Federal Information Security Policy Guideline

Startgids

21/11/2019

FISPDOC09 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).

Veiligheidsdoel van het document

Dit document is een how-to document voor de verschillende federale overheden, met algemene tips voor de toepassing en implementatie van FISP.

Toepassingsgebied

Dit beleid voor informatiebeveiliging is toepasselijk voor alle informatie die er circuleert in de federale organisaties.

Vertrouwelijkheid van het document

Publieke verspreiding

Vrijwaring

Deze informatie mag niet individueel gebruikt worden als referentie documentatie. De lezer van dit document gebruikt dit document niet als vervanger van wetgeving of standaarden, maar als leidraad bij het nemen van de gepaste beveiligingsmaatregen.

Verantwoordelijkheden

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

Eigenaar

De eigenaar van dit document is de FISP-werkgroep.

Inleiding

Het FISP project omvat een beleid voor informatiebeveiliging. In dit kader van informatiebeveiliging bevinden zich specifieke handleidingen o.a. voor cryptografie en logging. Echter omvat dit beleid niet de effectieve implementatie van de FISP beveiligingsaanbevelingen. Daarom helpen wij u graag verder met deze starterkit. In deze starterkit voorziet de FISP werkgroep enkele globale tips voor de overheidsinstanties om zelf zo probleemloos mogelijk de FISP beveiligingsaanbevelingen toe te passen en te implementeren. Hierbij houden we ook rekening met de stappen die men moet doorlopen voorafgaand de toepassing van de door FISP aanbevolen maatregelen.

De door FISP aanbevolen maatregelen houden rekening met de bestaande ISO 2700X-normen. Het pakket van voorgestelde maatregelen voor informatiebeveiliging is echter niet compleet, aangezien er beveiligingsobjectieven zijn die nog niet uitvoerig behandeld zijn in deze eerste release van FISP. Het is dus aangeraden om zich te wenden tot deze normen indien verdere informatie noodzakelijk is. Daarnaast adviseren we u ook gebruik te maken van de BSG (Baseline information Security Guidelines) geleverd door het Centrum voor Cybersecurity België (CCB) aangezien FISP een aanvulling op dit beleid vormt.

1. Beheersstrategie

De betrokkenheid van managers is van groot belang voor het succes van uw implementatie van FISP. Het door FISP aanbevolen informatiebeveiligingsbeleid en het daaruit voortkomende informatiebeveiligingsplan voor uw federale organisatie, vereist de validatie en ondersteuning van het management van de specifieke federale organisatie. Informatiebeveiliging maakt immers deel uit van een goed beheer van de organisatie en zal bovendien beïnvloed worden door de noden en de doelen van de organisatie, de beveiligingsvereisten, de gebruikte processen in deze organisatie en de structuur van de organisatie.

Het management betrekken bevordert bovendien de ontwikkeling van een veiligheidscultuur en de uitvoering van de voorgestelde beveiligingsmaatregelen.

Het is belangrijk dat er eerst een goed kader gecreëerd wordt door het management voor de implementatie van FISP. Dit kan door middel van een informatiebeveiligingsstrategie waarbij wet- en regelgevingen gerespecteerd worden. Het is bovendien aangewezen om de veiligheidscultuur vanaf het begin van een project te integreren.

De nodige instrumenten en ondersteuning voor deze implementatie zullen door het management voorzien moeten worden. Maar om de middelen ook effectief te kunnen inzetten, moeten ze worden gecommuniceerd aan alle belanghebbende partijen van uw organisatie.

Tot slot zullen regelmatige basis training en sensibilisering van alle interne en externe medewerkers en de organisatie als geheel, noodzakelijk zijn. Communicatie met alle belanghebbende partijen van de federale organisatie is essentieel.

1.1. Tips:

- Het is aangeraden om het informatiebeveiligingsplan voldoende aan te sluiten bij de strategie en operationele doelstellingen van uw federale organisatie zodat verwerping door het management vermeden kan worden.
- Benadruk de verantwoordelijkheid van het management (de verwerkingsverantwoordelijke).
- Informeer de managers tijdig.

2. Management van activa

2.1. Inventaris activa

Eerst moeten we kijken wat nu precies in gevaar kan worden gebracht, met andere woorden wat de federale organisatie bezit of wat het vermogen van de federale organisatie is. Beveiligingsbeheer is gebaseerd op duidelijk geïdentificeerde en gewaardeerde activa. Het is dus noodzakelijk dat er een inventaris wordt opgesteld met de activa van de federale organisatie. Het doel van informatiebeveiliging is om de federale organisatie en zijn activa te beschermen. Dit beperkt zich echter niet tot IT-infrastructuur of tastbare activa maar ook tot o.a. mensen of processen.

2.2. Categorisatie van essentiële activa

Het is vervolgens aangeraden om een hiërarchie te creëren binnen de geïnventariseerde activa op basis van de kriticiteit van deze activa. Het is dus belangrijk om een duidelijk inzicht te hebben in de waarde en het belang van de activa en in welke mate ze essentieel zijn voor de goede werking en organisatie van de federale instantie. Zo kan het dat een bepaald proces van groter belang voor de federale instantie i.v.m. een ander proces. Door middel van deze categorisatie zal het ook duidelijker zijn welke processen prioriteit dienen te krijgen op vlak van informatiebeveiliging.

2.3. Tips

- Definieer/identificeer in samenwerking met het management en de verschillende afdelingen de "essentiële activa".
- Ontmoet indien nodig de mensen die verantwoordelijk zijn voor deze verschillende activa om ze beter te identificeren en te definiëren.
- Stel er een lijst van op.
- Laat deze lijst formeel goedkeuren door het management, zodat het betrokken kan worden bij uw proces (bijvoorbeeld via een goedkeuringsrapport of een document ondertekend door het management).

Het is belangrijk om dit proces continu te verbeteren en dus opnieuw toe te passen om zo te voorkomen dat men nieuwe activa over het hoofd ziet.

3. Risicobeoordeling

Daarna onderzoeken we welke gevaren de essentiële activa bedreigen. Met risicoanalyse kunt u de bedreigingen en risico's identificeren voor de geïdentificeerde activa. Die dreigingen kunnen o.a. een brand zijn of een (on)opzettelijke menselijke dreiging. Bijvoorbeeld iemand die een vertrouwelijk document verliest. Bovendien zou er rekening moeten gehouden worden met zwakke elementen binnen de federale organisatie zoals verkeerd geïnstalleerde software waardoor een hacker bijvoorbeeld makkelijker in het systeem kan inbreken en zo toegang krijgt tot vertrouwelijke informatie. Het is dus aangeraden om zoveel mogelijke incidenten in rekening te brengen.

Bij het beoordelen van risico's zal er een onderscheid gemaakt moeten worden tussen het "inherente risico" en het "residuele" risico. Waarbij het "inherente" risico diegene zijn die een negatieve impact hebben wanneer men geen beveiligingsmaatregelen implementeert en het "residuele" risico's degene die waarschijnlijk een negatieve impact zullen hebben ondanks de genomen beveiligingsmaatregelen.

De resultaten van de risicoanalyse helpen het management een strategie op te stellen die rekening houdt met alle noodzakelijke kosten om geïdentificeerde activa tegen geïdentificeerde bedreigingen te beschermen, en een praktisch veiligheidsbeleid te ontwikkelen dat als leidraad dient voor beveiligingsactiviteiten. De hoge residuele

risico's zullen ook voldoende gecommuniceerd moeten worden met de directie zodat beslist kan worden of deze behandeld of aanvaard worden als een restrisico.

3.1. Tips

- De organisatie moet bij elk proces een risicobeoordeling rond informatieveiligheid uitvoeren, valideren, communiceren en onderhouden
- Een risicoanalyse is terug te vinden in de methode voor geoptimaliseerde risicoanalyse ("Monarc")[1]. Een meer gedetailleerde aanpak is ook te vinden in ISO 27005.
- De organisatie moet alle risicobeoordelingen met een hoog residueel risico communiceren naar de directie voor bespreking en beslissing: behandelen of aanvaarden.
- De risicoanalyse kan heel eenvoudig zijn, maar ze kan ook gedetailleerd zijn.
- De complexiteit van de analyse hangt af van de grootte van de federale organisatie, de complexiteit van de projecten en de gevoeligheid van de gegevens die u verwerkt, de beschikbaarheid van expertise, de beschikbare tijd en het budget.

4. Informatiecategorisatie

Vooraleer men specifieke veiligheidsmaatregelen kan toepassen is het noodzakelijk dat er een categorisatie van informatie plaatsvind. Het is aangewezen dat de federale organisaties, afhankelijk van de gevoeligheid van informatie, informatie dient te beschermen volgens een methodologie om de risico's te beheren en te beperken tot bepaalde beschermingsniveaus. Deze beschermingsniveaus zijn uitgedrukt in categorisatieniveau. Afhankelijk van de categorisatie waartoe de informatie behoort worden verschillende beveiligingsmaatregelen voorgesteld. De FISP werkgroep heeft een schema voor informatiecategorisatie opgesteld. Het is aan de federale organisatie om de interne procedures te definiëren om zijn informatie te markeren volgens de door FISP voorgestelde categorieën.

Zie: FISP – informatiecategorisatie (link nog toe te voegen)

5. Uitvoering van specifieke veiligheidsmaatregelen

Nadat de essentiële activa zijn geïdentificeerd en geëvalueerd en alle risico's gekend zijn die een gevaar kunnen betekenen voor de federale instantie, is het nodig om de door FISP geadviseerde beveiligingsmaatregelen te implementeren. Hierdoor worden de essentiële activa beschermt tegen eventuele risico's voor de integriteit, vertrouwelijkheid en toegankelijkheid. Er zullen echter altijd overblijvende risico's of restrisico's, blijven bestaan nadat de veiligheidsmaatregelen werden ingevoerd. Die restrisico's zijn niet te vermijden (bv. menselijke vergissingen) maar het doel is om deze zo klein mogelijk te houden.

De FISP werkgroep heeft gedetailleerde documenten opgesteld voor verschillende onderwerpen. In de meeste van deze documenten kan u aanbevolen beveiligingsmaatregelen terugvinden gekoppeld aan de voorgestelde informatie categorisatie van FISP, met uitzondering van de fysieke beveiligingsmaatregelen en de Cloud beveiliging.

[1] https://www.monarc.lu/

5.1. Handleiding voor cryptografie

Dit document beschrijft de aanbevolen maatregelen om onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatie verwerkende faciliteiten van federale organisaties te voorkomen.

Zie: Handleiding voor cryptografie

5.2. Handleiding voor cryptografie

Dit document beschrijft de aanbevolen maatregelen met betrekking tot cryptografie. Dit document bevat voldoende informatie om goede (beleid)keuzes te maken en bewustwording te creëren. De voorgestelde maatregelen zijn gekoppeld aan de voorgestelde informatie categorisatie van FISP en met de verschillende data contexten.

Zie: Handleiding voor cryptografie

Voor meer algemene informatie over cryptografie zie bijlage 7.1.

5.3. Handleiding voor logging en monitoring

Dit document beschrijft de aanbevolen maatregelen met betrekking tot logging. De voorgestelde maatregelen zijn gekoppeld aan de voorgestelde informatie categorisatie van FISP. Er wordt bovendien advies gegeven in de maatregelen die men moet nemen voor logbeheer, aanwijzingen over de retentie en beveiliging van audit records, hoe om te gaan met fouten in audit records en audit opvolging, analyse en rapportering.

Zie: Handleiding voor logging en monitoring

Indien u graag over meer informatie beschikt over logging en de geadviseerde maatregelen, zie bijlage 7.2.

5.4. Handleiding voor de beveiliging en het beheer van de identiteiten en de basistoegangen (IAM) en de geprivilegieerde toegangen (PAM)

In dit document worden de algemene maatregelen met betrekking tot IAM georganiseerd in lijn met de voorgestelde informatie categorisatie van de FISP werkgroep. Een algemene verwijzing naar ‘Privileged Access Management’ (PAM) komt ook aan bod in dit document.

Zie: Handleiding voor de beveiliging en het beheer van de identiteiten en de basistoegangen (IAM) en de geprivilegieerde toegangen (PAM)

Indien u graag over meer informatie beschikt betreffende de maatregelen voor IAM zie bijlage 7.3. Voor meer informatie betreffende de maatregelen voor PAM zie bijlage 7.4.

5.5. Handleiding voor de beveiliging in de cloud

Deze handleiding stelt de overheidsdiensten in staat om de risico's voor de informatieveiligheid in verband met clouddiensten systematisch te identificeren, te analyseren en te beoordelen. Ze beschrijft bovendien controles om deze risico's effectief te beheren.

Zie: Handleiding voor de beveiliging in de cloud

5.6. Handleiding voor de beveiliging van persoonsgegevens

Dit document omschrijft de vereisten om te voldoen aan de informatiebeveiliging zoals vooropgesteld door de Algemene Verordening Gegevensbescherming (AVG). Het bevat bovendien een gestandaardiseerde categorisatie volgens de interpretatie van FISP werkgroep.

