Rijndijk 235
2394 CD Hazerswoude
Tel. (071) 3416911
Email noordbeek@noordbeek.com

Ministerie van Volksgezondheid, Welzijn en Sport

ISAE 4401 Rapport van feitelijke bevindingen over Informatiebeveiliging

Aangaande een assessment Van de Hardware Security Module (HSM) omgeving Van de CoronaMelder (de 'notificatie app')

Definitieve versie: 1.00

Opdrachtgever	B. de Winter	Ministerie van VWS
Auteur	E. van Egmond	Noordbeek B.V.
	J.V. Kerstens	
Rapportnummer	VWSCOR0-2	
Classificatie	Openbaar	
Status	Definitief	
Datum	8 december 2020	
Bestandsnaam	Noordbeek Rapport Assessment HSM-omgeving CoronaMelder 2020	
KvK nummer	Rijnland 33265070	
BTW nummer	NL8203.45.180.B01	

Colofon

Opdrachtgever	B. de Winter Ministerie van VWS
Opdrachtnemer	Prof.dr.ir. R. Paans RE Directeur Noordbeek B.V.
Contactpersoon	Ing. E. van Egmond RE CISSP QSA 3DS-QSA PCIP CISA Senior Manager IT Audit
Auteurs	E. van Egmond J.V. Kerstens
Kwaliteitscontrole	W.H. Mulder

Inhoud

1. Inleiding

Het ministerie van Volksgezondheid, Welzijn en Sport (VWS) laat de CoronaMelder ontwikkelen. Dit is de 'notificatie app'. Als onderdeel van het ontwikkel- en implementatieproces wordt een Hardware Security Module (HSM)-omgeving ingericht en beheerd door de Justiële Informatiedienst van het ministerie van Justitie en Veiligheid (Justid) in samenwerking met het Agentschap Centraal Informatiepunt Beroepen Gezondheidszorg (CIBG), als uitvoeringsorganisatie van het ministerie van VWS.

Het ministerie van VWS heeft Noordbeek opdracht gegeven een assessment uit te voeren op de beheersingsmaatregelen binnen de HSM-omgeving, gericht op informatiebeveiliging en privacybescherming.

Een assessment levert een beperkte mate van zekerheid, en is gericht op specifieke vragen die zijn geformuleerd door de opdrachtgever. Noordbeek levert de rapportage in de vorm van de International Standard on Assurance Engagements 4401 (ISAE 4401), met de Nederlandstalige naam 'Opdrachten tot het verrichten van overeengekomen specifieke werkzaamheden'.

De opdracht aan Noordbeek is onderdeel van een reeks aan onderzoeken en audits op de CoronaMelder, gericht op transparantie naar de burger en de volksvertegenwoordiging. In dit kader is dit ISAE 4401-rapport bedoeld om publiekelijk te worden gedeeld.

2. Rapport van feitelijke bevindingen met betrekking tot de assessment

Aan: Opdrachtgever

2.1. Opdracht

Wij hebben overeengekomen specifieke werkzaamheden verricht met betrekking tot een assessment op de beheersingsmaatregelen binnen de Hardware Security Module (HSM)-omgeving, gericht op informatiebeveiliging.

De opdracht voor de assessment is overeengekomen met het ministerie van VWS en heeft als doel een beperkte mate van zekerheid te bieden dat de vereiste beheersingsmaatregelen in opzet en bestaan aanwezig zijn, en eventuele afwijkingen te beschrijven. Hierbij worden de getroffen beheersingsmaatregelen getoetst tegen de internationale standaard Payment Card Industry 3-D Secure (PCI 3DS) met betrekking tot de HSM-normen.

De overeengekomen specifieke werkzaamheden zijn tot stand gekomen in overleg met de beoogde gebruikers, zijnde het ministerie van VWS en CIBG.

De opdrachtvoorwaarden zijn omschreven in onze opdrachtbrief van 26 augustus 2020, uitgebracht door Vanberkel Professionals B.V., mede namens Noordbeek B.V.

De rapportage wordt publiekelijk beschikbaar gesteld. Het onderzoek dient op een reproduceerbare wijze te worden beschreven, zodat publieke verificatie mogelijk is.

