Afsprakenstelsel eHerkenning

Informatiebeveiliging

Versie 1.7

INHOUDSOPGAVE

COLOFON

Auteur	Status
Beheerorganisatie Afsprakenstelsel eHerkenning	Definitief
Product	**Datum**
Afsprakenstelsel eHerkenning	24 april 2013
Organisatie	**Classificatie**
Logius	Openbaar
Titel van het document	**Versie**
Afsprakenstelsel eHerkenning – Informatiebeveiliging	1.7

HISTORIE

Datum	Versie	Wijziging	Status	Verwerkt door
29/03/10	0.8def		T.b.v. proefimpl.	Projectbureau
06/09/10	1.0	Losstaande versie van hoofdstuk 6 uit 0.8def	Definitief	Projectbureau
17/12/10	1.0a	Geen wijzigingen	Definitief	Projectbureau
17/06/11	1.1	RFCs verwerkt conform besluit kernteam 31 mei	Definitief	Projectbureau
12/11/11	1.2	RFCs verwerkt conform besluit kernteam 11 oktober	Definitief	Projectbureau
29/11/11	1.3	RFCs verwerkt conform besluit kernteam 13 december	Definitief	Projectbureau
28/04/12	1.4	Geen wijzigingen	Definitief	Beheerorganisatie
12/07/12	1.5	RFC0178, RFC0180 verwerkt	Definitief	Beheerorganisatie
12/03/13	1.6	RFC0185, RFC0201 verwerkt	Definitief	Beheerorganisatie
24/04/13	1.7	RFC0200, RFC0210 verwerkt	Definitief	Beheerorganisatie

DISTRIBUTIE

Datum	Distributie	Versie
	Publicatie op www.eherkenning.nl	1.7

GOEDKEURING

Datum	Naam	Versie
24/04/13	Alle RFCs voor versie 1.7 goedgekeurd door Tactisch overleg	1.7

1 Inleiding

Dit document maakt deel uit van het afsprakenstelsel eHerkenning. Het kan niet los worden gezien van de andere documenten van het afsprakenstelsel. Voor een algemene introductie op, en een overzicht van alle documenten binnen eHerkenning wordt de lezer van dit document aangeraden eerst het document [eHerkenning – Algemene introductie] te lezen.

1.1 Doel en doelgroep van dit document

Dit document beschrijft de maatregelen die genomen worden om het vertrouwen in en de continuïteit van het stelsel eHerkenning te borgen.

1.2 Leeswijzer

Gezien de beperkte omvang geen nadere aanwijzingen voor de lezer.

1.3 Begrippenlijst

Binnen eHerkenning wordt één begrippenlijst gehanteerd. Zie de bijlage in document [eHerkenning – Algemene introductie]. In deze lijst zijn enkelvoudsvormen van zelfstandige naamwoorden en werkwoorden opgenomen. Waar in dit document de werkwoordsvorm van deze zelfstandige naamwoorden wordt gehanteerd, heeft deze dezelfde betekenis als de gedefinieerde zelfstandige naamwoorden. Dat zelfde geldt ook andersom: waar in dit document de zelfstandige-naamwoords-vorm van een werkwoord wordt gehanteerd, heeft deze dezelfde betekenis als het gedefinieerde werkwoord.

1.4 Terminologie

Ter wille van de leesbaarheid van de tekst is overal ‘hij’ geschreven waar ‘hij of zij’ bedoeld wordt.

De woorden “MOET”, “MAG NIET”, “ZOU MOETEN”, “ZOU NIET MOETEN”, en “MAG” in dit document moeten worden geïnterpreteerd gelijk aan hun Engelstalige equivalenten (“MUST", "MUST NOT / SHALL NOT", "SHOULD", "SHOULD NOT" en "MAY") als beschreven in RFC 2119 (http://www.ietf.org/rfc/rfc2119.txt). Waar deze exacte termen bedoeld zijn worden ze in hoofdletters weergegeven. De betekenis van deze woorden is:

- MOET: een absolute vereiste
- MAG NIET: een absoluut verbod
- ZOU MOETEN: sterke wens, tenzij er valide reden is in specifiek geval af te wijken
- ZOU NIET MOETEN: ongewenst, tenzij er valide reden is om het in specifiek geval toe te laten
- MAG: een vrije keuze, een optie

1.5 Typografie

In de meer technische delen van de documentatieset worden de woorden “MOET”, “MAG NIET”, “ZOU MOETEN”, “ZOU NIET MOETEN”, en “MAG” altijd in hoofdletters genoteerd.

2 Informatiebeveiliging en privacy

In het netwerk voor eHerkenning wordt informatie verwerkt die vertegenwoordigers van dienstafnemers toegang geeft tot diensten van dienstverleners. Informatiebeveiliging is essentieel voor de continuïteit van het stelsel en moet daarom worden beschouwd als integraal onderdeel van de bedrijfsvoering van de deelnemers in het netwerk en de beheerorganisatie van het netwerk.

Het netwerk voor eHerkenning is in essentie een 'makelaar van vertrouwen' tussen dienstafnemers en dienstverleners. Het vertrouwen van dienstverleners en dienstafnemers in het netwerk voor eHerkenning is essentieel voor het zakelijke succes ervan en wordt op twee manieren bereikt:

1. Organisatorisch en administratief door contracten en formele toetsing zoals certificatie en Third Party Mededelingen.
2. Gebruikerservaringen van de ongestoorde en veilige werking van de technische infrastructuur.

In het netwerk voor eHerkenning worden vertrouwelijke gegevens zoals identificerende persoonsgegevens, gegevens over het gebruik van diensten verwerkt. Er bestaat een wettelijke verplichting van dienstverleners, dienstafnemers, deelnemers en beheerorganisatie om dergelijke gegevens aantoonbaar afdoende te beschermen. Daarnaast wordt het netwerk in de praktijk een onmisbare schakel in de dienstverlening aan dienstafnemers. Naarmate er meer dienstverleners en meer dienstafnemers op het netwerk voor eHerkenning aangesloten worden, zal het belang van de continue werking van het netwerk toenemen en worden dus hogere eisen gesteld aan ongestoorde beschikbaarheid van de onderdelen van het netwerk.

