# Standaard Cryptografie

## De Kadaster standaard voor cryptografie

Versie

1.2

Auteur(s)

CISO

# Standaard Cryptografie

De Kadaster standaard voor cryptografie

**Opdrachtgever**
Directeur DGV

**Status**
In bewerking

**Verspreiding**
Bedrijfsvertrouwelijk

**Versiehistorie**

| Versie | Datum | Auteur | Opmerking |
|---|---|---|---|
| 1.00 | 16-3-2020 | Reinier Kernkamp | Definitieve versie |
| 1.01 | 4-11-2021 | Reinier Kernkamp | Wijziging m.b.t. PKI-O en QWAC |
| 1.1 | 3-11-2022 | Jodrik Krelekamp | Wijziging m.b.t. PKI-O en certificaten voor SaaS |
| 1.2 | 26-01-2024 | Jodrik Krelekamp, Rob Messelink | Update o.b.v. review en organisatorische wijzigingen |

**Recensiehistorie**

| Versie | Datum | Recensent | Opmerking |
|---|---|---|---|
| 0.1 | 20-12-2019 | R&C, CST, Architectuur, Pieter Kooistra en Brian Peeters | Input KSS, architectuur, Certificaatbeheerders en R&C |
| 1.01 | 3-11-2021 | Pieter Kooistra | Controle door certificaatbeheerders |
| 1.1 | 02-01-2024 | Pieter Kooistra, Elize van der Zee | Review KSS, TGD |

**Distributie**

| Versie | Datum | Wie | Verantwoordelijkheid |
|---|---|---|---|
| 1.00 | 16-3-2020 | Risk Committee | Goedkeuring |
| 1.01 | 4-11-2021 | CISO | Ter review |

# Inhoud

# 1 Standaard Cryptografie

## 1.1 Inleiding

Dit document beschrijft de geldende standaard en de bijbehorende onderliggende regels en/of richtlijnen die gelden voor het domein cryptografie, zoals genoemd in het Kadaster informatiebeveiligingsbeleid. Conform ISO 27001 (A10.1 Cryptografische beheersmaatregelen) helpt correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen. Gebaseerd op de vastgestelde BIV-classificatie, worden in voornoemd standaard eisen m.b.t. informatiebeveiliging als volgt weergegeven:

(B) = Beschikbaarheid

(I) = Integriteit

(V) = Vertrouwelijkheid

## 1.2 Noodzaak

Deze standaard is nodig om duidelijke kaders te stellen aan de cryptografische beheersmaatregelen en het gebruik, bescherming en levensduur (beheer) van cryptografische sleutels conform het ISO 11770-1 framework.

## 1.3 Doelstelling(en)

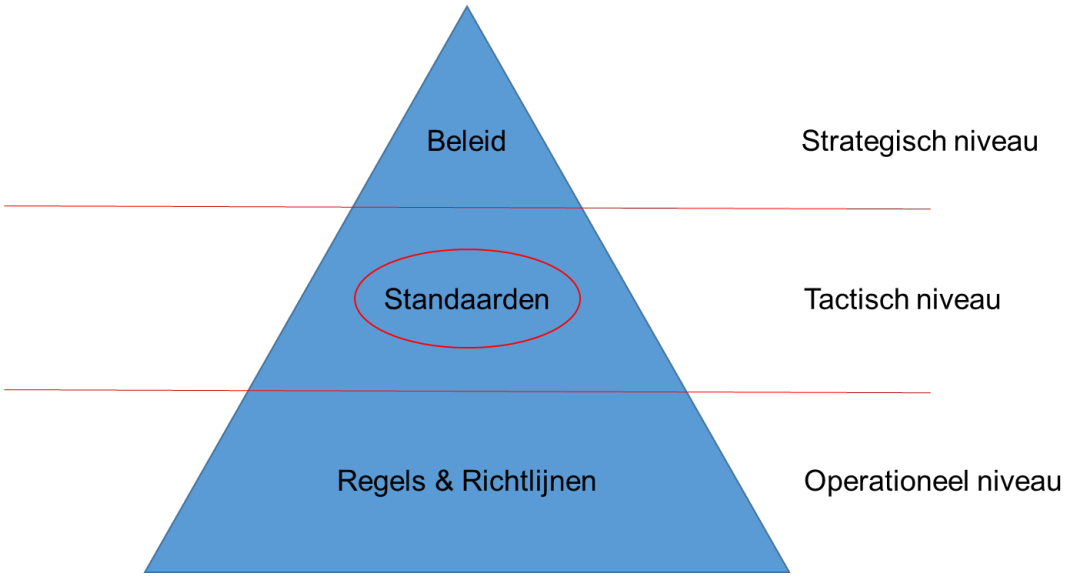
Zorgen voor het correct en het doeltreffend gebruik van cryptografie om de beschikbaarheid vertrouwelijkheid, authenticiteit en/of integriteit van informatie te kunnen borgen.

Hiermee worden de volgende beveiligingsdoelstellingen gerealiseerd:

- Vaststellen met wie er gecommuniceerd wordt;
- Vaststellen dat de ontvanger van een bericht zeker weet dat de verzender ook daadwerkelijk de afzender is en niet iemand anders (identiteit);
- Voorkomen dat tijdens transport en opslag van berichten en documenten de data wordt gewijzigd. Hierdoor heeft de ontvanger een zekere mate van garantie dat de inhoud van het bericht authentiek en integer is. Ook wordt daarbij een zekere mate van zekerheid verkregen dat de identiteit van de verzender overeenkomt met de identiteit van de ondertekenaar bij het bericht (Integriteit en authenticiteit);
- Afschermen van de inhoud van berichten voor ongeautoriseerden. (Vertrouwelijkheid);
- Aan kunnen tonen dat bepaalde gebeurtenissen of handelingen hebben plaatsgevonden door dit inzichtelijk te maken door berichten te ondertekenen met certificaten. (Onweerlegbaarheid)

## 1.4 Reikwijdte

Dit document is van toepassing op het Kadaster.




*Beleidspiramide Kadaster*

### 1.5 Eigenaarschap

De eigenaar van deze standaard is de directeur van de directie Data, Governance en Vernieuwing. De actiehouders van deze standaard zijn de verschillende diensteigenaren binnen het kadaster. Elke dienst moet de standaard toepassen binnen zijn werkgebied. Dit document wordt periodiek herijkt conform de regels uit het Kadaster Informatiebeveiliging beleid. De trigger voor herijking en de bewaking hierop is de verantwoordelijkheid van de CISO.

### 1.6 Positionering

Dit document beschrijft het rood omcirkelde gedeelte uit onderstaande figuur conform het informatiebeveiligingsbeleid.