2.2. Verantwoordelijkheden

Het is de verantwoordelijkheid van het ministerie van VWS om te bepalen of de overeengekomen specifieke werkzaamheden toereikend en geschikt zijn voor het hierboven beschreven doel.

Wij hebben onze werkzaamheden verricht in overeenstemming met de Nederlandse Standaard 4401 ‘Opdrachten tot het verrichten van overeengekomen specifieke werkzaamheden’ van de Nederlandse Orde van Register IT-Auditors (NOREA).

Bij het uitvoeren van deze opdracht hebben wij ons gehouden aan de voor ons geldende relevante ethische voorschriften in de Verordening Gedrags- en Beroepsregels Accountants (VGBA). Verder hebben wij de onafhankelijkheidsregels van de Verordening inzake de onafhankelijkheid van accountants bij assurance-opdrachten (ViO) in acht genomen.

2.3. Werkzaamheden en bevindingen

In aanvulling op de uitleg van de randvoorwaarden van de opdracht, zoals vermeld in de paragraaf 'Opdracht' is in deze paragraaf een beschrijving van de overeengekomen specifieke werkzaamheden en feitelijke bevindingen opgenomen.

Wij doen geen uitspraak over wat de feitelijke bevindingen betekenen voor informatiebeveiliging binnen de HSM-omgeving van de CoronaMelder in zijn totaliteit. Het ministerie van VWS, Justid en CIBG zullen hierover een eigen afweging moeten maken waarbij het ministerie van VWS, JustId en CIBG gebruik kunnen maken van dit rapport van feitelijke bevindingen en eventuele andere beschikbare informatie.

Conform de opdracht in de offerteaanvraag zijn wij bij deze assessment nagegaan of er een redelijke mate van zekerheid kan worden verkregen met betrekking tot het hebben genomen van relevante beveiligingsmaatregelen inzake de inrichtings- en beheerwerkzaamheden van de HSM's.

In overeenstemming met de opdrachtvoorwaarden zijn wij nagegaan of:
- De vereiste beheersingsmaatregelen voor informatiebeveiliging in de HSM-omgeving van de CoronaMelder binnen Justid zijn gedocumenteerd ('opzet');
- Deze maatregelen daadwerkelijk zijn getroffen ('bestaan');
- Deze maatregelen voldoen aan de internationale standaard PCI 3DS met betrekking tot de HSM-normen.

Wij hebben geen onderzoek gedaan naar de operationele effectiviteit ('werking') van de beheersingsmaatregelen.

De bevindingen van onze werkzaamheden zijn als volgt:

1. **Sleutelbeheer** (zie 3.1)
   Het proces van sleutelbeheer is ondergebracht bij Justid. Justid beheert ook de HSM's en voert de key ceremonies uit. Naar onze mening voldoet het proces van sleutelbeheer aan de relevante gerelateerde PCI 3DS-normen;

2. **Logische toegangsbeveiliging** (zie 3.2)
   Het proces voor logische toegangsbeveiliging voor de HSM's is in beheer bij Justid. Naar onze mening voldoen de door Justid geïmplementeerde processen en procedures voor logische toegangsbeveiliging voor de HSM's aan de relevante gerelateerde PCI 3DS-normen. Het proces voor logische toegangsbeveiliging bij CIBG hebben wij niet kunnen beoordelen, aangezien dat ten tijde van ons onderzoek nog in opbouw was;

3. **Fysieke toegangsbeveiliging** (zie 3.3)
   De fysieke toegangsbeveiliging is uitbesteed aan twee datacenters. Een van deze datacenters is PCI DSS compliant. De HSM's zijn gemonteerd in een afgesloten kabinet, die is geplaatst in een shared omgeving. Vanwege de shared omgeving hebben derden toegang tot het kabinet en daarmee mogelijk tot de HSM's. Naar onze mening voldoet de huidige inrichting van de fysieke toegangsbeveiliging niet aan de relevante gerelateerde PCI 3DS-normen.

