TASKFORCE
Bestuur & Informatieveiligheid Dienstverlening

# Encryptiebeleid

Een operationeel product op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR)

Rijksoverheid VNG Vereniging van Nederlandse Gemeenten Interprovinciaal Overleg ip MANIFESTgroep UNIE VAN WATERSCHAPPEN

## Colofon

Onderhavig operationeel product, behorende bij de Baseline Informatiebeveiliging Rijksdienst (BIR), is mogelijk gemaakt door de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID). Het product is gebaseerd op het operationele product ‘Encryptiebeleid (PKI)’ behorende bij de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Dit product is ontwikkeld door de Informatiebeveiligingsdienst voor gemeenten (IBD).

## Leeswijzer

Dit document is een van de operationele producten op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR).

**Doel**

Dit document biedt een handreiking voor een invulling van het encryptiebeleid voor organisaties binnen de Rijksoverheid. Deze uitgangspunten over informatiebeveiliging zijn afkomstig uit de BIR en het beleid voldoet daarmee aan de BIR.

**Doelgroep**

Dit document is van belang voor de directie en ICT-beheerders van organisaties binnen de Rijksoverheid.

**Reikwijdte**

Dit document heeft voornamelijk betrekking op maatregel 10.6.1, 10.8, 10.9.2, 10.10.2, 11.7.1, 12.3 en 15.1.6 van de Baseline Informatiebeveiliging Rijksdienst (BIR). Het document gaat in op personele, organisatorische en technische informatiebeveiligingsaspecten die organisaties binnen de Rijksoverheid dienen te overwegen in relatie tot encryptiebeleid.

**Relatie met overige producten**

- Baseline Informatiebeveiliging Rijksdienst (BIR). Tactisch Normenkader (TNK)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007)
- Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI:2013)
- Informatiebeveiligingsbeleid

## Inhoudsopgave

# 1 Inleiding

Dit document geeft algemene aanwijzingen over encryptie voor vertrouwde en integere berichtuitwisseling tussen daarvoor geautoriseerde personen en systemen, het borgen van onweerlegbaarheid van verzending, ontvangst bij berichtuitwisseling en het vertrouwd kunnen opslaan van bestanden. Tevens worden aanwijzingen gegeven over de beheersing van zowel de operationele- als de beheerprocessen die bij het toepassen van encryptie van belang zijn. Het gaat hierbij om de gehele levenscyclus van sleutelmateriaal: van het creëren tot het vernietigen van sleutels. Er wordt speciaal aandacht besteed aan de diensten van en certificatiedienstverleners[1], zoals Logius met die PKIoverheid[2] (Public Key Infrastructure overheid) als een (derde) vertrouwde partij, certificaten uitgeven en beheren voor verschillende organisaties die encryptie toepassen. Tenslotte is er aanvullend encryptiebeleid beschreven.

De Baseline Informatiebeveiliging Rijksdienst (BIR) heeft in hoofdstuk 10.8.4, 10.9.2 en 12.3.2 maatregelen beschreven die te maken hebben met het gewenste beleid betreffende encryptie en de daar voor benodigde Public Key Infrastructure (PKI).

## 1.1 Vraagstukken

De belangrijkste vraagstukken die door een betrouwbare elektronische communicatie opgelost worden, zijn:

1. Hoe kan worden vastgesteld met wie er wordt gecommuniceerd en hoe weet de ontvanger zeker dat de verzender ook daadwerkelijk de afzender is en niet iemand anders? (Identiteit)
2. Hoe kan worden voorkomen dat berichten tijdens transport en opslag onopgemerkt worden gewijzigd, zodat de ontvanger een zekere mate van garantie heeft dat het bericht integer is en dat het bericht afkomstig is van de identiteit, die als ondertekenaar bij het bericht staat vermeld? (Authenticiteit)
3. Hoe kan ervoor worden gezorgd dat de inhoud van berichten onleesbaar is voor derden? (Vertrouwelijkheid)
4. Waarmee kan worden aangetoond dat gegevens tijdens transport of opslag (niet) zijn gewijzigd? (Integriteit)
5. Waarmee kan worden aangetoond dat bepaalde gebeurtenissen of handelingen hebben plaatsgevonden, zoals het verzenden en ontvangen van elektronische documenten? (Onweerlegbaarheid)

## 1.2 Aanwijzing voor gebruik

Deze handleiding is geschreven om informatiebeveiligingsmaatregelen met betrekking tot encryptie en PKI aan te reiken, zodat invulling gegeven kan worden aan

[1] Ook wel Certification Service Provider (CSP) genoemd.
[2] http://www.logius.nl/producten/toegang/pkioverheid/

informatiebeveiligingsbeleid. Deze handleiding is geen volledige procesbeschrijving voor encryptie en bevat geen productbeschrijvingen, maar bevat wel voldoende informatie om goede (beleids)keuzes te maken en bewustwording te creëren met betrekking tot encryptie en de Public Key Infrastructure (PKI).

