



Ministerie van Veiligheid en Justitie

> Retouradres Postbus 20301 2500 EH Den Haag



Directoraat-Generaal
Rechtspleging en
Rechts-handhaving
Directie Juridische en
Operationele
Aangelegenheden
DJOA

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/venj
Contactpersoon



Datum 6 juli 2016
Onderwerp Uw wobverzoek inzake controle reisdocumenten

Ons kenmerk
769027

*Bij beantwoording de datum
en ons kenmerk vermelden.
Wilt u slechts één zaak in uw
brief behandelen.*

Geachte ,

Bij brief van 16 maart 2016, ontvangen op 18 maart 2016, heeft u namens de en , bij het ministerie een verzoek ingediend als bedoeld in artikel 3, eerste lid, van de Wet openbaarheid van bestuur (hierna: Wob).

Uw verzoek

Uw verzoek heeft betrekking op procedures die betrekking hebben op de controle van reisdocumenten met een chip.

Wettelijk kader

Uw verzoek valt onder de reikwijdte van de Wob. Voor de relevante Wob-artikelen verwijs ik u naar bijlage 1.

Inventarisatie documenten en gemaakte afspraken

In uw brief geeft u aan dat u eenzelfde verzoek heeft ingediend bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en het ministerie van Defensie. Tussen de ministeries heeft onderling contact plaatsgevonden over de afhandeling van uw Wob-verzoek. Hierbij is afgesproken dat documenten die bij meerdere ministeries berusten, slechts eenmaal aan u worden verstrekt en wel door het ministerie dat voor dat onderdeel van uw verzoek inhoudelijk het meest is aangewezen.

Veel van de door u gevraagde informatie is reeds openbaar. Eveneens is afgesproken dat voor zover dat zo is, dit per document wordt meegedeeld waar mogelijk onder vermelding van de vindplaats. Ook dit wordt gedaan door het ministerie dat voor dat onderdeel van uw verzoek inhoudelijk het meest is aangewezen.

Een deel van de informatie waarom u verzoekt is aanwezig bij het ministerie van

Veiligheid en Justitie. Het betreft documenten bij de Justitiële Informatiedienst (Justid) en documenten bij het Directoraat-Generaal Vreemdelingenzaken (DGVz).

Bij brief van 24 maart 2016 heb ik de ontvangst van uw verzoek aan u bevestigd.

Bij brief van 18 april 2016 is de termijn om op uw verzoek te beslissen met vier weken verlengd.

Op 23 mei 2016 heeft mijn medewerker [] met u afgesproken dat twee deelbesluiten zullen worden genomen; één besluit dat ziet op de documenten aanwezig bij Justid en één besluit dat ziet op de documenten aanwezig bij DGVz. Ten aanzien van het eerste deelbesluit is de termijn, met uw instemming verdaagd tot 3 juni. Ten aanzien van het tweede deelbesluit is afgesproken dat [] als contactpersoon fungeert.

De onderdelen van uw verzoek die op grond van het voorgaande aan de orde komen, zijn de onderdelen bij bullet 1, 2, 3, 4, 9, 10, 11, 12, 13, 14 en 15 van uw Wob-verzoek. Veel van de door u gevraagde informatie is zoals gezegd reeds openbaar. Waar dat het geval is zal ik hieronder bij de desbetreffende onderdeel verwijzen naar de relevante vindplaats.

1: de procedure voor het verkrijgen van de Country Signing Certificate Authority (hierna CSCA) sleutelgegevens en de Certificate Revocation List's van andere landen.

De procedures voor het verkrijgen van CSCA certificaten zijn beschreven in DOC 9303, 7e editie, van de internationale civiele luchtvaartorganisatie (ICAO). Meer in het bijzonder in deel 12, hoofdstuk 5, van genoemd document. Nederland is actief lid van de Public Key Directory (PKD) van ICAO en gedraagt zich naar de regels zoals vastgesteld binnen de PKD.

DOC 9303 is een openbare bron die u kunt raadplegen op:

<http://www.icao.int/publications/pages/publication.aspx?docnum=9303>

Voor de specifieke Nederlandse situatie verwijs ik daarnaast naar de brief van 20 augustus 2014 (Kamerstukken II 2013-2014, 25764, nr. 84) die mijn ambtgenoot van BZK aan de Tweede Kamer heeft gestuurd om deze onder meer te informeren over het instellen van een Single Point of Contact voor het uitwisselen van certificaten binnen de Europese Unie volgens uit EU-verordening 2252-2004.