2.4. Vrij gebruik van het rapport en de verspreidingskring

Bij het opstellen van deze rapportage is rekening gehouden met de verwachtingen van de beoogde gebruikers, namelijk de burgers en de volksvertegenwoordiging, en de eis van de opdrachtgever dat publieke verificatie mogelijk moet zijn. Daarom is deze rapportage zo opgezet dat deze publiekelijk kan worden gedeeld.

Hazerswoude, 8 december 2020

Ing. E. van Egmond RE CISSP QSA 3DS-QSA PCIP CISA
Senior Manager IT audit Noordbeek B.V.

3. Detailrapport: Waarnemingen en conclusies per aandachtsgebied

Wij hebben de in bijlage A genoemde functionarissen geïnterviewd of gesproken, en de in bijlage B genoemde documenten bestudeerd.

Wij hebben waarnemingen voor de fysieke toegangsbeveiliging uitgevoerd bij een datacenter en voor de HSM-sleutelceremonie en logische toegangsbeveiliging bij Justid en CIBG. Onze waarnemingen en conclusies zijn hieronder per aandachtsgebied uitgewerkt.

Het door ons ontwikkelde werkprogramma voor het inventariseren van de beheersingsmaatregelen in relatie tot de eisen voor informatiebeveiliging is gericht op het verkrijgen van de mate van inzicht dat nodig is voor het leveren van publieke transparantie. De aanpak en het werkprogramma zijn voorafgaand aan het onderzoek afgestemd met de opdrachtgever. De bevindingen zijn in concept afgestemd met Justid en CIBG.

In de onderstaande tekst refereren wij aan de documentatie in de vorm van '[doc x]', waarbij 'x' een volgnummer is in de volgorde van ons werkprogramma.

3.1. Sleutelbeheer

3.1.1. Beleid

Norm 1.1 is: *Policies and procedures for managing cryptographic processes and keys are maintained and implemented.*

Wij hebben de volgende documentatie ontvangen:

1	0 Referentiegids covid-19 HSM beheer.pdf	27-08-2020

Justid verzorgt de zogenaamde sleutelceremonies, welke onderdeel zijn van het key management beleid.

Wij hebben de sleutelceremonies bijgewoond, zowel bij Justid als CIBG, en gesproken met de deelnemers, de uitvoerder en de ceremoniemeester over het gevolgde proces. Bij de sleutelceremonies is het proces strikt gevolgd, zoals dat is beschreven het document 'Referentiegids covid-19 HSM beheer'.

De conclusie is: *De sleutelceremonies zijn beschreven en geïmplementeerd.*

3.1.2. HSM versie

Norm 1.2 is: *All key management activity for specified cryptographic keys is performed using an HSM that is FIPS 140-2 Level 3 (overall) or higher certified.*

Wij hebben tijdens de sleutelceremonies foto's gezien van de versie van de vijf in gebruik zijnde HSM's. Deze zijn Utimaco FIPS 140-2 Level 3.

De conclusie is: *De HSM's voldoen aan norm 1.2.*

3.1.3. HSM implementatie

Norm 1.3 is: *The HSM is deployed securely, in accordance with the security policy, and FIPS-approved HSMs are used, the HSM uses the FIPS-approved cryptographic primitives, data-protection mechanisms, and key-management processes for account data decryption and related processes*.

Wij hebben de volgende documentatie ontvangen:

1	0 Referentiegids covid-19 HSM beheer.pdf	27-08-2020

Wij hebben waargenomen dat de HSM beveiligd zijn geïmplementeerd en dat de sleutel primitieven volgens het FIPS-mechanisme worden gegenereerd, zoals het proces voorschrijft. Ten tijde van de sleutelceremonies werden de HSM's ingericht en voorbereid voor het genereren van sleutels. De sleutels zijn volgens het script gegenereerd. Dit is waargenomen door de IT-auditors.

De conclusie is: *De HSM's zijn op een veilige wijze ingericht, conform de richtlijnen*.

3.1.4. Cryptografische architectuur

Norm 1.4 is: *A documented description of the cryptographic architecture exists that includes:*

- *Description of the usage for all keys;*
- *Details of all keys used by each HSM*.