# 2 Encryptie en PKI

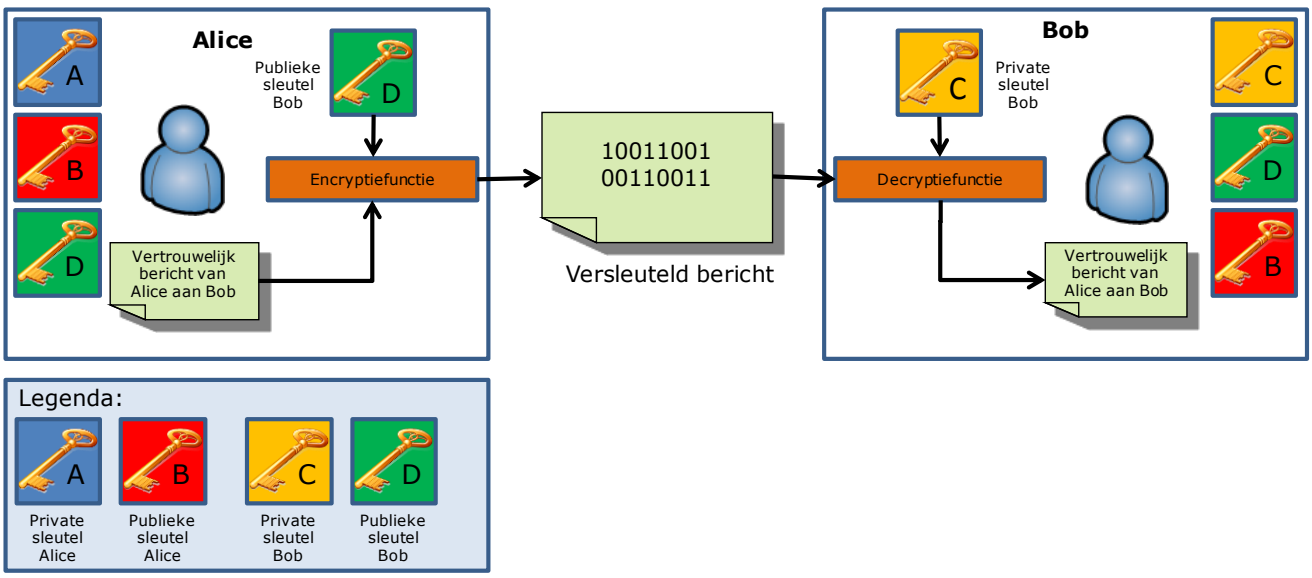
## 2.1 Introductie

Encryptie (versleuteling) is een manier om gegevens te beveiligen door ze onleesbaar te maken voor onbevoegden. Dit is van belang als informatie niet voor iedereen bestemd is. Encryptie biedt bijvoorbeeld bescherming tegen afluisteren (sniffing) of een man-in-the-middle aanval. Encryptie van berichten wordt ook gebruikt om te controleren of een bericht inderdaad van een bepaalde afzender afkomstig is.

## 2.2 Hoe werkt encryptie?

Om versleutelde berichten tussen afzender en ontvanger uit te wisselen en te lezen moeten beide partijen in het bezit zijn van een sleutelpaar. Een sleutelpaar bestaat uit een private (geheime) sleutel en een publieke (openbare) sleutel. Een bericht wordt onleesbaar gemaakt met de publieke sleutel van de ontvanger. Die kan het bericht vervolgens met zijn private sleutel weer ontsleutelen. De private sleutel moet de eigenaar goed beveiligen en is ook alleen bekend bij de eigenaar. De publieke sleutel mag in principe aan iedereen worden uitgedeeld.

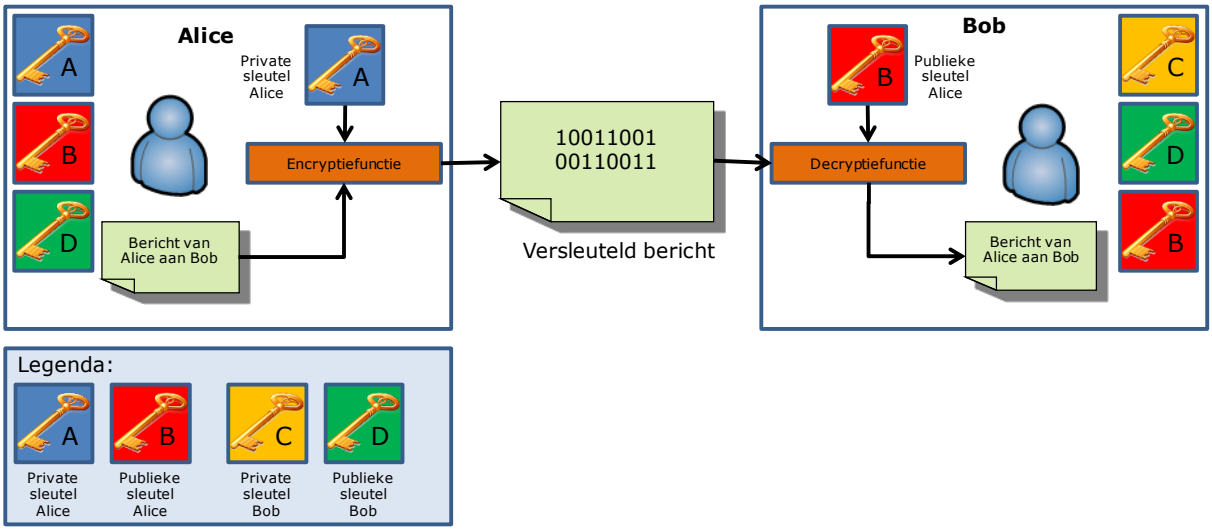
Figuur 1 licht dit toe. Alice wil een bericht naar Bob versturen en wil er zeker van zijn dat Bob de enige is die dit bericht kan lezen. Alice en Bob hebben hiervoor ieder een sleutelpaar nodig. Het sleutelpaar van Alice bestaat uit private sleutel A en publieke sleutel B. Het sleutelpaar van Bob bestaat uit private sleutel C en publieke sleutel D. Alice maakt haar publieke sleutel bekend aan Bob en vice versa.