U kunt deze brief vinden op:

<https://zoek.officielebekendmakingen.nl/dossier/25764/kst-25764-84?resultIndex=24&sorttype=1&sortorder=4>

Voorts verwijs ik u naar het besluit van de Minister van BZK, waarin de opdrachtbrief met bijlage van 5 juni 2015 die de Minister van BZK aan Justid heeft verzonden deels openbaar is gemaakt.

2: de procedure voor het distribueren van het verkregen sleutelmateriaal naar de systemen van de Nederlandse overheid die worden gebruikt bij de controle van reisdocumenten.

Nederland heeft, naar voorbeeld van ICAO, een eigen Nationale Public Key Directory (hierna: NPKD).

De NPKD is de betrouwbare bron voor de systemen van de Nederlandse overheid die worden ingezet bij de controle van relsdocumenten. De NPKD is ontworpen, ontwikkeld en beheerd door Justid. Distributie vanuit de NPKD wordt gedaan middels een zogenoemd Terminal Control Centre.

Met betrekking tot dit onderdeel van uw verzoek, beschik ik over 4 documenten.

1. Een informatiedocument , waarop de procedure wordt afgebeeld.
Dit document maak ik openbaar.
2. Document NL-E03. EAC-PKI-NL- Exploitatie- deel 3.1., NPKD Beheer.
3. Document EAC-PKI-NL-Architectuur—Deel 2: Overzicht architectuur en infrastructuur. Architectuuroverzicht (NL-A02).
4. Document EAC-PKI-NL—Architectuur—Deel 3: Communicatie.

De hiervoor genoemde documenten onder 2,3 en 4 maak ik deels openbaar. Voor zover ik informatie niet openbaar maak, volgt daarvoor hierna een motivering.

Eerbiediging van de persoonlijke levenssfeer

De naam van de behandelend ambtenaar die de 3 hiervoor genoemde desbetreffende documenten heeft opgesteld alsmede zijn/haar telefoonnummer maak ik niet openbaar in verband met de eerbiediging van de persoonlijke levenssfeer van betrokkenen (artikel 10, tweede lid, aanhef en onder e, van de Wob). Dit belang afwegende tegen het belang van openbaarmaking van deze gegevens, acht ik het belang genoemd in artikel 10, tweede lid, aanhef en onder e, van de Wob zwaarwegender.

Voor zover het de namen van ambtenaren betreft is hierbij het volgende van belang. Weliswaar kan, waar het gaat om beroepshalve functioneren van ambtenaren, slechts in beperkte mate een beroep worden gedaan op het belang van eerbiediging van hun persoonlijke levenssfeer. Dit ligt anders indien het betreft het openbaarmaken van namen van de ambtenaren. Namen zijn immers persoonsgegevens en het belang van eerbiediging van de persoonlijke levenssfeer kan zich tegen het openbaarmaken daarvan verzetten. Daarbij is van belang dat het hier niet gaat om het opgeven van een naam aan een individuele burger die met een ambtenaar in contact treedt, maar om openbaarmaking van de naam in de zin van de Wob. Tevens betreft het geen persoon die vanuit zijn of haar functie gewoonlijk in de openbaarheid treedt.

Het voorkomen van onevenredige bevoordeling of benadeling

Op grond van artikel 10, tweede lid, aanhef en onder g, van de Wob blijft verstrekking van informatie achterwege voor zover het belang daarvan niet opweegt tegen het belang van het voorkomen van onevenredige bevoordeling of benadeling van bij de aangelegenheid betrokken natuurlijke personen of rechtspersonen dan wel van derden.

Van het document zoals hiervoor genoemd onder 2 maak ik enkele zinsneden in paragraaf 5 en enkele passages in Annex A niet openbaar.

Van het document zoals hiervoor genoemd onder 3 maak ik de inhoud van de paragrafen in hoofdstuk 7 en Annex A en de daarin opgenomen figuren en tabellen

niet openbaar. Van het document zoals hiervoor genoemd onder 4 maak ik de inhoud van hoofdstuk 7, paragraaf 3 en hoofdstuk 8, paragraaf 2.1 en de daarin figuren en tabellen niet openbaar.

