Federal Information Security Policy Guideline

Handleiding voor cryptografie

21/11/2019

FISPDOC03 V1.1

Belangrijke opmerking: Dit document is een leidraad die het resultaat is van een samenwerking tussen informatiebeveiligingsexperts van de verschillende federale diensten (FOD, OIP, IPSS). De voorgestelde maatregelen worden beschouwd als minimummaatregelen die redelijkerwijs op een gemeenschappelijke manier van toepassing zijn op alle federale diensten. Deze zijn gebaseerd op internationale normen, goede praktijken op het gebied van informatiebeveiliging en de ervaringen van de deelnemers aan de FISP-werkgroep.

Indien strengere maatregelen vereist zijn voor een federale dienst omwille van reglementaire redenen of om andere formele en dwingende redenen, kan men ervan uitgegaan dat deze maatregelen voorrang hebben op de maatregelen die in deze gids worden beschreven.

Werkgroep

.be

Inhoudstafel

Inhoud van dit document

Oriëntatie van het document

Dit document maakt integraal deel uit van methodologie voor informatiebeveiliging binnen de Federale overheid (FISP-project).

Iedere federale organisatie dient te beschikken over een beleid en processen inzake het gebruik van cryptografische beheersmaatregelen. Dit beleid is te zien als middel om het organisatie-brede beveiligingsbeleid om te zetten in termen die geschikt zijn voor de cryptografische diensten die worden gebruikt bij de uitvoering van het gehele of een deel van het beveiligingsbeleid.

Veiligheidsdoel van het document

Dit beleid is geschreven om informatiebeveiligingsmaatregelen met betrekking tot cryptografie aan te reiken, zodat invulling gegeven kan worden aan het beveiligingsbeleid.

Toepassingsgebied

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

Vertrouwelijkheid van het document

Publieke verspreiding

Vrijwaring

Dit is een beleid op basis van de internationale praktijken m.b.t. cryptografische maatregelen. Indien u deze richtlijn voor uw organisatie wilt toepassen, moet u eerst een beoordeling maken en controleren of andere wettelijke beperkingen, regels of praktijken van toepassing zijn op uw organisatie. Pas het beveiligingsbeleid aan, in lijn met uw organisatie!

Tijdens de Ministerraad van 3 mei 2019 werd een voorontwerp van wet voorgelegd, namelijk de herziening van de wet van 11/12/1198. Indien deze wet wordt aangenomen, zal het FISP beleid worden geüpdatet aangezien het huidige beleid geen rekening houdt met toekomstige wettelijke ontwikkelingen.

Verantwoordelijkheden

Dit document is bestemd voor de informatieveiligheidsconsulent (CISO) en voor de functionaris voor de gegevensbescherming (DPO) van de openbare instelling van federale overheid, voor de verwerkers van informatie (ook de onderaannemers van informatiesystemen), de veiligheidsofficier en andere belanghebbenden in verwante gebieden (bv. de documentenbeheerder).

Eigenaar

De eigenaar van dit document is de FISP-werkgroep.

Inleiding

Dit beleid biedt informatiebeveiligingsmaatregelen aan met betrekking tot cryptografie voor de federale organisaties (o.a. encryptie en Key management).

Dit document bevat voldoende informatie om goede (beleid)keuzes te maken en bewustwording te creëren. De voorgestelde maatregelen zijn gekoppeld aan de voorgestelde informatie classificatie van het globale informatiebeveiligingsbeleid (FISP) en met de verschillende data contexten.

Er wordt bovendien advies gegeven in de maatregelen die men moet nemen voor de versleuteling. Daarnaast worden er ook aanwijzingen gegeven over de beheersing van zowel de operationele- als de beheerprocessen, die bij het toepassen van encryptie van belang zijn.

Het is echter geen volledige procesbeschrijving voor encryptie en bevat ook geen productbeschrijving. Dit document is niet geschreven om cryptografie en informatiebeveiligingsmaatregelen met betrekking tot cryptografie te verklaren. Een uitgebreide beschrijving betreffende het principe cryptografie en de bijhorende maatregelen kan men terug vinden in het FISP document “Cryptografie –Verklaring”.