**Figuur 1. Versleutelen van berichten**

Alice kan het bericht nu versleutelen met de publieke sleutel van Bob en het versleutelde bericht veilig naar hem versturen. Bob is de enige die dit versleutelde bericht kan ontsleutelen, aangezien alleen hij beschikt over de bijbehorende private sleutel.

Versleuteling kan ook gebruikt worden om te garanderen dat een bericht afkomstig is van een bepaalde afzender. In dat geval versleutelt de afzender een bericht met zijn private sleutel. Als de ontvanger er vervolgens weer een leesbaar bericht van kan maken door het te ontsleutelen met jouw publieke sleutel, dan is dat het bewijs dat het bericht van jou afkomstig is. Want elk sleutelpaar is uniek en alleen de afzender kent zijn private sleutel. Deze methode wordt in figuur 2 toegelicht. Alice versleutelt het bericht met haar private sleutel en verstuurt die naar Bob. Alleen de publieke sleutel van Alice maakt er weer een leesbaar bericht van, andere sleutels werken niet. Bob weet daarom na ontsleuteling zeker dat het bericht afkomstig is van Alice.




**Figuur 2. Garanderen dat een bericht afkomstig is van een bepaalde afzender**

Encryptie kan ook worden gebruikt om gegevens op een laptop, externe harde schijf, USB-stick of andere mobiele opslagmedia onleesbaar te maken. Bij verlies of diefstal kan niemand de versleutelde gegevens lezen.

*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. Een digitaal certificaat kan worden vergeleken met een paspoort of een rijbewijs. Ze worden gebruikt als officiële legitimatie, om aan te tonen dat je bent wie je zegt dat je bent.

Daarmee kan de 'echtheid' van een persoon en zijn publieke sleutel worden aangetoond. Het advies is om altijd de echtheid van de publieke sleutel te controleren, ook als de afzender een bekende is.

*Welke beveiliging toepassen?*

Hieronder wordt aangegeven welk beveiligingsaspect wordt ondersteund door welke cryptografische techniek:

| | |
|---|---|
| **Integriteit** | encryptie (hashing) |
| **Vertrouwelijkheid** | encryptie |
| **Onweerlegbaarheid** | digitale handtekening |
| **Authenticatie** | digitale handtekening |

*Veilig communiceren*

Organisaties stellen steeds meer diensten en informatie beschikbaar via internet. Zo is het voor overheidsorganisaties van belang dat burger zeker weten dat de website waarop zij gegevens invullen daadwerkelijk van een overheidsorganisatie is en of de communicatie met een overheidswebsite voldoende beveiligd is? Voor internet zijn hiervoor zogenoemde SSL-certificaten de oplossing. Een certificaat voegt een uniek zegel toe aan een website. Dit zegel is op websites beschikbaar voor controle van de echtheid en beveiliging van website. Er bestaan speciale SSL-certificaten van de Staat der Nederlanden voor overheidsorganisaties (PKIoverheid-certificaten; Public Key Infrastructure voor de overheid).

*PKIoverheid-certificaat*

PKIoverheid-certificaten bieden aanvullende zekerheden voor de echtheid en de beveiliging van website.[3] Een digitaal certificaat van PKIoverheid waarborgt op basis van Nederlandse wetgeving de betrouwbaarheid van informatie-uitwisseling via e-mail, websites of andere gegevensuitwisseling.

PKIoverheid-certificaten worden gebruikt bij het:

- zetten van een rechtsgeldige elektronische handtekening.
- beveiligen van websites.
- authenticeren op afstand van personen of services.
- versleutelen van berichten.

[3] http://www.logius.nl/producten/toegang/pkioverheid/

## 2.3 Encryptiebeleid

Overheidsorganisaties dienen beleid, richtlijnen en procedures voor encryptie en PKI te ontwikkelen en implementeren teneinde er zeker van te zijn dat de encryptie die zekerheid biedt die ervan wordt verwacht. Hierin dienen ten minste de volgende onderwerpen aan bod te komen:

1. Er wordt een beleid met gedragsregels en een geschikte implementatie van de techniek opgesteld ten aanzien van encryptie en PKI.
2. Versleuteling vindt plaats conform 'best practices' (de stand der techniek), waarbij geldt dat de vereiste encryptie sterker is naarmate gegevens gevoeliger zijn. Overheidsorganisaties gebruiken encryptie conform de PKIoverheid standaard.
3. Digitale documenten van de overheid waar burgers en bedrijven rechten aan kunnen ontlenen, maken gebruik van de PKIoverheid-certificaten voor ondertekening en/of encryptie.
4. De beveiliging van informatie, zowel gedurende transport als opslag, en het interne dataverkeer ('machine to machine') wordt conform beveiligingseisen in de informatiebeveiligingsarchitectuur en -classificatie beveiligd.
5. Er worden beheerprocedures opgesteld met betrekking tot het (centrale) beheer van sleutelmateriaal en beveiligingscertificaten.

De organisatie dient duidelijk te hebben van welke gegevens de beschikbaarheid, vertrouwelijkheid en integriteit gegarandeerd dienen te worden. Tevens dient duidelijk te zijn hoe dit wordt gegarandeerd. Denk hierbij aan de volgende maatregelen:

- Er is een overzicht van gegevens waarin is aangegeven op welke wijze deze versleuteld dienen te worden. Dit betreft de gegevenseigenaar, de te volgen procedure en de beschikbare hulpmiddelen om de versleuteling uit te voeren.
- Er zijn procedures voor gebruikers, voor het versleutelen van gegevens.
- Er is een procedure beschikbaar waarin sleutelvernieuwing en sleutelarchivering wordt beschreven.