Zie: Handleiding voor de beveiliging van persoonsgegevens

Indien u graag meer informatie heeft over de verschillende datatypes die beschreven zijn in het vademecum zie bijlage 7.5.

6. Evaluatie van veiligheidsmaatregelen

Het is aangeraden om jaarlijkse een evaluatie van de beveiligingsmaatregelen uit te voeren. Op deze manier wordt duidelijk waar verbeteringen noodzakelijk zijn en kan de status van het beveiligingsplan beoordeelt worden. de beveiliging van de federale instantie moet voortdurend bewaakt worden en de kans krijgen om zich aan te passen en te ontwikkelen, rekening houdend met de behoeften aan beveiliging en de omstandigheden waarin de federale instantie bestaat en werkt

Het is dus noodzakelijk om bedreigingen en kwetsbaarheden regelmatig opnieuw te analyseren (cyclus van continue verbetering: PDCA) en het beveiligingsplan ook naarmate aan te passen in het licht van deze evaluaties.

7. Bijlage

7.1. Cryptografie

Cryptografie is de wetenschappelijke discipline om aan de hand van wiskundige technieken informatie te beveiligen. Cryptografische technieken kunnen toegepast worden op opgeslagen informatie ('Data at Rest' of DAR), op informatie tijdens gebruik door een toepassing of systeem ('Data in Use' of DIU) of transport van informatie ('Data in Motion' of DIM). Een voorbeeld van de verschillende toepassingen van de data contexten kan terug gevonden worden in bijlage 1.

Door toepassing van cryptografische technieken kunnen een aantal **veiligheidsaspecten** gerealiseerd worden:

- **Vertrouwelijkheid**: waarborgen dat informatie enkel leesbaar is voor degenen die daartoe geautoriseerd zijn.
- **Integriteit**: waarborgen dat informatie of functionaliteit niet werd gewijzigd door onbevoegden.
- **Authenticatie** van entiteiten: verifiëren van de identiteit van een entiteit (entiteit= persoon, organisatie, proces, systeem ….).
- **Data-authenticatie**: waarborgen van de oorsprong en integriteit van informatie. Data-authenticatie heeft dus twee elementen: verifiëren dat de gegevens van de juiste entiteit afkomstig is en de integriteit van die gegevens valideren. Verwezenlijken van data-authenticatie is complexer dan vertrouwelijkheid.
- **Onweerlegbaarheid** ('non-repudiation'): voorkomen dat eerdere acties of verplichtingen kunnen worden ontkend.
- **Anonimiteit:** het waarborgen van de vertrouwelijkheid van communicerende entiteiten (i.e. metadata: wie communiceert met wie) is tevens een beveiligingsdienst waarvoor cryptografische technieken kunnen ingeschakeld worden**.**

Cryptografie omvat een scala aan technieken om aan bovenstaande veiligheidsaspecten tegemoet te komen. Hieronder kunt u een samenvatting vinden van welke veiligheidsaspecten worden ondersteund door welke technieken:

Vertrouwelijkheid	Encryptie
Integriteit	Encryptie (hash) en digitale handtekening
Onweerlegbaarheid	Digitale handtekening met certificaat
Authenticatie	Digitale handtekening met certificaat (v.b. : eID)

Mogelijke technieken voor technische activiteiten – deze zijn transparant voor een gebruiker:

- De uitgifte en beheer van digitale certificaten door middel van een PKI.
- Het sleutelbeheer en de levenscyclus van een sleutel of sleutelpaar.
- De vertrouwelijkheid en integriteit van informatie tijdens transport over een netwerk – vb. door het opzetten van VPN.
- De afkomst van software garanderen door middel van digitale handtekening.
- De authenticiteit van een website garanderen d.m.v. een (SSL) certificaat.
- Systeem authenticatie door middel van digitale certificaten.

Encryptie

Introductie

Encryptie is een mechanisme om informatie te beveiliging door het onleesbaar te maken voor onbevoegden. Het encrypteren gebeurt d.m.v. een wiskundig algoritme en cryptografische sleutel. Naast toegangscontrole als beveiligingsmaatregel, is encryptie een middel om vertrouwelijkheid van informatie te realiseren. Encryptie voorkomt dat een niet-geautoriseerde partij vertrouwelijke informatie kan lezen of wijzigen. Het biedt bovendien de mogelijkheid om te controleren of een bericht inderdaad van een bepaalde zender afkomstig is. 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.

Het encrypteren van informatie wordt ook wel versleutelen of vercijferen genoemd, decrypteren wordt ontcijferen genoemd.

Er zijn twee encryptie technieken: symmetrische en asymmetrische encryptie.

Hoe werkt encryptie?

Symmetrische encryptie

Bij symmetrische encryptie wordt een wiskundig algoritme gebruikt dat dezelfde (symmetrische) geheime sleutel nodig heeft om zowel te encrypteren als te decrypteren. Beide partijen dienen over dezelfde geheime sleutel te beschikken die bijgevolg vooraf op een veilige manier gedistribueerd dient te worden.

Met symmetrische systemen kan zowel vertrouwelijkheid van informatie als data-authenticatie verwezenlijkt worden, bijvoorbeeld door eerst encryptie van het document met symmetrische sleutel toe te passen om vervolgens de Macwaarde (Message Authenticatie Code) te berekenen van het versleuteld document.

Encryptie wordt niet alleen gebruikt om informatie die verstuurd wordt te beveiligen tegen onbevoegden, maar 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.

Symmetrische encryptie is snel maar wanneer er veel communicerende partijen actief zijn kan dit echter een complex proces worden. Bovendien is het moeilijk om de sleutel bij de ontvangende partij te krijgen zonder dat deze gestolen wordt door onbevoegden.

Voorbeelden van toepassingen in de praktijk:

- **KMS**: een ‘Key Management System’ beheert de cryptografische sleutels m.i. sleutel generatie, uitwisseling, opslag, gebruik, vernietiging en vervanging van deze sleutels.
- **Kerberos:** Kerberos is een authenticatiesysteem voor lokale netwerken met een client-serverarchitectuur, gebaseerd op een Trusted Third Party: een partij die door alle anderen wordt vertrouwd. Het beschermt servers tegen gebruik door niet-geautoriseerde partijen, en cliënten tegen interactie met valse servers. Ook is voorzien in het genereren van een sessie-sleutel voor de communicatie tussen cliënt en server, zodat indringers geen lopende sessies kunnen overnemen of afluisteren.
- Gekende voorbeelden van algoritmen voor symmetrische encryptie zijn DES en AES.

Asymetrische encryptie (Public key encryption)

Asymmetrische encryptie biedt een antwoord op de vraag over hoe je de geheime encryptie sleutel bij de ontvangende partij krijgt zonder dat deze gestolen wordt door onbevoegden. Daar waar men bij symmetrische encryptie een wiskundig algoritme gebruikt dat dezelfde (symmetrische) geheime sleutel nodig heeft om zowel te encrypteren als te decrypteren, werkt asymmetrische encryptie op basis van een sleutelpaar. De encryptie of decryptie hangt dus niet af van één sleutel maar van het hele paar.

Het sleutelpaar bestaat uit een publieke (of openbare) sleutel en een private sleutel. Eén sleutel is geheim (privaat) en de andere sleutel is openbaar (publiek). De cryptografische sleutel om encrypteren en decrypteren is dus verschillend.

Een bericht wordt onleesbaar gemaakt met de publieke sleutel van de ontvanger. Die kan het bericht vervolgens met zijn private sleutel weer ontsleutelen. Het is essentieel dat de private sleutel door de eigenaar van het sleutelpaar geheim gehouden wordt. 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 de publieke sleutel, dan is dat het bewijs dat het bericht van jou afkomstig is.

Het voordeel van asymmetrische encryptie is, dat het eenvoudig is om de decryptiesleutel aan de ontvangende partij te bezorgen. De publieke sleutel is openbaar en kan dus zonder problemen gedeeld worden met iedereen. Op deze manier kan men zich toeleggen op de beveiliging van de private sleutel. Dit is uiteraard veel gemakkelijker.

Er is echter ook een nadeel verbonden aan asymmetrische encryptie, namelijk het gebrek aan snelheid. Om dit probleem te verhelpen wordt asymmetrische encryptie vaak gecombineerd met symmetrische encryptie. Men kan op deze manier een symmetrische encryptie sleutel, nodig voor encryptie van een omvangrijk stuk informatie, versleutelen met de publieke sleutel van de ontvangende partij. De ontvangende partij zal vervolgens deze sleutel decrypteren met zijn private sleutel. Dit zorgt ervoor dat de sleutel bruikbaar is voor ontcijfering van de eigenlijke informatie.

Naargelang de gebruikte sleutel om te encrypteren (publieke of private sleutel), kunnen andere securitydiensten gerealiseerd worden:

- encryptie d.m.v. een publieke sleutel → *vertrouwelijkheid*
- encryptie d.m.v. een private sleutel → integriteit en onweerlegbaarheid (digitale handtekening)

Digitaal certificaat

De publieke sleutels bij asymmetrische encryptie hebben één nadeel. Het is voor de ontvanger moeizaam om te 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 (dit noemt men ‘spoofing’). Om dit probleem te verhelpen bestaat er een digitaal certificaat. Een digitaal certificaat kan worden vergeleken met een paspoort of een rijbewijs. Ze worden gebruikt als officiële legitimatie, om de echtheid van een entiteit en de relatie met zijn/haar publieke sleutel aan te tonen.

De partij die het digitaal certificaat uitgeeft bepaalt de geloofskracht van dit certificaat en de bijhorende controles die hieraan voorafgaan. Het is mogelijk om zelf een certificaat uit te geven, maar dan is de geloofwaardigheid eerder klein. Een certificaat uitgegeven door een overheid wordt echter wel als geloofwaardig en betrouwbaar beschouwd. De organisaties die certificaten uitgeven en beheren zijn over het algemeen commerciële organisaties én overheidsorganisaties.

SSL-certificaat

Federale organisaties stellen steeds meer diensten en informatie ter beschikking via het internet. Het is belangrijk dat de gebruiker zeker weet dat de website waarop hij/zij gegevens invult daadwerkelijk van de federale organisatie is en dat de communicatie met deze overheidswebsite ook voldoende beveiligd is. Om deze veiligheid te garanderen bieden SSL-certificaten een oplossing. Dit certificaat voegt een uniek zegel toe aan een website. Deze zegel is vervolgens op websites beschikbaar voor controle van de echtheid en beveiliging van website. Op deze manier wordt de integriteit van de overheidswebsite gegarandeerd. Het is één van de meest voorkomende types van certificaten.

Gegevens opgeslagen in een certificaat

Het certificaat bevat volgende gegevens:

- geregistreerde naam van de eigenaar: de certificaathouder;
- publieke sleutel van de eigenaar;
- geldigheidsperiode van het certificaat;
- identiteit van de uitgever van het certificaat: de certificaatautoriteit (CA);
- locatie van de 'Certificate Revocation List' (bij de uitgever van het certificaat);
- samenvatting van bovenstaande gegevens, aangemaakt door een hashfunctie, en vervolgens vercijferd met de geheime sleutel van de CA. Dit is de digitale handtekening en wordt gebruikt om de geldigheid en authenticiteit van bovenstaande gegevens te waarborgen.

Om bruikbaar te zijn in de meeste toepassingen, worden digitale certificaten opgemaakt volgens een algemeen erkende standaard: X.509. Deze erkende standaard biedt de mogelijkheid van eenvoudige tot uitgebreide identiteitscontrole van de certificaathouder

De kracht van het certificaat

De kracht van zo'n certificaat naar betrouwbaarheid toe zit in twee criteria:

1. Hoe betrouwbaar is de uitgever van het certificaat?
2. Hoe goed is de identiteit van de eigenaar van het sleutelpaar geverifieerd?

Voor het eerste punt, de uitgever van het certificaat, is het belangrijk om het certificaat zelf te verifiëren:

- Is het certificaat niet uitgegeven door de eigenaar zelf (dan is er immers geen enkele controle op de identiteit van de eigenaar gebeurd)?
- Is het certificaat nog geldig en niet gecompromitteerd (validiteit en revocatie)?
- Is het certificaat uitgegeven door een betrouwbare partij?