Openbaarmaking van de hiervoor genoemde passages zou naar mijn oordeel leiden tot onevenredige benadeling van Justid. De hiervoor genoemde passages hebben te maken met de Infrastructuur van PKI EAC. Het openbaren van deze informatie zou hackers inzicht geven in deze structuur en het daarmee eenvoudiger maken te hacken en daarmee toegang te krijgen tot informatie waaruit IP adressen zijn te herleiden of zelfs direct zijn opgenomen. Ik ben van oordeel dat de bescherming van deze gegevens zwaarder moet wegen dan het belang van openbaarheid.

3: de procedure voor het distribueren van de door de Nederlandse overheid gegenereerde CSCA-sleutelgegevens en de Certificate Revocation List's aan andere landen.

De procedures voor het distribueren van CSCA certificaten zijn beschreven in Doc 9303, 7^e editie, van de internationale civiele luchtvaartorganisatie, deel 12. Dit document is reeds openbaar. Voor de vindplaats verwijs ik u naar de website die ik onder 1 noemde.

Nederland is actief lid van de Public Key Directory (PKD) van ICAO en gedraagt zich naar de regels zoals vastgesteld binnen de PKD. De regels voor de ICAO zijn vooral vastgelegd in de Memorandum of Understanding en Rules of Procedure. U kunt deze vinden op:

<http://www.icao.int/Security/mrtd/Downloads/PKD%20Documents/Regulations%20of%20the%20ICAO%20PKD.pdf> (regulations for the ICAO PKD)

<http://www.icao.int/Security/mrtd/Downloads/PKD%20Documents/Memorandum%20of%20Understanding%20-%20English.pdf> (memorandum of understanding)

<http://www.icao.int/Security/mrtd/Downloads/PKD%20Documents/PKD%20Board%20-%20Rules%20of%20Procedure.pdf> (rules of procedure)

Ten overvloede wijs ik er daarbij nog op dat de CSCA's van Nederland en de van toepassing zijnde CRL's gepubliceerd zijn op de website van het RVIG.

<http://www.rvig.nl/documenten/publicaties/2015/10/20/csa-certificaten-en-de-certificate-revocation-list>

4: alle CSCA-sleutelgegevens en sleutels en de Certificate Revocation List's van andere landen in mijn bezit;

In de NPKD bevinden zich alleen certificaten/publieke sleutels die voldoen aan de voorwaarden zoals beschreven in genoemd DOC 9303 van ICAO. Ieder land geeft in een zogenaamde Masterlist aan over welke publieke CSCA certificaten van welke landen zij beschikt en welke worden gebruikt bij bijv. grenscontrole. Door Justid is ook een Masterlist gemaakt. Hierin zijn alle CSCA-certificaten die in het bezit zijn van de Justitiële Informatiedienst opgenomen. Deze masterlist betreft een binair bestand. Voor het lezen van de certificaten/publieke sleutels moet gebruik gemaakt worden van een programma wat in staat is om LDAP bestanden uit te pakken en om te zetten naar de desbetreffende certificaten. Gezien de aard van de informatie

(binaire bestanden) zal ik u deze separaat -digitaal- door middel van een e-mail verstrekken. Daarbij zal ik tevens een bestand verstrekken met daarin de technische informatie hoe de betreffende Masterlist is gemaakt en kan worden geopend.

Overigens wijs ik u er volledigheidshalve ook op dat er een aantal landen (Duitsland, Zwitserland, Spanje) zijn die de certificaten die ze in hun bezit hebben op een masterlist hebben gezet.

Daarvoor zijn verschillende bronnen beschikbaar. De masterlist van Duitsland is te vinden op:

https://www.bsi.bund.de/EN/Topics/ElectrIDDDocuments/CSCAcertGermany/cscGermany_node.html

Daarnaast zijn er diverse andere Masterlisten (zoals die van Spanje en Zwitserland) te vinden op <https://pkddownloadsg.icao.int/>

9: Informatie over de landen die het Active Authentication-mechanisme toepassen in de reisdocumenten die zij uitgeven.

Ik beschik niet over dergelijke informatie. Evenmin is mij een openbare bron bekend waarop dergelijke informatie raadpleegbaar is.