Wij hebben de volgende documentatie ontvangen:

1	0 Referentiegids covid-19 HSM beheer.pdf	27-08-2020
25	Draaiboek-prod.pdf	17-09-2020
26	Procedure Aanmaken Sleutels-v9.pdf	17-09-2020
27	Procedure in gebruik nemen nieuw certificaat-v3.pdf	17-09-2020
28	Procedure opnemen certificaat van andere server-v3.pdf	17-09-2020
29	Procedure opnemen extern ondertekend certificaat-v3.pdf	17-09-2020
30	Procedure Opsturen Gaen-sleutels-v6.pdf	17-09-2020
31	Procedure verifieren certificaatgebruik-v3.pdf	17-09-2020

Tijdens de sleutelceremonies zijn de sleutels geregistreerd. Dit is waargenomen door de IT-auditors. Tevens zijn de functies duidelijk beschreven in document 1.

De conclusie is: *De cryptografische architectuur is op een veilige wijze ingericht, conform de richtlijnen*.

3.1.5. Cryptografisch sleutelmanagement

Norm 1.5 is: *Cryptographic keys are securely managed throughout the cryptographic lifecycle including:*

- *Generation;*
- *Distribution/conveyance;*
- *Storage;*
- *Established crypto periods;*
- *Replacement/rotation when the crypto period is reached;*
- *Escrow/backup;*
- *Key compromise and recovery;*
- *Emergency procedures to destroy and replace keys;*
- *Accountability and audit.*

Wij hebben de volgende documentatie ontvangen:

1	0 Referentiegids covid-19 HSM beheer.pdf	27-08-2020
25	Draaiboek-prod.pdf	17-09-2020
26	Procedure Aanmaken Sleutels-v9.pdf	17-09-2020
27	Procedure in gebruik nemen nieuw certificaat-v3.pdf	17-09-2020
28	Procedure opnemen certificaat van andere server-v3.pdf	17-09-2020
29	Procedure opnemen extern ondertekend certificaat-v3.pdf	17-09-2020
30	Procedure Opsturen Gaen-sleutels-v6.pdf	17-09-2020
31	Procedure verifieren certificaatgebruik-v3.pdf	17-09-2020

Tijdens iedere sleutelceremonie was een IT-audit-team van twee IT-auditors aanwezig om het proces te beoordelen, zowel bij Justid als bij CIBG. De checklists zijn per afgerond onderdeel afgetekend door de teamleider van een IT-audit-team.

Tijdens de sleutelceremonies is de sleutelgeneratie uitgevoerd conform de beschrijving in document 1. Dit is waargenomen door de IT-auditors.

De distributie is tevens tijdens de sleutelceremonies gebeurd. Dit is waargenomen door de IT-auditors.

De opslag van de sleutel gebeurt door de stakeholders individueel in een kluis. De cryptoperiode voor de sleutels, die gebruikt worden voor Google Apple, is vastgesteld volgens de standaard die door Google Apple wordt gehanteerd (default is twee jaar). Justid heeft standaard processen voor het monitoren van de cryptoperiode en wordt automatisch tijdig geïnformeerd over expiratie.

Van elk Master Back-up Key (MBK) is een back-up gemaakt. De stakeholder krijgt twee kaarten met de MBK erop, die volgens de m of n methode zijn aangemaakt. Hierbij is m=3 en n=2. Justid monitort en beheert de sleutels en de restore ervan. Er zijn procedures opgesteld voor vernietiging en vervanging.

De conclusie is: *Het cryptografisch sleutelmanagement is op een veilige wijze ingericht, conform de richtlijnen.*

3.2. Logische toegangsbeveiliging

3.2.1. Toegangsbeveiliging

Norm 2.1 is: *Personnel with logical access to HSMs must be either at the HSM console or using an HSM non-console access solution that has been evaluated by an independent laboratory*.

Wij hebben de volgende documentatie ontvangen:
1 0 Referentiegids covid-19 HSM beheer.pdf 27-08-2020

Tijdens de sleutelceremonies wordt de standaard Admin op de HSM vervangen door een standaard gedefineerde admin, die kan worden ontsloten door de betreffende smartcard met pincode welke beveiligd worden opgeslagen.