Voor het tweede punt, de controle van de identiteit van de certificaathouder, zijn er drie opties bij het aankopen van een X.509 certificaat:

1. **Domein validatie**: certificaten met domein validatie bevatten geen bedrijfsgegevens. Er wordt alleen gecontroleerd of de aanvrager controle heeft over het domein waarvoor het certificaat wordt aangevraagd. Het certificaat wordt door alle browsers vertrouwd en zorgt voor een veilige verbinding d.m.v. encryptie. Bij SSL-certificaten met domein validatie toont de browser een slot-icoontje, vb.:

2. **Organisatie validatie**: De certificaten met organisatie validatie bevatten bedrijfsgegevens. De bezoekers van een website kunnen met deze bedrijfsgegevens controleren of ze op de website van het juiste bedrijf zijn. De

bedrijfsgegevens worden in het certificaat opgenomen, maar komen niet prominent in beeld zoals dat bij EV-certificaten het geval is. Ook hier toont de browser een slot-icoontje én zijn de bedrijfsgegevens in het certificaat opgenomen, maar komen niet prominent in beeld op de browser, vb.:

Uiterlijk zie je geen verschil met domein validatie, maar het certificaat geeft wel meer details vrij.

3. **Uitgebreide validatie** (EV: 'extended validation'): Naast de domeinvalidatie waarbij de aanvrager laat zien controle te hebben over het domein waarvoor het certificaat wordt aangevraagd, worden ook de bedrijfsgegevens gecontroleerd. Er wordt hiervoor naar een openbaar register gekeken, en er kan ter verificatie naar de organisatie worden gebeld. Soms is het noodzakelijk dat er bijkomende documenten worden ondertekend. Een website die gebruik maakt van EV SSL certificaten vertoont een groene balk met het slot-icoontje, vb.:

Buiten de groene kleur en het slot-icoontje toont de browser ook de identificatie van de organisatie door op het slot-icoontje te klikken. Dit soort validatie wordt typisch gebruikt door financiële instellingen en webshops.

Specifiek voor de beveiliging van websites, zijn er – naast de drie validatievarianten – ook nog eens drie verschillende types SSL-certificaten:

1. **Enkel domein**: dit type certificaten beschermt één enkel domeinnaam, vb. 'www.eendomein.com'.
2. **Multi domein**: hiermee is het mogelijk meerdere domeinnamen binnen één SSL-certificaat.
3. **Wildcard** certificaten: met een wildcard certificaat worden alle subdomeinen van één domein beveiligd. Wildcard certificaten zijn enkel beschikbaar bij domein- en organisatie validatie, bij uitgebreide validatie (EV-certificaten) moet elk subdomein een eigen certificaat krijgen en kan men dus geen wildcard certificaten toepassen.

Public Key Infrastructure

Een Public Key Infrastructure (PKI) is een set van technische en organisatorische voorzieningen, die een oplossing bieden voor het probleem van koppeling van een eigenaar (persoon of organisatie) aan zijn/haar crypto sleutelpaar door middel van het digitale certificaat. Op deze manier kunnen publieke sleutels in combinatie met de betreffende certificaten gebruikt worden voor authenticatie en het versturen van geheime (sleutel-) informatie over een niet vertrouwd netwerk. Een PKI biedt zo dus een uitbreiding op de asymmetrische encryptie techniek die ervoor zorgt dat authenticatie en onweerlegbaarheid aantoonbaar wordt.

De uitgifte en het beheer rond deze certificaten wordt op een geformaliseerde wijze uitgevoerd, zodat de status van het certificaat en de eigenaar gegarandeerd is. Een Certificate Service Provider (CSP) is een (derde) partij die de certificaten voor de ontvanger zal uitgeven. Deze CSP moet dan zowel door zender als ontvanger vertrouwd worden. De CSP beheert de PKI-omgeving en garandeert de echtheid en de oorsprong van de certificaten.

Een CSP moet zelf ook aan kwalitatieve verplichtingen voldoen. Certificaten kunnen in allerlei vormen worden uitgegeven. De bijbehorende private sleutels moeten beschermd zijn tegen niet bevoegde toegang en worden bij voorkeur uitgegeven en opgeslagen op afzonderlijk te beveiligen objecten als smartcards, USB-tokens, en Hardware Security Modules (HSM).

Er zijn verschillende soorten van PKI in gebruik en daaraan gekoppeld bestaan verschillende soorten van processen voor de uitgifte van certificaten door CSP's:

- Binnen een **organisatie**: hier worden certificaten uitgegeven door een eigen CSP.
- Binnen het **publieke domein**: uitgifte processen moeten hierbij voldoen aan de wet eIDAS en elektronische archivering[2].
- **Web van vertrouwen** ('web of trust'): in dit model wordt de controle van de identiteit uitgevoerd door de certificaathouders (de eigenaars van de certificaten). Ze staan zelf in voor de authenticiteit van de identiteit van de andere certificaathouders. Voorbeelden hiervan zijn Thawte, CAcert en PGP.

[2] Wet van 21 juli 2016 Wet tot uitvoering en aanvulling van de verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende de elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.

Sleutelbeheer

De mate van bescherming die cryptografie biedt hangt behalve van het gebruikte algoritme of protocol tevens af van de geheimhouding van het sleutelmateriaal (geheime sleutel, private sleutel) en de authenticiteit van de publieke sleutels. Het beheer van crypto sleutels speelt dus een essentiële rol bij de beveiliging op basis van cryptografische technieken.

Het sleutelbeheer betreft alle aan sleutelmateriaal gerelateerde activiteiten vanaf het genereren tot en met de vernietiging van sleutels. Sleutelbeheer omvat het aanmaken, registeren, opslaan, distribueren, in gebruik nemen, herroepen, archiveren en vernietigen van sleutels. Er zal naast de technische beveiligingsmaatregelen ook aandacht dienen te worden besteed aan de organisatorische, fysieke en procedurele beveiligingsmaatregelen. Voorbeelden zijn beveiligingsmaatregelen bij het aanmaken en opslaan sleutels, en functiescheiding om misbruik van sleutels te voorkomen, en te detecteren.

Volgende onderwerpen moeten aan bod komen in de procedures voor sleutelbeheer:

- Hoe de aanvragen van een sleutelpaar moet verlopen.
- Wie de sleutels mag genereren.
- Op welke manier de sleutelparen moeten worden overgedragen aan de eigenaar.
- Of de eigenaar zich moet legitimeren tijdens de overdracht van het sleutelpaar.
- Hoe lang de sleutels geldig zullen zijn.
- Wie de sleutels kan intrekken.
- Hoe de sleutels worden geüpdatet.

Onder Sleutelbeheer worden de volgende activiteiten verstaan:

- 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.

Hoe het sleutelbeheer wordt ingericht is voornamelijk afhankelijk van:

- het gewenste beveiligingsniveau,
- de schaalgrootte,
- de verscheidenheid waarop encryptie wordt toegepast,
- het belang van de versleutelde gegevens.

Het belang van versleutelde gegevens wordt bepaald door de classificatieschaal van de informatie die verwerkt wordt. Naarmate de informatie classificatie hoger is, zullen procedures strikter zijn en zal de mate van functiescheiding toenemen. Een risicoanalyse kan inzicht geven in welke risico’s dienen te worden afgedekt met organisatorische en/of technische maatregelen.

Sleutel hiërarchie

Er zijn verschillende mogelijkheden om crypto sleutels te genereren, sommige zijn open-source (vaak kosteloos), andere zijn leverancier- specifiek (niet kosteloos). Maar zodra een crypto sleutel is gegenereerd en gebruikt, moet deze sleutel veilig bewaard worden voor later gebruik, dit is echter niet zo eenvoudig. Sleutel hiërarchie biedt een oplossing voor dit voorgaande probleem.

Sleutel hiërarchie is een techniek waarbij een master sleutel (roots) gebruikt wordt om de crypto sleutel op zijn beurt te versleutelen. Op deze wijze voorziet sleutel hiërarchie in een krachtige methode om andere crypto sleutels te beveiligen. Men moet dan enkel deze master sleutel heel goed te beveiligen om de betrouwbaarheid van de andere sleutels te garanderen. Jammer genoeg is ook dit geen risicoloze oplossing want als de master sleutel gehackt wordt, zijn alle onderliggende sleutels eveneens gecompromitteerd!

Dit betekent o.a. dat deze master sleutel best bewaard wordt in een HSM-module bijvoorbeeld FIPS 140 gekeurd. Dit keurmerk waarborgt de goede beveiliging van de master sleutel.

De voordelen van sleutel hiërarchie:

- De hoeveelheid sleutels die hoge beveiliging beogen is gereduceerd tot de beveiliging van de master sleutel.
- Door gebruik te maken van één master sleutel is het eenvoudiger om verschillende sleutels te gebruiken voor de beveiliging van verschillende stukken informatie.
- Enkel de master sleutel moet behandeld worden in de HSM. Encryptie en decryptie moet niet langer uitgevoerd worden in de HSM waardoor bulk encryptie/decryptie sneller kan.

Een diepere hiërarchie voor sleutelbeheer is ook mogelijk: een HSM beveiligde master sleutel beveiligt een organisatorische sleutel die op zijn beurt een aantal bulk encryptie sleutels die doorheen de organisatie gebruikt worden voor de beveiliging van bulk informatie.

Tijdsstempel (‘Time stamping’)

Een elektronische tijdsstempel gaat gepaard met de digitale handtekening. In de eerste plaats moeten digitale handtekeningen gevalideerd worden direct na ondertekening. Dit vanwege een beperkte geldigheidsduur en de continue ontwikkeling van krachtiger wordende computers. Dit maakt digitale handtekeningen minder geschikt voor de lange termijn. Maar voor bijvoorbeeld digitale facturen en andere archiefdocumenten is juist validatie op langere termijn nodig.

De geldigheidsduur van een digitale handtekening is afhankelijk van de geldigheid van het gebruikte digitale certificaat. Als de geldigheid van dit certificaat is verstreken, geeft de digitale handtekening een foutmelding. Ook het bovenliggende rootcertificaat heeft een geldigheid van bepaalde duur. Een Certificaat Autoriteit (CA) kan ook ophouden met bestaan. In al deze gevallen is de validatie van een ondertekend document niet meer mogelijk.

De foutmelding kan voorkomen worden door het gebruik van een digitale handtekening in combinatie met een elektronische tijdsstempel. De elektronische tijdsstempel bewijst dat het certificaat tijdens de ondertekening wel degelijk geldig was. Op deze manier wordt een digitale handtekening met elektronische tijdsstempel nooit ongeldig. Dit maakt validatie op lange termijn ook zonder een geldig certificaat, rootcertificaat of actieve CA mogelijk. Elektronische tijdsstempels wordt ook gebruik in geavanceerde logging technieken om het tijdsstip van een log event vast te leggen.

Het is essentieel dat voor elektronische tijdsstempels een betrouwbare bron gebruikt wordt. Daarom worden de klokken van servers vaak gesynchroniseerd met een externe, betrouwbare tijdsbron, bijvoorbeeld een atomaire klok. Het is mogelijk om in te schrijven op een service (AWS Amazon Time Sync Service is een voorbeeld) die de tijd van zo’n atomaire klok aanlevert, waardoor de eigen interne klokken eveneens betrouwbaar worden.

De beveiligingsaspecten

Componenten voor vertrouwelijkheid

Berichten en bestanden worden op verschillende manieren via de niet vertrouwde “buitenwereld” uitgewisseld:

- Eindgebruikers versturen berichten via e-mail over het Internet.
- Eindgebruikers plaatsen bestanden op draagbare media (USB-stick, Cd-ROM, dvd, SD-kaarten etc.) die ze meenemen buiten de organisatie.
- Berichten worden via openbare netwerken naar een semi-vertrouwde of niet vertrouwde cliënt verstuurd, bijvoorbeeld voor telewerken of mobiel werken.
- Bij gebruik van draadloze verbindingen binnen de omgeving van de organisatie, waarvan te verwachten is dat ze buiten het gebouw te ontvangen zijn (zoals Wi-Fi).
- Er worden berichten uitgewisseld via openbare netwerken tussen systemen van de organisatie op verschillende locaties of met die van vertrouwde partners.
- Berichten en bestanden worden opgeslagen op een mobiele cliënt (laptop, PDA, smartphone) die meegenomen wordt buiten de organisatie.

Asymmetrische encryptie maakt het mogelijk dat communicerende entiteiten elkaar geheime berichten toezenden zonder vooraf geheime sleutels uit te wisselen. Zo kan je in theorie in een online communicatie een bericht encrypteren d.m.v. de publieke sleutel van de bestemmeling. De bestemmeling kan dan het ontvangen vercijferde bericht gaan decrypteren d.m.v. de bijhorende private sleutel. In de praktijk werkt men echter anders omdat asymmetrische encryptie tijdrovend is. Oplossing is het bericht te versleutelen met een symmetrische sleutel die op zijn beurt versleuteld wordt met de publieke sleutel van de ontvanger. Die kan dan de symmetrische sleutel ontcijferen met zijn/haar private sleutel waardoor het originele bericht ontcijferd wordt aan de hand van de symmetrische sleutel

Bij voorkeur vindt de symmetrische encryptie transparant voor de eindgebruiker plaats. Omdat symmetrische encryptie zich vaak afspeelt op het niveau van verbindingen, netwerken en systemen is dat ook meestal het geval.