Daarom MOET op het niveau van het stelsel verantwoording kunnen worden afgelegd over de status van de informatiebeveiliging aan de gebruikers van het stelsel en de deelnemers aan het stelsel. Deelnemers en beheerorganisatie MOETEN daarom afdoende beveiligingsmaatregelen treffen om een betrouwbare werking te garanderen.

2.1 Afspraken over verantwoordelijkheid en verantwoording

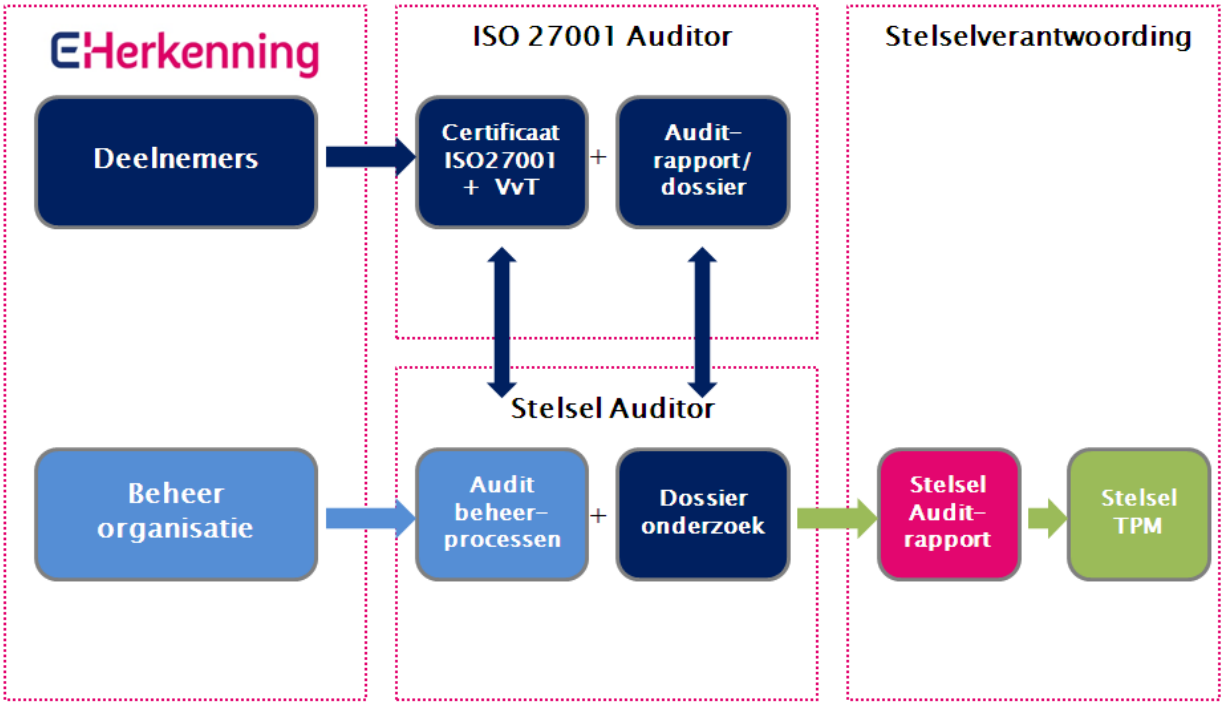
1. De beheerorganisatie MOET de verantwoordelijkheid nemen voor het management van de informatiebeveiliging op het niveau van het stelsel voor eHerkenning en de externe verantwoording daarover. De beheerorganisatie MOET daartoe een Third Party Mededeling (TPM) laten afgeven over de opzet, het bestaan en de werking van de informatiebeveiliging van het stelsel eHerkenning. Voor de TPM wordt o.a. gebruikt gemaakt van de auditdossiers over de verantwoording die de deelnemers en de beheerorganisatie afleggen (zie 2).
2. Iedere deelnemer aan het stelsel en de beheerorganisatie van het stelsel MOETEN de verantwoordelijkheid nemen voor de beveiliging en controle van de eigen systemen die gebruikt worden in eHerkenning. De deelnemers en de beheerorganisatie MOETEN een systeem voor het management van informatiebeveiliging inrichten waarin minimaal hun dienstverlening voor eHerkenning MOET zijn ondergebracht. Het managementsysteem MOET zijn ingericht conform de ISO/IEC 27001 standaard en ZOU formeel MOETEN zijn gecertificeerd. Als alternatief MAG de deelnemer en de beheerorganisatie beschikken over een TPM (inclusief conformiteitsverklaring) die

door een onafhankelijke Register EDP auditor is bevestigd. Hierna wordt kortweg gesproken over een TPM.
De toetsing van opzet, bestaan en werking van geïmplementeerde controls en implementatie van de stelselafspraken over de technische invulling maken onderdeel uit van het certificaat of de TPM (inclusief conformiteitsverklaring).