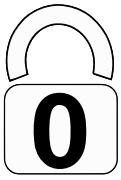
Informatieclassificatie - Cryptografie

Het nemen van een beslissing betreffende de vraag of een cryptografische oplossing geschikt is moet worden gezien als een onderdeel van het bredere proces van risicobeoordeling. Deze beoordeling kan vervolgens worden gebruikt om te bepalen welke en of een cryptografische maatregel geschikt is. Type, sterkte en kwaliteit worden in acht genomen.

Maatregelen

De voorgestelde maatregelen zijn gekoppeld aan de voorgestelde informatie classificatie van dit globale informatiebeveiligingsbeleid (FISP) en met de verschillende data contexten: data in use, data in motion, data at rest. Een voorbeeld van de verschillende toepassingen van de data contexten kan terug gevonden worden in het document “Cryptografie – verklaring”.

De voorgestelde maatregelen zijn gestapelde maatregelen. Dit impliceert dat de maatregelen van de onderliggend informatieklasse ook op de bovenliggende klassen van toepassingen blijven, met uitzondering van onverenigbare technische maatregelen. Bovendien evolueert de complexiteit en sterkte van de maatregelen mee met de stijging van de klasse.

Categorie[1]	
	Versleuteling vindt plaats conform ‘Common practices’, crypto algoritmes en protocollen. **Data in motion :** • Encryptie op transportniveau omwille van integriteitsdoeleinden (i.e. HTTPs ontsluiting van publieke websites). • Terminatie op de perimeter van het beveiligde netwerk. • Technische standaard: ○ TLS protocol: forward secrecy is noodzakelijk indien dit technisch mogelijk is. **Data in use :** • Mitigerende maatregelen na risicoanalyse. **Data at rest :** • Encryptie is niet noodzakelijk
 [2]	**Data in motion :** • Encryptie oplossingen moeten geherwaardeerd worden om niet enkel integriteitsdoeleinden te garanderen maar ook vertrouwelijkheid (i.e. vervang HTTS = one way SSL naar een two ways SSL of IPSec connectie, ….). **Data in use :** • Encryptie is niet noodzakelijk binnen de organisatie. Afscherming op niveau van organisatie d.m.v. fysieke en/of logische toegangsmaatregelen. **Data in rest :** • In een beschermde omgeving: afscherming op niveau van organisatie d.m.v. fysieke en/of logische toegangsmaatregelen. • In een onbeschermde omgeving: enkel de meest simpele encryptie is noodzakelijk (storage, werkposten, mobiele devices, back-up, ...).

[1] Cf informatie classificatie FISP
[2] Klasse 1 = Klasse 0 + extra maatregelen

	**Data in motion :** • Veilige export buiten de toepassing (application layer, database, ...): fysieke beveiliging, logische toegangsbeveiliging (incl. interapp/intralayer transport). • Veilige export buiten de organisatie: encryptie op het niveau van transport indien men gebruik maakt van een onbeschermd netwerk en terminatie op niveau van trusted infrastructuur (bv. in DMZ). • Technische standaard: ○ Transport (TLS) protocol (system-to-system): wederzijdse authenticatie (2-way TLS) ○ Transport (TLS) protocol (client-server): wederzijdse authenticatie • 2-way TLS of, • 1-way TLS + eIDAS substantiële authenticatie • Certificaten en sleutels implementatiecriteria: ○ controle op gebruik, ○ sterke codering plicht **Data in use :** • Extra maatregelen zijn hier niet noodzakelijk. **Data at rest :** • In een beschermde omgeving: afscherming op het niveau van functionele behoefte d.m.v. fysieke afscherming, logische toegangsbeveiliging. Enkel encryptie na risicoanalyse. • In een onbeschermde omgeving: encryptie voor de volledige verwerkingsketting (storage, werkposten, mobiele devices, back-up, ...).
	**Data in motion :** • Encryptie is noodzakelijke onafhankelijk van de transport context (zowel binnen als buiten de organisatie). • Technische standaard: ○ Gebruik van recentste versie TLS en forward secrecy verplicht **Data in use :** • Extra maatregelen zijn hier niet noodzakelijk. **Data at rest :** • Encryptie is noodzakelijk voor de volledige verwerkingsketting: opslag, DB of middleware, werkposten, mobiele devices, back-up, ...
 [3]	**Data in motion :** • Encryptie is verplicht en moet plaatsvinden aan de hand van een extern certificatie systeem van de nationale autoriteit (zowel berichtniveau als transportniveau). **Data in use :** • Encryptie is verplicht op het niveau van de applicatie indien dit technisch mogelijk is. **Data at rest :** • Encryptie is verplicht voor alle informatieve in rust. De organisatie dient gebruik te maken van de sterkste en meest up to date encryptie algoritme, beschikbaar op het moment van opslag.