*Figuur 1 – Scope van deze standaard is alleen cryptografie.*

In deze standaard wordt verwezen naar de volgende richtlijnen en of referenties:

*Encryptiebeleid CIP.* (2014). Opgehaald van https://cip-overheid.nl/media/1170/bid-operationale-producten-bir-018-encryptiebeleid-10.pdf

*Forum Standaardisatie*. (2021). Opgehaald van https://www.forumstandaardisatie.nl

IT, R. (2019). *Standaard leveranciersrelaties.* Opgehaald van Standaard leveranciersrelaties: https://hetkadaster.sharepoint.com/:b:/r/sites/directie-cf/Gedeelde%20documenten/20191113_Standaard%20leveranciersrelaties_1.0.pdf?csf=1&e=boYq4H

IT, R. (2020). *Richtlijn IT-middelen en diensten.* Opgehaald van https://hetkadaster.sharepoint.com/sites/directie-cf/SitePages/Informatiebeveiliging.aspx

NCSC. (2021). *Factsheet PKIoverheid stopt met webcertificaten.* Opgehaald van www.ncsc.nl: https://www.ncsc.nl/binaries/ncsc/documenten/factsheets/2021/september/29/factsheet-pkioverheid-stopt-met-webcertificaten/Factsheet+PKIoverheid+stopt+met+webcertificaten+v1.0.pdf

NCSC. (2021). *ICT-beveiligingsrichtlijnen voor Transport Layer Security v2.1 (TLS).* Opgehaald van ncsc.nl: https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1

Organization, I. S. (2010). *ISO/IEC 11770-1.* Opgehaald van International Standard Organization: https://www.iso.org/standard/53456.html

Organization, I. S. (2016). *ISO/IEC 154891.* Opgehaald van Informatie en documentatie - Informatie- en archiefmanagement - Deel 1: Concepten en uitgangspunten: https://www.nen.nl/NEN-Shop/Norm/NENISO-1548912016-nl.htm

*Programma van Eisen PKIoverheid.* (2020). Opgehaald van logius: https://www.logius.nl/diensten/pkioverheid/aansluiten-als-tsp/pogramma-van-eisen

*Kadaster Beveiligingsbeleid.* Opgehaald van https://hetkadaster.sharepoint.com/sites/directie-cf/SitePages/Beveiligingsbeleid-%26-andere-documenten.aspx

*Business Impact Analyse.* Opgehaald van https://hetkadaster.sharepoint.com/sites/directie-cf/SitePages/Business-Impact-Assessment-(BIA).aspx

*Kadaster Standaard dataclassificatie v1.01.* Opgehaald van https://hetkadaster.sharepoint.com/sites/directie-cf/SitePages/Beveiligingsbeleid-%26-andere-documenten.aspx

VNG. (2019). *Handreiking Encryptiebeleid (PKI).* Informatiebeveiligingsdienst.

### 1.7 Pas-toe-of-leg-uit

Deze standaard past het bovenliggende beleid toe. Dit betekent dat er geen afwijkingen zijn vanuit de eisen die in de Basesline Informatiebeveiliging Overheid staan.

### 1.8 Randvoorwaarden

Deze standaard is compliant aan alle vigerende wet- en regelgeving.

Expliciet moet er rekening worden gehouden met de ISO11770-1, de Archiefwet en NEN ISO15489 voor informatie en archiefmanagement.

# 2 Kaders voor cryptografie

## 2.1 Beleid

Doelstelling
*Beleid inzake het gebruik van cryptografische beheersmaatregelen: ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.*

2.1.1 Toepassen van cryptografie

De beleidsregels voor het toepassen van encryptie voor het Kadaster zijn:

a. (BIV) Vanuit wet- en regelgeving, waaronder AVG artikel 32, moet passende beveiliging worden toegepast. Denk aan versleutelen van harde schijven van servers, waar gevoelige persoonsgegevens op kunnen staan, het versleutelen van transport bij inkomende en uitgaande berichten van het Kadaster of het ondertekenen van akten die juridische waarde hebben.
b. (V) Alle gegevens anders dan met classificatie ‘Openbaar’, zoals beschreven in de Standaard dataclassificatie, worden versleuteld:
    I. Classificatieniveau ‘Bedrijfsvertrouwelijk’: transportversleuteling buiten het interne netwerk en opslag van data moet worden versleuteld.
    II. Classificatieniveau ‘Vertrouwelijk’: transportversleuteling en opslag van data moet worden versleuteld.
    III. Classificatieniveau ‘Geheim’: Zowel transport- als dataversleuteling tijdens communicatie en opslag van data moet worden versleuteld.
c. (V) Cryptografie vindt plaats conform ‘best practices’ (de stand der techniek), waarbij geldt dat de vereiste encryptie sterker is naarmate gegevens gevoeliger zijn. Hiervoor wordt gebruik gemaakt van het forum standaardisatie op basis van pas toe of leg uit
d. (I) Het gebruik van hashes voor integriteitscontroles is alleen toegestaan wanneer deze hashes minimaal als veiligheidsniveau goed worden vastgesteld conform de ‘ICT-beveiligingsrichtlijnen voor Transport Layer Security v2.1 (TLS)’. (NCSC, ICT-beveiligingsrichtlijnen voor Transport Layer Security v2.1 (TLS), 2021) of de vernieuwde versie van voorgenoemde richtlijn.
e. (I) Digitale documenten van het Kadaster waar burgers en bedrijven rechten aan kunnen ontlenen, maken gebruik van PKIoverheid -certificaten voor tekenen.
f. (I) Digitale documenten van het Kadaster waar burgers en bedrijven rechten aan kunnen ontlenen, maken minimaal gebruik van een OV-certificaat (Organization Validated-certificaat) geleverd door één van de door Kadaster geselecteerde leveranciers voor encryptie.
g. (IV) Ingeval van PKIoverheid certificaten worden de PKI-Overheid-eisen[1] t.a.v. het sleutelbeheer gebruikt. In overige situaties moet de standaard ISO-11770-1 gehanteerd

[1] Programma van eisen voor PKIoverheid: https://www.logius.nl/diensten/pkioverheid/pkioverheid-update en https://www.logius.nl/diensten/pkioverheid/aansluiten-als-tsp/pogramma-van-eisen

worden. Deze standaard beschrijft het framework voor sleutelbeheer. Dit omvat o.a. de sleutelbeheer aspecten, zoals beschreven in hoofdstuk 4 van deze standaard.