Daar waar de encryptie zich op applicatieniveau afspeelt, is vaak interactie van de eindgebruiker vereist. Voorbeelden hiervan zijn e-mail encryptie en aparte software voor encryptie van bestanden om deze op draagbare media op te slaan of als bijlage met e-mail te versturen. De encryptie is uiteindelijk zo sterk als de mate waarin de cryptografische sleutel geheim gehouden kan worden voor onbevoegden. Voor de sterkte van de encryptie spelen de volgende factoren een cruciale rol:

- Encryptiealgoritme;
- Sleutellengte;
- Distributie van sleutels;
- Lifecyclemanagement van sleutels.

Encryptiealgoritme en sleutellengte

Het meest robuuste en vaak toegepaste encryptiealgoritme is AES. Het AES-algoritme is geschikt voor de sleutellengtes van 128, 192 of 256 bits. De sleutellengte en de kwaliteit van de sleutel bepalen in belangrijke mate de tijdsduur die nodig is voor het ‘kraken’ van de encryptie.

Distributie van sleutels

Voor distributie van sleutels worden vaak weer andere encryptiemechanismen ingezet met de bijbehorende sleutels. Samen met de sleutels voor distributie en beheer worden er drie soorten cryptografische sleutels onderscheiden: Key Encryption Keys (KEK), periodieke sleutels en sessiesleutels.

Eigenschap	Key encryption key	Periodieke sleutel	Sessiesleutel
Doel	Encryptie van de periodieke of sessiesleutel	Symmetrische encryptie van de gevoelige gegevens	Symmetrische encryptie van de gevoelige gegevens
Soort	Publieke sleutel of geheime sleutel	Geheime sleutel	Geheime sleutel
Levensduur	1 jaar	Vastgestelde periode	1 sessie
Distributie	Fysiek (smartcard, CD-ROM, sleutellaadapparaat, papier) over vertrouwd pad	Beveiligd met KEK over communicatiepad zelf of over ander onvertrouwd pad	Beveiligd met KEK over communicatiepad zelf
		Fysiek over vertrouwd pad (geen KEK)	

Voorbeelden van versleuteling voor vertrouwelijkheid

- E-mail encryptie: PGP, S/MIME
- Encryptie van webverkeer: TLS
- VPN: IPsec
- Wi-Fi encryptie: WPA, WPA2

Componenten voor integriteit

Een cryptografische hashfunctie, kortweg een hash, is een cryptografische component dat zorgt voor integriteit. Hoewel er geen geheime sleutels worden gehanteerd bij een hash, spreekt men toch van encryptie, namelijk één-richtingvercijfering.

Een hashfunctie neemt als input een bericht van willekeurige lengte en genereert een code, de hashwaarde, die specifiek is voor dat bericht. Elke wijziging van het bericht leidt tot een wijziging in de hashwaarde. Bovendien is het niet mogelijk om vanuit een bepaalde hashwaarde het bericht te construeren (t.t.z. “niet mogelijk” betekent hier dat het rekenkundig niet haalbaar is om dit in redelijke tijd te doen).

Een hashfunctie kan de integriteit van informatie garanderen op voorwaarde dat de hashwaarde zelf correct beschermd is tegen manipulatie. Zo kan bijvoorbeeld in de context van DIM (‘Data in Motion’ = transport van data) de integriteit van een verzonden bericht worden aangetoond door de hashwaarde via een ander communicatiekanaal te versturen, of geëncrypteerd mee te sturen.

Hashfuncties worden gecombineerd met asymmetrische encryptietechnieken om een digitale handtekening te realiseren (zie verder). Een digitale handtekening levert de volgende veiligheidsdiensten: bericht-integriteit, authenticatie van de verzender, data-authenticatie en onweerlegbaarheid.

Bij een MAC (Message Authenticatie Code), soms ook gesleutelde hashfunctie genoemd, wordt een hashwaarde of MAC-waarde gegenereerd op basis van een geheime sleutel. Naast bericht-integriteit, wordt ook een (beperkte) vorm van data-authenticiteit gerealiseerd (garanties over de bron van het verzonden bericht). De geheime sleutel dient in dit geval wel vooraf uitgewisseld te worden.

Componenten voor authenticatie

De digitale handtekening in combinatie met een certificaat vormt de basis voor authenticatie van entiteiten (personen, apparatuur en organisaties) door de koppeling van de publieke sleutel aan een entiteit en de verificatie

van de identiteit. De technieken voor onweerlegbaarheid en authenticatie gaan dus hand in hand, namelijk door gebruik te maken van de digitale handtekening en het certificaat. De digitale handtekening in combinatie met een certificaat kan vergeleken worden met een gewone, met de hand gezette, handtekening.

Authenticatie aan de hand van een certificaat behoort tot de sterke authenticatie middelen, namelijk door multifactor authenticatie, waarbij minstens twee authenticatie vormen worden afgedwongen:

- iets wat je weet vb. een paswoord,
- iets wat je bezit, vb. een token, USB sleutel of certificaat,
- iets wat je bent (een persoonlijke eigenschap), vb. een vingerafdruk of retina scan.

De digitale handtekening moet aan een aantal eisen voldoen:

- De handtekening moet uniek zijn om de maker van de handtekening te kunnen verifiëren.
- De handtekening moet de inhoud van het bericht kunnen authentiseren.
- De handtekening moet door derden kunnen worden gecontroleerd, om eventuele problemen met betrekking tot de onweerlegbaarheid op te lossen.

Om de nodige garanties te kunnen geven zal een derde partij een soort stempel moeten zetten voor het garanderen van de echtheid van de sleutel, en de koppeling van de sleutel aan de juiste persoon. Een voorbeeld uit het niet- elektronische leven is een paspoort. Het aanvragen van een paspoort verloopt via een door de overheid opgestelde procedure. Het paspoort dient bijvoorbeeld in het buitenland als bewijs van de identiteit van de reiziger.

Vaak wordt een apart certificaat gebruikt voor authenticatie, integriteit en onweerlegbaarheid. De door de Belgische federale overheid uitgegeven elektronische identiteitskaart eID werkt op basis van twee certificaten: eentje voor authenticatie (bewijs door middel van een digitale handtekening) en eentje voor integriteit/onweerlegbaarheid (door middel van een wettelijk geldende, want gekwalificeerde digitale handtekening).

Digitale certificaten worden niet alleen gebruikt om personen te authentiseren, maar kunnen ook worden toegekend aan websites en apparatuur, zoals servers, routers, enz. Digitale certificaten kunnen worden onderverdeeld in twee varianten, server- en clientcertificaten:

1. Een **servercertificaat** wordt gebruikt door een server, bijvoorbeeld een webserver, om zich te authentiseren en om een versleutelde verbinding tussen cliënt en server op te zetten.
2. Een **clientcertificaat** wordt gebruikt door een eindgebruiker die dit certificaat kan gebruiken om zichzelf te authentiseren met behulp van dit clientcertificaat.

Om rechtsgeldig te zijn in België moeten digitale handtekeningen voldoen aan de wet van 21 juli 2016, de wet ‘eIDAS en elektronische archivering’ genoemd. Deze wet is een concrete vertaling en invulling van de EU eIDAS verordening. Wanneer een digitale handtekening aan bepaalde eisen voldoet, kan ze “geavanceerd” of “gekwalificeerd” zijn.

Een geavanceerde digitale handtekening:

- Moet op unieke wijze met de ondertekenaar verbonden zijn.
- Moet het mogelijk maken om de ondertekenaar te identificeren.
- Is tot stand gekomen met gegevens voor het aanmaken van digitale handtekeningen die de ondertekenaar, met een hoog vertrouwensniveau, onder zijn uitsluitende controle kan gebruiken.
- Is op zodanige wijze aan de daarmee ondertekende gegevens verbonden zijn, dat elke wijziging achteraf van de gegevens kan worden opgespoord (art. 26 van de eIDAS-verordening).

Een digitale handtekening is **gekwalificeerd** indien zij niet alleen geavanceerd is, maar ook aangemaakt is met een gekwalificeerd middel voor het aanmaken van digitale handtekeningen en gebaseerd is op een gekwalificeerd certificaat voor digitale handtekeningen.[3] Gekwalificeerde elektronische handtekeningen, waarbij een gekwalificeerd certificaat wordt gebruikt, zijn geldig als bewijs en hebben direct wettelijke effect zoals handgeschreven handtekeningen. [4]

Componenten voor onweerlegbaarheid

Een bericht kan versleuteld worden aan de hand van de private sleutel en dan ontcijferd door middel van de bijhorende publieke sleutel. Dit is dus de omgekeerde beweging van encryptie voor vertrouwelijkheid.

Omdat de private sleutel wordt geheim gehouden door de eigenaar ervan, is versleuteling met een private sleutel de basis voor een digitale handtekening - dit is het meest bekende gebruik van asymmetrische cryptografie. Gezien enkel de eigenaar beschikt over de private sleutel, kan hij niet ontkennen dat hij het bericht heeft versleuteld. Onweerlegbaarheid van data wordt dus gegarandeerd.

Indien men de asymmetrische encryptietechniek nog combineert met het gebruik van een message digest/hash, kan men ook nog bericht-integriteit garanderen. Alvorens het bericht te versleutelen d.m.v. de private sleutel, wordt het bericht eerst via een cryptografische hashfunctie gecomprimeerd.

Een digitale handtekening kan gecombineerd worden met asymmetrische encryptie om vertrouwelijkheid van informatie te garanderen. Dit doet men door:

1. De verzender/ondertekenaar plaatst zijn/haar digitale handtekening op het document met de eigen private sleutel.
2. Het volledige pakket wordt (document + handtekening) versleuteld met de publieke sleutel van de bestemmeling om het geheel onleesbaar te maken voor derden. In de praktijk echter zal men voor dit laatste meestal symmetrische encryptie gebruiken omwille van de snelheid ervan.

Tijdens transport en opslag vormt het onopgemerkt wijzigen van berichten (of wijzigen door onbevoegden) een risico. De ontvanger heeft geen garantie dat het bericht integer is en dat het bericht afkomstig is van de identiteit, die als ondertekenaar bij het bericht staat vermeld (onweerlegbaarheid).

[3] art. 3 §12 van de eIDAS-verordening

[4] art. 25 van de eIDAS-verordening

Het plaatsen van een digitale handtekening valt uiteen in twee delen.

1. Vastleggen van de unieke kenmerken van het bericht (in een 'hash').
2. Verbinden van de unieke identiteit van de zender aan de hash.

De mate van zekerheid die uit de toegepaste methode voortvloeit, wordt sterk beïnvloed door de aard en kwaliteit en de toepassing van algoritmen en methoden. Het gaat hierbij vooral om:

- Toevalsgetallen.
- Uniciteit en lengte van sleutels en toegangscodes.
- Sleuteluitgifte-, distributie- en bewaarprocessen en middelen.
- Kwalificatie van de certificaatuitgifte.

Onderstaande tabel geeft aan welke verbanden er bestaan tussen het zekerheidsniveau, de toegepaste sleutels en wie er door zender en ontvanger wordt vertrouwd.

Zekerheidsniveau	**Sleutelmodel**	**Proceskwaliteit**	**Zender en ontvanger vertrouwen:**
1: Laag, onzekere bewaartermijn	Symmetrisch	Gedeelde sleutels	Eigen organisatie of partner
2: Middel, onzekere bewaartermijn	Asymmetrisch	PKI-service of private PKI	Eigen organisatie of partner
3:Hoog ,gegarandeerde bewaartermijn	Asymmetrisch	Gecertificeerde PKI	Overheid of gecertificeerde partij

Data context :

DIU ('data in use')

Gegevens in tijdelijke opslag

Gevoelige gegevens zoals paswoorden en pincodes worden op systeem- of applicatieniveau versleuteld. Dit garandeert dat de waarden daarvan uitsluitend leesbaar zijn voor bevoegde processen.

DIM ('data in motion')

Versleuteling op applicatieniveau

Op applicatieniveau wordt versleuteling door twee met elkaar communicerende systemen end-to-end uitgevoerd. Alleen het dataveld van een pakket wordt hierbij versleuteld. Een bekende vorm van encryptie op applicatieniveau is de secure HTTP-techniek, die gebruikt wordt voor versleuteling van HTTP berichten.

Versleuteling op sessieniveau

Een voorbeeld van versleuteling op sessieniveau is Transport Layer Security (TLS). Deze techniek wordt gebruikt in combinatie met applicatieprotocollen, zoals HTTP(s), FTP(s), IMAP(s), POP(s) en SMTP(s), herkenbaar aan de S. Als TLS is toegepast bij (HTTP), dan wordt per sessie de webcommunicatie versleuteld (HTTPs) en zie je in de statusbalk van de browser een slot-icoontje weergegeven.