[3] Men dient voor deze klasse ook rekening te houden met andere veiligheidseisen op basis van de wet van 11/12/1998.

Maatregelen voor versleuteling[4]

Maatregelen

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

Zorgvuldigheid tijdens de versleuteling

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.

Zorgvuldigheid tijdens het gebruik van applicaties voor versleuteling

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;
- De regels voor zorgvuldig gebruik dienen door de medewerkers geaccepteerd en getekend te worden.

Kennis van cryptografie

Hiervoor dient een organisatie zorg te dragen dat:

- men 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.

Zorgvuldig omgaan met de private sleutel

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.

Snelle en adequate reactie bij compromitatie van de private sleutel

[4] Gebaseerd op BIR - Encryptiebeleid

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.

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.

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;
- de duidelijkheid van de rollen en verantwoordelijkheden;
- er dient duidelijk te worden gemaakt dat de medewerker achteraf ter verantwoording geroepen kan worden.

Maatregelen voor sleutelbeheer[5]

Maatregelen

De maatregelen voorgesteld in dit hoofdstuk zijn minimaal voor het sleutelbeheer. Het doel is om bij te dragen aan een organisatie-breed beveiligingsbeleid. De vertrouwelijkheid, integriteit en authenticiteit van cryptografische sleutels dient te zijn gewaarborgd tijdens generatie, gebruik, transport en opslag van de sleutels. De voorgestelde minimummaatregelen zijn gekoppeld aan de volgende activiteiten:

- Het bepalen van de levensduur van de sleutels;
- Genereren en registreren van sleutelparen en certificaten;
- Intrekken ('revocation') van sleutelparen;
- Archiveren van sleutels;
- Distributie van sleutels;
- Vervangen en update van sleutels;
- Herstellen van de sleutels;
- Vernietigen van sleutels.

Levensduur van de sleutels

De organisatie kan:

- alle sleutelparen bij 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.
- alle verlopen sleutelparen 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 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 organisatie kan:

- 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 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 leggen wanneer en hoe sleutels vervangen dienen te worden.
- vast 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 bewaren.

[5] Gebaseerd op BIR - Encryptiebeleid

- vaststellen 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

De organisatie kan:

- alle in omloop zijnde sleutels, inclusief wie de ontvanger is, op basis van een unieke identiteit vast leggen in een geautomatiseerd registratiesysteem. Hierdoor is de compromitterende partij direct bekend.
- vast leggen hoe certificaten en bijbehorende toegangscodes worden uitgegeven.

Vervangen (en updaten) van de sleutels

De organisatie kan:

- de frequentie waarmee sleutelparen worden vervangen 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

De organisatie kan:

- vast 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

De organisatie kan:

- vast 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

De organisatie kan:

- vast leggen in welke specifieke gevallen het archiveren van sleutels wordt toegepast, wie een aanvraag tot restore mag indienen en wie de procedure mag uitvoeren.
- vast leggen hoe op verzoek versleutelde gegevens op een gecontroleerde wijze kan worden gepubliceerd.
- versleutelde gegevens volgens dezelfde beheerprocedures (zoals back-up procedures) behandelen als ‘normale’ gegevens.
- bij gearchiveerde versleutelde gegevens ook de sleutels en algoritmen archiveren, om de beschikbaarheid van de gegevens te waarborgen.
- de mate van beveiliging van de versleutelde gegevens waarborgen gedurende de vereiste beschikbaarheidstermijn.

Vernietigen van de sleutels

De organisatie kan:

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

Link met andere maatregelen[6]

Toepassen van cryptografie en daarbij inbegrepen een adequaat sleutelbeheer zijn essentieel voor het garanderen van vertrouwelijkheid van informatie. Ze mogen echter niet als geïsoleerde maatregel ingevoerd worden. Men kan best een geheel van maatregelen invoeren. Andere maatregelen worden reeds toegelicht in de overige FISP-documenten.