h. (V) Dataverkeer (‘machine to machine’) wordt conform classificatie beveiligd met certificaten.
i. (V) Beveiligingscertificaten worden centraal beheerd voor infrastructuur en platform onderdelen en voor diensten. Als een dienst dit zelf beheert mag dat alleen als er een volledig door de ISO goedgekeurde, geautomatiseerde oplossing wordt gebruikt. Een oplossing dient minimaal aan FIPS 140-2 te voldoen. Daarbij zijn er 4 niveaus die per applicatie ingericht moeten worden. Role-based of Attribute-based authenticatie is minimaal voor het mogen beheren van beveiligingscertificaten.
j. (V) Transport encryptie (TLS- Transport Layer Security) is verplicht voor alle extern ontsloten webservers en alle interne webservers, webservices en Application Programming Interfaces (API’s), tenzij er kan worden uitgelegd met geldige redenen waarom hiervan wordt afgeweken (pas toe of leg uit). Dit besluit moet worden gedocumenteerd.
k. (I) Voor productieomgevingen is minimaal gebruik van een OV-certificaat, geleverd door één van de door Kadaster geselecteerde leveranciers voor encryptie, nodig.
   Voor de niet-productieomgeving, zoals test, acceptatie of bèta hoeven, voor de bescherming van informatie, geen OV-certificaten gebruikt te worden. Hiervoor mogen door een erkende Certificate Authority uitgegeven DV-certificaten worden gebruikt. Dit is alleen toegestaan wanneer dit geen geheime of vertrouwelijke informatie of persoonsgegevens betreft. Dan is ook minimaal gebruik van een OV-certificaat geleverd door één van de door Kadaster geselecteerde leveranciers voor encryptie nodig.
l. (V) Om de informatie met het classificatielabel ‘vertrouwelijk’ en ‘geheim’ op alle soorten opslagmedia te beschermen, zodat deze informatie niet in onbevoegde handen kan vallen bij onjuist gebruik, verlies of diefstal, dient deze te worden versleuteld. Deze versleuteling mag alleen worden toegepast wanneer dit niet ten koste gaat van de duurzame toegankelijkheid van de informatie, en wordt voldaan aan de eisen zoals beschreven in de Archiefregeling.
m. (V) Om authenticatiemiddelen zoals wachtwoorden te beschermen tegen inzage en wijzigingen door onbevoegden tijdens transport en opslag, dienen deze te worden versleuteld.
n. (V) Bij voorkeur wordt online gewerkt, zodat lokale opslag van data niet nodig is. Bestanden met de classificatie Openbaar mogen zonder encryptie worden opgeslagen, mits de bewaarlocatie voldoet aan de eisen zoals die worden gesteld in de vigerende wet- en regelgeving (Archiefregeling). Informatie geclassificeerd als openbaar mag als uitzondering lokaal op een mobiel apparaat worden opgeslagen zonder encrypted container. Informatie geclassificeerd als niet “openbaar” moet op binnen een versleutelde container worden opgeslagen op een mobiel apparaat. Daarmee wordt de opslag van privé en zakelijk duidelijk gescheiden en heeft een wisactie bijv. geen invloed op de privé bestanden op een eigen apparaat.
o. (V) Om bedrijfsinformatie op mobiele apparaten, zoals laptop, smartphones en tablets te beveiligen zijn deze zo ingericht dat geen bedrijfsinformatie wordt opgeslagen (‘zero footprint’). Voor het geval dat zero footprint (nog) niet realiseerbaar is, of functioneel

onwenselijk is, wordt de toegang tot het apparaat beschermd door middel van een wachtwoord en is apparaat versleuteling geïmplementeerd (conform classificatie-eisen). Voor meer informatie wordt verwezen naar de Richtlijn IT middelen en diensten en het Wachtwoordbeleid.

p. (BIV) Voor Clouddiensten (bijvoorbeeld toepassingen in SaaS, O365) geldt dat versleuteling geregeld is op een manier die recht doet aan beschermingseisen van het Kadaster, zoals vastgelegd in het Informatiebeveiligingsbeleid. De Kadaster Standaard dataclassificatie moet hiervoor worden toepast worden binnen de cloud omgeving. Daarnaast moet ook worden voldaan aan de eisen in de Archiefregeling (artikel 26: Voor zover op het tijdstip van overbrenging gebruik wordt gemaakt van encryptietechniek, wordt aan de beheerder van de archiefbewaarplaats de bijbehorende decryptiesleutel verstrekt.)
q. Indien een door Kadaster geregistreerde domeinnaam[2] (of subdomein hiervan) gebruikt wordt bij een derde partij (zoals SaaS of clouddienst) en die extern is ontsloten, moet er altijd gewerkt worden met een door Kadaster beheerd certificaat.
r. (BIV) Wildcard certificaten mogen alleen gebruikt worden na het uitvoeren van een risicoanalyse en zijn alleen toegestaan indien de toepassing van het certificaat beperkt wordt tot 1 dienst. Op deze manier wordt de schade beperkt als een certificaat ongeldig wordt verklaard of als er een private key gecompromitteerd is.

### 2.1.2 Verantwoordelijkheid implementatie

De diensteigenaren zijn verantwoordelijk om binnen de dienst zelf versleuteling toe te passen waar dat conform het Informatiebeveiligingsbeleid nodig is en conform de Archiefregeling mogelijk is. Dit gebeurt in overleg met de architecten, het Cyber Security Team en de ISO. Voor versleuteling op infrastructuur-niveau is de service provider of beheerder van het Kadaster platform verantwoordelijk en de betreffende contracteigenaar. Daar waar mogelijk wordt zoveel mogelijk geautomatiseerd gebruik gemaakt van oplossingen om automatisch versleuteling en beheer van certificaten toe te passen binnen een beheerd en gecontroleerd proces.

### 2.1.3 Verantwoordelijkheid sleutelbeheer

Sleutelbeheer wordt, waar dat mogelijk is, zoveel mogelijk geautomatiseerd, zodat er geen handmatige handelingen verricht hoeven te worden. Elk DevOps team en de gekoppelde product owner is verantwoordelijk en aansprakelijk voor het functioneel gebruik van de sleutels. Voor technisch sleutelbeheer is de serviceprovider verantwoordelijk op de onderdelen waar je als klant geen invloed op kunt uitoefenen. Daarvoor levert de serviceproviders het benodigde bewijs conform de eisen in de Standaard Levenciersrelaties. Bijvoorbeeld, een Platform-As-A-Service dienst regelt zelf versleuteling van het opslagmedium. De ISO toetst (conform de BIO, voor de diensten waar de betreffende ISO verantwoordelijk voor is, of de serviceprovider zich houdt aan de eisen die worden gesteld in het Informatiebeveiligingsbeleid, waaronder cryptografie. De ontwikkelteams binnen het Kadaster zijn zelf verantwoordelijk voor implementatie van versleuteling binnen de diensten die hierop worden aangesloten, mits het Informatiebeveiligingsbeleid, de Archiefregeling en de standaard cryptografie dit toelaten.