## 2.4 Definiëren van het toepassingsgebied

De BIR beschrijft maatregelen die nodig zijn voor het basis vertrouwelijkheidsniveau 'vertrouwelijk'[4] en 'persoonsvertrouwelijke informatie', zoals bedoeld in artikel 16 van de Wet bescherming persoonsgegevens (Wbp). De overheidsorganisatie dient daartoe een basis aan cryptografische maatregelen te implementeren, waarbij gedacht kan worden aan transportbeveiliging buiten en binnen het interne netwerk.

[4] Departementaal Vertrouwelijk volgens het Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013). http://wetten.overheid.nl/BWBR0033507/

Als de organisatie informatie verwerkt met een hoger vertrouwelijkheidsniveau dan ‘vertrouwelijk’, zullen mogelijk aanvullende maatregelen geïmplementeerd moeten worden. Deze aanvullende maatregelen dienen gebaseerd te zijn op de resultaten van een risicoanalyse die de organisatie heeft (laten) uitvoeren. Uit deze risicoanalyse zal naar voren komen welke beveiligingsaspecten van belang zijn.

## 2.5 Sleutelbeheer

Organisaties die encryptie toepassen dienen sleutelbeheer[5] in te richten voor de beheersing van de operationele- en beheerprocessen ten aanzien van encryptie. Sleutelbeheer betreft alle aan sleutelmateriaal gerelateerde activiteiten vanaf het genereren tot en met de vernietiging van sleutels. Een goede uitvoering van het sleutelbeheer is van belang doordat de versleuteling van gegevens net zo sterk is als de mate van geheimhouding van de sleutel. Ook geldt dat versleutelde gegevens net zo lang toegankelijk zijn als de beschikbaarheid van de bijbehorende sleutel.

Op het moment dat gebruik wordt gemaakt van encryptie, zal er naast de technische beveiligingsmaatregelen ook aandacht dienen te worden besteed aan de organisatorische en procedurele beveiligingsmaatregelen. Als organisatie zullen procedures op moeten worden gesteld, waarin onder andere de volgende onderwerpen moeten staan beschreven:

- Hoe moet het aanvragen van een sleutelpaar verlopen?
- Wie mag sleutels genereren?
- Op welke manier worden de sleutelparen overgedragen aan de eigenaar?
- Moet tijdens de overdracht van het sleutelpaar de eigenaar zich legitimeren?
- Hoe lang zijn de sleutels geldig?
- Wie kan sleutels intrekken?
- Hoe worden sleutels geüpdate?

Onder sleutelbeheer worden de volgende activiteiten verstaan:

*Bepalen levensduur van de sleutels*

Sleutelparen hebben een levensduur of geldigheidsduur. Dit houdt in dat een sleutel na het verstrijken van deze periode niet meer kan worden gebruikt om berichten te versleutelen. Met deze sleutel blijft het wel mogelijk om al versleutelde data te ontsleutelen. De organisatie dient:

- van alle sleutelparen bij te houden, wanneer sleutelparen zijn uitgegeven en wanneer deze weer verlopen. Dit is onder andere nodig om te kunnen bepalen wanneer een nieuw sleutelpaar moet worden gegenereerd.

[5] De Nederlandse Overheids Referentie Architectuur (NORA) heeft dit uitgewerkt in het beveiligingspatroon sleutelhuis (http://noraonline.nl/wiki/Patroon_voor_sleutelhuis).

- alle verlopen sleutelparen te bewaren om te kunnen garanderen dat alle data die ooit is versleuteld met deze nu ongeldige sleutel ook weer ontcijferd kan worden.
- een procedure op te stellen over hoe gebruikers op de hoogte worden gebracht van het feit dat er een nieuw sleutelpaar is gegenereerd.

*Genereren (en registreren) van sleutels*

De Wet Elektronische Handtekening (WEH)[6] stelt eisen aan de manier waarop sleutels worden gegenereerd. De organisatie dient:

- alle relevante informatie, zoals de cryptografische eigenschappen, 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. Een CISO kan hierin een centrale rol spelen. De verantwoordelijke:
  - verzamelt en verifieert de identiteitsgegevens van de aanvrager en autoriseert de aanvraag.
  - fungeert voor certificaataanvragen als interne Registration Authority (RA). Denk hierbij aan de volgende activiteiten: identificatie, authenticatie en autorisatie van de aanvraag, het bepalen en aanvullen van de juiste inhoud en het optreden als tussenpersoon naar de interne of externe Certificate Authority (CA).
  - per toepassing in een sleutelplan vast te leggen wanneer en hoe sleutels vervangen dienen te worden.
- vast te leggen waar beveiligingsincidenten gemeld moeten worden, wie een sleutel mag intrekken, hoe dat gecommuniceerd dient te worden, welke stappen verder moeten worden genomen en welke ingetrokken sleutels op een ‘revocation list’ komen.
- cryptografische sleutels veilig te bewaren.
- vast te stellen of, en zo ja, van welke sleutels een back-up gemaakt mag worden. Reden voor een back-up is het nog kunnen ontcijferen van informatie na verlies van de originele sleutel. Reden voor het juist niet toestaan van een back-up, kunnen de eisen zijn die de Wet Elektronische Handtekening (WEH) stelt aan authenticiteit en onweerlegbaarheid.

