|  |
| --- |
| CryptografieStandaard |

|  |  |
| --- | --- |
| Auteur(s): |  |
| Versie: |  |
| Datum: | Kies of typ een datum |
| Kenmerk: |  |
|  |  |
|  |  |

**Documentinformatie**

Dit document maakt onderdeel uit van een complete set (beleidspiramide) met formeel vastgestelde documenten op strategisch, tactisch en operationeel niveau. Dit document heeft betrekking op de laag Standaard in de beleidspiramide.



**Versiebeheer**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Auteur** | **Verwerking** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Distributielijst**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Ontvanger** | **Doel** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Vaststelling**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Vastgesteld door** | **Vastgesteld op** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Samenhang met andere documenten**

|  |  |  |  |
| --- | --- | --- | --- |
| **Naam** | **Bovenliggend** | **Gelijk niveau** | **Onderliggend** |
| [STRATEGISCH IB-BELEID] | x |  |  |
| [DATACLASSIFICATIE] |  | x |  |
| [DATAMANAGEMENT] |  | x |  |
| [RICHTLIJN CRYPTOGRAFIE] |  |  | x |
| [PROCEDURE SLEUTELBEHEER] |  |  | x |

**Verwijzingen naar SURFaudit Toetsingskader en ISO27001**

|  |  |
| --- | --- |
| **Kader** | **Verwijzing (tags)** |
| SURFaudit Toetsingskader | DM.02; DM.05; SM.03; SM.10 |
| ISO 27001 | 5.1; Appendix A 8.24;  |
| ISO 27002 | 5.11; 5.13; 5.33; 7.10; 7.14; 8.2; 8.3; 8.22; 8.24 |

**Creative Commons**

Dit template is een product van het SURF Security Expertise Centrum en beschikbaar onder de licentie Creative Commons Naamsvermelding 4.0 Internationaal. <https://creativecommons.org/licenses/by/4.0/deed.nl>

Inhoudsopgave

|  |
| --- |
| [Samenvatting 4](#_Toc180660188)[1 Inleiding 5](#_Toc180660189)[1.1 Doel 5](#_Toc180660190)[1.2 Reikwijdte en toepassingsgebied 5](#_Toc180660191)[1.3 Rollen en verantwoordelijkheden 5](#_Toc180660192)[2 Standaard cryptografie 6](#_Toc180660193)[2.1 Principes cryptografie 6](#_Toc180660194)[2.2 Gebruik van cryptografie 6](#_Toc180660195)[2.3 Gegevensbescherming 7](#_Toc180660196)[3 Cryptografische sleutels en certificaten 8](#_Toc180660197)[3.1 Sleutelbeheer 8](#_Toc180660198)[3.1.1 Algemeen 8](#_Toc180660199)[3.1.2 Sleutelgeneratie 8](#_Toc180660200)[3.1.3 Sleutelopslag 8](#_Toc180660201)[3.1.4 Sleuteldistributie 9](#_Toc180660202)[3.1.5 Sleutelwijziging en -intrekking 9](#_Toc180660203)[3.1.6 Sleutel back-up en Escrow 10](#_Toc180660204)[3.1.7 Sleutel (nood-) toegang en herstel 10](#_Toc180660205)[3.1.8 Sleutel deactivatie en vernietiging 11](#_Toc180660206)[3.2 Certificaatbeheer 11](#_Toc180660207)[3.2.1 Uitgifte van certificaten 12](#_Toc180660208)[3.2.2 Levensbeheercyclus van certificaten 12](#_Toc180660209)[3.2.3 Intrekken van certificaten 12](#_Toc180660210)[3.2.4 Beveiliging van private sleutels 12](#_Toc180660211)[3.2.5 Monitoring en audits 12](#_Toc180660212)[3.2.6 Incident en response 12](#_Toc180660213)[4 Vaststelling 13](#_Toc180660214)[Bijlage 1 Rollen 14](#_Toc180660215)[Bijlage 2 Verklarende woordenlijst 16](#_Toc180660216) |

Samenvatting

Hier komt een samenvatting, op zichzelf leesbaar, van de inhoud van dit document in max. 1 A4.