3. Deelnemers die voor het eerst willen toetreden en de genoemde certificaten of TPM's nog niet kunnen overleggen MOETEN om te worden toegelaten:
    a. zelf verklaren dat zij aan de materiële eisen van ISO 27001 (inclusief het Gemeenschappelijk Normenkader Informatiebeveiliging eHerkenning) voldoen, alsmede aan de gestelde eisen voor de dienstverlening van de betrouwbaarheidsniveaus die geleverd gaan worden.
    b. voorbereidingen in gang hebben gezet voor de ISO 27001 certificatie en/of een TPM van het managementsysteem voor informatiebeveiliging, zoals bedoeld in ISO 27001, alsook de specifieke eisen die zijn gesteld aan de betrouwbaarheidsniveaus van de te leveren diensten.
    c. een risicoanalyse overleggen die op de eHerkenningsdiensten betrekking heeft (en de Stelselrisicoanalyse als input heeft) met daarin aangegeven de reeds genomen, nog te nemen maatregelen en de restrisico's.
    d. een GAP-analyse overleggen waarin ten opzichte van het Gemeenschappelijke Normenkader Informatiebeveiliging is aangegeven welke maatregelen reeds zijn geïmplementeerd en welke maatregelen nog moeten worden geïmplementeerd.
4. Met ingang van 1 december 2012 geldt dat nieuwe deelnemers binnen een half jaar na hun initiële toetreding de certificaten en/of TPM's (tevens o.b.v. het Gemeenschappelijk Normenkader Informatiebeveiliging eHerkenning) MOETEN overleggen of hebben overlegd.
5. Aanpassingen in het Gemeenschappelijk Normenkader Informatiebeveiliging eHerkenning moeten aantoonbaar in de audit van het certificaat zijn gereviewd door de auditor.
6. Op de toepasselijke jaarlijkse momenten MOETEN door de deelnemers aan de Beheerorganisatie de volgende bewijsstukken worden overlegd:
    - Het ISO 27001 certificaat of TPM.
    - Een door de auditor bevestigde verklaring dat de scope van het certificaat de dienstverlening t.b.v. eHerkenning omvat[1].
    - De Verklaring van Toepasselijkheid (VvT) behorende bij het ISO 27001 certificaat of TPM .

1 De scopeverklaring wordt meestal op het afgegeven certificaat vermeld.

7. De Stelselauditor MOET op verzoek van de Beheerorganisatie inzage worden gegeven in de voor het netwerk relevante auditdossiers. De deelnemers MOETEN daarover afspraken maken met hun eigen onafhankelijke auditors.



Figuur 1: Opbouw stelselverantwoording

2.2 Maatregelen voor informatiebeveiliging

Maatregelen voor informatiebeveiliging MOETEN betrekking hebben op organisatie, processen en gebruikte technologie die voor het stelsel van eHerkenning wordt ingezet door de deelnemers en de beheerorganisatie.

1. De deelnemer in het stelsel beveiligt en controleert zijn eigen systemen die hij gebruikt voor eHerkenning overeenkomstig de rol die hij vervult in het netwerk. De deelnemer MOET daarvoor de toepasselijke controls implementeren uit de norm ISO/IEC 27001/27002 en maatregelen implementeren conform het Gemeenschappelijke Normenkader Informatiebeveiliging eHerkenning (zie document [eHerkenning – Gemeenschappelijk Normenkader Informatiebeveiliging] en dit document.
2. De beheerorganisatie beveiligt en controleert haar eigen systemen die zij gebruikt voor eHerkenning en MOET daarvoor de toepasselijke controls implementeren uit de norm ISO/IEC 27001/27002 en

maatregelen implementeren conform het Gemeenschappelijke Normenkader Informatiebeveiliging eHerkenning.

3. De beheerorganisatie MOET een beveiligingsplan voor het netwerk voor eHerkenning opstellen waarin de samenhang van de informatiebeveiliging binnen het netwerk is geborgd. Onderdeel van dit plan MOET o.a. de inrichting zijn van:
   - een proces voor het melden en afhandelen van beveiligingsincidenten;
   - een proces voor de juiste classificatie op betrouwbaarheidsniveaus conform document [Betrouwbaarheidsniveaus];
   - een proces voor de uitvoering van impactanalyses van wijzigingen in netwerk voor eHerkenning op de samenhang van de informatiebeveiliging van het netwerk;
   - een proces voor het faciliteren en/of coördineren van (ook forensische) onderzoeken naar de toedracht en oorzaken van beveiligingsincidenten (waaronder ook fraude) en bewijs van informatietransacties;
   - een proces voor het minimaal jaarlijks evalueren van de getroffen beveiligingsmaatregelen in het netwerk en het Gemeenschappelijke Normenkader voor Informatiebeveiliging;
   - een proces voor het uitvoeren van periodieke beveiligingstests (o.a. penetratietests) van het netwerk;
   - een proces voor het uitvoeren van een beveiligingstest (w.o. penetratietests) op de systemen van een potentiële deelnemer voorafgaande aan de acceptatie als deelnemer;
   - een gemeenschappelijke classificatie van de in het netwerk verwerkte gegevens inclusief de classificatie van persoonsgegevens conform de aanwijzingen van de Commissie Bescherming Persoonsgegeven (AV23 of opvolger daarvan);
   - een proces voor afstemming en besluitvorming over de eisen aan de inrichting van de audit trail bij de deelnemers.
4. Het bovengenoemde beveiligingsplan voor het netwerk KAN in verschillende iteraties worden ontwikkeld, bijvoorbeeld proces voor proces. Het plan wordt vastgesteld door het tactisch beheer overleg van eHerkenning. De deelnemers MOETEN aan de opstelling en de implementatie van het netwerkbreed beveiligingsplan actief meewerken, ongeacht of het maatregelen betreft in het gezamenlijke verantwoordelijkheidsdomein van het netwerk of maatregelen in het verantwoordelijkheidsdomein van de individuele deelnemer. Deelnemers MOETEN zich conformeren aan het gestelde in het beveiligingsplan.
5. De deelnemer MOET zijn verbindingen beveiligen en berichten ondertekenen conform de specificaties in de koppelvlakbeschrijvingen.
6. De te nemen beveiligingsmaatregelen MOETEN worden bepaald aan de hand van een risicoanalyse. De Stelselrisicoanalyse MOET als input meegenomen worden in de risicoanalyses van deelnemers en beheerorganisatie (zie document [eHerkenning – Stelsel risicoanalyse]).