De onderliggende non console toegang via VPN is onafhankelijk beoordeeld door AIVD/NBV goedgekeurde CompuWall software.

De conclusie is: *VPN-toegang tot de HSM-omgeving is alleen mogelijk via goedgekeurde software en twee factor authenticatie.*

3.2.2. Externe toegangsbeveiliging

Norm 2.2 is: *Devices used to provide personnel with non-console access to HSMs are secured as follows:*

- *Located in a designated secure area or room that is monitored at all times;*
- *Locked in room/rack/cabinet/ drawer/safe when not in use;*
- *Physical access is restricted to authorized personnel and managed under dual control;*
- *Authentication mechanisms (e.g., smart cards, dongles etc.) for devices with non-console access are physically secured when not in use;*
- *Operation of the device requires dual-control and multifactor authentication;*
- *Devices have only applications and software installed that is necessary;*
- *Devices are verified as having up-to-date security configurations;*
- *Devices cannot be connected to other networks while connected to the HSM;*
- *Devices are cryptographically authenticated prior to the connection being granted access to HSM functions*.

Wij hebben de volgende documentatie ontvangen:

1	0	Referentiegids covid-19 HSM beheer.pdf	27-08-2020

De apparatuur met toegang tot de HSM-omgeving staat in een afgesloten kamer, die met een badge reader door bevoegd personeel kan worden betreden. De afdeling waarin de kamer zich bevindt is extra beveiligd. Alleen bevoegd personeel kan op deze afdeling komen door middel van een badge.

Smart cards, welke worden gebruikt voor het beheer van de HSM-omgeving, worden bewaard in een kluis. De kluis is geobserveerd door auditor ten tijde van de key ceremonie.

Het beheer van de HSM gebeurt door middel van de smartcard en de bijbehorende pincode, waarmee two factor authenticatie is ingericht.

De software wordt up-to-date gehouden, evenals de windows software op de laptop. De laptop volgt de standaard Patch Tuesday van Microsoft.

De laptop heeft alleen toegang tot de netwerkconnectie van de HSM's. Er is geen andere connectie mogelijk. De laptop heeft standaard disk encryptie aanstaan.

De actieve regieorganisatie verzorgt de communicatie naar de betrokkenen en de daadwerkelijke aansturing.

De conclusie is: *De apparatuur met toegang tot de HSM-omgeving is op een veilige wijze ingericht en aangesloten, conform de richtlijnen*.

3.3. Fysieke toegangsbeveiliging

3.3.1. Plaatsing

Norm 3.1 is: *HSMs are stored in a dedicated area(s).*

Wij hebben de volgende documentatie ontvangen:
1 0 Referentiegids covid-19 HSM beheer.pdf 27-08-2020

De fysieke toegangsbeveiliging is uitbesteed aan twee datacenters. Een van deze datacenters is PCI DSS compliant.

De HSM's zijn gemonteerd in een afgesloten kabinet, die is geplaatst in een shared omgeving.

Vanwege de shared omgeving hebben derden toegang tot de ruimte rondom het afgesloten kabinet. Door slordigheid met het wel of niet afsluiten van het kabinet, of door braak, bestaat de mogelijkheid dat derden fysiek toegang kunnen krijgen tot de HSM's.

Wij hebben tijdens de sleutelceremonies foto's van de plaatsing van de HSM's gezien en hebben een locatiebezoek gebracht aan een van twee datacenters.

De conclusie is: *De HSM-omgeving voldoet niet aan norm 3.1 voor fysieke toegangsbeveiliging. De kabinetten met HSM's zijn niet geplaatst in een dedicated area, maar in een shared omgeving, waar derden toegang toe hebben.*

3.3.2. Toegang

Norm 3.2 is: *Physical access to the HSMs is restricted to authorized personnel and managed under dual control.*

Wij hebben de volgende documentatie ontvangen:
1 0 Referentiegids covid-19 HSM beheer.pdf 27-08-2020

Vanwege de shared omgeving hebben derden toegang tot de ruimte rondom het afgesloten kabinet met de HSM's. Door slordigheid met het wel of niet afsluiten van het kabinet, of door braak, bestaat de mogelijkheid dat derden fysiek toegang kunnen krijgen tot de HSM's.