# Inleiding

Dit document beschrijft de standaard voor Cryptografie binnen onze instelling, inclusief de vereisten met betrekking tot het beheer van cryptografische sleutels en digitale certificaten gedurende hun levenscyclus. Daarnaast stelt het de principes vast die de basis vormen voor de Richtlijn Cryptografie en de Procedure Sleutelbeheer. In Bijlage 1 zijn rollen en verantwoordelijkheden beschreven en in Bijlage 2 de definities en begrippen.

## Doel

Het doel van deze standaard is om het juiste en doeltreffende gebruik van cryptografie binnen en voor onze instelling te borgen. Dit gebeurt in overeenstemming met het [Strategisch Informatiebeveiligingsbeleid], relevante wet- en regelgeving, statutaire en contractuele vereisten. Bovendien moet cryptografie voldoen aan de beperkingen op de import, export en het gebruik van cryptografische hardware en software. De naleving van deze standaard wordt periodiek geëvalueerd om te verzekeren dat de cryptografische processen in lijn blijven met de vastgestelde principes. Dit omvat ook het beheer van cryptografische sleutels en digitale certificaten.

## Reikwijdte en toepassingsgebied

De scope van deze standaard voor cryptografie omvat alle cryptografische sleutels en digitale certificaten die door of voor onze instelling worden gegenereerd, gedistribueerd, opgeslagen, gebruikt, ingetrokken of verwijderd.

## Rollen en verantwoordelijkheden

Aanvullend op het [Strategisch Informatiebeveiligingsbeleid] zijn specifieke rollen en verantwoordelijkheden toegewezen worden om de effectieve implementatie, monitoring en naleving van cryptografische beheersmaatregelen te waarborgen.

De expliciete toewijzing van deze cryptografische rollen en verantwoordelijkheden is essentieel voor de operationele informatiebeveiliging en het risicobeheer binnen onze instelling. Er wordt een centraal register bijgehouden voor de toewijzing van cryptografische rollen aan functionarissen.

Zie Bijlage 1 voor een gedetailleerde beschrijving van deze rollen en verantwoordelijkheden.

# Standaard cryptografie

## Principes cryptografie

De standaard cryptografie van onze instelling is gebaseerd op de volgende kernprincipes:

1. **Minimale toegang**
Cryptografische sleutels en gevoelige gegevens mogen alleen toegankelijk zijn voor diegene die deze ook strikt nodig hebben voor hun werk.
2. **Sterke cryptografie**Onze instelling maakt gebruik van sterke, geaccepteerde cryptografische algoritmen en protocollen die voldoen aan de actuele internationale standaarden en richtlijnen.
3. **End-to-End encryptie**Gevoelige communicatie tussen systemen en gebruikers wordt beschermd door middel van *‘end-to-end’* encryptie, om ervoor te zorgen dat gegevens niet leesbaar zijn door onbevoegden tijdens en na de transmissie.
4. **Regelmatige evaluatie en actualisatie**Cryptografische methoden en technieken worden regelmatig geëvalueerd en bijgewerkt in overeenstemming met de nieuwste wetenschappelijke inzichten en technologische ontwikkelingen.

## Gebruik van cryptografie

Met betrekking tot het gebruik van cryptografie schrijft onze standaard het volgende voor:

1. **Risicobeoordeling**
Cryptografische beheersmaatregelen worden toegepast op basis van een risicobeoordeling, waarbij rekening wordt gehouden met de gevoeligheid van de informatie. Dit gebeurt volgens een BIA[[1]](#footnote-1) en BIV-classificatie[[2]](#footnote-2).
2. **Vertrouwelijkheid**
Cryptografie wordt gebruikt om de vertrouwelijkheid van gegevens te beschermen terwijl ze worden opgeslagen, verwerkt en/of verzonden.
3. **Integriteit**
Cryptografie wordt gebruikt om de integriteit van gegevens beschermen (bijv. door hash-functies uit te voeren of digitaal te ondertekenen).
4. **Authenticiteit**
Cryptografie wordt gebruikt om sterke authenticatie te bieden voor gebruikers en systemen (bijv. door gebruik te maken van digitale certificaten en smartcards).
5. **Onweerlegbaarheid**Cryptografie wordt gebruikt om de identiteit van een initiator van een kritieke transactie of communicatie te bewijzen en bewijs te leveren van het al dan niet plaatsvinden van een gebeurtenis of actie (bijv. door digitaal te ondertekenen).
6. **Cryptografische oplossingen**Er worden uitsluitend goedgekeurde cryptografische oplossingen en tools gebruikt. De specifieke lijst hiervoor wordt onderhouden in de [Richtlijn voor Cryptografie].
7. **Cryptografische algoritmen**Er worden uitsluitend door de industrie geaccepteerde en gestandaardiseerde cryptografische protocollen en algoritmen met minimale en aanbevolen versies en sleutellengtes gebruikt. De specifieke lijst hiervoor zal wordt onderhouden in de [Richtlijn voor Cryptografie].
8. **Cryptografische processen en middelen**
Verantwoordelijke binnen en buiten onze instelling beschikken over processen, procedures en middelen om cryptografische oplossingen te beheren, waaronder:
	* Het toewijzen van verantwoordelijkheden voor het beheer van cryptografische oplossingen, zie voor deze rollen Bijlage 1: Rollen en verantwoordelijkheden.
	* Het omgaan met conflicterende wet- en regelgeving met betrekking tot het gebruik van cryptografische oplossingen in verschillende rechtsgebieden (bijv. door advies in te winnen bij de afdeling Juridische Zaken).
	* Het up-to-date houden van cryptografische oplossingen.
	* Het faciliteren van sleutelbeheer.
	* Het bepalen van de impact van het gebruik van versleutelde informatie op beheersmaatregelen die afhankelijk zijn van inhoudelijke inspectie (bijv. detectie van malware of filteren van inhoud).

## Gegevensbescherming

Deze standaard cryptografie schrijft voor dat encryptie wordt toegepast voor het beschermen van gegevens in de verschillende stadia.

1. **Data-at-Rest**
Encryptie wordt gebruikt om gevoelige gegevens te versleutelen terwijl ze zijn opgeslagen om effectieve bescherming te bieden tegen onbevoegde toegang en diefstal.
2. **Data-in-Transit**
Encryptie wordt gebruikt om alle gegevens tijdens het transport te beschermen tegen onbevoegde onderschepping, afluisteren, manipulatie en toegang.
3. **Data-in-Use**
Encryptie wordt gebruikt om gegevens tijdens gebruik te beschermen tegen onbevoegde onderschepping, toegang en diefstal, vooral voor gegevens die als “kritiek” of “(zeer) geheim” zijn geclassificeerd (Bijv. ‘Master keys’, HSM-sleutels, KMS-sleutels).

# Cryptografische sleutels en certificaten

## Sleutelbeheer

Effectief sleutelbeheer is cruciaal voor het beveiligen van de processen voor het genereren, opslaan, archiveren, herstellen, ophalen, distribueren, intrekken en vernietigen van cryptografische sleutels. Deze standaard schrijft dan ook voor wat hiervoor de minimale vereisten zijn voor onze instelling, gebaseerd op ISO/IEC 11770-1 en ISO/IEC 27002:2022 par. 8.24.

### Algemeen

1. Sleutel levenscyclusbeheer
Alle Systeemeigenaren moeten beschikken over processen, procedures en middelen om de levenscyclus van cryptografische sleutels te beheren.
2. Aanstellen van Sleutelbewaarders
Systeemeigenaren moeten Sleutelbewaarders aanstellen om cryptografische sleutels en sleutelbeheersystemen te beschermen en beheren.
3. Bescherming van Cryptografie
Alle cryptografische sleutels moeten worden beschermd tegen wijziging en verlies. Bovendien moeten geheime en private sleutels aanvullend worden beschermd tegen ongeoorloofd gebruik en openbaarmaking. Apparatuur die gebruikt wordt om sleutels te genereren, op te slaan en te archiveren moet fysiek beschermd worden.
4. Eigenaarschap
Cryptografische sleutels die worden gebruikt voor het beschermen van gevoelige of geheime gegevens van onze instelling, zijn eigendom van het organisatieonderdeel van onze instelling dat eindverantwoordelijk is voor de bescherming van deze gegevens.