[2] https://wiki.kadaster.nl/architectuurwiki/index.php/Kadaster_Internet_Domein_Namen

## 2.2 Toepassingen

Cryptografie heeft verschillende toepassingen. Hieronder worden verschillende voorbeelden beschreven die minimaal moeten worden toegepast.

**Gegevens veilig bewaren door versleuteling van de data**

Cryptografie kan worden gebruikt om gegevens af te schermen voor zowel opslag bij het Kadaster zelf als opslag van gegevens bij derde partijen. Denk hierbij aan opslag middels het opslagmedium van een client, server of appliance. Hieronder vallen externe harde schijven, backup tapes, of andere mobiele opslagmedia. Bij verlies, diefstal of ongeauthoriseerde toegang tot deze opslagmedia, kan niemand de versleutelde gegevens lezen wanneer deze zijn versleuteld.

**Digitale certificaten**

Publieke sleutels hebben één nadeel: als ontvanger kun je lastig controleren of de publieke sleutel afkomstig is van de ‘echte’ zender. Het zou namelijk ook van iemand kunnen zijn, die zich voordoet als de zender (Spoofing). In zo'n geval helpt een digitaal certificaat. Daarmee kan de ‘echtheid’ van een persoon en zijn publieke sleutel worden aangetoond door middels van een vertrouwde derde partij. De echtheid van de publieke sleutel moet altijd gecontroleerd worden, ook als de afzender een bekende is. Een digitaal certificaat kan worden vergeleken met een paspoort of een rijbewijs. Digitale certificaten worden gebruikt als een vergelijkbare legitimatie, om aan te tonen dat de afzender van een bericht ook daadwerkelijk degene is die hij of zij claimt te zijn.

**Veilig communiceren met de overheid**

De Nederlandse overheid stelt steeds meer diensten en informatie beschikbaar via internet. Dit geldt ook voor het Kadaster. Om ervoor te zorgen dat gebruikers van de diensten van het Kadaster zekerheid hebben over de echtheid van de Kadaster-website en dat hun ingevulde gegevens en de communicatie met het Kadaster beveiligd is, gebruikt het Kadaster een verificatiemiddel. Om te voorkomen dat voornoemde gegevens niet 'op straat' komen te liggen, zijn zogenoemde SSL-certificaten. Een certificaat voegt een uniek zegel toe aan een website die is ondertekend door een vertrouwde partij. Een van de vertrouwde partijen is de “Staat der Nederlanden” voor overheidsorganisaties (PKIoverheid certificaten). Om in de vertrouwde lijst van een web browser opgenomen te worden moet je als vertrouwde partij aan strenge voorwaarden voldoen. In de BIO[3] worden bij controlnummer 13.2.3.3 PKI overheid certificaten verplicht gesteld bij web- en mailverkeer van gevoelige gegevens. Gevoelige gegevens zijn o.a. digitale documenten binnen de overheid waar gebruikers rechten aan kunnen ontlenen.
Aangezien de leverancier van PKI overheidcertificaten is gestopt met het leveren van webcertificaten zal het Kadaster conform de handreiking van het NCSC[4] een andere certificaatleverancier, ook wel TSP, hanteren voor het aanvragen van dergelijke webcertificaten.

**PKIoverheid-certificaat**

[3] https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/
[4] https://www.ncsc.nl/documenten/factsheets/2021/september/29/factsheet-pkioverheid-stopt-met-webcertificaten

PKI staat voor Public Key Infrastructure en is een systeem waarmee uitgifte en beheer van certificaten worden gerealiseerd. PKIoverheid Certificaten zijn ontworpen voor betrouwbare elektronische communicatie binnen en met de Nederlandse overheid. Een digitaal certificaat van PKIoverheid (Public Key Infrastructure voor de overheid) waarborgt op basis van Nederlandse wetgeving de betrouwbaarheid van informatie-uitwisseling via e-mail of andere gegevensuitwisseling.

PKIoverheid-certificaten worden gebruikt bij:

- het zetten van een rechtsgeldige elektronische handtekening. Indien hiervan afgeweken wil worden afgeweken zal de betreffende directie deze uitzondering aangevraagd moeten worden bij de ISO van de betreffende directie;
- het authentiseren van personen of services;
- het versleutelen van berichten.

**E-mail**

Binnen de mailomgeving[5] moet versleuteling van transport van een bericht altijd afgedwongen worden bij het versturen van e-mails om informatie af te schermen. Ook dient een e-mailserver Domain Keys Identified Mail (DKIM) te gebruiken, zodat ontvangers kunnen achterhalen of een e-mail legitiem is. Op basis van dataclassificatie kan een gebruiker zelf vaststellen of de informatie in een bericht versleuteld moet worden om de vertrouwelijkheid van informatie te kunnen waarborgen.
De totale e-mail beveiliging is uiteraard een set aan maatregelen, zie hiervoor ook factsheet[6] van het NCSC m.b.t. bescherming van domeinnamen tegen phishing.

[5] https://docs.microsoft.com/en-us/microsoft-365/compliance/email-encryption
[6] https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-bescherm-domeinnamen-tegen-phishing

# 3 Standaarden

## 3.1 Toegepaste normen

De verplichte normen[7] van de forum standaardisatie dienen te worden toegepast volgens onderstaande vaststelling en indien deze van toepassing zijn in de context van de oplossing.

| Naam verplichte standaard | Typering |
|---|---|
| **Ades Baseline Profiles** | Geavanceerde en gekwalificeerde digitale handtekeningen |
| **Digikoppeling** | Veilige berichtenuitwisseling en steunt op TLS |
| **DKIM** | Bescherming tegen e-mail phishing |
| **HTTPS en HSTS** | Beveiligde websiteverbinding en webservices |
| **TLS** | Beveiligde internetverbinding |
| **STARTTLS** | Beveiligde verbinding tussen mailservers |

De volgende aanbevolen standaarden worden toegepast conform het Informatiebeveiligingsbeleid of indien dit door een risicoanalyse vanuit het CST of ISO wordt geadviseerd:

| Naam aanbevolen standaard | Typering |
|---|---|
| **S/MIME** | E-mail beveiliging |
| **SHA-2** | authenticatie en integriteitscontrole. De SHA-2 familie bestaat uit 224, 256, 384 of 512 bits. |
| **SSH-2** | Versleuteld inloggen |
| **DNSSEC** | Domeinnaambeveiliging |
| **DANE**[8] | Beveiligde verbinding tussen mailservers |
| | |

Voor TLS encryptie moet de Richtlijn ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) of de vernieuwde versie daarvan (NCSC, ICT-beveiligingsrichtlijnen voor Transport Layer Security v2.1 (TLS), 2021) worden toegepast.