10: Informatie over de landen aan wie Nederland haar Extended Access Controlsleutels (hierna: EAC) ter beschikking stelt.

Met betrekking tot dit verzoek geldt dat er geen specifieke Extended Access Control sleutels bestaan maar ik heb aangenomen dat u doelt op het publieke deel van het CVCA-certificaat. Hiervoor geldt dat Nederland aan geen enkel land deze informatie beschikbaar heeft gesteld. Voor zover dit in de toekomst zal gebeuren, zal dit worden gedaan binnen de werking van de 'Common Certificate Policy for the Extended Access Control Infrastructure for passports and travel documents by EU member states' als besloten door de Europese Commissie op 30 september 2013 en gepubliceerd onder kenmerk BSI TR-03139.

Dit document is openbaar en kunt u raadplegen op:

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03139/BSI-TR-03139_pdf.pdf?__blob=publicationFile

11: de procedure voor het distribueren van het Nederlandse EAC-sleutelgegevens naar systemen van derden.

Deze procedure voor het distribueren naar systemen van derden staat eveneens beschreven in "Common Certificate Policy for the extended control Infrastructure for passports and travel documents issued by EU member states, BSI TR-03139, Version 2.1.

U kunt dit document raadplegen door middel van de hiervoor onder 10 genoemde link.

12: Informatie over de geldigheidstermijn van de Nederlandse EAC-sleutels;

Ik heb uw verzoek zo geïnterpreteerd dat u vraagt naar de geldigheidsduur van het publieke deel van het CVCA-certificaat. Er bestaan namelijk geen specifieke Extended Access Control sleutels. De huidige geldigheidstermijn hiervan is 3 jaar.

Zoals hiervoor vermeld wordt dit certificaat nog niet gebruikt. Als dit certificaat wel gebruikt gaat worden, wordt bij distributie aan andere landen waarschijnlijk het voorbeeld van de RVIG gevolgd door het publieke deel van de CVCA te publiceren op een website. BZK en V&J zijn daarvoor voornemens een voor dit doel gezamenlijke website in te richten (Eac-pki.nl).

De geldigheidsduur staat overigens vermeld in het document dat ik hiervoor onder 10 noemde: het 'Common Certificate Policy for the Extended Access Control Infrastructure for passports and travel documents by EU member states' als besloten door de Europese Commissie op 30 september 2013 en gepubliceerd onder kenmerk BSI TR-03139, onder 4.7.

13: Informatie over de landen van wie Nederland EAC-sleutels ontvangt.

Nederland beschikt nog niet over CVCA certificaten van andere landen. Zoals ook door de minister van BZK in zijn brief van 20 augustus 2014 (Kamerstukken 2013-2014, 25764, nr 84) aan de Tweede Kamer is toegelicht, wordt op dit moment wel getest hoe het uitleesproces (EAC-proces) in zijn werk moet gaan. Nederland test op dit moment met 9 landen binnen de Europese Unie.

U kunt deze brief vinden door middel van de link genoemd onder 1.

14: de procedure voor het ontvangen van EAC-sleutelgegevens van andere landen.

De procedure staat eveneens beschreven in "Common Certificate Policy for the extended control infrastructure for passports and travel documents issued by EU member states, BSI TR-03139, Version 2.1.

U kunt dit document raadplegen door middel van de hiervoor onder 10 genoemde link.

15: de procedure voor het distribueren van de ontvangen EAC-sleutelgegevens van andere landen naar de systemen van de Nederlandse overheid die worden gebruikt voor het controleren van reisdocumenten;

Deze procedure staat omschreven in Het Architectuuroverzicht (NL-A02) zoals genoemd bij uw deelverzoek nummer 2.

Codering van gelakte delen

Met behulp van letters is per document aangegeven welk type gegeven is weggehaald en in de gedeeltelijk openbaar te maken documenten op welke passages op welke gronden zijn geweigerd.

A. Persoonsgegevens zoals namen, telefoonnummers, (email)adressen en handtekeningen (artikel 10, tweede lid, aanhef en onder e, Wob);

B. Het belang van het voorkomen van onevenredige bevoordeling of benadeling van bij de aangelegenheid betrokken natuurlijke personen of rechtspersonen dan wel van derden (artikel 10, tweede lid, aanhef en onder g, van de Wob).

