# 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>MIIGbDCCBVSgAwIBAgIUPGt8dNs1m4QrseJ2GUMcRjrjVlAwDQYJKoZIhvcNAQELBQAwMjEUMBIG
            A1UEChMLSURWQVVMVC1BQ0MxGjAYBgNVBAsTEU9yZ2FuaXphdGlvbmFsIENBMB4XDTI0MDgyNzEz
            MTUwMFoXDTI5MDgyNzEzMTUwMFowdDEUMBIGA1UEAxMLaWRwLXNpZ25pbmcxDDAKBgNVBAsTA0lU
            UzEdMBsGA1UEChMUVW5pdmVyc2l0ZWl0IFV0cmVjaHQxEDAOBgNVBAcTB1V0cmVjaHQxEDAOBgNV
            BAgTB1V0cmVjaHQxCzAJBgNVBAYTAk5MMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA ug8OhzDfuC9Ddw/
            sdd2NPtx9LlbPNUkouYPn1XzHlJ7bEEbZVDFlZ0CFNR9DZRLap1WZ2iC2meyz a0pSyagh6H9p177O7OHhJ+0yZLPggINcrbw3dPo4BOjrf9nPRqt5iG07h7ON
            +bJYwDSyJSxLT+Fx eAa9c3Xv9/Lt3PQjyklCQadJCrKHMucDbK5drvo1mxXhoyTdWjyeBGZtHxKiD4aMnDYo2bHA4ata
            mhb8OKFZGtLvu0b7WojGtWzjE07ebDpazb5FGUiUol0QLO5uA1mnqNqWI82nbrI84zaSWNTNyMhj 4ipcVeq+375pLXXa3+NKJEHFSL4AsZPP+sf8LURv5t1n
            +q9LcRxqbm8sE+ZvqAGrRxFeGowVP6ah 0AlfQnvGTChCsqD3HI0gDYQQLqfpOXcfO1ZdGlQtX/jsuJ6lf6+Y73dxt8Iu5CDocw4hi4y542Jj
            vXRlzg7iJ0hlyLTAkIXpEqab/c9q7yM6vmdODZZlXPNrky7HWUHOQF4ay7JhrBxoaBt97XPhNouT
            t9oVrEED4oD4DMHgWYfVkgCusOGkNLqpmy1LalUoY0a3F40Eh4PIPekJaXVnJc9exTHsGdaP7ago hLaGIzSPG1WsRu0Ub1n8UcEyJzdB9
            +SKOAc49y3SIOxEVzAxXs8tYSSbysqGwcHnjuBM/fM1DHcC AwEAAaOCAjYwggIyMB0GA1UdDgQWBBS0zWNE4SR6m2MzZ9PUVd+TI9aepzAfBgNVHSMEGDAWgBSg
            zr5Uq3yDhJuMGyfzfsHdI9VcfzALBgNVHQ8EBAMCBaAwggHMBgtghkgBhvg3AQkEAQSCAbswggG3 BAIBAAEB/
            xMdTm92ZWxsIFNlY3VyaXR5IEF0dHJpYnV0ZSh0bSkWQ2h0dHA6Ly9kZXZlbG9wZXIu
            bm92ZWxsLmNvbS9yZXBvc2l0b3J5L2F0dHJpYnV0ZXMvY2VydGF0dHJzX3YxMC5odG0wggFIoBoB
            AQAwCDAGAgEBAgEAMAgwBgIBAQIBAAIBAKEaAQEAMAgwBgIBAQIBADAIMAYCAQECAQACAQCiBgIB AAEB/
            6OCAQSgWAIBAgICAP8CAQADDQCAAAAAAAAAAAAAAADCQCAAAAAAAAAADAYMBACAQACCH// ////////AQEAAgQG8N9IMBgwEAIBAAAIIf/////////
            8BAQACBAbw30ihWAIBAgICAP8CAQADDQBA AAAAAAAAAAAAAADCQBAAAAAAAAAADAYMBACAQACCH/////////AQEAAgQR/6+JMBgwEAIBAAII f/////////
            8BAQACBBH/r4miTjBMAgECAgEAAgIA/wMNAIAAAAAAAAAAAAAAAMJAIAAAAAAAAAA MBIwEAIBAAAIIf/////////8BAQAwEjAQAgEAAgh/////////
            wEBADATBgNVHSUEDDAKBggrBgEF BQcDATANBgkqhkiG9w0BAQsFAAOCAQEAm2ZTJ+Cls1zCoDD2N5C550mwUV1nFMUcDaRvDGEYX4rD
            plV8uHlaA17W7jq5fY7KJvuNtIWYcftsv2QCBH4iml8bojqMbE9FbNXNa84WAI88HAWVdMH2PHeK 0BZjCitQIxiLnvnNU14IW1AVHDYUX
            +YSM275Z1VcNVJRtK3SEeEOyeSFEvUJWdbSCeKqQg7Bs1gh 5BRl16IJz0R79rlwXipdVAqrL8MIO7H5e8BvrMM8NL4wPyr25OazQLr7lU2VUWFWljaUXdpoXN9n
            8qaJeNcn8L9HuX7owqQljJ0g+UJZnIT2fyJr+SvigyIH9LiGv+//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)