## 3.2 Beschermingsniveau

Naast de eisen uit het Informatiebeveiligingsbeleid, wordt het beschermingsniveau vastgesteld middels de Business Impact Analyse[9] (BIA). In een BIA wordt zowel de BIV-classificatie, het Basis

[7] https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht
[8] DNSSEC en DANE worden bij sommige leveranciers nog niet ondersteund, waaronder Azure. MTA-STS moet dan als alternatief worden gebruikt, omdat Cloud providers dit wel (gaan) ondersteunen.
[9] https://hetkadaster.sharepoint.com/sites/directie-cf/SitePages/Business-Impact-Assessment-(BIA).aspx

beveiligingsniveau (BBN) en indien nodig, een Quickscan Privacy Impact Assessment (PIA) uitgevoerd. Het vastgestelde basisbeveiligingsniveau geeft aan in hoeverre bepaalde maatregelen vanuit de BIO van toepassing zijn. Dit is tevens van tevoren vast te stellen in de Self Assessment BIO. Daarnaast is het van belang dat, naast passende beveiliging van informatie, de beveiliging niet ten koste gaat van de duurzame toegankelijkheid van informatie, zoals ook in de Archiefregeling wordt geeist.

### 3.3 Afstemming

Voor uitwisseling van data binnen de overheid wordt bij voorkeur Diginetwerk gebruikt. Bij uitwisseling van gegevens dient rekening te worden gehouden met de dataclassificatie van het document. Dit betekent dat vertrouwelijke documenten zelf ook versleutelt verstuurd moeten worden, naast getroffen maatregelen uit de standaard transport beveiliging. Openbare of bedrijfsvertrouwelijke gegevens hoeven niet zelf ook nog versleuteld te worden (dataversleuteling).

Voor elektronische berichtenuitwisseling is er de dienst Digikoppeling[10] die bestaat uit een set van standaarden voor elektronisch berichtenverkeer tussen overheidsorganisaties. Zoals een brief in een enveloppe gaat voor verzending, zo gaat een elektronisch bericht in een digitale verpakking. Deze digitale verpakking is Digikoppeling. Denk hierbij aan bijvoorbeeld basisregistraties, het Omgevingsloket of Digilevering.

[10] Zie https://www.logius.nl/diensten/digikoppeling

# 4 Sleutelbeheer

Doelstelling
Sleutelbeheer: Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld en geïmplementeerd.

De paragrafen in dit hoofdstuk zijn gebaseerd op de ISO 11770-1 norm, welke wordt gebruikt om te voldoen aan de eisen uit het Informatiebeveiligingsbeleid. Tevens zijn de eisen uit de Archiefregeling in het kader van duurzame toegankelijkheid genoemd. Hieronder de mapping van de paragrafen naar het framework, zoals beschreven in de ISO 11770-1 norm.

| Paragraaf | Titel | ISO norm 11770-1 |
|---|---|---|
| 4.1 | Algemeen | 4.2.1 General aspects of key management |
| 4.2 | Inrichting sleutelbeheer | 5.1.1 Summary of key management services |
| 4.3 | Levensduur van sleutels | 4.3 Generic key life cycle model |
| 4.4 | Genereren en registreren van sleutels | 5.1.2 Generate-Key (key generation)<br>5.1.3 Register-Key (key registration)<br>5.1.4 Create-Key-Certificate (key certification) |
| 4.5 | Verspreiden van sleutelmateriaal | 5.1.5 Distribute-Key (key distribution) |
| 4.6 | Vervangen (en updaten) van de sleutels | 5.1.6 Install-Key (key installation)<br>5.1.7 Store-key (key storage) |
| 4.7 | Herstellen van sleutels | 5.1.8 Derive-Key (key derivation) |
| 4.8 | Archiveren van sleutels | 5.1.9 Archive-Key (key archiving) |
| 4.9 | Intrekken van de sleutels | 5.1.10 Revoke-Key (key revocation)<br>5.1.11 Deregister-Key (key deregistration |
| 4.10 | Vernietigen van de sleutels | 5.1.12 Destroy-Key (key destruction) |
| 4.11 | Afspraken voor reservecertificaten van alternatieve leverancier | 5.2.1 Key management facility services |

## 4.1 Algemeen

Het Kadaster en de verschillende DevOps teams dienen, conform de ISO1170 en de Archiefregeling, sleutelbeheer in te richten voor de beheersing van de operationele- en beheerprocessen. Zoals de Archiefregeling (artikel 17) dit voorschrijft moet het Kadaster als zorgdrager van archiefbescheiden altijd de besturingsprogrammatuur of toepassingsprogrammatuur waarmee de archiefbescheiden worden bewaard of beheerd, kunnen vaststellen. Dit is toepasbaar op alle, vanaf het genereren van- tot en met de vernietiging van sleutels en het geheel aan sleutelmateriaal, aan sleutelbeheer gerelateerde activiteiten. Bij versleuteling van gegevens geldt, dat deze versleutelde gegevens net zo lang toegankelijk zijn als de beschikbaarheid van de bijbehorende sleutel, zolang wij conform wet- en regelgeving de gegevens dienen te bewaren (zorgdrager). De versleuteling is net zo sterk als de mate van de geheimhouding van de sleutel. Sleutels moeten bij hoge uitzondering op verzoek aan

geautoriseerde personen worden overgedragen. Denk hierbij aan sommige wettelijke verplichtingen in de Wet op de inlichtingen- en veiligheidsdiensten (WIV)[11]. In artikel 143 van de WIV staat vermeld dat het al dan niet opzettelijk hinderen bij het ontsleutelen van gegevens als overtreding of misdrijf strafbaar gesteld wordt.

### 4.2 Inrichting Sleutelbeheer

De inrichting van het sleutelbeheer hangt binnen het Kadaster af waar het organisatorisch is belegd.