7. De deelnemers MOETEN aan de aansluiting van een dienstverlener of dienstafnemer de eis stellen dat de dienstverlener of dienstafnemer verantwoordelijkheid neemt voor de informatiebeveiliging van de eigen systemen van de dienstverlener of dienstafnemer.
8. Indien deelnemers voldoen aan de voorgaande afspraken 1 t/m 7, dan MOGEN deelnemers bij interconnectie NIET om aanvullende zekerheden omtrent de beveiliging van een andere deelnemer vragen bij het gezamenlijk vormgeven van dienstverlening in het kader van het netwerk.
9. De beheerorganisatie MOET het Gemeenschappelijke Normenkader Informatiebeveiliging eHerkenning en de Stelselrisicoanalyse opstellen en beheren:
    1. Het Gemeenschappelijke Normenkader voor informatiebeveiliging MOET generieke beveiligingseisen bevatten die voor elke rol in het netwerk van toepassing zijn. De generieke eisen omvatten minimaal de beveiligingseisen aan koppelvlakken, berichten en verbindingen en het beheer daarvan en de inrichting van het management voor informatiebeveiliging.
    2. Het Gemeenschappelijke Normenkader ZOU naast de generieke eisen ook specifieke eisen MOETEN stellen die verschillen per rol in het netwerk.
    3. Het Gemeenschappelijke Normenkader Informatiebeveiliging ZOU onderscheid MOETEN maken naar toepasselijkheid voor de verschillende betrouwbaarheidsniveaus van de aan te bieden eHerkenningsdiensten.

2.3 Beheer Stelselrisicoanalyse en Gemeenschappelijk Normenkader Informatiebeveiliging

De beheerorganisatie MOET de Stelselrisicoanalyse en het Gemeenschappelijke Normenkader Informatiebeveiliging eHerkenning onderhouden:

1. Tenminste jaarlijks of bij gebeurtenissen met een grotere impact op het netwerk MOET de Stelselrisicoanalyse worden herijkt om te bezien of beoordeling van de gedefinieerde stelselrisico's nog actueel is, of risico's kunnen vervallen of nieuwe risico's moeten worden toegevoerd en gemitigeerd.
2. Tenminste jaarlijks of bij gebeurtenissen met een grotere impact op het netwerk MOET het gemeenschappelijke normenkader MOETEN worden herijkt met medeneming van de resultaten van de herijkte Stelselrisicoanalyse.
3. De herijkingen van de Stelselrisicoanalyse en het normenkader MOETEN door de beheerorganisatie worden geïnitieerd en ZOUDEN minimaal MOETEN worden uitgevoerd met een representatieve vertegenwoordiging vanuit de deelnemers.
4. De beheerorganisatie MOET er zorg voor dragen dat de vaststelling van de herijkte Stelselrisicoanalyse en het herijkte normenkader het wijzigingsproces van het stelsel doorloopt. Herijkte Stelselrisicoanalyse en normenkader worden door de beheerorganisatie ingebracht in het tactisch overleg ter vaststelling en het tactisch overleg besluit tevens over de datum waarop de herijkte risicoanalyse en het herijkte normenkader van kracht is.

5. De beheerorganisatie MOET er voor zorgdragen dat de herijkte risicoanalyse en het herijkte normenkader voor de vastgestelde datum formeel ter beschikking komen van de deelnemers en van formele kandidaat-deelnemers.

6. De beheerorganisatie MOET een controleplan opstellen voor alle activiteiten die nodig zijn om het beheer van de stelselrisicoanalyse, het gemeenschappelijk normenkader en de stelselaudit uit te voeren.

7. De beheerorganisatie MOET het versiebeheer van de Stelselrisicoanalyse en het normenkader voeren. Dit betekent eveneens dat de beheerorganisatie per deelnemer MOET bijhouden welke versie van het normenkader van toepassing was bij de audits in het kader van de certificering.

3 Nadere specificaties

3.1 Implementatie Gemeenschappelijk Normenkader Informatiebeveiliging en certificatie

Het gemeenschappelijke normenkader is opgesteld op basis van de analyse van de risico's die voor het stelsel als geheel relevant zijn. Dit betekent ook dat alleen die maatregelen (normen) zijn geselecteerd die van betekenis zijn op het niveau van het stelsel en dus voor elke deelnemer.

Deelnemers en beheerorganisatie MOETEN om voor certificatie of TPM in aanmerking te komen individueel een risicoanalyse uitvoeren en MOETEN daarbij onder meer de Stelselrisicoanalyse als input gebruiken.

Op basis van de individuele risicoanalyse (Plan-fase van het ISMS zie de bijlage) selecteren de deelnemers beheersmaatregelen uit de Appendix van de norm IEC/ISO 27001:2005 of formuleren deze maatregelen eventueel zelf. De geselecteerde maatregelen nemen zij op in de Verklaring van Toepasselijkheid (VvT). Iedere deelnemer beargumenteert individueel zijn keuze voor maatregelen of uitsluiting van maatregelen.

Op stelselniveau is in het kader van het programma eHerkenning onder verantwoordelijkheid van de (tijdelijke) Beheerorganisatie en vertegenwoordigers van deelnemers een risicoanalyse uitgevoerd op de gemeenschappelijke processen en objecten van het Netwerk voor eHerkenning. Mede op basis van deze risicoanalyse zijn ten behoeve van de informatiebeveiliging van eHerkenning als geheel de minimaal te nemen beheersmaatregelen geselecteerd uit de Appendix van de ISO 27001:2005 norm. De geselecteerde beheersmaatregelen zijn opgenomen in het Gemeenschappelijk Normenkader Informatiebeveiliging van eHerkenning.

De beheersmaatregelen uit dit "Gemeenschappelijk Normenkader Informatiebeveiliging eHerkenning" MOETEN door deelnemers (afhankelijk van hun rol(len) in het stelsel) in hun individuele VvT worden opgenomen.