Versleuteling op netwerkniveau

Een voorbeeld van versleuteling op netwerkniveau is IPSec. Op basis van dit protocol worden versleutelde communicatietunnels gelegd tussen netwerkeindpunten, waarmee veilige communicatie mogelijk is. Met deze tunnels kunnen Virtual Private Networks (VPN's) worden gebouwd. Draadloze netwerken worden versleuteld met eigen protocollen als WPA (Wi-Fi Protected Access).

De versleuteling eindigt op de netwerkcomponent en is dus niet end-to-end. Als het eindpunt vb. een proxyserver is, dan wordt de communicatie versleuteld tot op de proxy server, maar verloopt verder in klare tekst tot aan de PC van de gebruiker.

Versleuteling op datalinkniveau

De versleuteling vindt plaats op het 'laagste niveau' van het netwerk uitgevoerd tussen twee netwerkknooppunten. Alle data die wordt uitgewisseld, dus ook protocolinformatie is daarbij versleuteld. Een voorbeeld van datalink encryptie is het PPTP-protocol.

DAR ('data at rest')

Gegevens in opslag

De versleuteling van informatie op gegevensdragers vindt plaats op drie niveaus:

1. Encryptie op opslagniveau ('storage'), vaste en mobiele media:
    - Versleuteling van mobiele geheugenmedia, zoals harddisks van laptops, USB-stick, CDROM, Tape of insteek-memorymodules maar ook in geheugens van Pda's en smartphones.
    - Versleuteling van vaste geheugenmedia, zoals harddisk arrays van databases, tape en optische media.
2. Encryptie op database niveau.
3. Encryptie op applicatie niveau.

7.2. Logging

Logging bestaat uit het verzamelen en bijhouden van informatie om systeem- en gebruikersactiviteiten op te sporen en te koppelen aan gebeurtenissen ('events'). Deze informatie wordt op haar beurt gebruikt voor relevante opvolging en dient als controle input voor beveiliging en risico beheersing. Gebruik makend van de juiste tools en procedures kunnen audit logs bijdragen tot de detectie van inbreuken op informatie- en ICT veiligheid, het opsporen van technische problemen en non-conformiteit t.o.v. beleidslijnen.

Monitoring gaat nog een stap verder door (near) real-time opvolging van gebeurtenissen.

In oplopende volgorde van complexiteit bestaat het loggen uit:

- Manuele logboeken,
- Geautomatiseerde audit logs,
- Audit trails.

Manuele logging is het handmatig bijhouden van activiteiten en registratie ervan in een logboek. Deze methode is het meest gevoelig is voor fouten, onregelmatigheden en het ontbreken van activiteiten. Manuele logging is namelijk gebaseerd op de discipline en de capaciteit van de uitvoerder. Het bezoekerslogboek is een goed voorbeeld van manuele logging.

Er worden verschillende geautomatiseerde audit logs erkend:

- Technische logs of systeem logs: hierin worden gebeurtenissen (events) opgenomen zoals het gebruik van technische en functionele beheersfuncties, activiteiten onder beveiligingsbeheer, verstoringen en (veiligheids-)incidenten.
- Applicatie logs: verzamelt gebeurtenissen van een toepassing zoals berichten, uitzonderingen en fouten. Het formaat en de inhoud van deze logs wordt bepaald tijdens de design fase van een toepassing.

Het verwerken van de log informatie, ook weer in oplopende volgorde van complexiteit, bestaat uit:

- Analyse van de audit logs, bij voorkeur a.d.h.v. filtering tools,
- Correlatie van diverse audit logs, al dan niet met externe bronnen,
- (real-time) veiligheidsmonitoring,
- Security incident & event monitoring (SIEM).

Logging als maatregelen

Een audit log is een verzameling chronologische records (een flat file, gestructureerd bestand, database of fysiek logboek). Deze verzameling voert bewijs aan van een activiteit of geheel van activiteiten in een verwerking, procedure of gebeurtenis.

Een audit trail is een beveiligde en geautomatiseerde verzameling chronologische records. Deze verzameling (een flat file, gestructureerd bestand, database of fysiek logboek), laat toe om een reeks gebeurtenissen te reconstrueren volgens hun tijdsstip van voorkomen en gerelateerd aan de aanmaak, wijziging en verwijdering van elektronische records. Dankzij deze structuur is de audit informatie toegankelijker en makkelijker te ontginnen dankzij het gebruik van analyse tools.

Er zijn vele verschillende soorten mechanismen voor logging van componenten die naast elkaar kunnen voorkomen. Voorbeelden van deze mechanismen zijn:

- SYSLOG is een standaard voor computerlogging. De logging is gescheiden tussen systemen die de logging genereren en systemen die de logging opslaan.
- SNMP staat voor Simple Network Management Protocol. Dit protocol kan worden gebruikt voor het besturen van netwerkapparaten. Het protocol voorziet ook in statusmeldingen (traps).
- De Windows Event log is standaard in de Windows-besturingssystemen aanwezig en kan ook naar een centrale logvoorziening worden verzonden.
- Losse logbestanden zoals tekstbestanden, komma gescheiden (CSV) bestanden en andere varianten.
- Vanuit applicaties en binnen databases wordt vaak gelogd binnen de database zelf of een aparte database. Deze logging is doorgaans gestructureerd en ook door te zenden aan een centraal logsysteem.
- Logging van beveiligingssystemen, zoals Intrusion Detection Systems

Om aanvallen efficiënt te kunnen detecteren is het belangrijk de log informatie op één centraal punt op te slaan, hierdoor heeft men een duidelijk zicht op alle informatie vanuit de verschillende componenten. De voordelen van centraal loggen zijn:

- Gebruiksgemak: Er hoeft maar op één plaats gekeken te worden.
- Beschikbaarheid: De logging is beschikbaar, ook als het systeem dat logt niet beschikbaar is.
- Veiligheid: De logging is ook beschikbaar als het bronsysteem gehackt of besmet is.
- Veiligheid: De logging kan worden afgeschermd tegen onbevoegd inzien en modificatie, bijvoorbeeld door digitaal ondertekenen.
- Eenvoud: Een centrale logging is eenvoudiger veilig te stellen op bijvoorbeeld een back-up.
- Automatische analyse van logbestanden geeft sneller de samenhang van incidenten weer en maakt het mogelijk om logische verbanden tussen geïsoleerde incidenten te detecteren.

Toch is ook lokaal loggen interessant. Op deze manier kan men immers de coherentie en consistentie van de log informatie garanderen. De log informatie moet dan minstens zolang lokaal worden bijgehouden tot men een bevestiging krijgt van goed ontvangst van de log informatie door het centrale opslag systeem.

Auditeerbare gebeurtenissen

Hiermee worden de geïdentificeerde activiteiten voor logging bedoeld:

- succes en falen van aanloggen,
- succes en falen van authenticatie,
- succes en falen in autorisatie,
- succes en falen in het uitvoeren van geprivilegieerde activiteiten,
- succes en falen in toegang tot bestanden, folders, toepassingen en systeemtools,
- succes en falen in toegang tot functionele en technische beheersfuncties,
- creatie, wijziging, verwijdering van accounts, bestanden, folders,
- creatie, wijziging, verwijdering van systeem parameters (inclusief database),
- creatie, wijziging, verwijdering in policies,
- creatie, wijziging, verwijdering in toegangsparameters zoals rechten en privileges,
- systeem- en toepassingsactiviteiten zoals shutdown, reboot, fouten,
- wijzigingen aan systemen en toepassingen.

Daarnaast moet men de nodige drempelwaarden (‘thresholds’) definiëren, waarmee wordt bepaald vanaf welke grens een auditeerbare gebeurtenis wordt aanzien als een (potentieel) incident.

Inhoud van audit records

Audit records moeten voldoende informatie bevatten om weer te geven welke gebeurtenis heeft plaats gevonden, wat de oorzaak en wat de gevolgen zijn. Daarnaast moet het mogelijk zijn om elke menselijke interventie in verband met een gebeurtenis te identificeren.

Een correct geïmplementeerde log moet antwoord kunnen bieden op volgende vragen:

- wat gebeurde er?
- Wanneer gebeurde het?
- Waar gebeurde het?
- Wie was betrokken?
- Waar komt het vandaan?

Concreet betekent dit voor het opzetten van een succesvolle audit trail:

- datum en tijdsstip,
- userid/domein, herleidbaar tot een persoon, systeem, locatie,
- bron IP of toepassing,
- gebruikte toepassing, URL of service,
- gebruikte module of functie,
- uitgevoerde actie (creatie, wijziging, consultatie, verwijdering),
- dataveld gewijzigd of geconsulteerd.

Monitoring als maatregelen

Security monitoring bestaat uit het verzamelen en analyseren van informatie teneinde verdacht gedrag of niet-geautoriseerde toegang en activiteiten te detecteren, hierop alarmen te genereren en actie te ondernemen.

Een bijzondere vorm van security monitoring is SIEM: hierbij gaat men diverse bronnen raadplegen om op basis van deze informatie en de correlatie ervan verdacht gedrag of niet-geautoriseerde toegang en activiteiten te detecteren, hierop alarmen te genereren en actie te ondernemen.

Deze maatregelen onderscheiden zich van de logging als maatregelen door de nood aan gespecialiseerde tools en kennis om monitoring te kunnen implementeren. Als dusdanig worden ze dan ook voorzien als maatregel na risico analyse.

Security monitoring

Security Monitoring is een samenspel van mensen, processen en techniek. Er is techniek nodig om zichtbaar te maken wat er in gebeurt op gebied van informatie veiligheid. Daarna zijn er analisten nodig om gebeurtenissen te analyseren en om daar opvolging aan te geven.

Wat er precies door security monitoring wordt opgevolgd, wordt in principe bepaald door een risico-analyse. Die risico-analyse laat zien welke assets kritiek zijn en welke minder kritiek zijn. Aan de hand daarvan kan bepaald worden welke logging of alarmen relevante informatie kunnen opleveren rondom die assets. Als een risico-analyse is uitgevoerd, kan er een kwalificatie toegekend worden aan de assets en bepaald worden wat wel en niet is toegelaten met die assets. De logging en alerting rond die assets en die van de maatregelen leveren relevante informatie op rondom de gebeurtenissen die plaatsvinden richting die assets. Een verzameling maatregelen en

assets kunnen bijvoorbeeld zijn: een active directory, een firewall, een intrusion detection systeem, de antivirus software en de logging van de betrokken assets.

Security monitoring bestaat er dan verder in om de relevante informatie te verzamelen, te analyseren en op te volgen. Zo kunnen kwetsbaarheden, verdachte activiteiten en potentiële en effectieve veiligheidsincidenten in het oog worden gehouden en waar nodig wordt dan actie genomen. Er kunnen ook trends geanalyseerd en gerapporteerd worden om preventieve acties te identificeren en in te plannen.

SIEM

Een SIEM oplossing biedt de mogelijkheid om informatie uit andere bronnen te gebruiken, b.v. AD en e-mail logs, perimeter security logs, enz. Deze informatie wordt gebruikt om veiligheidsincidenten op te sporen. Het extraheren van incidenten uit logs is wat SIEM-systemen op een geautomatiseerde manier beloven te doen.

Een SIEM-oplossing voorziet in continu loggen en real-time monitoren van beveiligingsmaatregelen en alarmen veroorzaakt door afwijkend gedrag. Daarnaast wordt ook lange termijn opslag van log informatie en historische/trend analyses en koppeling met incident beheer en forensisch onderzoek.

SIEM is samengesteld uit een aantal security oplossingen:

- Log management: verzamelen en opslaan van log informatie van systemen en toepassingen;
- Security event management (SEM): real-time monitoring van gebeurtenissen rond informatieveiligheid;
- Security information management (SIM): legt zich toe op opslaan van informatie, analyse en rapportering;
- Security event correlatie (SEC): correlatie van de verzamelde informatie.

Vanuit diverse bron systemen wordt informatie verzameld en verwerkt door de SIEM oplossing:

- Audit records worden verzameld uit de diverse bron systemen,
- Audit records worden in een bepaald formaat gebracht voor verdere verwerking,
- De informatie wordt verrijkt vanuit andere bronnen (bv. AD voor linken van accounts aan gebruikersinformatie zoals naam, afdeling, locatie, …),
- Informatie wordt geaggregeerd en gecorreleerd,
  Analyse en rapportering.

  Implementatie van een SIEM heeft de meeste toegevoegde waarde als aan twee voorwaarden is voldaan:
- Er moet een solide logging basis zijn,
- Er moeten goede use-cases uitgewerkt worden.

7.3. Maatregelen voor IAM

Identificatie als maatregel

Identificatieprocessen zijn processen die instaan voor het bepalen van de identiteit van een persoon. Een voorbeeld is het intypen van de gebruikersnaam om een persoon ten overstaan van een computer te identificeren, of het meesturen van het netwerkadres van de afzender van een elektronisch bericht om de identiteit van de afzender bekend te maken aan de ontvangende computer.

Identificatieprocessen kunnen opgesplitst worden in twee grote groepen op basis van de kenmerken: zwakke en sterke identificatie.