- Generiek is er een team veantwoordelijk voor het accorderen van certificaten die gebruikt worden binnen de verschillende diensten.
- De serviceproviders die gebruikt worden zijn verantwoordelijk voor het sleutelbeheer van de afgenomen diensten.
- Er is een trusted third party (TTP) leverancier en alternatieve leverancier, zoals beschreven in paragraaf 4.11 die certificaten ondertekend voor:
    - DV- en OV-certificaten voor websites;
    - PKIoverheid Private Root certificaten voor Machine to Machine (M2M) koppelingen binnen de overheid;
    - PKIoverheid Private Root certificaten die moeten worden gebruikt voor berichten signing (payload) in Machine to Machine (M2M) koppelingen.
- Deze partijen ondertekenen het certificaat via een aanvraag verzoek.
    - Indien mogelijk worden certificaat verzoeken middels een Automatic Certificate Management Environment (ACME)[12] aangevraagd.
- Er wordt een ‘key recovery’ -dienst ingericht voor specifieke toepassingen voor data encryptie[13] (dit geeft de mogelijkheid voor de gebruiker om zijn sleutel te herstellen, nadat deze verloren is gegaan).
    - Voor transport laag encryptie mag de private echter nooit de technische voorziening verlaten, waarin de sleutel is gegenereerd, zoals bijvoorbeeld een High Security Module (HSM).
- Er wordt een ’key escrow’ -dienst ingericht (de sleutels zijn toegankelijk voor daartoe bevoegde personen).
- Voor de Kadaster Signing Services voor klanten, waaronder notarissen is een aparte dienst en diensteigenaar ingeregeld. KSS wordt gebruikt voor het ondertekenen van documenten naar buiten voor het verifiëren van handtekeningen van notarissen.
- Sleutelmanagement in de cloud zal zo veel mogelijk geautomatiseerd worden. Opslag en back-up van de sleutels dient aan dezelfde eisen te worden voldaan.
- De product owner van elke dienst is aansprakelijk voor goed sleutelbeheer. De ISO monitort dit middels de self assessment informatiebeveiliging van de diensten.

[11] Artikel 45 lid negen en 143 van de WIV te vinden op https://wetten.overheid.nl/BWBR0039896/2018-05-01
[12] Zie https://tools.ietf.org/html/rfc8555
[13] Dit is bijvoorbeeld ingeregeld voor het opslaan van de Bitlocker keys op Werkplek 2.0.

### 4.3 Levensduur van sleutels

Sleutelparen hebben een levensduur/geldigheidsduur. Dit houdt in dat een sleutel na het verstrijken van deze periode niet meer mag worden gebruikt om berichten te versleutelen. Met deze sleutel blijft het wel mogelijk om alle versleutelde data te ontcijferen.

Een eigenaar van sleutels moet binnen het Kadaster:

- Bij voorkeur geautomatiseerd van alle sleutelparen, bijhouden wanneer sleutelparen zijn uitgegeven en wanneer deze weer verlopen. Dit is onder andere nodig om te kunnen bepalen wanneer een nieuw sleutelpaar al dan niet geautomatiseerd moet worden gegenereerd.
- SSH-sleutels via een geautomatiseerde oplossing[14] beheren. Deze sleutels na het aanmaken uiterlijk om de 2 jaar weer worden vervangen.
- Verlopen sleutelparen voor symmetrische encryptie bewaren om te kunnen garanderen dat alle data die ooit is versleuteld ook weer ontcijferd kan worden. Als de sleutel vervangen is, moet alle data weer versleuteld worden met de nieuwe sleutel.
- Een oplossing implementeren (procedureel of technisch) om gebruikers op de hoogte te brengen van het feit dat er een nieuw sleutelpaar is of moet worden gegenereerd. Uitgangspunt is dat het vernieuwen van sleutels zoveel mogelijk wordt geautomatiseerd.

### 4.4 Genereren en registreren van sleutels

De Wet Elektronische Handtekening (WEH) stelt eisen aan de manier waarop sleutels gegenereerd worden. Voor gekwalificeerde handtekeningen gelden nog hogere eisen.

Het Kadaster dient:

- Alle relevante informatie, zoals de cryptografische eigenschappen, de ontvanger(s), het eigenaarschap en de levensfases van het sleutelmateriaal, vast te leggen in een geautomatiseerd registratiesysteem.
- De taken, verantwoordelijkheden en bevoegdheden met betrekking tot het aanvragen en generen van sleutels en certificaten vast te leggen:
    - Verzamel en verifieer de identiteitsgegevens van de aanvrager en autoriseer de aanvraag.
    - De dienst verantwoordelijk voor certificatenbeheer, nader genoemd PKI-beheerder fungeert voor certificaataanvragen als interne Registration Authority (RA). Daarbij wordt het volgende gecontroleerd:
        - identificatie, authenticatie en autorisatie van de aanvraag al dan niet geautomatiseerd.
        - het bepalen en aanvullen van de juiste inhoud en het optreden als tussenpersoon naar de interne of externe Certificate Authority (CA).

[14] Dit kan bijvoorbeeld via een PAM (Privilege Account Management) oplossing

        - Per sleuteldoel in een sleutelplan vast te leggen wanneer en hoe sleutels vervangen dienen te worden. Voor Transport Layer Security sleutels is er bijvoorbeeld maar 1 sleutelplan.
    - Beveiligingsincidenten m.b.t. sleutelmateriaal worden gemeld via het reguliere beveiligingsincidenten proces. CST coördineert samen met de PKI-beheerder en betreffende verantwoordelijken van de dienst(en) het incident.
- Cryptografische sleutels moeten veilig worden bewaard. Geheime sleutels mogen nooit geëxporteerd worden buiten de vertrouwde zone conform de eisen van de Certificate Authority.
- Een Certificate Signing Request (CSR) wordt alleen binnen een vertrouwde zone aangemaakt. De reden is dat de gekoppelde private key bij een signing request minder snel gecompromitteerd kan raken.
- De PKI-beheerder zorgt ervoor dat er van sleutels voor dataencryptie (data at rest) voor het Kadaster een back-up wordt gemaakt. Deze back-up dient te voldoen aan de eisen uit de Archiefregeling (o.a. art. 16;26;17). **LET OP:** Voor sommige sleutels is een back-up niet toegestaan als er sprake is van de Wet Elektronische Handtekening (WEH) vanwege authenticiteit en onweerlegbaarheid.
- Binnen Cloud mogen encryptiesleutels alleen worden opgeslagen in een sterk versleutelde kluis die is afgeschermd met toegangsrechten en welke wordt beheerd middels het Kadaster Identiteiten systeem.
- Het genereren van de sleutels moet altijd herleidbaar zijn middels logging of aansluiting op SIEM.