Wijze van openbaarmaking

De documenten genoemd onder 2 treft u bij dit besluit in kopie aan. De bestanden genoemd onder 4, zult u separaat per e-mail ontvangen. Daarnaast zullen de openbaar gemaakte stukken worden geplaatst op rijksoverheid.nl.

Ingebrekestelling

Op 23 juni 2016 ontving ik uw brief waarin u mij in gebreke stelt omdat de beslistermijn voor de behandeling van uw verzoek is overschreden. In het tweede deelbesluit zal ik inhoudelijk op uw ingebrekestelling reageren.

Ik ga er vanuit u met het vorenstaande afdoende te hebben geïnformeerd.

Hoogachtend,
de Minister van Veiligheid en Justitie
namens deze, [redacted]

[redacted]
[redacted]
[redacted]
[redacted] Coördinerend specialistisch adviseur Juridische zaken

Tegen dit besluit en het tweede deelbesluit gezamenlijk kunt u binnen zes weken na bekendmaking van het laatste deelbesluit een bezwaarschrift indienen. Het bezwaarschrift moet door de indiener zijn ondertekend en bevat ten minste zijn naam en adres, de dagtekening, een omschrijving van het besluit waartegen het bezwaar is gericht en de gronden waarop het bezwaar rust. Dit bezwaarschrift moet worden gericht aan: de Minister van Veiligheid en Justitie, t.a.v. Directie Wetgeving en Juridische Zaken, Sector Juridische Zaken, Postbus 20301, 2500 EH Den Haag.

Bijlage – Relevante artikelen uit de Wob

Artikel 1

In deze wet en de daarop berustende bepalingen wordt verstaan onder:

- a. document: een bij een bestuursorgaan berustend schriftelijk stuk of ander materiaal dat gegevens bevat;
- b. bestuurlijke aangelegenheid: een aangelegenheid die betrekking heeft op beleid van een bestuursorgaan, daaronder begrepen de voorbereiding en de uitvoering ervan;
- c. intern beraad: het beraad over een bestuurlijke aangelegenheid binnen een bestuursorgaan, dan wel binnen een kring van bestuursorganen in het kader van de gezamenlijke verantwoordelijkheid voor een bestuurlijke aangelegenheid;
- d. niet-ambtelijke adviescommissie: een van overheidswege ingestelde instantie, met als taak het adviseren van een of meer bestuursorganen en waarvan geen ambtenaren lid zijn, die het bestuursorgaan waaronder zij ressorteren adviseren over de onderwerpen die aan de instantie zijn voorgelegd. Ambtenaren, die secretaris of adviserend lid zijn van een adviesinstantie, worden voor de toepassing van deze bepaling niet als leden daarvan beschouwd;
- e. ambtelijke of gemengd samengestelde adviescommissie: een instantie, met als taak het adviseren van één of meer bestuursorganen, die geheel of gedeeltelijk is samengesteld uit ambtenaren, tot wier functie behoort het adviseren van het bestuursorgaan waaronder zij ressorteren over de onderwerpen die aan de instantie zijn voorgelegd;
- f. persoonlijke beleidsopvatting: een opvatting, voorstel, aanbeveling of conclusie van een of meer personen over een bestuurlijke aangelegenheid en de daartoe door hen aangevoerde argumenten;
- g. milieu-informatie: hetgeen daaronder wordt verstaan in artikel 19.1a van de Wet milieubeheer;
- h. hergebruik: het gebruik van informatie die openbaar is op grond van deze of een andere wet en die is neergelegd in documenten berustend bij een overheidsorgaan, voor andere doeleinden dan het oorspronkelijke doel binnen de publieke taak waarvoor de informatie is geproduceerd;
- i. overheidsorgaan:
 - 1°. een orgaan van een rechtspersoon die krachtens publiekrecht is ingesteld, of
 - 2°. een ander persoon of college, met enig openbaar gezag bekleed.