Er zijn twee typen maatregelen:

1. Het eerste is een verplichte maatregel die NIET MAG ontbreken in de VvT. Voor dit type maatregel zijn er op stelselniveau reeds uitwerkingen vastgesteld zoals koppelvlakspecificaties, operationeel handboek en procedure- en procesbeschrijvingen.
2. Het tweede type is een maatregel die de deelnemer of beheerorganisatie vanuit zijn rol ZOU MOETEN nemen en waarvan met dus mag verwachten dat deze in de VvT is opgenomen. De deelnemer MAG echter de beheersmaatregel 'niet van toepassing' verklaren maar in dat geval MOET deze uitsluiting met argumenten zijn omkleed.

De gemeenschappelijke maatregelen MOETEN dus op de VvT van de deelnemers herkenbaar voorkomen (geselecteerd of beargumenteerd niet geselecteerd).

Het Gemeenschappelijke normenkader en Stelselrisicoanalyse worden tenminste jaarlijks geëvalueerd en zo nodig bijgesteld. Dit betekent ook dat:

1. een deelnemer bij toetreding tot het Netwerk voor eHerkenning contractueel de verplichting tot certificatie op zich neemt en dus de op dat moment geldende versie van het normenkader MOET gebruiken.

2. een redelijke termijn in acht genomen ZOU MOETEN worden om de bestaande deelnemers de gelegenheid te geven de bijstellingen uit het normenkader te implementeren. Deze termijn wordt gesteld op 3 maanden na vaststelling van de bijstelling tenzij het tactisch beheer overleg anders besluit.

3.2 Eisen ten aanzien van archivering en opvraging

Vanuit het oogpunt van een betrouwbare elektronische communicatie en vanuit het oogpunt van informatiebeveiliging en betrouwbaarheid van het netwerk voor eHerkenning, gelden de volgende eisen ten aanzien van archivering.

- Elke deelnemer MOET alle door haar ondertekende en alle door haar ontvangen ondertekende berichten minimaal 7 jaar te archiveren. Na deze periode ZOUDEN ten minste de in deze berichten voorkomende persoonsgegevens vernietigd MOETEN worden.
- Authenticatiediensten MOETEN tevens een referentie naar het gebruikte middel opslaan, zodat de audit trail naar de uitvoerend natuurlijk persoon sluitend wordt.
- Machtigingenregisters MOETEN tevens een referentie naar de geregistreerde bevoegdheid waarop de verklaring van bevoegdheid berust opslaan, zodat de audit trail naar de vertegenwoordigde dienstafnemer sluitend wordt.
- Middelenuitgevers en Machtigingenregisters ZOUDEN tevens bewijsstukken die zijn gebruikt bij uitgifte/registratie van middelen of machtigingen 7 jaar MOETEN archiveren zodat de audittrail naar handelend natuurlijk persoon of machtigingenbeheerder sluitend wordt.
- Een deelnemer MAG NIET persoonsgegevens afkomstig van berichten of bewijsstukken langer bewaren dan noodzakelijk voor het doel waarvoor ze worden verwerkt (conform Wet Bescherming Persoonsgegevens).
- Elke deelnemer MOET gearchiveerde gegevens beveiligd opslaan zodat zij niet toegankelijk zijn voor onbevoegden.
- Elke deelnemer MOET een verzoek waarbij gearchiveerde gegevens worden opgevraagd honoreren in de volgende gevallen:
    - Wanneer er beroep is ingesteld tegen een bestuursrechtelijk besluit dat de dienstverlener heeft genomen op basis van gegevens die zijn verkregen middels een eHerkenningsdienst en de dienstverlener deze bewijsstukken nodig heeft in het kader van de beroepsprocedure moeten de gegevens worden verstrekt aan zowel betreffende dienstverlener als dienstafnemer of de uitvoerend natuurlijk persoon die het beroep heeft ingesteld.
    - Op vordering van een bevoegde opsporingsinstantie, een inlichtingen- of veiligheidsdienst of een bevoegde toezichthouder moeten de gegevens aan betreffende instantie worden verstrekt.
    - Op verzoek van de beheerorganisatie. Bijv. omdat elders in de keten informatie verloren is gegaan en met als doel dat het informatiegat wordt hersteld.
- Een partij ZOU een verzoek voor het vrijgeven van gearchiveerde informatie in beginsel MOETEN indienen bij de betreffende deelnemer. Een dienstverlener ZOU een dergelijk verzoek in beginsel MOETEN indienen bij haar eHerkenningsmakelaar. In geval van geschillen, of bij onvoldoende medewerking MAG een partij een verzoek indienen bij de beheerorganisatie, die vervolgens de coördinatie op zich MOET nemen.

3.2.1 Logging

- Elke deelnemer MOET het volledige HTTP bericht van binnenkomende communicatie als gevolg van eHerkenning loggen. Elke deelnemer MOET alle uitgaande SAML en XACML berichten loggen.
- Elke deelnemer MOET logging beveiligd opslaan en MOET deze alleen toegankelijk maken voor bevoegde personen. Een deelnemer MAG logging NIET verwijderen binnen de verplichte bewaartermijn.
- Elke deelnemer MOET logging kunnen inzetten ten behoeve van foutopsporing.

Uitzondering op de loggingvereisten vormen cookieservers. Deze MOGEN NIET logging toepassen om gebruikers te volgen.

Op basis van logging MOET de deelnemer in staat zijn om vragen te beantwoorden. Er is een onderscheid in eerstelijns en tweedelijns vragen.

3.2.2 Eerstelijns vragen

Elke deelnemer MOET met behulp van logging over elke periode vragen over transacties kunnen beantwoorden waarin een van de volgende criteria, of een combinatie ervan, zijn opgenomen:

1. OIN per rol deelnemer
2. OIN dienstafnemer
3. OIN intermediaire partij (indien van toepassing)
4. OIN van dienstverlener
5. Dienst uit dienstencatalogus
6. Intern pseudoniem van een uitvoerend natuurlijk persoon
7. Extern pseudoniem van een uitvoerend natuurlijk persoon
8. Betrouwbaarheidsniveau

Daarnaast MOET de deelnemer op basis van logging inzicht kunnen geven in het totaal aantal geslaagde transacties en het totaal aantal foutieve transacties in een periode.