*Distribueren van de sleutels*

Het distribueren van de sleutels dient op een veilige en gecontroleerde wijze te gebeuren. Distributie kan fysiek of elektronisch verlopen, afhankelijk van de toepassing. De organisatie dient:

- alle in omloop zijnde sleutels, inclusief wie de ontvanger is, op basis van een unieke identiteit vast te leggen in een geautomatiseerd registratiesysteem. Hierdoor is bij compromittering direct bekend welke partijen het betreft.

[6] http://wetten.overheid.nl/BWBR0015046/

- Vast te leggen hoe certificaten en bijbehorende toegangscodes worden uitgegeven. Denk hierbij aan fysieke of elektronische distributie, op smartcard of als bestand, en distributie van certificaten en bijbehorende toegangscode op verschillende momenten en langs verschillende wegen.

*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. Een andere reden kan zijn dat een sleutelpaar met een vermelde geldigheidsduur verlopen is. De organisatie dient:

- de frequentie waarmee sleutelparen worden vervangen te bepalen. Deze frequentie hangt af van het toepassingsgebied. Sleutelparen die gebruikt worden voor de versleuteling van gegevens, zullen een kortere levensduur hebben dan sleutelparen die gebruikt worden voor het maken van een digitale handtekening.

*Herstellen van de sleutels*

Een van de problemen van encryptie is 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 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 ondertekende documenten van een overheidsorganisatie waar burgers en bedrijven rechten aan kunnen ontlenen. De organisatie dient:

- vast te leggen in welke specifieke gevallen het herstellen van sleutels toegepast mag worden, voor welk type sleutels, welke methode/oplossing wordt geïmplementeerd, wie een aanvraag mag indienen en wie de herstelprocedure mag uitvoeren.

*Intrekken van de sleutels*

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

- vast te leggen in welke specifieke gevallen het intrekken van sleutels wordt toegepast, wie een aanvraag mag indienen, wie de procedure mag uitvoeren en via welke methode het overzicht van ingetrokken sleutels wordt gepubliceerd (Certificate Revocation List (CRL) en/of Online Certificate Status Protocol (OCSP)).

*Archiveren van de sleutels*

Onder het archiveren van sleutels wordt het maken van een back-up van een sleutel verstaan. Na de operationele fase is het van belang dat back-ups van sleutels gearchiveerd blijven, zolang gegevens met die sleutel geraadpleegd behoren te kunnen worden.

Versleutelde gegevens dienen leesbaar te zijn gedurende een door het bedrijfsproces vereiste periode. De organisatie dient hiertoe:

- vast te leggen in welke specifieke gevallen het archiveren van sleutels wordt toegepast, wie een aanvraag tot restore mag indienen en wie de procedure mag uitvoeren. Hierbij dient rekening gehouden te worden met wet- en regelgeving. Bijvoorbeeld de Wet op de inlichtingen- en veiligheidsdiensten (WIV) [7] en de Wet openbaarheid van bestuur (WOB)[8].
- vast te leggen hoe op verzoek versleutelde gegevens op een gecontroleerde wijze kan worden gepubliceerd.
- versleutelde gegevens volgens dezelfde beheerprocedures (zoals back-up procedures) te behandelen als 'normale' gegevens.
- bij gearchiveerde versleutelde gegevens ook de sleutels en algoritmen te archiveren, om de beschikbaarheid van de gegevens te waarborgen.
- de mate van beveiliging van de versleutelde gegevens te waarborgen gedurende de vereiste beschikbaarheidstermijn. Bijvoorbeeld door een versleuteld archief opnieuw te versleutelen, indien een nieuw algoritme en/of nieuwe sleutellengte wordt gekozen voor versleuteling van gegevens.

*Vernietigen van de sleutels*

Niet meer toegepaste sleutels dienen op een veilige wijze vernietigd te worden. De organisatie dient:

- van alle in omloop zijnde sleutels vast te leggen in een geautomatiseerd registratiesysteem wie, waar en welke sleutels in gebruik heeft, inclusief de sleutels in back-ups en het archief.
- vast te leggen welk type sleutel wanneer mag worden vernietigd. Hierbij dient rekening gehouden te worden met wet- en regelgeving, zoals juridische bewaartermijnen.

## 2.6 Verschillend beheer voor encryptie of digitale handtekening

De organisatie dient vast te stellen of er verschillende eisen zijn voor bijvoorbeeld de geldigheidsduur van de sleutel voor encryptie (vertrouwelijkheid) of een digitale handtekening (authenticatie en onweerlegbaarheid). Om aan deze verschillende eisen te kunnen voldoen kan gebruik gemaakt worden van twee sleutelparen in plaats van één.

Het gebruik maken van twee sleutelparen heeft een aantal voordelen. Een eerste reden om gebruik te maken van twee sleutelparen is om ondersteuning verlenen aan 'key recovery' (back-up). Het maken van een kopie (back-up) van de private-sleutel kan noodzakelijk zijn op het moment dat het gaat om de vertrouwelijkheid (encryptie) van de gegevens, zoals in

[7] http://wetten.overheid.nl/BWBR0013409/
[8] Zie hiervoor http://www.vng.nl/onderwerpenindex/recht/wet-openbaarheid-van-bestuur

het geval dat e-mailberichten of data op een harde schijf is versleuteld met behulp van de publieke sleutel van de gebruiker. Bij verlies van de private–sleutel is het zonder deze kopie van de private-sleutel onmogelijk om deze data weer leesbaar te maken. Verlies of diefstal van de private-sleutel ondermijnt de vertrouwelijkheid van het dataverkeer en kan uiteindelijk de continuïteit van de organisatie in gevaar brengen.
Een tweede reden om gebruik te maken van twee sleutelparen is de ondersteuning van verschillende algoritmen voor encryptie en digitale handtekeningen, waaronder bijvoorbeeld het DSA (Digital Signature Algorithm)-algoritme. Dit algoritme ondersteunt geen versleuteling en om dit te realiseren is dan ook een ander algoritme, en dus ook een ander sleutelpaar, noodzakelijk.