De conclusie is: *De HSM-omgeving voldoet niet aan norm 3.2, aangezien de fysieke toegang tot de kabinetten met HSM's niet is beperkt tot alleen geautoriseerd personeel. Tevens is geen sprake van dual control.*

Bijlage A Overzicht waarnemingen

In het kader van de privacy van de betrokken functionarissen zijn hieronder alleen hun functies benoemd.

Nr.	Waarneming	Datum
1.	Locatiebezoek datacenter: technicus	21-08-2020
2.	Sleutelceremonies HSM in de testomgeving: vertegenwoordigers van de participerende organisaties en IT-auditors	28-08-2020
3.	Sleutelceremonies HSM in de acceptatieomgeving: vertegenwoordigers van de participerende organisaties en IT-auditors	10-09-2020
4.	Sleutelceremonies HSM in de productieomgeving: vertegenwoordigers van de participerende organisaties en IT-auditors	17-09-2020

Bijlage B Lijst van geraadpleegde documentatie en steekproeven

Wij hebben de volgende documentatie ontvangen, waarbij de stukken zijn genummerd conform ons werkprogramma voor de assessment:

Nr.	Dossierstuk	Datum
1	0 Referentiegids covid-19 HSM beheer.pdf	27-08-2020
2	C5b Proces Verbaal creatie MBK op Test-HSM_getekend 28082020_excl pin.pdf	28-08-2020
3	C5c Stakeholder Proces Verbaal_getekend 28082020_excl pin.pdf	28-08-2020
4	C6a Key Ceremonie Creatie Admin smartcard_getekend 28082020.pdf	28-08-2020
5	C6b Proces Verbaal creatie Admin smartcard_getekend 28082020_excl pin.pdf	28-08-2020
6	C7a Key Ceremonie Creatie Users op Test-HSM_getekend 28082020.pdf	28-08-2020
7	C7b Proces Verbaal creatie users op Test-HSM_getekend 28082020_excl password.pdf	28-08-2020
8	10a Key ceremonie creatie Users op Acceptatie HSM covid-19_draaiboek_getekend 10092020.pdf	10-09-2020
9	10b Key ceremonie creatie Users op Acceptatie HSM covid-19_proces-verbaal excl password_getekend 10092020.pdf	10-09-2020
10	11a Key ceremonie MBK porteren naar fail-over Acceptatie HSM covid-19_draaiboek_getekend_10092020.pdf	10-09-2020
11	11b Key ceremonie MBK porteren naar fail-over Acceptatie HSM covid-19_proces-verbaal_getekend_10092020.pdf	10-09-2020
12	8a Key ceremonie creatie MBK op Acceptatie HSM covid-19_draaiboek _getekend10092020.pdf	10-09-2020
13	8b Key ceremonie creatie MBK op Acceptatie HSM covid-19_proces-verbaal excl pin_getekend 10092020.pdf	10-09-2020
14	8c Key ceremonie creatie MBK op Acceptatie HSM covid-19_proces-verbaal ontvangst smartcard stakeholders excl pin_getekend 10092020.pdf	10-09-2020

