Flyttar från md.swamid.se till **mds.swamid.se**
 - <http://mds.swamid.se/md/md-signer2.crt>
 - SHA256 fingerprint:
A6:78:5A:37:C9:C9:0C:25:AD:5F:1F:69:22:EF:76:7B:
C9:78:67:67:3A:AF:4F:8B:EA:A1:A7:6D:A3:A8:E5:85
 - Subject: CN=**SWAMID metadata signer v2.0**
 - Giltigt från **6 dec 2016** till **6 dec 2036**
 - <http://mds.swamid.se/md/swamid-2.0.xml> för IdP:er
 - <http://mds.swamid.se/md/swamid-idp.xml> för SP:s (bara SWAMID)
 - <http://mds.swamid.se/md/swamid-idp-transitive.xml> för SP:s (SWAMID+eduGAIN)



SWAMID

Konfigurera ADFS

- Gäller SWAMIDs rekommenderade importskript för ADFS,
`New-RelyingPartyFromMetadata.ps1`

`Invoke-WebRequest http://mds.swamid.se/md/swamid-2.0.xml`



SWAMID

Konfigurera Shibboleth Identity Provider v3

1. Ladda ner nya md-signer2.crt och lägg bredvid md-signer.crt

```
wget http://mds.swamid.se/md/md-signer2.crt
```

2. Verifiera nyckelns signatur

```
openssl x509 -noout -fingerprint -sha256 -in md-signer2.crt  
A6:78:5A:37:C9:C9:0C:25:AD:5F:1F:69:22:EF:76:7B:  
C9:78:67:67:3A:AF:4F:8B:EA:A1:A7:6D:A3:A8:E5:85
```



SWAMID

Konfigurera Shibboleth Identity Provider v3

3. Ändra sökväg till nyckeln i metadata-providers.xml

```
certificateFile="%{idp.home}/credentials/md-signer2.crt"
```

4. Ändra metadataflöde i metadata-providers.xml

```
metadataURL="http://mds.swamid.se/md/swamid-2.0.xml"
```

5. Starta om Shibboleth och kontrollera så det inte skrivs något fel i loggarna



SWAMID

Konfigurera Shibboleth Service Provider v2

1. Ladda ner nya md-signer2.crt och lägg bredvid md-signer.crt

```
wget http://mds.swamid.se/md/md-signer2.crt
```

2. Verifiera nyckelns signatur

```
openssl x509 -noout -fingerprint -sha256 -in md-signer2.crt  
A6:78:5A:37:C9:C9:0C:25:AD:5F:1F:69:22:EF:76:7B:  
C9:78:67:67:3A:AF:4F:8B:EA:A1:A7:6D:A3:A8:E5:85
```



SWAMID

Konfigurera Shibboleth Service Provider v2

3. Ändra sökväg till nyckeln i shibboleth2.xml

```
certificate="md-signer2.crt"
```

4. Ändra metadataflöde i shibboleth2.xml

```
uri="http://mds.swamid.se/md/swamid-idp-transitive.xml"
```

alternativt

```
uri="http://mds.swamid.se/md/swamid-idp.xml"
```

5. Starta om shibd och kontrollera så det inte skrivs något fel i loggarna



SWAMID

Tidsplan

- Den nya metadatan finns tillgänglig från 7 dec 2016
- Den gamla metadatan slutar fungera 30 apr 2017
- Gamla metadatan (md.swamid.se) kommer att fungera parallellt med nya metadatan (mds.swamid.se) fram till sista april 2017
- Samma innehåll i metadatan på md.swamid.se och mds.swamid.se, endast ny signeringsnyckel
- Bytet kan göras när som helst i IdP:er och SP:s, endast kort avbrott för omstart



SWAMID

Mer information

Nyckelceremonin

<https://wiki.swamid.se/display/SWAMID/Nyckelrullning+2016+-+Nyckelceremoni>

Konfiguration

<https://wiki.swamid.se/display/SWAMID/Nyckelrullning+2016>