### 4.5 Verspreiden van sleutelmateriaal

Het verspreiden van sleutelmateriaal is alleen toegestaan onder strekte voorwaarden:

- Geheime of privé sleutels mogen standaard nooit geëxporteerd worden.
- Op de vertrouwde zone plek waar de decryptie plaatsvindt moeten privé sleutels worden gegenereerd die niet buiten deze context mogen komen.
- Het ondertekenen van publieke delen wordt op een gecontroleerde manier gedaan na goedkeuring van de PKI-beheerder.
- Binnen Cloud moet een goedgekeurde kluis[15] gebruikt worden voor het verspreiden van de sleutels. De verspreiding van de sleutels moet altijd herleidbaar zijn middels logging of aansluiting op SIEM.
- Voor bewaarderscertificaten gelden andere regels, zoals vastgelegd bij het team van de Kadaster Signing Service (KSS):
    - Toegang en verspreiding kan alleen middels de closed enveloppe-procedure van de hoofdbewaarder van het Kadaster
    - Van fysieke of elektronische distributie, op smartcard/token is geen sprake bij de KSS

[15] Binnen Azure heb je hiervoor Key Vault https://azure.microsoft.com/nl-nl/services/key-vault/

- De distributie van certificaten en bijbehorende toegangscode op verschillende momenten geschied via een ceremonie.
- De ingebruikname van het sleutelmateriaal op de HSM vindt gecontroleerd via een daarvoor opgestelde procedure.
- De qualified trust service provider (QTSP) is verantwoordelijk om voor alle in omloop zijn de sleutels, vast te leggen wie de ontvanger is, op basis van een unieke identiteit vast te leggen in een geautomatiseerd registratiesysteem. Bij compromittering is bij de QTSP direct bekend is welke personen / organisatie worden geraakt.

### 4.6 Vervangen (en updaten) van de sleutels

Het vervangen van sleutels is noodzakelijk op het moment dat de gebruiker zijn wachtwoord is vergeten, waarmee de private sleutel is beveiligd of het opslagmedium defect of gestolen is. De voornaamste reden om een sleutelpaar te vervangen is wegens het verlopen van de geldigheid van een certificaat. Het is hierbij natuurlijk wel van belang dat de gebruikers continu veilig kunnen blijven doorwerken.

Het Kadaster moet hiervoor:

- Minimaal om de 2 jaar sleutelparen vervangen, tenzij hier een uitzondering voor is vastgelegd.
- Sleutelparen voor een digitale handtekening en zegelcertificaten minimaal om de 3 jaar te vervangen.
- Bijhouden wanneer sleutelparen vernieuwd moeten worden.

### 4.7 Herstellen van sleutels

Een van de problemen van encryptie is het feit dat als op een of andere manier de sleutel is ‘verloren’, alle data die is versleuteld met deze sleutel onbruikbaar is geworden. Het herstellen van sleutels maakt het mogelijk om bij ‘verlies’ van de sleutel, waarmee data is versleuteld, deze data weer te kunnen achterhalen. Het herstellen van sleutels is niet toegestaan op het moment dat onweerlegbaarheid (non-repudiation) aangetoond moet kunnen worden. Denk aan digitale documenten van het Kadaster, waar burgers en bedrijven rechten aan kunnen ontlenen, die digitaal worden ondertekend.
Voor de Kadaster Signing Service kan een sleutel alleen worden hersteld met hulp van 3 ACS kaarten die via alleen via een vaste sleutelprocedure kunnen worden uitgegeven.

Het Kadaster dient:

- De sleutels op van werkplekken (clients) geautomatiseerd vastleggen in een afgeschermd registratiesysteem.
- Een back-up te maken van de systemen waar het sleutelmateriaal op is opgeslagen.
- Ondertekende publieke sleutels te bewaren bij de Serviceprovider en een kopie op een aparte locatie.

### 4.8 Archiveren van sleutels

Onder archiveren van sleutels wordt het maken van een niet meer aan te passen kopie van symmetrische en publieke asymmetrische sleutels verstaan. Na de operationele fase is het van belang dat sleutels gearchiveerd blijven en niet meer aangepast kunnen worden, zolang de opgeslagen en nog te raadplegen berichten en bestanden nog beveiligd zijn met die sleutels en wanneer deze voor verificatiedoeleinden worden gebruikt. Versleutelde gegevens dienen leesbaar te zijn, gedurende de door het bedrijfsproces vereiste periode.

Het Kadaster dient:

- Symmetrische sleutels en asymmetrische publieke sleutels terug te kunnen halen als daar aanleiding voor is vanuit wet- en regelgeving, waaronder:
    - Wet op de inlichtingen- en veiligheidsdiensten (WIV) en
    - de Wet open overheid (WOO).
- Een procedure vast te leggen hoe versleutelde gegevens gepubliceerd kunnen worden.
- Versleutelde gegevens volgens dezelfde beheerprocedures (zoals back-up procedures) te behandelen als ‘normale’ gegevens.
- De, bij de gearchiveerde versleutelde gegevens, behorende sleutels en algoritmen ook te archiveren, om de beschikbaarheid van de gegevens te waarborgen. Dit is niet nodig als dit al technisch is opgeslagen in het sleutelmateriaal zelf.
- Gedurende de vereiste beschikbaarheidstermijn de mate van beveiliging van de versleutelde gegevens te waarborgen. Bijvoorbeeld door een versleuteld archief opnieuw te versleutelen, indien een nieuw algoritme en/of nieuwe sleutellengte wordt gekozen voor versleuteling van gegevens.

### 4.9 Intrekken van de sleutels

Gebruikers en/of beheerders moeten de mogelijkheid hebben om sleutels in te trekken (revocation). Het intrekken van sleutels heeft alleen zin op het moment dat de geldigheidsduur van de sleutel nog niet is verlopen.

Het intrekken van sleutels is mogelijk bij het Kadaster via onderstaande voorwaarden:

- Intrekken wordt altijd als beveiligingsincident ingeschoten door een diensteigenaar binnen het Kadaster;
- Het verzoek wordt beoordeeld door de PKI-beheerder in overleg met het Cyber Security Team (CST);
- Na akkoord worden de ingetrokken sleutels automatisch aangemeld voor publicatie:
    - Certificate Revocation List (CRL) en/of Online Certificate Status Protocol (OCSP).

### 4.10 Vernietigen van de sleutels

Niet meer toegepaste sleutels dienen op een veilige wijze vernietigd te worden. Redenen hiervoor kunnen bijvoorbeeld zijn dat een medewerker het Kadaster heeft verlaten of dat er een sleutel is verlopen.

Sleuteleigenaren binnen het Kadaster dienen:

- Vast te leggen welk type sleutel wanneer mag worden vernietigd. Hierbij dient rekening gehouden te worden met wet- en regelgeving. Bijvoorbeeld de juridische bewaartermijnen.
- Sleutelmateriaal voor het ondertekenen en versleutelen van data dat niet meer geldig is op te ruimen. Het sleutelmateriaal moet worden vernietigd indien er geen geldige reden meer is om deze te bewaren.

