Nya certifikat i IdP 2022

Innehåll:

- Tidsplan för certifikatsbyten
- IdP SAML Metadata
  - Tidsplan för byte av nyckel för signering av biljett
  - Utförande på er SP
  - Adresser för nerladdning av metadata
- OIDC RP-information
  - Adresser för nerladdning av signeringsnycklar (OIDC)

Eftersom det nya certifikatet kommer med en förnyad nyckel för signering av SAML-biljetten så kommer detta att påverkar alla tjänster (SP/RP) som använder IdP.

SP/RP måste se till att ladda ner den nya nyckeln. För SAML-SP betyder det att byta ut IdP-metadata. För OIDC-RP måste förvaltaren kontrollera rutinen för att byta ut denna och vidta åtgärder ifall byte inte sker automatiskt.

Läs om strategin för bytet nedan om du ansvarar för en SAML-SP och längst ner på sidan för RP/OIDC-information!

Under våren går certifikaten som används för signering av metadata och meddelanden i Ineras IdP ut. Certifikaten och nycklarna byts därför ut.

Notera att det också är ett **annat utfärande certifikat** från SITHS än tidigare:

- För PRODUKTION: SITHS e-id Function CA v1
- För TEST/QA: TEST SITHS e-id Function CA v1

Tidsplan för certifikatsbyten

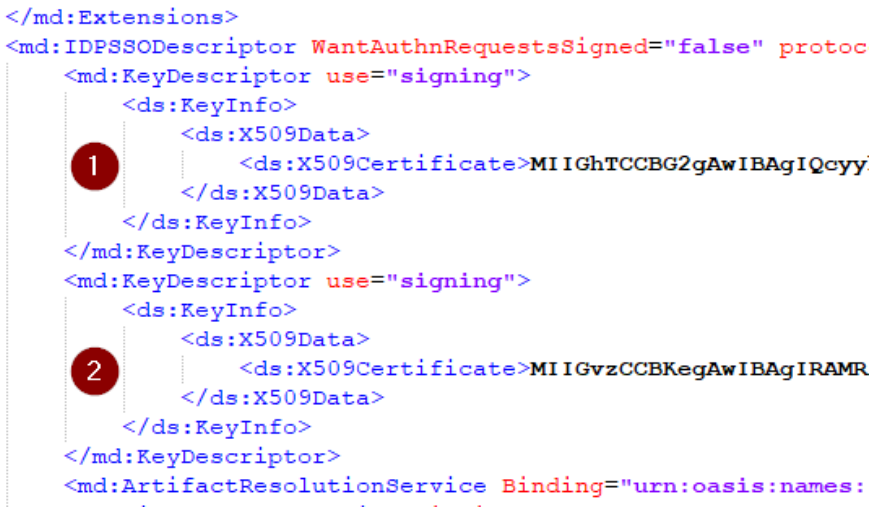
Datum	Miljö	Aktivitet
10 Mar 2022	**TEST/QA**	Publicering av nytt metadata för anslutna SP:s (se nedan)
07 Apr 2022 Klockan 11:00	**TEST/QA**	Byte av IdP:ns certifikat och nyckel för signering av biljetter.
10 Mar 2022	**PRODUKTION**	Publicering av nytt metadata för anslutna SP:s (se nedan)
04 May 2022 Klockan 11:00	**PRODUKTION**	Byte av IdP:ns certifikat och nyckel för signering av biljetter.

IdP SAML Metadata

> **SP-INFO**
>
> INFORMATION TILL DE SOM ANSVARAR FÖR EN SERVICE PROVIDER (SP), ELLER RELAYING PARTY (RP), ANSLUTEN TILL INERAS IdP

Nyckeln som ligger i certifikatet i befintligt metadata som används av IdP för signering av SAML-biljetten/OIDC tokens kommer att förnyas i samband med certifikatsbytet. Därför förväntas alla Service Providers (SP:ar) anslutna till Säkerhetstjänsters IdP ladda ner och byta ut metadata för denna enligt informationen i detta dokument.

För att alla SP:ar ska kunna få en sömlös övergång till det nya certifikatet kommer alla IdP under en period innan certifikatsbytet att publicera metadata med dubbla certifikat (KeyDescriptors) där endast ett av certifikaten används för signering av SAML-biljetten. SP:ar som har laddat ner och installerat detta metadata kommer då alltså vara förberedda att fungera med både det gamla och nya certifikatet och får då en sömlös övergång.