## 2.7 Beoordelen van kwaliteit sleutelbeheer

Als het sleutelbeheer is uitbesteed, dient het sleutelbeheer bij de externe dienstverlener te worden beoordeeld. De onderstaande vragenlijst kan worden gebruikt om het sleutelbeheer te beoordelen. Deze vragenlijst is zeker niet volledig, maar geeft voldoende handvatten om een eerste inschatting van de status met betrekking tot sleutelbeheer te maken.

- Heeft de organisatie beleid vastgesteld voor het gebruik van cryptografie?
- Is bekend van welke gegevens, die op elektronische wijze worden verzonden, de integriteit vast moet staan? Als dat het geval is, wordt voor de verzending van berichten gebruik gemaakt van cryptografische technieken, zodat de authenticiteit ervan kan worden vastgesteld?
- Wordt encryptie toegepast ter bescherming van vertrouwelijke informatie?
- Is het voor bepaalde processen nodig om onomstotelijk vast te kunnen stellen dat een bericht door de verzender is verzonden en door de ontvanger is ontvangen?
- Vereist de bescherming van de authenticiteit en de integriteit van elektronische documenten het gebruik van digitale handtekeningen?
- Is het nodig om de identiteit vast te kunnen stellen van diegene die het elektronisch document heeft ondertekend, en om vast te stellen of de inhoud van het ondertekende document is veranderd?
- Is de integriteit van de publieke sleutel voldoende beschermd door middel van een certificaat?
- Is het gebruikte type algoritme voor de digitale handtekening voldoende sterk, en is de sleutellengte voldoende sterk voor de duur van de archivering van de digitale handtekening?
- Worden voor de digitale handtekening andere sleutels gebruikt dan die voor de encryptie?
- Is het sleutelbeheer georganiseerd voor de volgende algemene cryptografische technieken:
  - Symmetrisch algoritme met een paar geheime sleutels?
  - Asymmetrisch algoritme met een private sleutel en een publieke sleutel?
- Zijn de private sleutels beschermd tegen ongeautoriseerde inzage?
- Zijn alle sleutels beschermd tegen wijziging of vernietiging?

- Is de apparatuur waarmee sleutels worden aangemaakt, verwerkt, tijdelijk opgeslagen of gearchiveerd, of fysiek beveiligd tegen ongeautoriseerde inzage?
- Is die apparatuur geplaatst in een extra beveiligde ruimte?
- Wordt er bij de selectie van die apparatuur als voorwaarde gesteld dat deze moet voldoen aan internationale of nationale normen?
- Is de toegepaste apparatuur gecertificeerd door onafhankelijke en deskundige instituten?
- Past de apparatuur in de ICT-architectuur (netwerk en de computersystemen)?
- Is voor het sleutelbeheer gebruik gemaakt van gestandaardiseerde procedures en werkwijzen voor de:
  - aanmaak van sleutels voor verschillende cryptografische systemen en toepassingssystemen?
  - aanmaak en ontvangst van certificaten op basis van de publieke sleutel?
  - sleuteldistributie naar gebruikers, met beschrijving hoe de sleutels na ontvangst kunnen worden geactiveerd?
  - opslag van sleutels, met beschrijving hoe geautoriseerde gebruikers toegang kunnen krijgen tot hun sleutels?
  - verandering of vernieuwing van sleutels met richtlijnen, voor wanneer en hoe sleutels moeten worden gewijzigd?
  - omgang met gecompromitteerde sleutels?
  - inname van sleutels, met een beschrijving hoe sleutels moeten worden ingetrokken of onbruikbaar moeten worden gemaakt?
  - de sleutels die verloren zijn gegaan of zijn beschadigd?
  - archivering van sleutels?
  - vernietiging van sleutels?
  - controle van activiteiten op het gebied van sleutelbeheer?
- Is het sleutelbeheer beschreven in handboeken en procedurebeschrijvingen?
- Zijn de taken op het gebied van sleutelbeheer expliciet toegewezen aan functionarissen met voldoende kennis en ervaring?
- Houdt de organisatie regelmatig tests op het gebied van sleutelbeheer, om kennis en ervaring op peil te houden?
- Worden sleutels ingenomen bij vertrek van een medewerker?
- Hebben de sleutels een vastgestelde levensduur met een duidelijke begin- en eindtijd?
- Wordt die levensduur vastgesteld aan de hand van de kans op schade, de sterkte van het algoritme en de omstandigheden waaronder de sleutels worden gebruikt?
- Is de back-up en de opslag van sleutelgegevens duidelijk geregeld?
- Is er een inventarisatie aanwezig van welke overeenkomsten, wetten, voorschriften of andere instrumenten van kracht zijn met betrekking tot de toegang of het gebruik van cryptografie?
- Is juridisch advies ingewonnen om te bepalen welke wetgeving van toepassing is?
- Wordt de vertrouwelijkheid van gegevens in acht genomen, indien nationaal bevoegde instanties toegang tot versleutelde informatie eisen?
- Zijn er procedures opgesteld voor het geval dat versleutelde informatie toegankelijk moet worden gemaakt, om te dienen als bewijsmateriaal bij een juridische procedure?