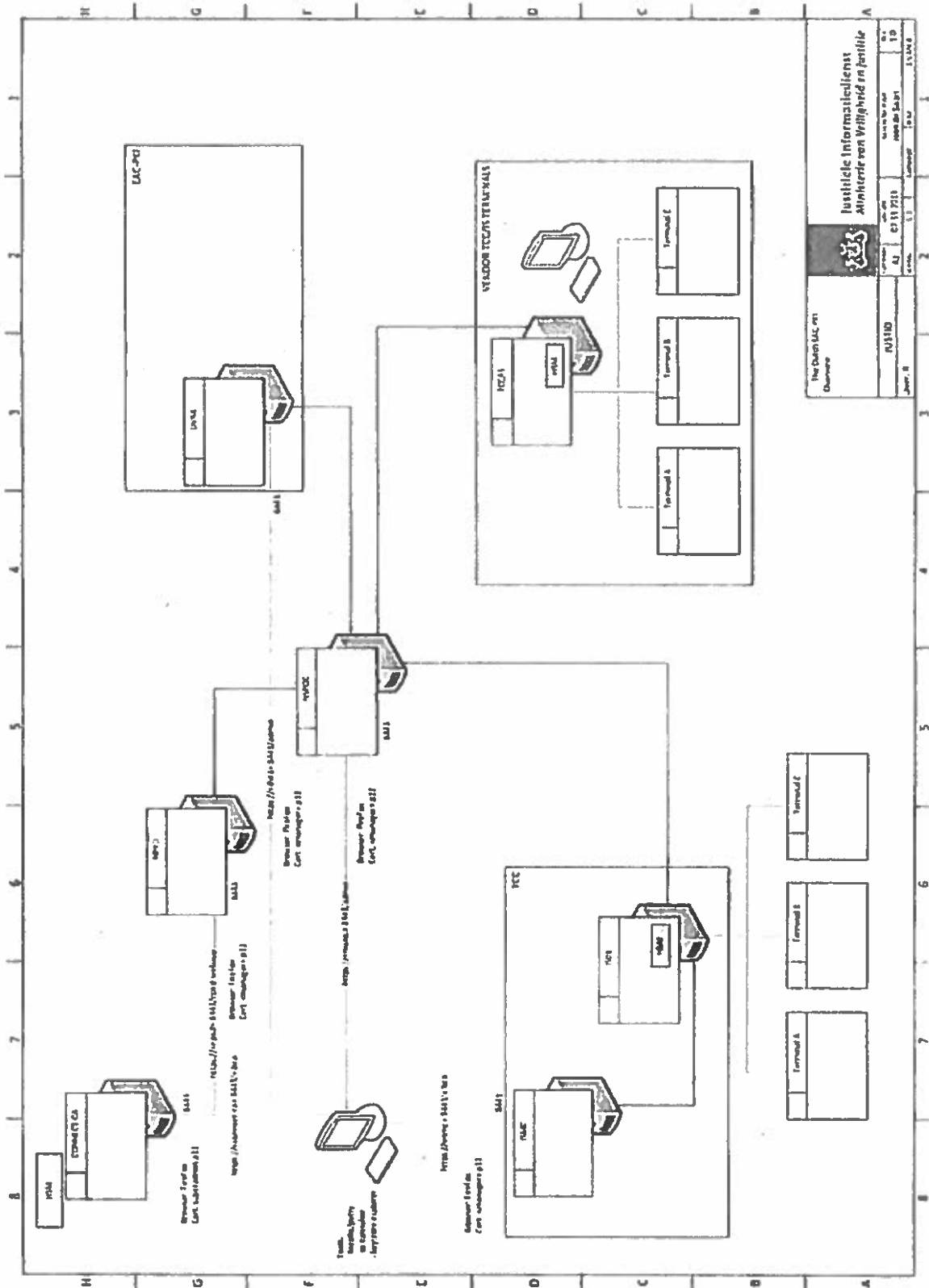
Artikel 3

1. Een ieder kan een verzoek om informatie neergelegd in documenten over een bestuurlijke aangelegenheid richten tot een bestuursorgaan of een onder verantwoordelijkheid van een bestuursorgaan werkzame instelling, dienst of bedrijf.
2. De verzoeker vermeldt bij zijn verzoek de bestuurlijke aangelegenheid of het daarop betrekking hebbend document, waarover hij informatie wenst te ontvangen.
3. De verzoeker behoeft bij zijn verzoek geen belang te stellen.
4. Indien een verzoek te algemeen geformuleerd is, verzoekt het bestuursorgaan de verzoeker zo spoedig mogelijk om zijn verzoek te preciseren en is het hem daarbij behulpzaam.
5. Een verzoek om informatie wordt ingewilligd met inachtneming van het bepaalde in de artikelen 10 en 11.