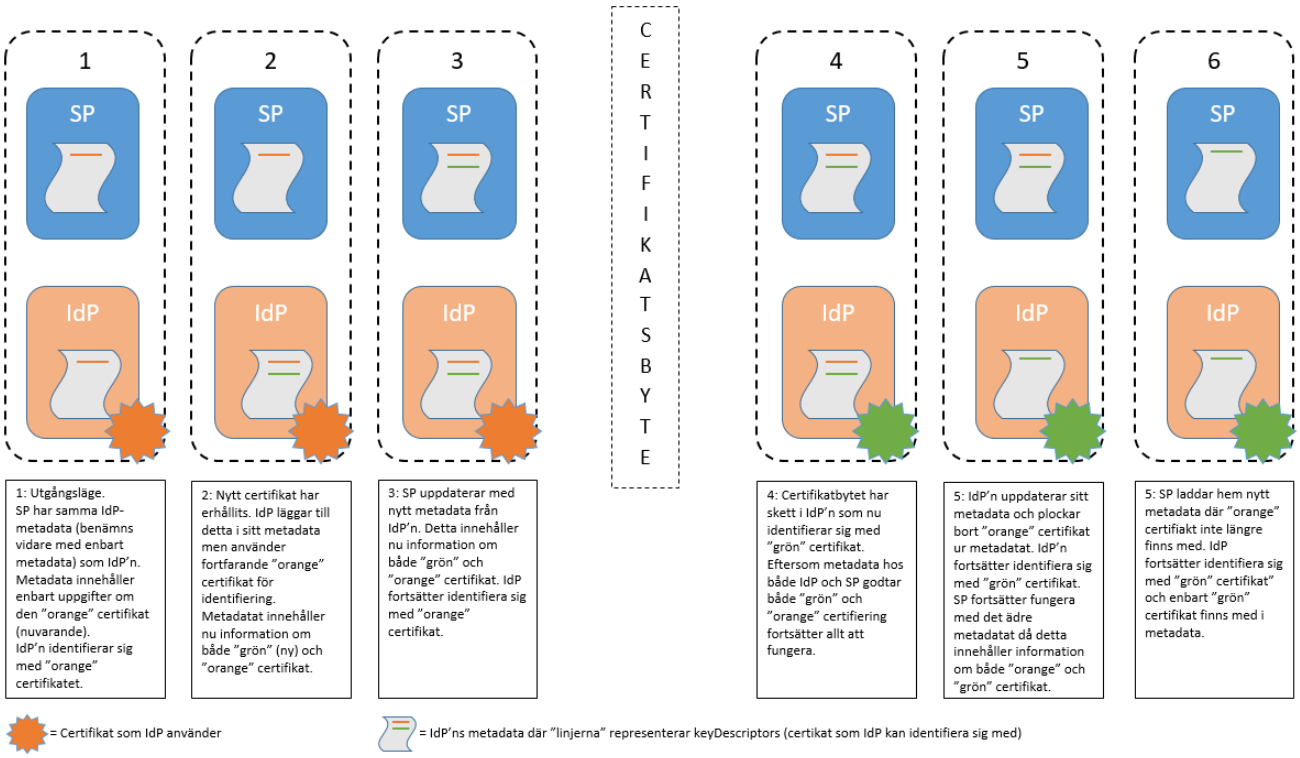

```
</md:Extensions>
<md:IDPSSODescriptor WantAuthnRequestsSigned="false" protoc
    <md:KeyDescriptor use="signing">
        <ds:KeyInfo>
            <ds:X509Data>
                <ds:X509Certificate>MIIGhTCCBG2gAwIBAgIQcyy
            </ds:X509Data>
        </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:KeyDescriptor use="signing">
        <ds:KeyInfo>
            <ds:X509Data>
                <ds:X509Certificate>MIIGvzCCBKegAwIBAgIRAMR
            </ds:X509Data>
        </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:ArtifactResolutionService Binding="urn:oasis:names:
```

Alla SP:ar förväntas stödja dubbla KeyDescriptors i IdP:ns metadata och ha verifierat detta innan arbetet med certifikatsbytet påbörjas. Detta enligt SP-kraven i IdPns SAML-Profil (Saml2Int).