3.2.3 Tweedelijns vragen

Elke deelnemer MOET op verzoek van een daarvoor bevoegde instantie een (gearchiveerd) ondertekend verzonden of ontvangen bericht aan de instantie beschikbaar stellen. Tevens MOET een deelnemer op verzoek van een daarvoor bevoegde instantie de persoonsgegevens (van een houder van een authenticatiemiddel of betrokkene bij een machtiging) beschikbaar stellen aan de instantie.

3.3 Eisen aan de classificatie van informatie

Deze paragraaf beschrijft de nadere specificatie van de norm A.7.2 Classificatie van informatie (A7.1.1 en A.7.2.2) in de ISO 27001:2005. Doelstelling van de norm is: bewerkstelligen dat informatie een geschikt niveau van bescherming krijgt.

3.3.1 Reikwijdte

Deze uitwerking van de norm heeft betrekking op gegevens die binnen eHerkenning (deelnemers en beheerorganisatie inclusief 'bestuurlijke opdrachtgever') worden gegenereerd, uitgewisseld en opgeslagen.

De uitwerking van de norm is niet bedoeld als classificatie van systemen of netwerkcomponenten. Een normering van de classificatie van eHerkenning-systemen heeft geen toegevoegde waarde vanwege het ontbreken van generieke typering van systeemcomponenten van eHerkenning. De individuele deelnemers zijn vrij in de wijze waarop zij hun infrastructurele omgevingen concreet inrichten en moeten in staat blijven hun eigen classificatiemethodiek te volgen.

3.3.2 Classificatie en maatregelen

De classificatie is niet gekoppeld aan een generieke set maatregelen. De te classificeren informatie betreft uiteenlopende typen gegevens op uiteenlopende gegevensdragers. De concretisering van maatregelen MOET door de individuele deelnemers en beheerorganisatie worden gedefinieerd op basis van de Stelselrisicoanalyse en de eigen risicoanalyses. De voorbeelden van geclassificeerde gegevens dienen als input voor individuele risicoanalyses.

3.3.3 De classificatie

In tabel 1 is de classificatie van informatie binnen eHerkenning beschreven. De tabel legt met voorbeelden uit hoe de classificatie moet worden begrepen. Tabel 2 geeft een lijst van voorbeelden die als referentie dienen voor de classificatie van de overige en nieuwe eHerkenningsinformatie.

Tabel 1: Classificatie van informatie binnen eHerkenning

Classificatie	eHerkenning Intern	eHerkenning Gevoelig	eHerkenning Publiek/Openbaar
Uitleg	• Informatie die door alle direct betrokkenen bij eHerkenning wordt uitgewisseld. • De informatie is niet bedoeld voor anderen maar als onverhoopt deze informatie met derden wordt gedeeld treedt er geen substantiële financiële schade of imago schade op.	• Informatie die extra bescherming nodig heeft. • Openbaring aan niet bevoegden brengt substantiële schade toe aan het Netwerk voor eHerkenning; financieel, imago gerelateerd of anderszins.	• Alle informatie over eHerkenning bedoeld voor (potentiële) klanten of breder publiek.
Voorbeeld	• Agenda's en vergaderverslagen • Mails (tenzij expliciet is aangegeven dat	• Contractgegevens • Testgegevens • Klantenregistratie • MU en MR • Logbestanden	• De Stelsel documentatie • Informatie over de aanbieders van eHerkenningsdien

	deze vertrouwelijk zijn) • Dienstencatalogus • Meta Data		sten op de website van eHerkenning • Factsheets etc.
Referentie	• Vertrouwelijkheid is laag • WBP/AV 23 Maatregelniveau: • Baseline • WBP Risicoklasse 1	• Vertrouwelijkheid is Midden/Hoog • WBP/AV 23 Maatregelniveau: • Baseline + Specifiek • WBP Risicoklasse 2	• Vertrouwelijkheid is n.v.t. • NB: er worden wel eisen gesteld aan de juistheid en beschikbaarheid van deze informatie

323

324 Tabel 2: Referentietabel met voorbeelden van geclassificeerde gegevens binnen eHerkenning

	Referentietabel met gegevens binnen eHerkenning (niet uitputtend)	Classificatie
1	Logbestanden van berichten-/transactieverkeer	Gevoelig WBP Risicoklasse 2
2	Contractgegevens	Gevoelig
3	Registraties MU en MR	Gevoelig WBP Risicoklasse 2
4	Metadata	Intern*)
5	Dienstencatalogus	Intern*)
6	Testgegevens	Gevoelig
7	Auditrapporten	Gevoelig
8	Informatie betreffende de toetreding van deelnemers exclusief het advies aan het 'tactisch beheer overleg'.	Gevoelig
9	Berichten (verkeer)	Gevoelig
10	SLA rapportages van individuele deelnemers	Gevoelig
11	Generieke managementrapportages	Intern
12	Vergaderverslagen tactisch beheer overleg, gebruikersraad etc.	Intern
13	Beveiligingsincidenten-registratie	Gevoelig
14	Generieke beveiligingsrapportage (trends)	Intern

15	Het afsprakenstelsel voor eHerkenning	Publiek
16	Informatie op de website eHerkenning	Publiek
17	RFC's	Intern/Gevoelig**)
18	Rapporten van security-audits of penetratietesten	Gevoelig

*) Betreft slechts het aspect vertrouwelijkheid. Er zal wel sprake zijn van extra maatregelen i.v.m. eisen aan de integriteit van de gegevens.

**) Per RFC dient de mate van gevoeligheid te worden vastgesteld en de consequenties voor de behandeling van de RFC in de wijzigingsprocedure.

3.4 Eisen aan screening van medewerkers

Deze paragraaf bevat de nadere specificatie van de norm A.8.1.2 Screening in de ISO 27001:2005

3.4.1 Doel en reikwijdte van screening

Doel van de screening is om te voorkomen dat door de beheerorganisatie of deelnemers medewerkers worden aangenomen die door hun gedrag de integriteit en betrouwbaarheid van eHerkenning in gevaar brengen.