Zwakke identificatie

Validatie van de identiteit van een fysiek persoon zal plaatsvinden op basis van een identiteitsattribuut dat niet onder controle valt van een door de overheid geregistreerd of gecertifieerde bron. Dit kan gaan over een emailadres, een telefoonnummer, enz. De gebruikte identiteit attributen komen meestal van een al dan niet commerciële organisatie. Op deze manier biedt de verificatie procedure onvoldoende waarborg over de identiteit van het betrokken individu (Risico op identity spoofing).

Sterke identificatie

Identificatie zal plaatsvinden op basis van een door de Belgische federale overheid geregistreerd of gecertifieerde bron (Identity provider). Vandaag kan enkel de Federale overheid een sterke validatie van een identiteit uitvoeren om te voldoen aan de kenmerken van een sterke identificatie. De unieke identificatie labels van een identiteit (Fysiek persoon) zijn:

- Rijksregisternummer (Ook gekend als RRN)
- Rijksregister-BIS nummer (Ook gekend als BIS-Nummer)

Identificatie van buitenlandse identiteiten

De uitwisselbaarheid van identiteiten van buitenlandse individuen, ook binnen de EU is opgevangen door de registratie van het individu in het RijksRegister-BIS.

Erkende afgeleide bronnen voor sterke identificatie

De Belgische federale overheid maakt gebruik van een aantal erkende afgeleide bronnen zoals INSZ en ItsMe®.

Authenticatie als maatregel

Het is echter relatief makkelijk om een identiteit te vervalsen. Het is dus nodig dat de identiteit niet alleen bepaald maar vervolgens ook geverifieerd wordt. Authenticatie, ook wel bronauthenticatie genoemd, is het verifiëren van de identiteit van een persoon. Men maakt hiervoor gebruik van een uniek kenmerk, specifiek verbonden aan de identiteit die geverifieerd wordt.

Factor authenticatie

Wat verstaat men onder factoren?

Bij de authenticatie van een persoon bestaat het unieke kenmerk uit een of meer persoonsgebonden gegevens (factors). We kunnen daarbij de volgende persoonsgebonden gegevens onderscheiden:

- Iets wat je kent, een wachtwoord of pincode
- Iets wat je hebt, bijvoorbeeld een pinpas of smartcard
- Iets wat je bent, verwijzend naar biometrische gegevens, zoals je vingerafdruk

Single factor authenticatie

In zijn meest eenvoudige vorm gebruiken we éénfactor-authenticatie vrijwel elke dag onder vorm van een toegangsbadge tot onze gebouwen, maar ook onder een veiliger vorm: onze toegang tot het werkstation door gebruik te maken van een gebruikersID met bijhorend wachtwoord.

Éénfactor authenticatie verwijst naar de unieke wijze op basis van waarop de identiteit gevalideerd kan worden:

- Voor de validatie tot toegang voor een gebouw zal het toegangscontrole systeem de toegang enkel valideren op iets dat in het bezit is van de gebruiker
- Bij de toegang tot het werkstation door middel van een gebruiker ID en paswoord zal de controle enkel gevalideerd worden op basis van iets wat de gebruiker weet

Het probleem bij het gebruik van enkelvoudige factoren, is dat deze niet altijd voldoende garantie biedt om een identiteit te verifiëren. Om een betere garantie te geven bij het afschermen van informatie is het sterk geadviseerd om minimaal bijkomende maatregelen te nemen die het risico op misbruik kan verminderen.

Multifactor authenticatie

Bij de Belgische federale overheid ligt de focus vooral op (multi)factor authenticatie.

Multifactor baseert zich bij de validatie van een identiteit op meerdere factoren door deze factoren te combineren in het authenticatieproces. Het bekendste voorbeeld van het toepassen van een multifactor-authenticatie is de creditcard (iets wat je hebt) en de bijhorende pincode (iets wat je kent). Het authenticatie proces gebruikt daarbij twee factoren om de identiteit van een gebruiker vast te stellen.

Een belangrijk concept hierbij is dat multifactor uitgaat van twee los van elkaar bestaande factoren. Gebruiker ID en paswoord bevinden zich beide in dezelfde factor klasse (iets dat je weet) en worden dus niet beschouwd als multifactor.

- Tweefactor-authenticatie gaat uit van meerdere factoren.
- Tweetraps-authenticatie baseert zich op twee uit te voeren authenticatie stappen met een gelijkwaardige factor. (vb. 2x met iets dat men ‘weet’)

Tweefactor-authenticatie is dus altijd tweetraps-authenticatie (want gaat over twee stappen), maar andersom is tweetraps-authenticatie niet altijd tweefactor-authenticatie (want er kan ook één factor worden gebruikt)

Van identiteit tot Account

Om de identiteit van een individu te bewijzen heb je in de eerste plaats een authentieke bron nodig, een gecontroleerd en betrouwbaar identiteitsregistratieproces dat toelaat de identiteit van een individu te registreren.

Identiteiten worden gecentraliseerd in het rijksregister en rijksregister-BIS van de Belgische federale overheid maar deze identiteiten zijn niet rechtstreeks bruikbaar als authenticatiemiddel. Een gebruiker kan niet simpelweg verwijzen naar dit registratieproces om zijn identiteit te bewijzen. Daarom krijgt het individu een 'middel', dat door iedereen en elke organisatie, op zich erkend word als identiteitsreferentie. Namelijk een identiteitsbewijs (inclusief paspoorten, geboortebewijzen, …). De Belgische identiteitskaart (eID) is het referentiemiddel voor de burger. Het is echter beperkt inzetbaar als authenticatie bij interactieve identificatie tussen fysieke personen en integratie met de federale CSAM diensten.

Om de beperkingen in gebruik van ons identiteitsbewijs weg te werken gebruikt de Federale overheid een toegangsbeheer systeem, dat toelaat om aangepaste authenticatie middelen aan een identiteit te koppelen, zodat de gebruiker op een aangepaste manier toegang kan krijgen tot applicaties en diensten. Dit authenticatiemiddel noemt men een account. Het account heeft steeds een relatie met een identiteit van een fysiek persoon.

De vorm waaronder een account zich voordoet is volledig afhankelijk van de gebruikte technologie. Het Belgische eID ondersteunt zowel fysieke als elektronische authenticatievormen.

Account lifecycle

Een 'lifecycle' beschrijft alle processen, criteria en doelstellingen van het betrokken object, in dit geval het account object.

Aanmaak van accounts

Het aanmaken van een account wordt bepaald op basis van de aanwezige motivatie van een individu om toegang te krijgen. Hieruit volgt dat personen die niet geacht worden toegang te hebben tot diensten of informatie geen beschikking mogen hebben tot een (actief) account.

Status van een account

Een account is actief wanneer het technisch de mogelijkheid bied om gebruikt te worden als authenticatiemiddel**.** De criteria om een actief account te beschouwen zijn afhankelijk van de vorm waarin het account werd aangeleverd**.** Een account is echter inactief wanneer het op basis van de criteria uitgesloten werd als actief account

Controle maatregel

Na het inventariseren van alle bestaande accounts, inclusief het type en bijhorende categorie met volgende indicatoren, kan men de accounts controleren:

- Slapend(e) account(s): Het account is niet meer gemotiveerd indien het niet werd gebruikt in de laatste 13 maand. De status actief, of inactief heeft geen invloed op de 'slapende' toestand van het account
- Ongemotiveerd(e) account(s): Het account is niet gekoppeld aan een gevalideerd identiteit van een fysiek persoon
    - Toepassingen en systemen kunnen technisch gezien ook gebruikt worden als identiteiten. In IAM context koppelen we accounts echter steeds aan een fysiek persoon
    - Het is toegestaan koppelingen te maken via een toepassing, waarachter onrechtstreeks een koppeling plaatsvindt met een fysiek persoon, onder vorm van een 'toepassingsbeheerder'.
    - Inactief(ve) account(s): De accounts zijn technisch niet in staat deel te nemen aan een authenticatie proces.
        - Een account kan bvb tijdelijk geblokkeerd of slechts gebruikt tijdens bepaalde uren (bv. kantooruren).
    - Ongecontroleerd(e) account(s): Het account voldoet niet aan de minimale technische vereisten van de paswoordpolicy die werd toegekend aan de account categorie of –type
        - Leeftijd van het paswoord
        - Complexiteit van het paswoord
        - Omkeerbare encryptie van het paswoord
        - Geen paswoord
        - …

Provisioning

Provisioning is het deelproces dat wordt gebruikt voor alle activiteiten die leiden tot het verstrekken van een account aan een geïdentificeerd persoon. Afhankelijk van de implementatie van het proces worden accounts actief of inactief aangeleverd aan de rechtmatige persoon. Bij de aanlevering van inactieve accounts zorgt het provisioning proces voor een geautoriseerd en gedocumenteerd activatie (sub)proces.

De-provisioning

De-provisioning is het deelproces dat er voor zorgt dat een account niet langer ter beschikking voor een eindgebruiker als bruikbaar authenticatiemiddel.

- Afhankelijk van de vorm van het authenticatiemiddel en|of de-provisioning methodiek spreekt men van verwijderen, deactiveren (blokkeren), revoke (weigering), …

De-provisioning kan in één of meerder stappen worden uitgevoerd. Gefaseerde de-provisioning processen wordt steeds ondersteund door geïdentificeerde behoeften aan het account lifecycle proces.

- Een account al dan niet tijdelijk deactiveren, vooraleer effectief te verwijderen is afhankelijk van de behoefte om dit account op een later tijdstip te heractiveren.
- Indien accounts op basis van geïdentificeerde regelgeving niet effectief verwijderd mogen worden zal deze behoefte expliciet opgenomen zijn in de beschrijvende procesdocumentatie.

Betrouwbaarheid van het authenticatieproces

De maatregelen genomen in het account registratie proces worden verder uitgebreid met een aantal technische maatregelen die het dupliceren en oneigenlijk gebruik van een account moeten voorkomen. Men spreekt over de vertrouwelijkheidsgraden van de authenticatie.

Op Europees vlak werden een aantal afspraken gemaakt in verband met deze authenticatie vertrouwelijkheidsgraden. De eID.AS authenticatie vertrouwelijkheidsgraden zorgen ervoor dat authenticatieplatformen van de individuele Europese lidstaten op een uniforme, gestandaardiseerde manier aangeven welke kwaliteitseisen ze stellen aan de vertrouwelijkheid van een authenticatie verzoek.

Deze vertrouwelijkheidsgraden worden onderverdeeld in 3 eID.AS LoA schalen

- High: Hoge vertrouwelijkheid van het authenticatieproces, of sterke authenticatie
- Substantial: Substantiële vertrouwelijkheid van het authenticatieproces, of betrouwbare authenticatie
- Low: Lage vertrouwelijkheid van het authenticatieproces, of zwakke authenticatie

We gaan in dit document niet verder in detail betreffende de eID.AS authenticatie vertrouwelijkheidsgraden.

Autorisatie als maatregel

Autorisatie is het toekennen van rechten aan personen en aan de processen die ten behoeven van deze personen geïnitieerd worden. Hiermee krijgen personen vervolgens toegang tot bepaalde gegevens en functies. Concreet is het de toestemming tot gebruik van een dienst of applicatie. Men maakt onderscheid tussen:

- Toegangsbeheer, (Het proces) als organisatorische maatregel.
- Toegangscontrole (De techniek) als technische maatregel.
- Scheiding van functies (Het principe) als organisatorische controle maatregel

Toegangsbeheer als maatregel

Autorisatie is gebaseerd op toegangsprofielen, waarin verduidelijkt wordt welke personen toegang hebben tot welke gegevens en functies. Het gaat hier dus om een organisatorische maatregel die steunt op een toegangsbeleid. Dit proces legt uit, hoe en onder welke omstandigheden een individu toegang krijgt tot de organisatiemiddelen. Volgende attributen zijn aanwezig in het toegangsbeheer om een auditeerbaar proces te garanderen:

Beschikbare informatie bij de verwerking van een toegang

- Basis attributen van het verzoek tot toegang (Datum, tijd, aanvrager, volgnummer, …)
- Onderwerp, als referentie naar het individu die de toegang wenst te gebruiken
- Motivatie van het verzoek en de bevestiging van de motivatie
- Basis attributen van het validatie van de toegang (Datum, tijd, …)
- Identiteit van de persoon die de goedkeuring(en) geeft
- Vervaldag van het toegangsrecht, afhankelijk van de categorie van de verwerkte informatie binnen de dienst of toepassing
- Periodiek herhaalde (her)validatie van een recht, afhankelijk van de categorie van de verwerkte informatie binnen de dienst of toepassing

Toegangscontrole als maatregel

Toegangscontrole is een set van technische maatregelen die steunen op de technische specificaties van de toegepaste technologie. Bij het aanmelden aan een toepassing of dienst zal de identiteit (authenticatie) gevalideerd worden, waarbij de technische afhandeling van het validatieverzoek afhankelijk is van de gebruikte technologie. Afhankelijk van de gebruikte methode zal datzelfde authenticatieplatform bepalen welke autorisaties er aan het betrokken individu (op basis van zijn account of gekoppeld recht) worden toegekend.