En SP som inte har stöd för dubbla KeyDescriptors i IdP:ns metadata kommer att vara tvungen att byta ut sitt metadata i samma stund som IdP:n byter certifikat för att kunna verifiera signeringen av SAML-biljetten efter bytet.

Efter certifikatsbytet återgår IdP:erna till att publicera metadata med endast det nya certifikatet och SP:ar kan "städa upp" genom att ladda ner nytt metadata igen innehållandes endast det nya certifikatet.

Strategin visualiseras med bilden nedan:



Klicka på bilden för en större bild...

Tidsplan för byte av nyckel för signering av biljett

Miljö	Publicering av nytt metadata med dubbla certifikat (steg 2)	Certifikatsbyte - metadata publiceras åter med endast ett certifikat (steg 5)
TEST/QA https://idp.ineratest.org/ https://idp.ineraqa.org/	10 Mar 2022	07 Apr 2022 Klockan 11:00
PRODUKTION https://idp.inera.se	10 Mar 2022	04 May 2022 Klockan 11:00

Utförande på er SP

1. Säkerställ att er SP är förberedd för metadata med dubbla certifikat/KeyDescriptors innan ni går till punkt 2.
   - Observera att om detta stöd inte finns eller införs måste SP:n byta metadata i samma stund som IdP:n byter certifikatet.
   - En SP utan detta stöd kan dock fortsätta att använda sitt gamla IdP-metadata tills dess att IdP:n byter certifikatet.

2. **Mellan datum för Publicering av nytt metadata med dubbla certifikat och Certifikatsbyte:** Ladda ner IdP:ns nya metadata och installera detta i er SP för att klara av både det gamla och nya certifikatet och få en sömlös övergång.
   - Nedladdningslänkar för aktuell IdP hittas i listan över *Adresser för nerladdning av metadata* nedan.

3. **Efter datum för Certifikatsbyte:** Ladda ner IdP:ns nya metadata och installera detta i er SP för att endast ha det nya certifikatet i IdP:ns metadata (uppstädning).

Adresser för nerladdning av metadata

- **Test**: https://idp.ineratest.org/saml
- **QA/Stage**: https://idp.ineraqa.org/saml
- **Produktion**: https://idp.inera.se/saml

Vissa .NET-bibliotek validerar inte metadata ovan p.g.a. en skillnad i kanonisering av xml när det kommer till namespace-deklarationen xmlns: xml. IdP använder OpenSAML som i sin tur använder Apache Santuario vars kanonisering skiljer sig från den som utförs av .NET System. Security.Cryptography.Xml.SignedXml.CheckSignature()

Om er tjänst inte validerar IdP-metadata från länkarna ovan så finns modifierat metadata tillgängligt för nerladdning nedan. Den enda skillnaden är att namespace-deklarationerna `xmlns:xml="http://www.w3.org/XML/1998/namespace"` är borttagna manuellt där de förekommer inuti `<md:Organization>` -elementet.

- **Test:** idp-metadata_test_remove_ns.xml
- **QA/Stage:** idp-metadata_qa_remove_ns.xml
- **Produktion:** idp-metadata_prod_remove_ns.xml

OIDC RP-information

I OIDC-världen finns ingen utväxling av metadata som för SAML utan här sker ofta uppdatering av IdP:ns nycklar, som används för signering, automatiskt i bakgrunden. Även här kommer dubbla nycklar att publiceras enligt tidsplanen ovan så att RP:n kan få en sömlös övergång till den nya nyckeln.

⚠️ Ansvaret ligger dock på den förvaltning som ansvarar för RP:n att säkerställa att funktionalitet finns för att automatiskt hämta båda nycklarna eller vidta manuella åtgärder för att byta den tilltrodda publika IdP-nyckeln.

Adresser för nerladdning av signeringsnycklar (OIDC)

- **Test**: https://idp.ineratest.org/oidc/jwks.json
- **QA/Stage**: https://idp.ineraqa.org/oidc/jwks.json
- **Produktion**: https://idp.inera.se/oidc/jwks.json

För frågor kontakta Ineras Kundservice