- Wordt er een kopie van de cryptografische sleutels opgeslagen op een andere, eveneens fysiek goed beveiligde, locatie?
- Gebeurt het aanmaken van certificaten op een betrouwbare manier, en door een betrouwbare certificerende instelling?
- Bevat de dienstverleningsovereenkomst met leveranciers van cryptografische diensten, passages over aansprakelijkheid, betrouwbaarheid van de dienstverlening en maximaal toelaatbare duur van uitval?

## 2.8 PKIoverheid

Op het moment dat een organisatie gebruik gaat maken van PKIoverheid certificaten, dient de organisatie zorg te dragen dat[9]:

- geen enkele andere persoon, dan de certificaathouder, toegang zal hebben tot de private sleutel die is gekoppeld aan de publieke sleutel in het PKIoverheid certificaat.
- de toegangscodes van smartcards en/of USB-tokens[10],waarin de private sleutel is opgeslagen, steeds veilig en gescheiden van de smartcards en/of USB-tokens bewaard zullen worden.
- het PKIoverheid certificaat enkel zal worden gebruikt voor de doelen waartoe deze is uitgereikt.
- direct na ontvangst van het certificaat, maar in ieder geval alvorens over te gaan tot installatie en gebruik, het digitale certificaat op haar volledige en juiste inhoud zal worden gecontroleerd.
- direct tot intrekking van het PKIoverheid certificaat zal worden overgaan en elk gebruik daarvan direct zal worden gestaakt, wanneer:
  - er onvolledigheden en/of onjuistheden in het PKIoverheid certificaat worden geconstateerd dan wel deze door gewijzigde omstandigheden dreigen te ontstaan of zijn ontstaan
  - de private sleutel verloren, gestolen of anderszins gecompromitteerd is geraakt
  - smartcards en/of USB-tokens of de toegangscodes van smartcards en/of USB-tokens in onbevoegde handen zijn gekomen, of kunnen zijn gekomen.
- smartcards en/of USB-tokens waarop private sleutels worden bewaard, zullen worden beveiligd conform de wijze waarop gevoelige gegevens en/of bedrijfskritische middelen zijn beveiligd.[11]
- sleutelmateriaal van certificaathouders zal worden gegenereerd in een veilig middel dat is gecertificeerd tegen de Common Criteria op niveau EAL4+[12] of aan gelijkwaardige

[9] Zie hiervoor ook het Programma van Eisen deel 3a van PKIoverheid (https://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/pve/PvE_deel3a_v3.6.pdf) en de documentatie (meestal bijzondere voorwaarden) van de toegetreden certificatiedienstverleners tot PKIoverheid (http://www.logius.nl/producten/toegang/pkioverheid/aansluiten/toegetreden-csps/).
[10] Binnen PKIoverheid ook vaak aangeduid als Secure Signature Creation Device (SSCD) en/of Secure User Device (SUD).
[11] Zie hiervoor ook het operationele product 'Dataclassificatie' bij de Baseline Informatiebeveiliging Rijksdienst (BIR).

beveiligingscriteria, dan wel op een softwarematige wijze in een omgeving die aldus is ingericht dat ongeoorloofde toegang tot en/of gebruik van de sleutels wordt uitgesloten.

[12] De Evaluation Assurance Levels (EAL1 tot EAL7) van Common Criteria, een internationale standaard (ISO/IEC 15408) sinds 1999. Common Criteria evalueert ICT-producten of -systemen (https://www.commoncriteriaportal.org/ en http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=50341).

## Bijlage 1: Gebruiksvoorwaarden voor versleuteling van gegevens <organisatie>

De volgende gebruiksvoorwaarden en gedragsregels kunnen als voorbeeld dienen voor de omgang met versleuteling van gegevens. Tevens is aangegeven welke maatregelen een organisatie moet nemen om dit te realiseren.

1. De medewerker dient zorgvuldig om te gaan met het versleutelen van gegevens.
   Hiervoor dient een organisatie zorg te dragen dat:
   - de medewerker beschikt over de benodigde hulpmiddelen en tools voor het versleutelen van gegevens.
   - de medewerker beschikt over de benodigde procedures voor het versleutelen van gegevens.
   - de medewerker kennis heeft van de procedures voor het versleutelen van gegevens.

2. De medewerker dient zorgvuldig om te gaan met de te gebruiken applicaties voor versleuteling van gegevens.
   Hiervoor dient een organisatie zorg te dragen dat:
   - de medewerker opleidingen volgt voor het gebruik van de versleutelapplicaties.
   - de medewerker over duidelijke handleidingen beschikt van de versleutelapplicaties.

3. De medewerker dient bekend te zijn met, en bewust te zijn van, de betekenis van het gebruik van cryptografie.
   Hiervoor dient een organisatie zorg te dragen dat:
   - er bij de introductie van nieuwe medewerkers voldoende aandacht wordt besteed aan de betekenis en het gebruik van cryptografie, inclusief de potentiële risico's van cryptografie die uiteindelijk een nadelig effect kunnen hebben op de effectiviteit ervan.
   - regelmatig in voorlichtingen en opleidingen wordt ingegaan op het gebruik, en de risico's van, de cryptografische toepassingen.
   - de directie het belang van encryptie onderkent en ondersteunt, en dit ook uitdraagt.
   - de medewerker aan een bewustwordingsprogramma deelneemt.

4. De medewerker dient zorgvuldig om te gaan met zijn private sleutel zodat compromittering wordt voorkomen.
   Hiervoor dient een organisatie zorg te dragen dat:
   - De medewerker wordt aangesproken op onzorgvuldige behandeling van zijn private sleutel. Bijvoorbeeld als de medewerker zijn of haar smartcard met de private sleutel onbeheerd achter laat op zijn of haar werkplek.