Voorbeeld(en) van authenticatieplatformen:

- LDAP authenticatie valideert enkel het account. Een toepassing zal, via code, steeds een bijkomende validatie af handelen om groep lidmaatschap te valideren.
- Een ACL (Access Control List) op een bestand, folder of disk zal gevalideerd worden door het disk subsysteem op basis van de ACE (Access Control Entry) op het betrokken object.

De toegangscontrolemaatregel moeten echter in lijn zijn met de toegangsbehoefte van de specifieke rol, tot de verwerkte informatie. We suggereren het 'least access privilege' principe te volgen en toegangen voor eindgebruikers te scheiden van de toegangen voor beheer.

Functiescheiding als maatregel

Functiescheiding is een organisatorische controle maatregel. Het implementeert een passend niveau van scheiding van rechten als een veiligheidsprincipe. Men gaat dan taken en bijbehorende rechten voor een specifiek bedrijfsproces over meerdere organisaties, rollen, individuen en/of accounts verspreiden.

Er zijn verschillende benaderingen voor functiescheiding:

- Sequentiële scheiding (twee handtekeningen principe)
- Individuele scheiding (vier ogen principe)
- Ruimtelijke scheiding (afzonderlijke rechten op afzonderlijke accounts)
- Faculteit scheiding (verschillende factoren dragen bij tot voltooiing)

Enkele voorbeelden in praktijk zijn:

- Gescheiden beheer van sleutelbeheer en encryptie implementatie
- Gescheiden accounts voor eindgebruiker applicatie toegangen en beheer accounts
- Gescheiden rollen toegangsbeheer, toegangsaanvragen en (re)validatie

7.4. De informatiebeveiliginsmaatregel PAM

PAM of 'Privileged Access Management' is een strikte toepassing en opvolging van een aantal basis processen. In dit document zal het belang van de verschillende processen voor het PAM proces, besproken worden. Het gaat om de volgende basis processen:

- Beheer van wijzigingen binnen de informatieverwerking of 'Change management'
- Beheer van configuraties binnen de informatieverwerking of 'Configuration management'
    - Het configuratiebeheer bevat naast de informatieverwerking configuratie ook alle details over de toegangsmogelijkheden tot de informatieverwerking
- Identiteit en toegangsbeheer of 'Identity & Access Management (IAM)'
- Log beheer of Log management
- Risico beheer of risk management op basis van rapportering van operationele risico's op basis van historiek informatie uit bovenstaande processen of operationeel risk management (ORM).

Change management als maatregel

Het change management proces vormt een invulling van de criteria 'Motivatie' en 'Goedkeuring', die van belang zijn voor het 'PAM' proces.

Het 'change management proces' verzamelt alle elementen, van zowel de organisatorische behoeften als de technische behoeften. Bovendien motiveert dit proces de noodzaak van bevoorrechte toegang tot de technische componenten. Eventueel kan het ook gaan om de toegang tot verwerkte informatie tijdens de beheerstaken. Dit proces zorgt dus voor de nodige validatie en toestemming ter begeleiding van deze beheersactiviteiten.

Concreet helpt dit proces ons om wie/wanneer/waarom te identificeren bij elke vraag tot een bevoorrechte toegang tot een informatie verwerking component, alsook wie/wanneer de nodige autorisatie(s)/goedkeuring(en) heeft gegeven.

Identity & Access Management als maatregel

Het Identity & Access Management proces vult volgende criteria in die van belang zijn voor het 'PAM' proces:

- Identity management: identificeert elk fysiek persoon die deelneemt aan een PAM proces
- Access management:
    - Draagt bij aan de authenticatie behoeften.
    - Draagt bij aan de behoeften voor toegangsbeheer.

Het configureren van maatregelen op het technische component (access control) is ingevuld via het proces configuratie beheer. 'Least access' implementatie vindt plaats op basis van accounts en de daaraan gekoppelde rollen.

Configuratie beheer als maatregel

Het configuratie beheersproces controleert de implementatie parameters en omvat o.a.:

- De toegangscontroles, aanwezig bij correct toegangsbeheer:
    - Wat zijn de functionele verwachtingen die worden ingevuld door de betrokken toegangscontroles (Least access principe is een noodzaak)?
    - Hoe zijn de verschillende toegangsrollen technisch uitgewerkt?
    - Hoe wordt implementatie van deze toegangscontroles gecontroleerd?
    - …
- Log configuratie, deze worden gebruikt als basis element in de context van auditeerbaarheid van de operationele informatieverwerking:
    - Wat zijn de functionele verwachtingen die worden ingevuld door de betrokken log configuratie?
    - Hoe is deze configuratie technisch uitgewerkt?
        - Operationele opvolging op basis van rapporten?
        - Operationele opvolging op basis van alerts (real-time mogelijk)?
    - Welke correlatie, interpretaties van log informatie resulteren in aantoonbare controle

Log management als maatregel

Log management verzameld bron materiaal, zowel uit technisch als operationele bronnen. Dit bron materiaal zal dan gebruikt worden om de nodige controle maatregelen mogelijk te maken.

- Het laat toe om log informatie uit verschillende bronnen te combineren om inzicht te krijgen op operationele risico's (Risico beheer)
- Het laat toe om in geval van een incident bij informatieverwerking een reconstructie van de verwerkingsactiviteiten te maken
- …

We maken onderscheid tussen volgende bronnen als log informatie: (Onderstaande opsomming van maatregelen is niet beperkt tot deze voorbeelden)

- Technische bronnen
    - Her configuratie beheer proces garandeert de correcte log configuratie parameters.
        - Log entries in bestanden of databases afkomstig uit systemen, middleware en toepassingen. (Vb. Security log Windows)
        - Geautomatiseerde (4EYES) controle van de beheersactiviteiten (Session recording) van de beheersactiviteiten (Niet geautomatiseerde controles worden gezien als organisatorische controle maatregelen)
            - Dit omvat ook de garantie op de beschikbaarheid van deze informatie door middel van archivering of retention. (Technische uitwerking van de 4EYES controle)
- Organisatorische bronnen
- Change management: Operationele log van alle change registraties in het change management proces of tool
- Operationele opvolging van de activiteiten: Opname van alle activiteiten die manueel worden uitgevoerd door een onafhankelijke fysieke persoon, binnen een beheer sessie.
    - Deze 'fysieke' logboeken worden conform de behoeften van een geautomatiseerd systeem, geregistreerd en gearchiveerd voor potentiele audit doeleinden.
- …

Het wordt geadviseerd om de verwerking van de controle maatregel te optimaliseren d.m.v. het automatisch verzamelen van de logs.

Risico beheer als maatregel

Deze maatregel is een deel van het operationeel risico beheer verbonden aan de informatieverwerking. Rapportering en de operationele opvolging van deze rapporten zijn een belangrijke bron van bewijs. De organisatie toont hiermee aan dat er effectieve opvolging plaats vindt op de activiteiten van de informatieverwerker en dat alle maatregelen die genomen werden resulteren in een correcte limitering van de overige risico's.

Basis rapportering operationeel risico beheer, gebruikt binnen PAM

Onderstaand type rapportering is aanwezig in de generieke context van de informatieverwerking en worden niet specifiek hernomen in context van PAM

- Beschikbaarheid bronnen (Output van Log beheer)
- Beschikbaarheid van de noodzakelijke bronnen verzekeren, deze bronnen zijn noodzakelijk zijn om de rapportering en opvolging te garanderen
- Interpretaties van technische log informatie op basis van technische criteria - Voorbeeld: Failed paswoord pogingen, account lockout, slapende accounts, Paswoord reset, …
- Interpretaties van organisatorische log informatie op basis van organisatorische criteria - Voorbeeld: Workflow validatie door onbevoegden
- …

Rapportering in functie van PAM

Proces anomalieën

- Proces anomalieën worden opgespoord op basis van de correlaties van informatie uit verschillende processen of hun ondersteunende technische platformen

Configuratie anomalieën

- Configuratie anomalieën worden opgespoord op basis van de correlaties van informatie uit het PAM proces en de technische log uit de informatie verwerkingscomponenten

7.5. Datatypes voor de beveiliging van persoonsgegevens

Data types van de Informatiecategorie 0

Er werden geen standaard data types gerelateerd aan persoonsgegevens, geïdentificeerd in de Informatiecategorie 0

Data types van de Informatiecategorie 1

Contactgegevens

Deze categorie van persoonsgegevens omvat enkel informatie die toelaat contact te nemen met een individu in professionele context. Deze contact informatie is beperkt tot de directe en unieke relatie met de Vlaamse overheid.

- Naam en Voornaam
- Professionele adresgegevens
  (Gebouw, straat, nummer, bus, postcode en gemeente)
- De organisatie waarvoor het individu zijn professionele opdracht uitvoert
- De functie binnen de organisatie
- Telefoonnummer vaste lijn. Er is geen onderscheid op basis van technologie (Analoog/digitaal)
  (Inclusief SoIP/VoIP/ToIP/Mobiele telefonie/Fax)
- Email adres
- Contact foto
- (persoonlijke) Professionele sociale media contact referenties
  (Facebook, Google+, LinkedIn)

Data types van de Informatiecategorie 2

Persoonlijke contactgegevens

Deze categorie van persoonsgegevens omvat enkel informatie, uitgesloten door categorie 1, die toelaat contact te nemen met een individu.

- Naam en Voornaam
- Adresgegevens
  (Gebouw, straat, nummer, bus, postcode en gemeente)
- Telefonie referenties: Vaste lijn, GSM, FAX
  (Inclusief SoIP/VoIP)
- Email adres
- Persoonlijke sociale media contact referenties
  (Facebook, Google+, LinkedIn)

Identificatiegegevens

Deze categorie van persoonsgegevens omvat enkel informatie die toelaat om een individu uniek te identificeren.

- Identificatiegegevens uitgegeven door de overheidsdiensten: identiteitskaartnummer, paspoortnummer, VoID, rijbewijsnummer, pensioennummer, nummerplaat persoonlijk(e) voertuig(en)
- Identificatiegegevens uitgegeven door de werkgever: Personeelsnummer.
- Technische accountnamen, onafhankelijk de vorm waarin ze voorkomen: badge nummer, UserID, email adres, telefoonnummer, …
- Elektronische identificatiegegevens: MAC-adressen, IP-adressen, cookies en gelijkwaardige unieke identificatiesleutels van toestellen.

Persoonlijke kenmerken

Dit data type bevat de persoonlijke kenmerken van het individu:

- Geslacht, geboorte- en overlijdensdatum en afgeleide informatie
- Geboorteplaats en nationaliteit.
- Burgerlijke staat

Consumptiegewoonten

Deze categorie van persoonsgegevens omvat informatie in verband met de consumptie van goederen en diensten, aangeboden door de Federale overheid.

- Persoonlijke prijsvragen, offertes, bestellingen, facturen, aankooptickets en tickets
- Logging gebruik toepassingen bij de federale overheid

Woningkenmerken

Informatie en kenmerken in verband met eigenaars, bewoners, gerelateerde fiscale informatie en fysieke kenmerken van het gebouw.

- Kadastrale basisgegevens: Adres, aard van de woning
- Fiscale kenmerken, waaronder kadastraal inkomen
- Energie prestatie certificaten
- Ouderdom woning
- Identiteit van de eigenaar
- Duur van de verblijfsstatus in relatie met de woning
- Personen met toegang tot private gebouwen
- Gebruiksrelatie van de bewoners (huur/…/koop)
- Woningtype (rijtjeswoning/…/vrijstaand)
- Staat van onderhoud (goed/slecht/gerenoveerd)
- Fysieke kenmerken (Groote van het gebouw/binnenruimtes/plan)
- Openstaande administratieve activiteiten

Opleiding, ervaring en vorming

- Interesse, Informatie en kenmerken van opleiding en vorming in relatie tot een individu.
- Academische loopbaan, overzicht van de betrokken scholen, academische instellingen en universiteiten
- Overzicht van de behaalde diploma's en beroepsbekwaamheden en licenties
- Ervaringsbewijzen (Professioneel en interesse)
- Lidmaatschap beroepsorganisaties en uitgeoefende functies
- Publicaties
- Interne vorming (tot functie)

Beroep en betrekking.

- Actuele en historische betrekkingen en beroepen
- Actuele en historische relatie tot de werkgever, incl. werkgever, professionele titel, functiebeschrijving, uitgeoefende functies, graad, aanwervingsdetails, werkplaats, specialisatie en type onderneming
- Militaire situatie
- Interesse, Informatie en kenmerken van het beroep en relaties tot werkgevers in relatie tot een individu
- Openbare mandaten
- Alle overheden, gemeente, provinciën gewest en federaal
- Deelname aan overheidscomités
- Deelname aan werk- en bezinningsgroepen

Vrije tijd besteding en interesses

Deze categorie van persoonsgegevens omvat enkel informatie die toelaat de vrije tijd en interesses van het individu te identificeren.