Nr.	Dossierstuk	Datum
15	9a Key ceremonie creatie Admin smartcard op Acceptatie HSM covid-19_draaiboek_getekend 10092020.pdf	10-09-2020
16	9b Key ceremonie creatie Admin smartcard op Acceptatie HSM covid-19_proces-verbaal_getekend 10092020.pdf	10-09-2020
17	12a Key ceremonie creatie MBK op Productie HSM covid-19 HSM beheer definitief getekend.pdf	17-09-2020
18	12b Proces verbaal creatie MBK op Productie HSM covid-19 HSM beheer getekend EXCL PINCODES.pdf	17-09-2020
19	13a Key ceremonie creatie Admin smartcard op Productie HSM covid-19 HSM beheer definitief getekend.pdf	17-09-2020
20	13b Proces verbaal creatie Admin smartcard op Productie HSM covid-19 HSM beheer definitief getekend.pdf	17-09-2020
21	14a Key ceremonie creatie Users op Productie HSM covid-19 HSM beheer definitief getekend.pdf	17-09-2020
22	14b Proces Verbaal creatie Users op Productie HSM covid-19 HSM beheer definitief getekend EXCL Passoword.pdf	17-09-2020
23	15a Key ceremonie MBK porteren naar fail-over Productie HSM covid-19 HSM beheer defintief getekend.pdf	17-09-2020
24	15b Proces verbaal MBK porteren naar fail-over Productie HSM covid-19 HSM beheer definitief getekend.pdf	17-09-2020
25	Draaiboek-prod.pdf	17-09-2020
26	Procedure Aanmaken Sleutels-v9.pdf	17-09-2020
27	Procedure in gebruik nemen nieuw certificaat-v3.pdf	17-09-2020
28	Procedure opnemen certificaat van andere server-v3.pdf	17-09-2020
29	Procedure opnemen extern ondertekend certificaat-v3.pdf	17-09-2020
30	Procedure Opsturen Gaen-sleutels-v6.pdf	17-09-2020
31	Procedure verifieren certificaatgebruik-v3.pdf	17-09-2020

Bijlage C Het werkprogramma

Het onderstaande door ons ontwikkelde werkprogramma voor het inventariseren van de beheersingsmaatregelen in relatie tot de eisen voor informatiebeveiliging en privacybescherming is gericht op het verkrijgen van de mate van inzicht dat nodig is voor het leveren van publieke transparantie.

ID	Onderwerp	Norm voor controlemaatregel
1	**Sleutelbeheer**	
1.1	Beleid	Policies and procedures for managing cryptographic processes and keys are maintained and implemented.
1.2	HSM-versie	All key management activity for specified cryptographic keys is performed using an HSM that is FIPS 140-2 Level 3 (overall) or higher certified.
1.3	HSM-implementatie	The HSM is deployed securely, in accordance with the security policy and FIPS-approved HSMs are used, the HSM uses the FIPS-approved cryptographic primitives, da-ta-protection mechanisms, and key-management processes for account data decryption and related processes.
1.4	Cryptografie architectuur	A documented description of the cryptographic architecture exists that includes: ♦ Description of the usage for all keys; ♦ Details of all keys used by each HSM.
1.5	Cryptografie sleutelmanagement	Cryptographic keys are securely managed throughout the cryptographic lifecycle including: ♦ Generation; ♦ Distribution/conveyance; ♦ Storage; ♦ Established crypto periods; ♦ Replacement/rotation when the crypto period is reached; ♦ Escrow/backup; ♦ Key compromise and recovery; ♦ Emergency procedures to destroy and replace keys; ♦ Accountability and audit.
2	**Logische toegangsbeveiliging**	
2.1	Toegangsbeveiliging	Personnel with logical access to HSMs must be either at the HSM console or using an HSM non-console access solution that has been evaluated by an independent laboratory.
2.2	Externe toegangsbeveiliging	Devices used to provide personnel with non-console access to HSMs are secured as follows: ♦ Located in a designated secure area or room that is monitored at all times; ♦ Locked in room/rack/cabinet/ drawer/safe when not in use;

ID	Onderwerp	Norm voor controlemaatregel
		♦ Physical access is restricted to authorized personnel and managed under dual control; ♦ Authentication mechanisms (e.g., smart cards, dongles etc.) for devices with non-console access are physically secured when not in use; ♦ Operation of the device requires dual-control and multifactor authentication; ♦ Devices have only applications and software installed that is necessary; ♦ Devices are verified as having up-to-date security configurations; ♦ Devices cannot be connected to other networks while connected to the HSM; ♦ Devices are cryptographically authenticated prior to the connection being granted access to HSM functions.
3	**Fysieke toegangsbeveiliging**	
3.1	Plaatsing	HSMs are stored in a dedicated area(s).
3.2	Toegang	Physical access to the HSMs is restricted to authorized personnel and managed under dual control.