### 4.11 Afspraken voor reservecertificaten van alternatieve leverancier

Voor het cryptografie proces is een herstelplan aanwezig. Daarin omschrijft het Kadaster op welke manier er gehandeld moet worden als de primaire leverancier voor certificaten gecompromitteerd is.

Het kadaster heeft hiervoor de volgende maatregelen getroffen:

- Met een alternatieve leverancier is een overeenkomst gesloten;
- In het herstelplan voor certificaten wordt opgegeven op welk manier binnen afzienbare tijd een certificaat opnieuw wordt uitgegeven;
- In een jaarlijkse test wordt het aanvragen van een nieuw certificaat getest om de werking van de alternatieve partij te toetsen op effectiviteit en om eventuele verbeteringen toe te voegen in het herstelplan.

Voor de Kadaster Signing Service is redundantie ingeregeld doordat we gebruik maken van zegels van 3 leveranciers voor de zegelondertekening, met elk een verschillend rootcertificaat. Daarbij moet de 2e en 3e leverancier aan de volgende eisen voldoen:

- leveranciers mogen niet van hetzelfde qualified datacenter of cloud provider gebruik maken als de 1e leverancier;
- certificaten zijn niet door PKIoverheid uitgegeven om single point of failure te voorkomen;
- er wordt gebruik gemaakt van een andere QTSP;
- er mag niet dezelfde qualified signature creation device (QSCD) gebruikt worden;
- de QTSP’s hebben verschillende rootcertificaten.

## Bijlage A - Definities

De volgende definities worden in deze standaard gehanteerd:

- **Encryptie:** Binnen de cryptografie staat encryptie voor het versleutelen van gegevens op basis van een bepaald algoritme. Deze versleutelde gegevens kunnen nadien weer ontcijferd worden zodat men de originele informatie weer terugkrijgt. Dit proces wordt decryptie genoemd.
- **Symmetrische encryptie:** Bij symmetrische encryptie wordt gebruik gemaakt van dezelfde geheime sleutel voor het versleutelen en ontsleutelen van data.
- **Asymmetrische encryptie:** Bij asymmetrische encryptie wordt gebruik gemaakt van een publieke en geheime sleutel. De publieke sleutel wordt gebruikt bij het versleutelen en de geheime sleutel wordt gebruikt voor het ontsleutelen van data.
- **Hashing:** Bij hashing wordt gebruikgemaakt van dezelfde technieken als bij versleuteling en hashing is ook vaak een onderdeel van versleutelingsprotocollen. Het verschil tussen hashing en encryptie is dus dat hashing maar 1 kant op kan (alleen hashen) en dat er bij encryptie twee kanten op gewerkt kan worden (coderen en decoderen).
- **Spoofing:** Spoofing is het vervalsen van kenmerken met als doel om tijdelijk een valse identiteit aan te nemen. Een voorbeeld is vervalsing van e-mail, een website of een telefoonnummer.
- **Certificaat:** een bestand dat fungeert als een digitaal paspoort voor de eigenaar. Een digitaal certificaat is een combinatie van identiteit en openbare sleutel die gewaarmerkt is door de uitgever c.q. certificaatautoriteit (CA).
- **PKI:** Een public key infrastructure (PKI) is een systeem waarmee uitgiften en beheer van digitale certificaten kan worden gerealiseerd.
- **DKIM:** DomainKeys Identified Mail (DKIM) is een techniek waarbij een organisatie verantwoordelijkheid kan nemen voor een bericht dat per e-mail wordt verzonden.
- **QTSP:** De Qualified Trust Service Provider (QTSP) moeten de gekwalificeerde status en toestemming van een toezichthoudende overheidsinstantie krijgen om gekwalificeerde digitale certificaten te mogen verlenen in overeenkomst met strenge voorschriften. Een QTSP moet conform eIDAS op een vertrouwde lijst staan met gekwalificeerder aanbieders (EU Trust List).
- **QSCD:** een qualified signature creation device is een apparaat dat op basis van techniek en een procedure een gekwalificeerde electrinische handtekening kan aanmake.
- **DV:** Domain Validation is het basis niveau van controle van de aanvrager door na te gaan of de eigenaar overeenkomt in de WHOIS-databases.
- **OV:** Organisation Validation certificaat met redelijke controle van aanvrageridentiteit.
- **EV:** Extended Validation certificaat met substantiele controle van aanvrageridentiteit.
- **QWAC:** Qualified Website Authentication Certificates met hoge controle van aanvrageridentiteit en compliant met eIDAS wetgeving.
    - In het verleden was er groene balk voor OV-, EV- of QWAC certificaten. Geen van de populaire browsers doet dit meer, waardoor de meerwaarde hiervan beperkt is.
- **WHOIS:** "Who is responsible for this domain name" protocol om na te gaan wie de eigenaar is van een domein.

## Bijlage B - BIO beheersmaatregelen

In onderstaande tabel zijn de beheersmaatregelen en de corresponderende paragrafen met Kadaster beleidsregels uit dit document opgesomd.

| **BIO nummer** | **Omschrijving** | **Paragraaf uit dit document** |
|---|---|---|
| 10.1.1 | Beleid inzake het gebruik van cryptografische beheersmaatregelen: Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd. | 2.1 |
| 10.1.1.1 | In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt:<br>(a) wanneer cryptografie ingezet wordt;<br>(b) wie verantwoordelijk is voor de implementatie;<br>(c) wie verantwoordelijk is voor het sleutelbeheer;<br>(d) welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum worden toegepast;<br>(e) de wijze waarop het beschermingsniveau vastgesteld wordt;<br>(f) bij inter-organisatie communicatie wordt het beleid onderling vastgesteld. | a. 2.1.1 en 2.2<br>b. 2.1.2<br>c. 2.1.3<br>d. 3.1<br>e. 3.2<br>f. 3.3 |
| 10.1.1.2 | Crypografische toepassingen voldoen aan passende standaarden. | 3.1 |
| 10.1.2 | Sleutelbeheer: Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld en geïmplementeerd. | Heel hoofdstuk 4 |
| 10.1.2.1 | Ingeval van PKIoverheid certificaten: hanteer de PKIoverheid-eisen t.a.v. het sleutelbeheer. In overige situaties: hanteer de standaard ISO-11770 voor het beheer van cryptografische sleutels. | 2.2.1 en 4 |
| 10.1.2.2 | Er zijn (contractuele) afspraken over reservecertificaten van een alternatieve leverancier als uit risicoafweging blijkt dat deze noodzakelijk zijn. | 4.11 |