- Lidmaatschap van vereniging zonder raciale, etnische, religieuze of politieke achtergrond
- Functie binnen een vereniging zonder raciale, etnische, religieuze of politieke achtergrond

Rijksregisternummer(-BIS) / Identificatienummer van de sociale zekerheid.

Het gebruik van het rijksregisternummer(-BIS) is **minimaal ondergebracht in informatiecategorie 2** als gevolg van het wijdverspreid gebruik als unieke sleutel bij verwerking van persoonsgegevens. Dit maakt dat het rijksregisternummer(-BIS) kan gebruikt worden om via correlatie tussen datasets, (context) gevoelige informatie te onthullen.

Data types van de Informatiecategorie 3

Financiële en fiscale gegevens

Dit dataelement beschrijft de financiële en fiscale gegevens van het individu:

- Financiële identificatiegegevens: identificatie- en bankrekeningnummers, nummers van krediet- en debet kaarten
- Lasten, Inkomsten, bezittingen, investeringen, pensioen en alle detail en afgeleide informatie
- Schulden, uitgaven, huurgelden, kredieten (Incl. Leningen en hypotheken) en alle detail en afgeleide informatie
- Beoordelingen financiële toestand en statuten (Incl. Solvabiliteitsstudie en evaluatie)
- Uitkeringen, hulp, giften en subsidies
- Verzekeringsproducten incl. alle detail en afgeleide informatie
- Financiële transacties incl. alle detail en afgeleide informatie
- Overeenkomsten, schikkingen en compensaties incl. alle detail en afgeleide informatie
- Vergunningen incl. alle detail en afgeleide informatie
- Grond, eigendommen en andere bezittingen

Informatie en kenmerken van fiscale en financiële diensten, voordelen en goederen in relatie tot een individu.

Leefgewoonten

- Gebruik van genotsmiddelen (tabak, alcohol, verdovende en stimulerende middelen)
- Bijzonderheden betreffende het gebruik van goederen en diensten aangeboden buiten de Vlaamse overheid
- Bijzonderheden betreffende reizen en verplaatsingen
- Sociale contacten, andere vetrekkingen dan die met verwanten
- Lidmaatschap van vereniging, andere dan professionele, filosofische, politieke of vakbondsmaatschappen
- Gebruik van media en communicatiemiddelen

Fysieke kenmerken, Medische of psychische gegevens en behandelingen

- Algemeen overkoepelende kenmerken en behandelingen:
  - Risicosituaties
  - Handicap en/of gebrek
  - Diëten en andere aangepaste leefpatronen

- Bijzondere vereisten in verband met fysieke, psychische of medische behandelingen van een verplaatsing of woning
- Genetische gegevens in het kader van familiaal erfelijkheidsonderzoek
- Gegevens met betrekking tot zorg, incl. gebruikte middelen en procedures voor medische en paramedische zorg

➢ Fysieke kenmerken:

- Medische gegevens en behandelingen
- Psychische gegevens en behandelingen
- Lichaamslengte, lichaamsgewicht
- Huidskleur, haarkleur, kleur van de ogen
- Onderscheidende fysieke kenmerken

➢ Psychische gegevens:

- Onderzoeken, diagnoses en rapporten
- Behandelingen en medicatie
- Karaktereigenschappen
- Risicogedrag

➢ Medische gegevens:

- Onderzoeken, diagnoses en rapporten
- Behandelingen en medicatie

Samenstelling van het gezin

- Samenlevingsvormen
- Data in relatie tot de actuele en historische samenlevingsvorm (partner, huwelijksdatum, datum samenlevingscontract en verbreking relatievorm)
- Relatie met andere rechtstreekse verwanten (Kinderen, ouders en afstammelingen)
- Aantal kinderen
- Bijzonderheden in relatie tot bloedverwanten in zijlijn en adoptie en pleegouders

Juridische en gerechtelijke gegevens

- Klachten, incidenten en ongevallen
- Detailinformatie met betrekking tot het individu in context van klachten, incidenten, ongevallen
- Detailinformatie met betrekking tot gerechtelijke onderzoeken en conclusies
- Verdenkingen en inbeschuldigingstelling, verdenking van inbreuken
- Samenspanning en relatie van verdachte en veroordeelde individuen
- Onderzoeken, klachten en rechtsvorderingen die ondernomen zijn door en/of tegen het individu
- Veroordelingen en straffen
- Gerechtelijke maatregelen in relatie tot het individu: voogdijschap, voorlopig bewindvoerder, internering en plaatsing
- Administratieve sancties van louter disciplinaire aard
- Administratieve sancties die worden opgelegd aan niet-ambtenaren die aan een openbare dienst hun medewerking verlenen (Geneesheren, apothekers, paramedici, aannemers van openbare werken)
- Administratieve sancties van louter disciplinaire aard die aan de gebruikers van openbare diensten kunnen worden opgelegd

- Administratieve sancties van louter disciplinaire aard dewelke wegen niet-nakoming van wettelijke en verordening bepalingen kunnen worden opgelegd (GAS-boetes)
- Genetische en biometrische gegevens die worden verwerkt in het kader van de wet van 22 maart 1999 betreffende de identificatieprocedure in strafzaken

Raciale of etnische gegevens

- Informatie met betrekking op ras en etnische achtergrond

Gegevens over seksuele geaardheid

- Informatie met betrekking seksuele geaardheid
- Gecombineerde data waaruit de seksuele geaardheid van het individu kan afgeleid worden

Politieke, filosofische of religieuze relaties en overtuigingen

- Politieke, filosofische en religieuze overtuiging
- Politieke, filosofische en religieuze functies, titels en erkenningen
- Lidmaatschap van organisaties met politieke, filosofische en religieuze achtergrond (incl. vakbonden)
- Lidmaatschap van/of steun aan belangengroepen en miltante organisaties

Beeld- en geluidopnamen

Deze dataelementen hebben betrekking op het individu:

- Deze zijn toepasbaar onafhankelijk het opslagmedium (Fysiek, analoog of digitaal)
- Registratie van stilstaande of bewegende beelden, ook buiten het visuele spectrum
- Registratie van audio

Genetische en biometrische gegevens

Dit data type bevat alle referentie gegevens naar de biologische identiteit van een individu

- DNA-gegevens en afgeleide informatie die toelaat de oorsprong te identificeren
- Vinger-, stem-, netvlies-, gezicht, handpalm afdrukken en afgeleide informatie
- Morfologische registratie van het lichaam, geheel of gedeeltelijk, inclusief de afgeleide informatie
- Motoriek registratie inclusief de afgeleide informatie (vb. Dynamische handtekening)

Locatiegegevens

Dit data type bevat voornamelijk elektronische sporen die verwijzen naar de plaats en tijd waarmee een individu kan gerelateerd worden. De onderstaande lijst is niet beperkend, andere technologische ontwikkelingen worden ook gevat in deze data type bepaling:

Algemeen

- Werktijd registratie
- Fysieke toegangsregistratie
- (Bewakings-) Camerabeelden
- Locatiegegevens mobiele telefonie
- Locatiegegevens (mobiele) telefonie gesprekken. (vb. Internationale gesprekken)
- Locatiegegevens IOT ‘baken’ informatie in (afleidbare) combinatie met het individu
- Locatiegegeven GPS systemen in (afleidbare) combinatie met het individu
- Informatie verkeersovertredingen (PV)
- Informatie wagenpark/tankkaart gebruik in (afleidbare) combinatie met het individu

Mobiele telefonie

- Locatie bepaling op netwerken

Deze netwerk-gebaseerde techniek maakt gebruik van de infrastructuur van de serviceprovider om de locatie van de mobiele telefoon te bepalen. (driehoeksmeting)

- Locatie op basis van handset-(Incl. GPS)

In deze techniek is het nodig dat de cliënt (de gebruiker) software installeert op zijn mobiel toestel. Deze software zal worden gebruikt om de positie te bepalen. De software zal hiervoor gebruikmaken van onder andere celgegevens, IMEI, signaalsterkte tussen toestel en mast, signaalsterktes tussen cel en naburige cellen. E-OTD of U-TDOA. Als het toestel dan ook nog is uitgerust met gps, kan de plaatsbepaling nog nauwkeuriger worden uitgevoerd.

- Locatie op basis van Sim

Door gebruik te maken van de Simkaart in mobiele toestellen is het mogelijk om ruwe data van het netwerk op te vragen. Vb. de nabije cel informatie met dewelke het toestel contact heeft, de signaalsterktes.

- Locatie op basis van combinaties van data sets (Hybride)

In deze techniek worden de methodes van de netwerk- en de handset-gebaseerde methodes gecombineerd om een nauwkeurigere plaatsbepaling te verkrijgen. Een voorbeeld hiervan is A-gps. Hier wordt een combinatie van gps-signalen en signalen uit andere bronnen (vb. wifi) gebruikt. Deze techniek wordt ook gebruikt door onder andere Google Latitude, Buddyway, …

- Locatie op basis van Wifi/Bluetooth/NFC-tracking

De lokalisatie van mobiele telefoons kan ook gebeuren met behulp van technologie gebaseerde trackers. Deze techniek wordt bijvoorbeeld toegepast bij het volgen van bezoekers in winkelstraten en gebouwen, bij evenementen, verkeer opvolging. Hierbij gebruikt men het unieke MAC-adres dat aanwezig is in elk toestel.

Global positioning systems

Locatiegegevens op basis van GPS-technologie aanwezig in andere toestellen en toepassingen

GPS systemen

- GPS /Verenigde staten
- GLONASS /Russisch
- Galileo /Europees

Contractuele detail met werkgever

- Ambtenaar statuut en overzicht
- Militair statuut en overzicht
- Arbeidscontracten

Evaluatie en prestatie informatie

- Geestelijke, burgerlijke, professionele- en militaire onderscheidingen
- Sociale en werkgever (financiële) beloningen en bestraffingen op basis van prestaties
- Resultaten en detail van academische opleiding
- Resultaten en detail van evaluatie opleiding

- Resultaten en detail van evaluatie professionele prestatie

Gegevens sociale zekerheid

- Gegevens in verband met de sociale ondersteuning van het individu
- Sociale uitkeringen, tegemoetkomingen en premies
- Werkloosheidstatus en aanverwante detailinformatie

Statuten en vergunningen

- Vergunningen, incl. werk- en arbeidsvergunningen
- Visa, reisvisa
- Immigranten- en vluchtelingenstatuut.
- Bijzonderheden in verband met visum
- Verblijfs- en verplaatsingsbeperkingen
- Bijzondere voorwaarden betreffende het verblijfsrecht

Data types van de Informatiecategorie 4

Er werden geen standaard data types gerelateerd aan persoonsgegevens, geïdentificeerd in categorie 4.

Documentbeheer

Historiek

Datum	*Auteur*	*Versie*	*Omschrijving wijzigingen*
22/10/2019	BOSA	V0.1	Eerste draft
05/11/2019	BOSA	V.1	Update op basis van comments van FISP leden o.a.: • Vermelding residuele risico • Update beschrijving van de handleiding voor Cloud beveiliging • Verwijderen tabel betreffende de link met andere documenten
21/11/2019	FISP workgroup	V1.1	Publieke verspreiding

Goedkeuringen

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

Bronnen

Dit document werd samengesteld met behulp van de volgende bronnen:

- ISO/IEC 27001
- BSG (Baseline information Security Guidelines) geleverd door het Centrum voor Cybersecurity België (CCB)

Link met een ander beleid

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

Sectie	*Doelstellingen en referentiemaatregelen*	*In relatie (X = Ja*
4	*Context van de organisatie*	
5	*Leiderschap*	*x*
6	*Planning*	
7	*Ondersteuning*	
8	*Operatie*	
9	*Evaluatie van de prestaties*	
10	*Verbeteringen*	

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

Sectie	*Doelstellingen en referentiemaatregelen*	*In Relatie (X = Ja)*	*Doelstellingen/ Maatregelen (Detail)*
A5	*Informatiebeveiligingsbeleid*		
A6	*Organisatie van informatiebeveiliging*		
A7	*Human Resources Veiligheid*		
A8	*Asset Management*		
A9	*Toegangscontrole*		
A10	*Geheimschrift*		
A11	*Fysieke en ecologische veiligheid*		
A12	*Operationele veiligheid*		
A13	*Beveiliging van communicatie*		
A14	*Aankoop, ontwikkeling en onderhoud van informatiesystemen*		
A15	*Relaties met leveranciers*		
A16	*Beheer van informatiebeveiligingsincidenten*		
A17	*Informatiebeveiliging in Business Continuity Management*		
A18	*Conformiteit*		