

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>
        MIIGbDCCBVSgAwIBAgIUPG8tdNs1m4QrseJ2GUMcRjrjVlAwDQYJKoZIhvcNAQELBQAwMjEUMBIG
        A1UEChMlSURwQVVMVC1BQ09ucjYAYBgNVBAsTEU9yZ2FuaXphdGlvbmFsIENBMB4XDTI0MDYnZez
        MTUwMfOxDTI5MDYnZezMTUwMfOWFdeUMBIGA1UEAxMLaWRwLXNpZ25pbmcxDDAKBgNVBAsTA0lU
        UzEdMBsGA1UEChMlVUV5pdmVyc2l0ZWl0FV0cmVjaHQxEDA0BgNVBAsTB1V0cmVjaHQxEDA0BgNV
        BagTB1V0cmVjaHQxZCzAJBgNVBAYTAk5MMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEa
        ug80hzDfuc9Ddw/
        sdd2NPtX9LlBPNUkouYpN1Xzh1J7bEEbZVDFLZ0CFNR9DZRLap1WZ2iC2meyz a0pSyagh6H9p177070HhJ+0yZLPggIncrbw3dPo4B0jrf9nPRqt5iG07h7ON
        +bJYwDSyJSxLt+Fx eAa9c3Xv9/Lt3PQjykLCQadJCrKHMCDbk5drvo1mxXhoyTdlwjeBGZtHxKiD4aMnDyo2bHA4ata
        mhb8OKfZGtLvu0b7WoJgtWzJf07ebDpazb5FGUiu0l0QL05uA1mmqNqWl82nhrI84zaSWNTNymHj 4ipcVeq+375pLXXa3+nKJEHfSL4AsZPP+sf8LURv5t1n
        +q9LcRxbq8msE+ZvqAGRrXFeGowVP6ah 0AlfQnvGTChCsQd3HI0gDYQLqfPOXCf012dG1QtX/jsuJ6lf6+y73dxt8Iu5DCdoc4hi4y542Jj
        vXR1vgr7i0hlyLTAKIXpEqab/c9q7yM6vmd0ZZLXPnrky7HwUHQF4ay7JhrBxoaBt97XPhNout
        t90rREED4oD4DMHgwYfVkgCusOGKnlqpm1LaUoY0a3F40Eh4P1ePeJkAXvNjC9exTHSGdaP7ago hLaGiZSPG1WsRu0Ub1n8UcEyJzdB9
        +SK0Ac49y3SIOxEVzAXs8tYSSbysqGwcHnJubM/fm1DHcC AwEAAAOCAjYwggIyMB0GA1UdDgQWBBS0zWNE4SR6m2mZ9PUVd+TI9aepzAFBgNVHSMEGDAWBgSB
        zrsUq3pDhJUMGyFzshdI9VcfZALBgNVHQ8EBAMCBAwggghMBGtghkgBhv3AQKEAQSCABswggG3 BAIBAABE/
        xMdTm92WxsfINL1Y3VyaXR5IEF0dHJpYnV0ZSh0bSkwQ2h0dHA6Ly9kZXZlZG9wZXIu
        bms92WxsfLmVyb59yZXBvc2l0b3J5L2F0dHJpYnV0ZXMyY2VydG90dHJzX3YxMCS0dG9wggFIOBoB
        AQAACDAGAGFEBAGFAMAQwBgIBAQAIBAAIBAKEaAQEAMAgwBgIBAQAIBADAIMAYCAQECAQACQCIgIB AAEB/
        60CAQ5gWIAgIBAGICAP8CAQADDQCAAAAAAAAAAAAAAAAAADQCAAAAAAAAAADAYMBACAQACCH/ //AQEAAQ68N9IMBgwEIABAIIIf////////
        8BAQACBAbw30ihWtBAGICAP8CAQADDQBA AAAAAAAAAAAAAAAAAADQCAAAAAAAAAAADAYMBACAQACCH////////AQEAAQ6R/6+JMBgwEIABAII f////////
        8BAQACBBH/r4mITjBMAgCAEAGIAA/WMNAIAAAAAAAAAAAAAAAAAAAIAIAAAAAAAAA MBiWEAIBAAIIIf////////8BAQAwEjAAQAgEAAgh////////
        wEBADATBgNVHsUEDAKBggrBgEF BQCDATANBgkqhkiG9w0BAQsFAAOCAQEAm2ZTj+ClS1zcODD2N5C550mwUV1nFMUCDaRvDGEYX4rD
        plV8uhlaA17w7jq5FY7KJvUuNIwvcFtsv2QCBAHinl8bojQmBE9fBNXNa84WA18HAWwDMH2PHeK 0BZJCitQIXiLvnvNU14Iw1AVHDYUX
        +YSM275Z1vNCvJRTk3SEeOySEFvUJWdbSCEkQg7Bs1gh 5BR116IJz0R79r1wXipdVaqR18MI07H5e8BvrMM8NL4Wpyr250azQLr71U2VUWFWlJauXdpOXN9n
        8qaJenCn8L9Hux7owwQLlJ0g+UJZnIT2fyJr+SVigYIH9LiGv+/lJwRSlgjX7TmEvong==
      </ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
  <md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#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.