

Nyckelrullning 2016

SWAMID:s gamla certifikat för signering av SWAMID:s metadata upphör att gälla 1 Maj 2017. På denna sida, inklusive undersidor, beskrivs hur du uppdaterar för att det skall fungera i framtiden.

Den 8 december 2016 genomfördes ett webinar som presenterade vad nyckelbytet innebär för dig som IdP eller SP, se [SWAMID Webinar 5 2016](#). Den 21 mars 2017 genomfördes ett andra webinar om nyckelbytet, se [SWAMID Webinar 1 2017 - SWAMID:s signeringsnyckel löper ut](#).

Vilka använder fortfarande fel metadata?

SWAMID sammanställer kontinuerligt en lista med de IP-adresser som laddar ner metadata som är signerade med den gamla nyckeln. De som laddar ner dessa metadata måste genomföra bytet av nedladdningsplats och signeringsnyckel senast den sista april 2017!

Listan finns på SWAMID:s sida att hämta på följande adress: <http://md.swamid.se/md/deprecated-metadata-downloads/>

1. SWAMID skapar nytt signeringsnyckelpar

Första steget i att byta signeringsnyckel för SWAMID är att skapa en ny signeringsnyckelpar enligt en väl definierad process.

- [Nyckelrullning 2016 - Nyckelceremoni](#)

Den nya signeringsnyckeln finns på adressen <http://mds.swamid.se/md/md-signer2.crt> och har

- 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 och
- är giltig från 6 december 2016 till 6 december 2036

2. SWAMID skapar nya metadataflöden signerade av den nya signeringsnyckeln

Ny nyckel och metadata signerad med den nya nyckeln finns på adressen <http://mds.swamid.se/md/>.

3. Identitetsutgivare (IdP) ändrar så att de använder metadata signerat med den nya signeringsnyckeln

Identitetsutgivare använder metadataströmmen

- <http://mds.swamid.se/md/swamid-2.0.xml>

Instruktioner för identitetsutfärdare:

- [Nyckelrullning 2016 - ADFS med SWAMID importskript](#)
- [Nyckelrullning 2016 - Shibboleth Identity Provider v3](#)

4. Tjänsteleverantörer (SP) ändrar så att de använder metadata signerat med den nya signeringsnyckeln

Tjänsteleverantörer använder metadataströmmen

- <http://mds.swamid.se/md/swamid-idp.xml> om endast användare inom SWAMID ska kunna använda tjänsten eller
- <http://mds.swamid.se/md/swamid-idp-transitive.xml> om användare både inom SWAMID och internationella användare genom inter federationen eduGAIN ska kunna använda tjänsten.

Instruktioner för tjänsteleverantörer:

- [Nyckelrullning 2016 - Shibboleth Service Provider v2](#)