5. De medewerker dient snel en adequaat te reageren op een situatie waarbij zijn of haar private sleutel is gecompromitteerd.
   Hiervoor dient een organisatie zorg te dragen dat:
   - De medewerker over procedures beschikt waarin de vereiste handelwijze is beschreven bij compromittering van zijn of haar private sleutel.

6. De medewerker is op de hoogte en heeft kennis van de regels.
   Hiervoor dient een organisatie zorg te dragen dat:
   - de risico's met betrekking tot encryptie aandacht dienen te krijgen in bewustwordings- en trainingsmateriaal.

## Bijlage 2: Encryptie aanwijzing voor <organisatie>

### Uitgangspunten encryptie

Ten behoeve van encryptie zijn er regels om te voorkomen dat de dienstverlening van <organisatie> hinder ondervindt van de risico's, in geval van gedeeltelijk of geheel verlies, of beschadiging van data en/of programmatuur en hardware.

Er dient ook nagedacht te worden over welke diensten door <organisatie> zelf moeten worden ingevuld en welke diensten moeten worden uitbesteed.

De volgende onderwerpen dienen terug te komen in (aanvullend) beleid betreffende encryptie:

1. Het opstellen van gebruiksvoorwaarden voor versleuteling van gegevens. In deze gebruiksvoorwaarden staan aanwijzingen over hoe omgegaan dient te worden met de private sleutel, het versleutelen van gegevens, de applicaties voor versleuteling van gegevens en hoe adequaat gereageerd dient te worden op incidenten.

2. Het opstellen van regels voor acceptabel gebruik. Deze regels dienen door de medewerker geaccepteerd en getekend te worden. Binnen de regels voor acceptabel gebruik is aandacht voor:
   - het proces in geval van verlies, diefstal of compromittering van de private sleutel, waarbij meldingen binnen 4 uur gedaan moeten worden.
   - niet voldoen aan beleid en regels kan resulteren in een disciplinair proces.
   - het voldoen aan ICT-standaarden en nadere afspraken.

3. Toestemming en verantwoording betreffende het versleutelen van informatie:
   - de organisatie dient ook aandacht te hebben voor de impliciete toestemming aan gebruikers, welke informatie zij wel of niet mogen inzien tijdens het telewerken.
   - er dient duidelijk te worden gemaakt dat de medewerker achteraf ter verantwoording geroepen kan worden.

4. Algemene maatregelen om te zorgen voor bescherming van gegevens:
   - de organisatie hanteert classificatieregels voor gegevens en zorgt voor passende maatregelen om deze gegevens te beschermen.
   - bedrijfsapplicaties worden bij voorkeur zo aangeboden dat er geen informatie van de organisatie wordt opgeslagen op het device ('zero footprint'). Informatie en bedrijfsinformatie van derde partijen, waar de organisatie niet de bronhouder is maar welke bijvoorbeeld via een platform wordt ontsloten, dienen te worden versleuteld bij transport en opslag, conform de classificatie-eisen. Voorzieningen als webmail, alsook sociale netwerken en clouddiensten (Dropbox, Gmail, et cetera), zijn door het

lage beschermingsniveau (veelal alleen naam en wachtwoord, en het ontbreken van versleuteling) niet geschikt voor het delen van vertrouwelijke en geheime informatie.

- toegang tot vertrouwelijke informatie wordt verleend op basis van multifactor authenticatie.
- versleuteling vindt plaats conform ‘best practices’ (de stand der techniek), waarbij geldt dat de vereiste encryptie sterker is naarmate gegevens gevoeliger zijn.
- digitale documenten van de overheidsorganisatie waar burgers en bedrijven rechten aan kunnen ontlenen, maken gebruik van PKIoverheid certificaten voor ondertekening en/of encryptie. Hiervoor wordt een richtlijn PKI en certificaten opgesteld.
- de organisatie maakt gebruikt van encryptie conform PKIoverheid.

## Bijlage 3: Literatuurlijst

Voor dit document is gebruik gemaakt van onderstaande literatuur:

**Titel: Beveiligingspatronen van de Nederlandse Overheids Referentie Architectuur**
Wie: Nederlandse Overheids Referentie Architectuur
Datum: geraadpleegd in februari 2014
Link: http://noraonline.nl/wiki/Beveiligingspatronen

**Titel: Programma van Eisen (PvE) van PKIoverheid**
Wie: Logius (onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties)
Datum: 28 januari 2014 (versie 3.6)
Link: http://www.logius.nl/producten/toegang/pkioverheid/aansluiten/programma-van-eisen/

**Titel: Encryptie: het versleutelen van informatie en veilig communiceren met de overheid**
Wie: Waarschuwingsdienst.nl (een dienst van het Nationaal Cyber Security Centrum).
Datum: 16 november 2012
Link:
https://www.waarschuwingsdienst.nl/Computer+beveiligen/Besturingssysteem/Encryptie.html
en
https://www.waarschuwingsdienst.nl/Veilig+internetten/Websites+bezoeken/Veilig+communiceren+met+de+overheid.html

**Titel: Technische beveiligingsstudie Encryptie**
Wie: Platform Informatiebeveiliging (opgegaan in Platform voor Informatiebeveiliging (PvIB))
Uitgeverij: LEMMA BV
Datum: september 2002
ISBN-10: 90-5931-113-2 (niet meer leverbaar)
Link: http://pvib.nl/links&collectionId=6391811