### Sleutelgeneratie

Voor de generatie van cryptografische sleutels geldt dat zij worden gegenereerd:

1. Door de eigenaar van die sleutel of door een vertrouwde partij (Sleutelbewaarder) die gemachtigd is om sleutels te genereren en deze op een veilige manier aan de eigenaar te verstrekken.
2. Met een hardware-, firmware- of software-gebaseerde cryptografische module die voldoet aan wet- en regelgeving en internationale standaarden.
3. In overeenstemming met de [Richtlijn voor Cryptografie].

### Sleutelopslag

Cryptografische sleutels moeten op het minimale aantal locaties worden opgeslagen. Dit waarborgt volledige controle en toezicht op alle sleutellocaties en minimaliseert het risico op misbruik of ongeautoriseerde toegang tot de sleutels.

Medewerkers die omgaan met cryptografische sleutels:

1. Beveiligen deze zowel logisch als fysiek.
2. Slaan sleutels op via een goedgekeurde opslagmethode (zie ook: Richtlijn voor Cryptografie)
3. Registreren alle locaties, metadata, certificaten en logs van sleutelbeheeractiviteiten in een centraal sleutelbeheer-systeem (Key Management System, KMS). Deze registraties moeten worden beschermd tegen verlies, vernietiging of vervalsing en toegankelijk blijven gedurende hun gehele bewaarperiode, in overeenstemming met wettelijke eisen voor het decoderen van versleutelde archieven.

*Opmerking: Niet van toepassing op openbare (publieke) sleutels.*

### Sleuteldistributie

Het verspreiden van cryptografische sleutels met zo min mogelijk partijen helpt onze instelling om alle sleutellocaties bij te houden en te controleren, en minimaliseert de kans dat sleutels worden blootgesteld aan onbevoegde partijen.

Medewerkers die omgaan met cryptografische sleutels:

1. Delen deze sleutels alleen met degenen die daartoe uitdrukkelijk zijn gemachtigd.
2. Beperken de verspreiding van sleutels tot zo min mogelijk ontvangers.
3. Waarborgen de vertrouwelijkheid en integriteit van overgedragen sleutels via goedgekeurde cryptografische methoden (zie ook: Richtlijn voor Cryptografie).
4. Verspreiden sleutels via een goedgekeurd transportmechanisme (zie ook: Richtlijn voor Cryptografie).

*Opmerking: Niet van toepassing op openbare (publieke) sleutels*

### Sleutelwijziging en -intrekking

Het tijdig vervangen, (tijdelijk) buiten gebruik stellen of intrekken van cryptografische sleutels in overeenstemming met vastgestelde processen, procedures en methoden (zie ook: Richtlijn voor Cryptografie) is essentieel om de veiligheid van cryptografische systemen te waarborgen.

Bij beëindiging van een dienstverband of contractuele relatie moeten cryptografische sleutels die externe partijen of medewerkers in hun bezit hebben, worden geretourneerd. Dit moet gepaard gaan met intrekkings- of herroepingsprocessen voor de betrokken sleutels in het centrale sleutelbeheerregister.

Wijzigingen en intrekkingen van cryptografische sleutels worden:

1. Uitgevoerd volgens vastgestelde processen, procedures en methoden.
2. Gedocumenteerd inclusief de redenen en de datum van de wijziging of intrekking in een (centraal) sleutelbeheersysteem.
3. Gevalideerd door bevoegde personen (zoals de Sleuteleigenaar) om te garanderen dat het proces in overeenstemming met beleid is uitgevoerd.
4. Gecontroleerd door IT Auditors, Compliance Officers en/of Information Security Officers via periodieke audits om naleving van dit sleutelbeheerbeleid te waarborgen.

Cryptografische sleutels worden gewijzigd:

1. Wanneer er significante veranderingen in de beveiligingsrisico’s optreden.
2. Volgens een vastgesteld rotatieschema per type sleutel.
3. Na het uitvoeren van kritieke updates of aanpassingen in de cryptografische algoritmes.

Cryptografische sleutels worden ingetrokken:

1. Bij het vermoeden van compromitteren (zoals verlies of diefstal), als onderdeel van de reactie op een informatiebeveiligingsincident.
2. Bij het beëindigen van een contractuele relatie met een externe partij die toegang had tot de cryptografische sleutels.
3. Bij functieverandering of beëindiging van de arbeidsrelatie van medewerkers met toegang tot de cryptografische sleutels.
4. Bij gewijzigde beveiligingseisen voor het einde van de levensduur.
5. Wanneer deze niet langer meer nodig zijn.