Het kan gaan om (potentiële of reeds in dienst zijnde) medewerkers die met voorbedachte rade dan wel onder druk van andere personen de integriteit en betrouwbaarheid van de organisatie moedwillig zouden willen schenden, of medewerkers die door een gebrek aan kennis en inzicht de integriteit en betrouwbaarheid zullen schenden.

Bij integriteit en betrouwbaarheid gaat het zowel om het handelen in overeenstemming met algemeen aanvaarde maatschappelijke normen en waarden, (wettelijke) richtlijnen en procedures als het nakomen van afspraken en toezeggingen aan klanten, medewerkers, leveranciers en andere belanghebbenden.

De maatregel heeft betrekking op al het vaste en tijdelijke personeel dat werkzaamheden uitvoert binnen de scope van eHerkenning.

3.4.2 Procedure

Inleiding

Deze paragraaf beschrijft de welke wijze waarom deelnemers en de beheerorganisatie screening MOETEN toepassen. Deze procedure maakt onderdeel uit van het Gemeenschappelijk Normenkader Informatiebeveiliging eHerkenning. Het doel van de procedure is om binnen eHerkenning tot een gemeenschappelijk - minimaal - niveau van screening te komen.

Het staat deelnemers en de BO overigens vrij om, bijvoorbeeld naar aanleiding van de eigenrisico-analyse, een strenger screening-regime dan in deze procedure is beschreven toe te passen.

De wijze en diepgang van de screening MOET zijn gerelateerd aan de bevoegdheden en taakstelling van de betreffende medewerker. Zo mag worden verwacht dat de screening voor een systeembeheerder met

speciale bevoegdheden ten aanzien van systeemprogrammatuur strenger zal zijn dan voor een ondersteunende stafmedewerkers.

Basisniveau van screening
Het basisniveau van screening voor alle personeel, bestaat uit:

- het controleren van de juistheid van de identiteit (WID-document);
- controleren van de juistheid van gegevens in het curriculum vitae en met name van opleidingsgegevens;
- controleren van relevante referenties.

Vast personeel t.b.v. eHerkenning

- Medewerkers die met activiteiten voor eHerkenning zijn belast MOETEN een Verklaring Omtrent Gedrag (VOG) aanvragen c.q. overleggen in relatie tot de omgang van gegevens waarbij integriteit en vertrouwelijkheid van belang zijn.
- De (originele of digitale kopie) VOG MOET worden opgenomen in het personeelsdossier of digitale registratie.
- Na een periode van 3 jaar MOET de VOG worden hernieuwd (opnieuw aangevraagd).Als In het geval een zwaardere screening aantoonbaar al reeds heeft plaatsgevonden KAN de deelnemer of beheerorganisatie besluiten om de VOG achterwege te laten. Zwaarder dan een VOG zijn bijvoorbeeld: veiligheidsonderzoek door de AIVD (A, B of C onderzoek) of de MIVD, antecedentenonderzoek door een erkend onderzoeksbureau, Pre employment screening (PES-onderzoek) door DSI.

Ingehuurd personeel
Deze beheersmaatregel is ook van toepassing op van externe leveranciers ingehuurd personeel. De eisen die aan ingehuurd personeel worden gesteld worden MOETEN van het zelfde niveau zijn als de eisen aan het vaste personeel.

In het contract met de leverancier MOET zijn opgenomen:

- welke verantwoordelijkheden deze heeft ten aanzien van het screeningproces en;
- de verplichting daarover om direct de opdrachtgever te informeren als de screening van een in te zetten of ingezette medewerker niet (volledig) heeft plaatsgevonden of tot een negatief resultaat heeft geleid.

3.4.3 Verantwoordelijkheden

De organisatie (deelnemer, beheerorganisatie) MOET een functionaris aanwijzen die verantwoordelijk is voor het laten uitvoeren van dit proces. In veel gevallen ligt deze verantwoordelijkheid bij een securityofficer of een risk manager.

- De werkgever MOET de medewerker verzoeken om een VOG aan te vragen.
- In de aanvraag MOET de werkgever aan wat de aard van het werk is dat de medewerker gaat uitvoeren.

3.4.4 Frequentie

Het screeningsproces MOET worden doorlopen voor elk personeelslid (vast of ingehuurd):

- Bij indiensttreding.
- Ingeval van een bestaand dienstverband als de screening nog niet heeft plaatsgevonden of is verlopen.

- Bij verandering van functie of werkgebied van een medewerker als de nieuwe werkzaamheden meer omvatten of in hoge mate afwijken van de vroegere werkzaamheden.

Gelet op de periode waarop de VOG betrekking heeft, nl. 3 jaar, MOET na deze periode de medewerker worden verzocht een nieuwe VOG aan te vragen.

3.4.5 Aantoonbaarheid en borging

De VOG's en eventueel andere screeningsdocumenten MOETEN vanuit privacyoverwegingen veilig worden bewaard maar ook makkelijk terugvindbaar en raadpleegbaar zijn.

Periodiek, bijvoorbeeld eenmaal per jaar, MOET worden nagegaan of alle voor eHerkenning werkzame medewerkers (vast en ingehuurd) een actuele screening hebben ondergaan.

3.5 Beleid en doel penetratietesten

Organisaties hebben diverse, zowel technische als organisatorische, maatregelen genomen om te voorkomen dat niet-geautoriseerden zich toegang kunnen verschaffen tot hun informatie en informatiesystemen.

Om te toetsen of het stelsel van maatregelen dat genomen is daadwerkelijk effectief en adequaat is, wordt bij de deelnemers van eHerkenning en bij de Beheerorganisatie periodiek, in beginsel twee maal per jaar, een zogenaamde penetratietest uitgevoerd. Deze test wordt uitgevoerd door een externe specialist.