Link met IAM als maatregel

Verificatie en beheer van identiteiten is een cruciaal onderdeel van het werken met digitale certificaten. Digitale certificaten vormen trouwens een authenticatie mechanisme dat opgenomen is in de minimale maatregelen – IAM.

Link met functiescheiding als maatregel

Functiescheiding is een organisatorische controlemaatregel met als voornaamste doelstelling het voorkomen van fraude en fouten. Dit wordt bereikt door de taken en bijbehorende rechten voor een specifiek bedrijfsproces over meerdere organisaties, rollen, individuen en of accounts te spreiden.

Link met logging als maatregel

Cryptografische maatregelen worden ook toegepast om (gevoelige) gegevens in logbestanden te beschermen:

- Encryptie kan dan toegepast worden om de vertrouwelijkheid van deze informatie te garanderen
- Om de integriteit van logbestanden te garanderen, kan deze beveiligd worden door middel van hashing of het plaatsen van een digitale handtekening.
- Door het toevoegen van een tijdszegel (‘time stamp’) is het mogelijk om een correcte tijdssynchronisatie te realiseren. Dit is namelijk belangrijk voor de log analyse.

Link met netwerken als maatregel

Cryptografie wordt vaak gebruikt om netwerken te beveiligen, hierbij wordt data in transit of ‘data in motion’ (DIM) versleuteld in het kader van:

〉 Integriteit: door middel van hashing of digitale handtekening voorkomen dat data in motion ongecontroleerd gewijzigd wordt;

[6] VO-informatieclassificatie – Cryptografie

〉 Confidentialiteit: door middel van versleuteling, bv. van niet-publieke data over een publiek netwerk door middel van tunneling.

Documentbeheer

Historiek

Datum	*Auteur*	*ersie*	*Omschrijving wijzigingen*
09/05/2019	BOSA	V0.1	• First draft
15/05/2019	FISP workgroup	V0.2	• Tekst aangevuld en herwerkt • Data contexten verplaatst naar bijlage • Technische verklaring geïntroduceerd in een apart document
20/05/2019	FISP workgroup	V1.0	• Wijziging in de inleiding • Data in rest onder klasse 1 is gewijzigd • Verwijzing naar de wet voor klasse 4 • Verplaatsing van de bijlage “data in context” naar het verklarend document
21/11/2019	FISP workgroup	V1.1	• Publieke verspreiding

Goedkeuringen

Datum	*Approver(s)*	*Versie*
21/11/2019	FISP workgroup	V.1.1

Bronnen

Dit document werd samengesteld met behulp van de volgende bronnen:

- VO-informatieclassificatie – Cryptografie
- BIR - Encryptiebeleid
- IEC 27001/2

Link met een ander beleid

Afhankelijkheid van interne documenten

Ref	*Titel*
FISPDOC05	*Handleiding voor de beveiliging en het beheer van de identiteiten en de basistoegangen (IAM) en de geprivilegieerde toegangen (PAM)*

Positionering van het beleid t.o.v. de ISO 27001-norm

Sectie	***Doelstellingen en referentiemaatregelen***	*In relatie (X = Ja*
	Context van de organisatie	
	Leiderschap	
	Planning	
	Ondersteuning	
	Operatie	
	Evaluatie van de prestaties	
	Verbeteringen	

Positionering van het beleid t.o.v. de ISO 27002-norm

Sectie	**Doelstellingen en referentiemaatregelen**	In Relatie *(X = Ja)*	Doelstellingen / Maatregelen *(Detail)*
	Informatiebeveiligingsbeleid		
	Organisatie van informatiebeveiliging		
	Human Resources Veiligheid		
	Asset Management		
	Toegangscontrole		
	Geheimschrift	*x*	*10.1*
	Fysieke en ecologische veiligheid		
	Operationele veiligheid		
	Beveiliging van communicatie		
	Aankoop, ontwikkeling en onderhoud van informatiesystemen		
	Relaties met leveranciers		
	Beheer van informatiebeveiligingsincidenten		
	Informatiebeveiliging in Business Continuity Management		
	Conformiteit		