### Sleutel back-up en Escrow

Voor het herstel van cryptografische sleutels worden back-ups gemaakt. Optioneel kan een Escrow van toepassing zijn.

Sleutel back-up

1. Reserve kopieën (back-ups) van cryptografische sleutels worden versleuteld opgeslagen in een hoog beveiligde omgeving die fysiek gescheiden is van de data en de primaire sleutelopslaglocatie, om fysieke beveiliging te garanderen.
2. De toegang tot reserve kopieën van cryptografische sleutels is strikt beperkt tot geautoriseerd personeel (Sleutelbewaarder) en voldoet aan het principe van ‘least privilege’.
3. Periodieke testen worden uitgevoerd om de integriteit en beschikbaarheid van back-up sleutels te verifiëren.
4. Eigenaren van geheime en private sleutels die gebruikt worden voor het versleutelen van informatie van onze instelling, maken een verplichte reserve kopie van deze encryptiesleutels om gegevensverlies te voorkomen.

Sleutel Escrow

1. Het escrow-proces voldoen aan de wettelijke en organisatorische eisen, waarbij de privacy en integriteit van de gegevens worden gewaarborgd.
2. De vertrouwde (derde) partij die cryptografische sleutels in escrow bewaart, is onafhankelijk en betrouwbaar, en is gebonden aan strikte veiligheids- en privacyrichtlijnen.
3. De toegang tot escrow-sleutels vindt uitsluitend plaats onder strikte voorwaarden, zoals gedefinieerd in het escrow-beleid, en wordt altijd gedocumenteerd en geautoriseerd door bevoegde personen.
4. Het gebruik van sleutel escrow blijft minimaal om de risico’s op misbruik of onbevoegde toegang te beperken.

### Sleutel (nood-) toegang en herstel

Sleutel toegang:

1. Toegang tot cryptografische sleutels is beperkt tot uitsluitend geautoriseerde personen op basis van het principe van 'least privilege' (minimale toegangsrechten).
2. Op de rollen binnen het cryptografisch proces is het IAM proces voor de identity lifecycle van toepassing (Instromers, Doorstromers, Uitstromers).

Noodtoegang:

1. Er zijn procedures ontwikkeld voor veilige en gecontroleerde noodtoegang tot cryptografische sleutels in geval van een incident of noodsituatie.
2. Noodtoegang moet uitsluitend worden verleend aan geautoriseerde individuen na goedkeuring van de bevoegde autoriteiten, en alleen voor de duur van de noodsituatie.
3. Elke vorm van noodtoegang wordt volledig gedocumenteerd, met vermelding van de redenen, het moment van toegang, de verleende toegangsrechten en de genomen acties.

Bij gerechtelijke verzoeken voor toegang tot versleutelde gegevens wordt een strikt proces gevolgd voor het gecontroleerd vrijgeven van cryptografische sleutels. Alle verzoeken en handelingen worden geregistreerd en uitgevoerd onder toezicht van juridische en beveiligingsfunctionarissen.

Herstel (key-recovery):

1. Er zijn procedures vastgesteld voor het veilig en gecontroleerd herstellen van cryptografische sleutels in geval van verlies, beschadiging of in noodsituaties.
2. Herstelprocedures zijn alleen toegankelijk voor geautoriseerde personen en zijn voorzien van sterke authenticatie en autorisatie om ongeautoriseerde toegang te voorkomen.
3. Alle sleutelherstelactiviteiten worden vastgelegd, inclusief de uitgevoerde stappen, betrokken personen en de tijdslijnen van het herstelproces. Herstelacties moeten na afloop worden geëvalueerd voor toekomstige verbetering van (calamiteiten)herstelplannen.