Een dergelijke controle kan nuttig zijn om zwakke plekken in het systeem te ontdekken en om te controleren hoe doeltreffend de beheersmaatregelen zijn bij het voorkómen van onbevoegde toegang als gevolg van deze zwakke plekken.

Penetratietesten geven een momentopname van een systeem in een bepaalde toestand op een bepaald tijdstip. De momentopname blijft beperkt tot die delen van het systeem die werkelijk zijn getest tijdens de penetratiepoging(en). De penetratietest vormt daarmee een aanvulling op de risicoanalyses en de audits.

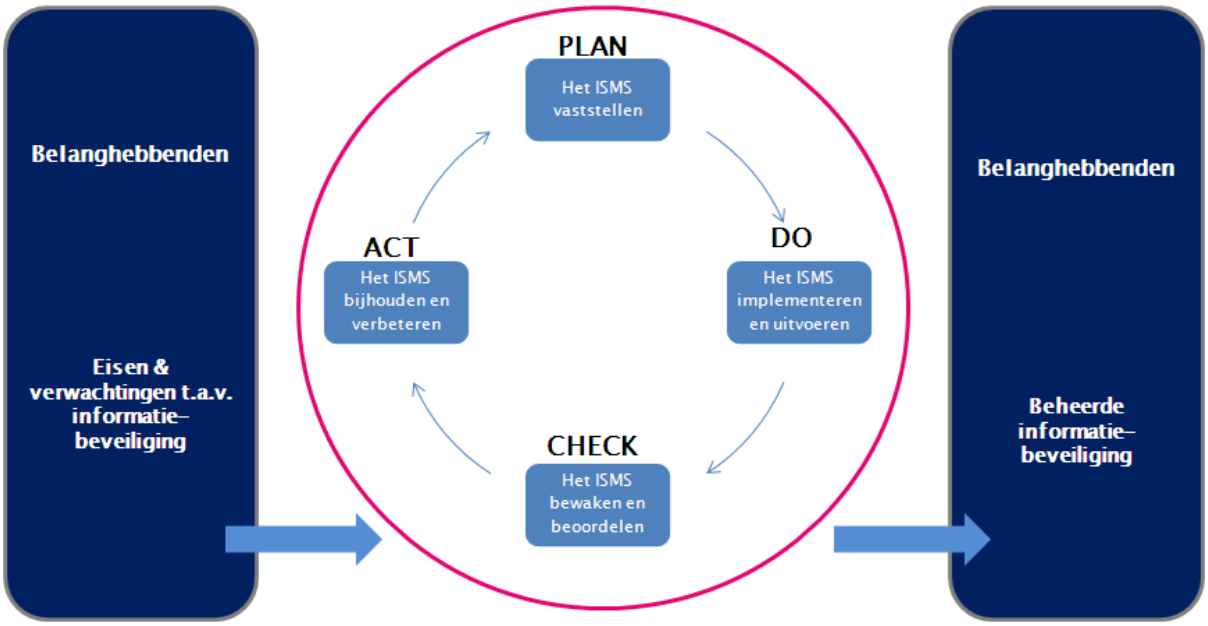
4 Bijlage Toelichting ISO 27001 certificatie

4.1 Inleiding op de norm NEN-ISO/IEC 27001:2005

De organisatie die zijn IB (Informatiebeveiliging) wil inrichten en wil laten certificeren tegen de ISO/IEC 27001 norm moet een "gedocumenteerd Information Security Management System (ISMS) vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren binnen het kader van de bedrijfsactiviteiten en -risico's van de organisatie. Het proces dat in het kader van deze norm wordt gehanteerd, is gebaseerd op het PDCA-model zoals in de figuur hierna is weergegeven in de norm" (zie 4.1 Algemene eisen in het normdocument NEN-ISO/IEC 27001:2005).

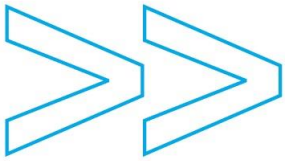
4.2 Toelichting op het ISMS en de PDCA-cyclus

In de hoofdstukken 4 t/m 8 van het ISO normdocument staat gedetailleerd en normatief beschreven wat een organisatie moet doen om een werkend ISMS te implementeren. Op deze plaat volstaan met een beknopte samenvatting op van de PDCA-cyclus.



Figuur 2: Activiteiten in de PDCA cyclus van het ISMS

Het systematisch doorlopen van deze PDCA-cyclus "dwingt" de organisatie als het ware tot het verbeteren van de Informatiebeveiliging. De uitgevoerde risicoanalyses en de in de VvT opgenomen beheersmaatregelen vormen de basis voor een ISMS van goede kwaliteit.



4.2.1 *Activiteiten in de Plan-fase:*

- Beschrijf de scope van het ISMS in termen van processen, systemen en organisatie.
- Voer een risico-analyse uit op deze scope en bepaal of en hoe de bepaalde risico's worden behandeld.
- Selecteer waar de van toepassing zijn de maatregelen uit de Appendix van de norm of beschrijf eigen specifieke maatregelen.
- Stel een Verklaring van Toepasselijkheid op.
- Verkrijg goedkeuring van het verantwoordelijk management en stel het ISMS vast.

4.2.2 *Activiteiten in de Do-fase:*

- Implementeer het plan voor risico-behandeling ofwel voer de geselecteerde maatregelen in, zorg dat deze gaan werken en beheerd worden.
- Richt de bijbehorende organisatie in, definieer rollen en verantwoordelijkheden.

4.2.3 *Activiteiten in de Check-fase*

- Controleer en beoordeel de werking van het ISMS.
- Beoordeel hierbij vooral of de gedachte risico's ook daadwerkelijk beheerst worden.
- Laat interne audits, reviews en controles uitvoeren.
- Beheer documentatie en registraties.

4.2.4 *Activiteiten in de Act-fase*

- Identificeer mogelijke verbeteringen en maak het mogelijk dat er corrigerende of preventieve maatregelen genomen worden die bewerkstelligen dat de beheersdoelstellingen worden bereikt.