

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>
        MIIGbDCCBVSgAwIBAgIUPGt8dNs1m4QrseJ2GUMCjrjvV1AwDQYJKoZIhvcNAQELBQAwMjEUMBIG
        A1UECHMLSURVQVVMVC1BQ0MxGjAYBgNVBAsTEU9yZ2FuaXphdGlvbmFsIENBMjE0MDgyNzEz
        MTUwMmF0XDTI0MDgyNzEzMTUwMmF0XDTI0MDgyNzEzMTUwMmF0XDTI0MDgyNzEzMTUwMmF0
        UzEDMBsGA1UEChMUUWV5pdmVyc2l0ZWl0IFV0cmVjaH0xQXEDAOBgNVBACTB1V0cmVjaH0xQXEDAOBgNV
        BAgTB1V0cmVjaH0xQXEDAOBgNVBAYTAzE1IENBMBEwDQYJKoZIhvcNAQELBQAwMjEUMBIG
        sdd2NPTx9L1bPNukouYpN1XzH1J7bEEbZVDF1Z0CFNR9DZRLap1WZ2iCmeyz a0pSyagh6H9p177070HhJ+0yZLPggINrbcw3dPo4B0jrf9nPRqt5iG07h70N
        +bJYwDSyJ3xLT+Fx eAa9c3Xv9/Lt3PQjyk1CQadJCrKHMucDbK5drvo1mxXhoyTdwjyeBGZtHxKiD4aMnDY02bHA4ata
        mhb8OKfZGtLvU0b7wojGtwjE07ebDpazb5FGUiu0L05uA1mnqNqWI82nBrI84zaSwnTNyMhj 4ipcVeq+375pLXXa3+nKJEHfSL4AsZPP+sf8LURV5t1n
        +q9LcRxbm8sE+ZvQAGRxfGowVP6ah 0AlfQnvGTChCsQD3HI0gDYQQLfP0Xcf01ZdG1QtX/jsuJ61f6+Y73dxt8IU5CDocw4hi4y542Jj
        vXRlZg7i30hlyLTAKIXpEqab/c9q7yM6vmdODZLXPnrky7HwUHQf4ay7JhrBxoaBt97XPhNout
        t9ovrEED4oD4DMHgWfYkgCusOGKnlqpmY1LaUoY0a3F40Eh4PIPeKJaXVnJc9exTHSGdaP7ago hLaGiZSPG1WsRu0Ub1n8UcEyJzdB9
        +SKOAc49y3SIOxEVzAxS8tYSSbysqGwChnjuBM/fm1DHcc AwEAAOCAjYwggIyMB0GA1UdDgQWBBS0zWNE4SR6m2MzZ9PUVD+TI9aepzAfBgNVHSMGDAwBgSg
        zr5Uq3yDhJUmGyYzfsHdI9vcfzALBgnVHQ8EBAMCBAAwggHMBgtghkgBhv3AQKEAQSCAbswggG3 BAIBAAB/
        xMdtM92ZwxsIFN1Y3VyaXR5IEF0dHJpYnV0ZSh0bSkwQ2h0dHA6Ly9kZXZlbg9wZXIu
        bm92ZwxsLmNvbS9yZXBvc2l0b3J5L2F0dHJpYnV0ZSh0bSkwQ2h0dHA6Ly9kZXZlbg9wZXIu
        AQAACDAGAGEBAGEMAgwBgIBAQIBAAIBAKEaAQEAMAgwBgIBAQIBADAIMAYCAQEAQACiBgIB AAEb/
        6OCAQSGwIBAgICAP8CAQADDQCAAAAAAAAAAAAAAAAAADCCQAAAAAAAAAADAYMBACAQACCH// //AQEAAGQ8N9IMBgwEAIbAAIIf////////
        8BAQACBAbw30ihWAIBAgICAP8CAQADDQBA AAAAAAAAAAAAAAAAAADCCQAAAAAAAAAADAYMBACAQACCH//AQEAAGQ8N9IMBgwEAIbAAIIf////////
        8BAQACBBH/r4miTjBMAgEACAgEAAgIA/wMNAIAAAAAAAAAAAAAAAAAAAMJAIAAAAAAAAAAA MBIwEAIbAAIIf////////8BAQAwEjAQAgEAAgh////////
        wEBADATBgNVHSEUDDAKBggrBgEF BQCcDANBgkqhkiG9w0BAQsFAAOCAQEAQm2ZTJ+ClS1zCoDD2N5C550mwUV1nFMUCdaRVDGEYX4rD
        pLV8uHlaA17Wj7q5fY7KJvutIwYcftsv2QCCH4im18bojqMbE9FbNXNa84WAI88HAWdMH2PHeK 0BZjCitQixiLnnvNU14IWI1AVHDYUX
        +YSM275Z1VcNVJrtK3SEeOyeSFEVUJwdbSceKqQg7Bs1gh 5BR161Jz0R79rlwXipdVAqrL8MI07H5e8BvrMM8NL4wPyr250azQLr7LU2VUMFWLjaUXdpOXN9n
        8qaJenCn8L9Hux7owqQLjJ0g+UJZnIT2fyJr+SvivyIH9LiGv+/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.

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)