### Sleutel deactivatie en vernietiging

Sleutel deactivatie:

1. Cryptografische sleutels worden onmiddellijk gedeactiveerd en/of ingetrokken wanneer ze niet langer nodig zijn, zoals na de beëindiging van een overeenkomst, het verlopen van de sleutellevensduur, of bij vermoeden van compromitteren.
2. Deactivatieprocessen moeten ervoor zorgen dat de sleutels niet langer toegankelijk of bruikbaar zijn, en dat alle betrokken systemen en gebruikers op de hoogte worden gesteld van de deactivatie.
3. Gedeactiveerde sleutels worden opgeslagen in een beveiligde omgeving totdat een beslissing is genomen over hun definitieve vernietiging of hergebruik.

Sleutel vernietiging:

1. Sleutels worden op een veilige en onherroepelijke manier vernietigd zodra ze niet langer nodig zijn of wanneer de beveiligingsregels dit vereisen, om het risico van ongeautoriseerde toegang of hergebruik te voorkomen.
2. Apparaten die cryptografische sleutels bevatten, moeten op veilige wijze worden verwijderd of vernietigd aan het einde van hun levenscyclus.
3. De vernietiging van sleutels wordt uitgevoerd via goedgekeurde methoden overeenkomstig de gevoeligheid van de gegevens die door de sleutels zijn beschermd, zoals fysieke vernietiging, overschrijven en/of cryptografische processen voor het wissen, zoals gespecificeerd in de Richtlijn voor Cryptografie.

Alle acties met betrekking tot deactivatie en sleutelvernietiging, inclusief de datum, methode van vernietiging, en de verantwoordelijke personen, worden gedocumenteerd en opgeslagen voor audit- en nalevingsdoeleinden.

## Certificaatbeheer

Digitale certificaten worden gebruikt om identiteit te waarborgen, gegevens te versleutelen en veilige communicatie te faciliteren, zowel binnen de infrastructuur van onze instelling als bij interacties met externe partners. De certificaatbeheerprocessen moeten voldoen aan internationale normen, standaarden en richtlijnen, zoals gedefinieerd door onder andere ISO, NCSC, NIST, ETSI, IETF en CA/B Forum.

### Uitgifte van certificaten

1. Certificaten worden uitsluitend uitgegeven door vertrouwde certificaatautoriteiten (CA's). De lijst van goedgekeurde CA’s wordt door [Security Team] bijgehouden in de Richtlijn voor Cryptografie.
2. Onze instelling maakt gebruik van een interne Public Key Infrastructure (PKI) voor de uitgifte digitale certificaten die alleen worden vertrouwd binnen onze instelling, waarbij de uitgifte- en beheerprocessen volledig onder controle van de centrale IT organisatie vallen. Deze PKI dient als basis van vertrouwen (“Root-of-Trust”) voor onze gehele instelling.
3. Certificaten voor externe doeleinden worden uitgegeven door externe, wereldwijd vertrouwde publieke CA’s, die voldoen aan de eisen van het CA/Browser Forum en internationale normen zoals ISO/IEC 21188 en ETSI EN 319 411-1. Hierdoor kunnen externe partijen erop vertrouwen dat de communicatie met onze instelling veilig is.

### Levensbeheercyclus van certificaten

1. De levenscyclus van digitale certificaten worden beheerd en ondersteund door een centraal certificaat beheerssysteem van onze instelling dat volledig onder controle van de centrale IT organisatie valt.
2. De certificaat beheerprocessen worden verregaand geautomatiseerd, om menselijke fouten te minimaliseren, systeemuitval door verlopen certificaten te voorkomen en efficiënter certificaten te kunnen vernieuwen.

### Intrekken van certificaten

1. Een certificaat wordt onmiddellijk ingetrokken bij compromitteren van de sleutel, bij onjuiste gegevens, beëindiging van de dienst of het contract, of bij wijzigingen in de beveiligingseisen.
2. Onze instelling maakt gebruik van geautoriseerde mechanismen om de status van certificaten te kunnen valideren, zoals gespecificeerd in de [Richtlijn voor Cryptografie].

### Beveiliging van private sleutels

1. Private sleutels worden veilig gegenereerd, gedistribueerd en opgeslagen in overeenstemming met de [Richtlijn voor Cryptografie].
2. Toegang tot private sleutels wordt strikt gecontroleerd en gelogd.
3. Multi-factor authenticatie (MFA) wordt toegepast om de toegang te beveiligen.

