

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> MIIGBDCCBVSgAwIBAgIUPGt8dNs1m4QrseJ2GUMcrjrjv1AwDQYJKoZIhvcNAQELBQAwMjEUMBIG
      A1UECHMLSURWQVVMVC1BQ0MxGjAYBgNVBAsTEUy9yZ2FuaXphdGlvbmFsIENBMB4XDTE0MDgyNzEz
      MTUwMFOXTD15MDgyNzEzMTUwMFOwDEUMBIGA1UEAxMLaWRwLXNpZ25pbmcxODAKBgNVBAsTA0lU
      UzEdMBsGA1UEChMUW5pdmVyc2l0ZWl0IFV0cmVjaHQxEDA0BgNVBAClB1V0cmVjaHQxEDA0BgNV
      BAgTB1V0cmVjaHQxZCZAJBgNVBAYTAk5MMIICjANBgkqhkiG9w0BAQEFAAOCAg8AMIICcKCAgEA ug80hzDfuc9Ddw/
      sdd2NPtx9L1bPNukouYPN1XzH1J7bEEbZVDF1Z0CFNR9DZRLap1WZ2iC2meyz a0pSyagh6H9p177070HhJ+0yZLPggINcrbw3dPo480jrf9nPRqt5iG07h7ON
      +bJYwDsYJ5xLT+Fx eAa9c3Xv9/Lt3PQjyKlCQadJCRKHMucDbK5drvo1mxXhoyTdwjyeBGZtHxKiD4aMnDY02bHA4ata
      mhb8OKFZGTlvu0b7wojGtwzje07ebDpazb5FGUiu0L05uA1mnqNqWI82nbnrI84zaSwnTnyMhj 4ipcVeq+375pLXXa3+nKJEHFSL4AsZPP+sf8LURv5t1n
      +q9LcRxbm8Se+ZvqAGRxfFgGowVP6ah 0AlfQnvGTChCsQD3HI0gDYQLqfPOxcf01ZdGLQtX/jsuJ6lf6+Y73dxt8Iu5CDocw4hi4y542Jj
      vXRlZg7iJ0hlyLTAKIXpEqab/c9q7yM6vmdODZLXPnrky7HwUHQf4ay7JhrBxoaBt97XPhNouT
      t9oVrEED4oD4DMHgWYfVkgCusOGKnlqpmY1LaUoY0a3F40Eh4PIPeKJaXVnJc9exTHsGdaP7ago hLaGiZSPG1wsRu0Ub1n8UcEyJzdB9
      +SKOAc49y3STOXEVZAxS8tYSSbsysqGwcHnjubM/fm1DHcC AwEAAaOCAjYwggIyMB0GA1UdDgQWBBS0zwNE4SR6m2MzZ9PUVd+TI9aepzAfbgNVHSMGDAWgBSg
      zr5Uq3yDhJumGyFzfsHdI9vcfzALBgnVHQ8EBAMCBaAwggHMBgtghkgBhVg3AQKEAQSCAbswggG3 BAIBAAEB/
      xMdTm92ZwxsIFN1Y3VyaXR5IEF0dHJpYnV0ZSh0bSkwQ2h0dHA6Ly9kZXZlbg9wZXIu
      bm92ZwxsLmNvbS9yZXBvc2l0b3J5L2F0dHJpYnV0ZXMvY2VydgF0dHJzX3YxMC5odG0wggFIoBoB
      AQAwCDAgAgEBAgEAMAgwBgIBAgIBAAIBAKEaAQEAMAgwBgIBAgIBADAIMAYCAQCAQACQcIbGIB AAEb/
      60CAQSGWAIBAgICAP8CAQADDQCAAAAAAAAAAAAAAAAAADQCAAAAAAAAAADAYMBACAQACCH// //AQEAAgQG8N9IMBgwEABAAIIf////////
      8BAQACABaw30ihwAIBAgICAP8CAQADDQBA AAAAAAAAAAAAAAAAAADQCAAAAAAAAAADAYMBACAQACCH//AQEAAgQR/6+JMBgwEABAAIIf////////
      8BAQACBBH/r4miTjBMAgECAGFAAgIA/wMNAIAAAAAAAAAAAAAAAAAAMJAIAAAAAAAAA MBiWEAIBAAIIf////////8BAQAwEjAQAgEAAgh////////
      wEBADATBgNVHUEDAKBggrBgEF BQcDATANBgkqhkiG9w0BAQsFAAOCAQEAm2ZTJ+C1s1zCoDD2N5C550mmUV1nFMucDaRvDGEYX4rD
      p1V8uHla17W7jQ5fY7KJvuntIwCftsv2QCBH4im18bojqMbE9FbnXNa84WAI88HAWvdMH2PHeK 0BzJCitQixiLnnvNU14IW1AVHDYUX
      +YSM275Z1VcNVJRTK3SEeOyeSFEVUJWdbSceKqQg7Bs1gh 5BR16IJJz0R79rlwXipdVqRl8MI07H5e8BvrMM8NL4wPyr25OazQlR71U2VUMFWljauXdpoxN9n
      8qaJecNc8L9Hux7owqQl1jJ0g+UJznIT2fyJr+SvivyIH9LiGv+//ljwRsLgJX7tMnEvong==
    </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.

Revision #21

Created 3 March 2025 09:42:15 by Schmidt, M.S. (Mick)

Updated 3 March 2025 14:14:35 by Schmidt, M.S. (Mick)