

Certificaatverloop

SAML SP controleren

- Instructie

Instructie

Als beheerder of contactpersoon van een Service Provider (SP) ben je zelf verantwoordelijk voor het beheren van het certificaat dat wordt gebruikt voor ondertekenen (en eventueel versleutelen) bij een SAML-integratie. Een veelgestelde vraag is: "Wanneer verloopt ons certificaat?" Dit artikel helpt je om dit zelf te achterhalen.

Waar vind ik het certificaat?

Het certificaat dat de SP gebruikt, is meestal te vinden in:

1. **De configuratie van de applicatie.** Hoe en waar dit staat, hangt af van de specifieke applicatie. Raadpleeg de documentatie van de leverancier of je eigen IT-team.
2. **De SP-metadata.** Veel SAML SP's publiceren metadata in XML-formaat, waarin het certificaat staat vermeld. De URL van de SP-metadata wordt vaak ingesteld in de applicatieconfiguratie of is beschikbaar via de beheerinterface van de applicatie.

Zoek in de metadata naar een **<ds:X509Certificate>**-tag binnen een **<KeyDescriptor use="signing">** of **<KeyDescriptor use="encryption">** sectie. Dit bevat het certificaat in Base64-formaat en ziet er zo uit:

```
<md:KeyDescriptor use="signing">
  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:X509Data>
      <ds:X509Certificate> MIIGbDCCBVSgAwIBAgIUPGt8dNs1m4QrseJ2GUMcRjr-jV1AwDQYJKoZIhvcNAQELBQAwMjEUMBIG
      A1UECHMLSURWQVVMVC1BQ0MxGjAYBgNVBAsTEU9yZ2FuaXphdGlvbmF5IENBMjEUMDgyNzEz
      MTUwMmFoXDTI5MDgyNzEzMTUwMmFoZDEUMBIGA1UEAxMLaWRwLXNpZ25pbmcxDDAKBgNVBAsTAE1U
      UzEdMBsGA1UEChMVUWV5pdmVyc2l0ZWl0IFV0cmVjaHQAQgNVBACB1V0cmVjaHQAQgNVBACB1V0cmVjaHQAQgNV
      BACB1V0cmVjaHQAQgNVBAYTAk5MMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAGEA ug80hzDfuc9Ddw/
      sdd2NpTx9L1bPNukouYPn1XzH1J7bEEbZVDFLZ0CFNR9DZRLap1WZ2iC2meyz a0pSyagh6H9p177070HhJ+0yZLpggINcrbw3dPo4B0jrf9nPRqt5iG07h70N
      +bJYwDSyJSxLT+Fx eAa9c3Xv9/Lt3PQjyk1CQadJCrKHMucDbK5drvo1mxXhoyTdwjyebGZtHxKiD4aMnDY02bHA4ata
      mhb8OKFZGTlvu0b7WojGtwzje07ebdpazb5FGUiu010QL05uA1mngNqWI82nbrI84zaSWNTNymhj 4ipcVeq+375pLXXa3+nKJEHFSL4AsZPP+sf8LURv5t1n
      +q9LcRxbm8sE+ZvqAGrRxFGoWVP6ah 0AlfQnvGTChCsQd3HI0gDYQQLqfpOXcf01Zd6lQtX/jsuJ6lf6+Y73dxt8Iu5CDocw4hi4y542Jj
      vXR1zg7iJ0hlyLTAKIXpEqab/c9q7yM6vmdODZLXPnRky7HwUHQF4ay7JhrBxoaBt97XPhNout
      t9ovrEED4oD4DMHgwYfVkgCusOGkNLqpmY1LaUoY0a3F40Eh4PIpekJaXVnJc9exTHSGdaP7ago hLaGIzSPG1WsRu0Ub1n8UcEyJzdB9
      +SKOAc49y3SIOxEVZAxXs8TYSsbysqGwcHnJuBM/fm1DHcC AwEAAOCAjYwggIyMB0GA1UdDgQWBBS0zWNE4SR6m2MzZ9PUVd+TI9aepzAfBgNVHSMEGDAWgBSg
      zr5Uq3yDhJUmGyFzfsHdI9VcfzALBGNVHQ8EBAMCBAAwggHMBgtghkgBhv3AQkEAQSCAbswggG3 BAIBAAEB/
      xMdTm2Z2WxsIFNlY3VyaXR5IEF0dHJpYnV0ZSh0bSkwQ2h0dHAg6L9yKZXLb69wZXIu
      bm92Z2WxsLmNvbS9yZXBvc2l0b3J5L2F0dHJpYnV0ZXMvY2VydGF0dHJzX3YxMC50dG0wgGFI0BoB
      AQAwCDAGAgEBAGFAMAgwBgIBAQAIBAIAKEaAQEAMAgwBgIBAQAIBADAIMAYCAQECAQACACiBgIB AAEB/
      60CAQSGwAIBAgICAP8CAQADDQCAAAAAAAAAAAAAAAAAADCCAAAAAAAAAADAYMBACAQACCH// /AQAAGQG8N9IMBgwEABAAIIf////////
      8BAQACABw30ihwAIBAgICAP8CAQADDQBA AAAAAAAAAAAAAAAAAADCCAAAAAAAAAADAYMBACAQACCH// /AQAAGQG8N9IMBgwEABAAIIf////////
      8BAQACBBH/r4miTjBMAGECAGAAIA/wMNAIAAAAAAAAAAAAAAAAAAJIAAAAAAAAAA MBiWEABAAIIf////////8BAQAwEJAQAAGAAgh////////
      wEBADATBgNVHUEDDAKBggrBgEF BQCxDATANBgkqhkiG9w0BAQsFAAOCAQEAm2ZTJ+ClS1zCoDD2N5C550mwUV1nFMucDaRvDGEYX4rD
      pLV8uHlaA17W7jq5fY7KJvunTIWYcftsv2QCBH4im18bojqmBE9FbnXNa84WAI88HAWVdMH2PHeK 0BZjCitQixiLnvNNU14IWIvHDYUX
      +YSM275Z1VcNVJrtK3SEeOyeSFEVUJWdbSceKqQg7Bs1gh 5BR116IjZ0R79r1wXipdVAqrL8MI07H5e8BvrMM8NL4wPyr250azQLr7LU2VUWFWlJaUXdpoXN9n
      8qaJeNcn8L9Hux7owqQLjJ0g+UJZnIT2fyJr+SvgyIH9LiGv+/1jWRsLgJx7tMnEvong==
    </ds:X509Certificate>
  </ds:X509Data>
</ds:KeyInfo>
<md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmenc#tripledes-cbc"/>
</md:KeyDescriptor>
```

Hoe achterhaal ik de verloopdatum?

Als je het certificaat hebt gevonden (meestal als een lange Base64-string), kun je de verloopdatum als volgt controleren:

Kopieer de Base64-gecodeerde tekst van het certificaat (tussen **<ds:X509Certificate>** en **</ds:X509Certificate>**) en plak deze in een tool zoals: [SSL Shopper - Certificate Decoder](#). Hier zie je direct de verloopdatum en andere details van het certificaat.

Wat als het certificaat binnenkort verloopt?

- Neem contact op met je leverancier of technisch beheerder van de SP.
- Werk het certificaat op tijd bij in de applicatieconfiguratie.
- **Let op:** de IdP ondersteunt geen automatische update van metadata via de metadata-URL. Dit betekent dat de SP-metadata handmatig op de IdP moet worden bijgewerkt als de SP-configuratie verandert.
- Om onderbrekingen te beperken, is het belangrijk om deze acties goed op elkaar af te stemmen met de IdP-beheerders.