### Monitoring en audits

1. Continue monitoring wordt uitgevoerd om de geldigheid en integriteit van certificaten te waarborgen.
2. Regelmatige audits van het certificaatbeheerproces worden uitgevoerd om compliance met wet- en regelgeving, internationale normen en richtlijnen te waarborgen.

### Incident en response

1. Bij een incident met betrekking tot cryptografische certificaten, zoals een datalek of compromitteren van een CA, wordt onmiddellijk het Cyber Security Incident Responseplan in werking gesteld, conform [ISO/IEC 27035].
2. Er zijn duidelijke procedures voor het escaleren van certificaat gerelateerde incidenten en het tijdig informeren van betrokken partijen (belanghebbenden).

# Vaststelling

Deze standaard is aldus vastgesteld.

[Plaats], [Datum].

[NAAM]

[FUNCTIE].

[Na (her)vaststelling, ook de tabel op p.2 bijwerken]

1. Rollen

|  |  |  |
| --- | --- | --- |
| **Rol** | **Beschrijving** | **Verantwoordelijkheden** |
| Sleuteleigenaar | Een *Sleuteleigenaar* (‘Key Owner’) is de persoon of entiteit[[3]](#footnote-3) die de functionele verantwoordelijkheid draagt voor een cryptografische sleutel. De *Sleuteleigenaar* is eindverantwoordelijk voor de beveiliging en het correcte gebruik van de cryptografische sleutel gedurende zijn levenscyclus en heeft de autoriteit om beslissingen te nemen over het gebruik van de sleutel. Voor alle informatie-systemen binnen onze instelling is de *Systeemeigenaar* tevens de *Sleuteleigenaar*. | * **Toegangsbeheer**: Toekennen van toegangsrechten tot de sleutel aan geautoriseerde gebruikers, zoals de *Sleutelbeheerder* en *Sleutelbewaarder* en het registreren hiervan in een centraal sleutelbeheerregister.
* **Beveiliging**: Vaststellen van de beveiligingsmaatregelen rondom het gebruik en de opslag van de sleutel.
* **Compliance**: Zorgdagen voor naleving van interne en externe cryptografische normen, richtlijnen en procedures.
* **Incidentbeheer**: Beslissingen nemen over sleutelrotatie, -intrekking of -verwijdering in geval van IT security incidenten zoals sleutelcompromittering of -verlies.
 |
| Sleutelbeheerder | Een *Sleutelbeheerder* (‘Key Manager’), is verantwoordelijk voor het dagelijks operationeel beheer van cryptografische sleutels gedurende hun gehele levenscyclus. Een *Sleutelbeheerder* maakt gebruik van een Key Management System (KMS) en zorgt ervoor dat sleutels correct worden gebruikt en opgeslagen volgens dit Beleid, de Standaard en operationele procedures.Binnen onze instelling is de rol van *Sleutelbeheerder* toegewezen aan een *Systeembeheerder* die de gedelegeerde verantwoordelijkheid heeft (namens de *Sleuteleigenaar*) voor het gebruik en beheer van cryptografische sleutels conform dit Beleid en de Standaard. | * **Implementeren:** Implementeren van goedgekeurde cryptografische oplossingen, methoden en algoritmen in hun respectievelijke systemen.
* **Configureren:** Zorgen voor correcte configuratie en up-to-date houden van cryptografische oplossingen en tools.
* **Documenteren:** Documenteren van de toegepaste cryptografische oplossingen, methoden en algoritmen, waarbij de cryptografische componenten worden opgenomen in de SBoM van het informatiesysteem.
* **Logging:** Registreren van alle sleutelbeheeractiviteiten, zoals generatie, toegang, rotatie, intrekking (deactivering) en vernietiging van sleutels met ondersteuning van een (centraal) sleutelbeheerssysteem (‘Key Management System’, KMS).
* **Beheren:** Beheren van de levenscyclus van systeem specifieke cryptografische sleutels.
* **Bewaken:** Monitoren van de effectiviteit van cryptografische beheersmaatregelen en rapporteren van problemen.
* **Incident response:** Assisteren bij cybersecurity incident response gerelateerd aan cryptografische sleutels en digitale certificaten (bijv. Sleutelcompromittatie of verlopen van een certificaat).
* **Awareness & training:** Deelnemen aan relevante trainingen om up-to-date te blijven met de cryptografische praktijken.
 |
| Sleutelbewaarder | Een Sleutelbewaarder (‘Key Custodian’) is een hoog vertrouwde functionaris binnen onze instelling of bij een vertrouwde derde partij die gedelegeerd verantwoordelijk is voor het beheer van de fysieke en logische beveiliging van cryptografische sleutels. De sleutelbewaarder zorgt ervoor dat alleen geautoriseerde personen (zoals *Sleutelbeheerders*) toegang hebben tot de sleutels en ondersteunt bij het distribueren van sleutels. Een *Sleutelbewaarder* is NIET verantwoordelijk voor het genereren van sleutels, maar kan wel betrokken zijn bij het documenteren van het sleutelbeheerproces en het implementeren van beveiligingsprotocollen.  | * **Beveiligde opslag**: Opslaan van cryptografische sleutels conform vastgestelde procedures;
* **Distributie**: Distribueren van cryptografische sleutels volgens vastgestelde procedures;
* **Deactivatie**: Buiten gebruik stellen en intrekken van cryptografische sleutels volgens vastgestelde procedures;
* **Destructie**: Vernietigen van cryptografische sleutels volgens vastgestelde procedures;
* **Logging**: Vastleggen van alle fysieke en logische toegangshandelingen met cryptografische sleutels in een sleutelbeheerssysteem;
* **Key ceremony**: Participeren bij een sleutelgeneratie ceremonie door (een deel van) een cryptografische sleutel in te brengen.
 |

1. Verklarende woordenlijst

Tekst

| **Begrip** | **Omschrijving** |
| --- | --- |
| ‘Data-at-Rest’ bescherming | Verwijst naar de beveiligingsmaatregelen die worden genomen om gegevens te beschermen wanneer ze worden opgeslagen in niet-vluchtige opslag. |
| ‘Data-in-Transit’ bescherming | Verwijst naar de beveiligingsmaatregelen die worden geïmplementeerd om gegevens te beveiligen terwijl ze worden verzonden van de ene locatie naar de andere via een netwerk. |
| ‘Data-in-Use’ bescherming | Verwijst naar de beveiligingsmaatregelen die zijn geïmplementeerd om gegevens te beveiligen terwijl ze actief worden benaderd, verwerkt of gebruikt door applicaties, diensten of gebruikers. |
| Key Escrow | Key Escrow is een beveiligingsmethode waarbij een cryptografische sleutel, die gebruikt wordt voor het versleutelen van data, wordt opgeslagen bij een vertrouwde derde partij (TTP), de zogenaamde ‘escrow-agent.’ Deze agent bewaart een kopie van de sleutel op een veilige manier, zodat deze kan worden vrijgegeven onder specifieke, vooraf vastgestelde omstandigheden. |
| Sleutelcompromittering | Sleutelcompromittering (‘key compromise’) verwijst naar het ongeautoriseerd verkrijgen of blootstellen van cryptografische sleutels, waardoor de beveiliging van systemen, data of communicatie in gevaar komt. |
| Software Bill of Materials | Een ‘Software Bill of Materials' (SBoM) is een gedetailleerde lijst van alle componenten, afhankelijkheden en modules die in een softwaretoepassing of systeem zijn opgenomen. Het biedt een overzicht van de gebruikte softwarecomponenten, inclusief open-source en commerciële software, evenals hun versies, licenties en leveranciersinformatie. |
| Vertrouwde derde partij | Een vertrouwde derde partij (‘Trusted Third Party’, TTP) is een onafhankelijke entiteit die optreedt als tussenpersoon om vertrouwen en beveiliging te waarborgen tussen twee of meer partijen in een transactie of communicatie. De TTP heeft een cruciale rol in het beheren en verifiëren van vertrouwelijke gegevens, zoals digitale certificaten, sleutels en identiteit. De partijen vertrouwen erop dat de TTP eerlijk en betrouwbaar is, en de nodige beveiligingsmaatregelen handhaaft. |

1. Business Impact Analysis [↑](#footnote-ref-1)
2. Beschikbaarheid, Integriteit en Vertrouwelijkheid [↑](#footnote-ref-2)
3. groep, organisatie, apparaat, systeem of cryptografische module [↑](#footnote-ref-3)