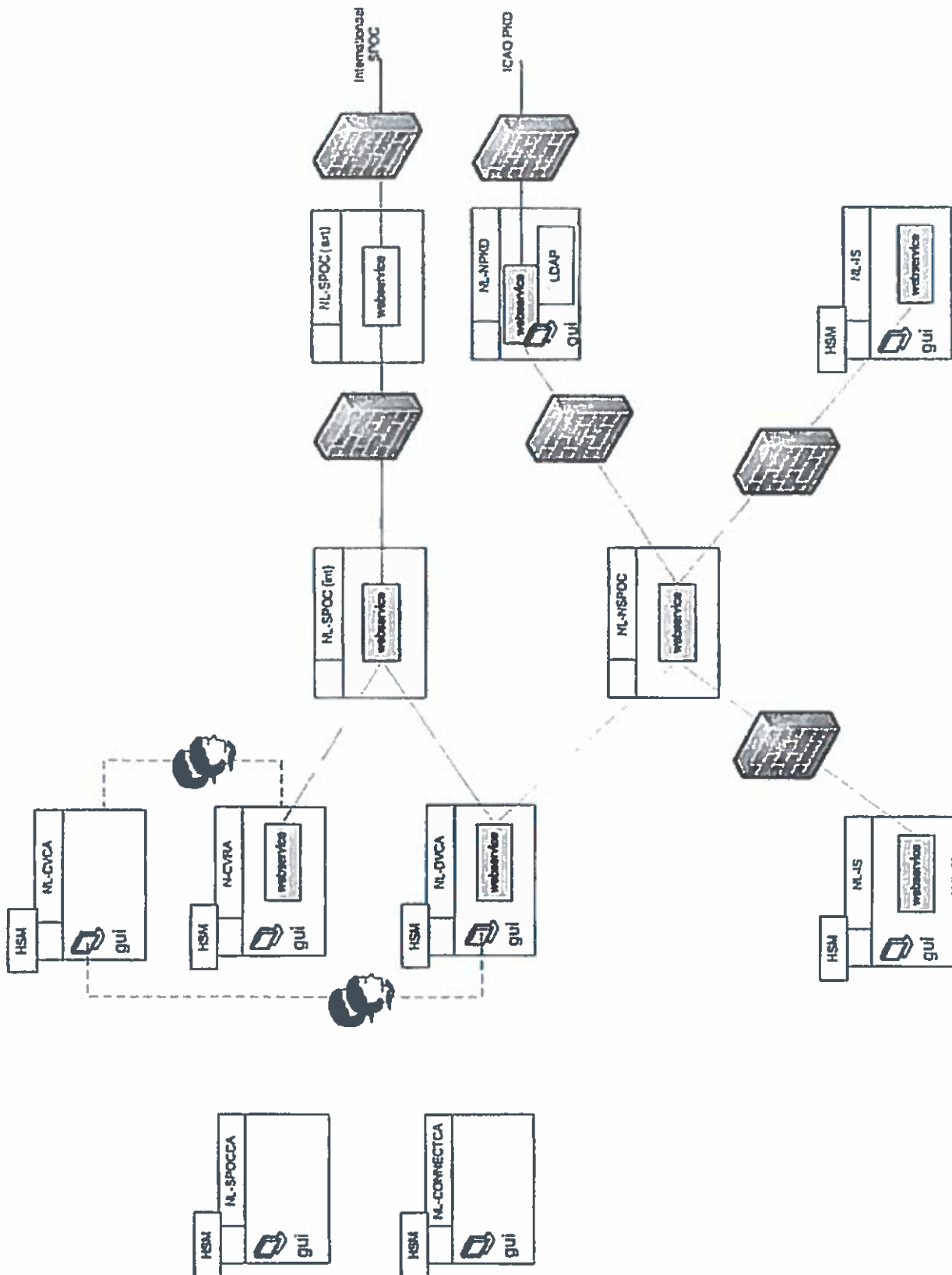
Artikel 10

1. Het verstrekken van informatie ingevolge deze wet blijft achterwege voor zover dit:
 - a. de eenheid van de Kroon in gevaar zou kunnen brengen;

- b. de veiligheid van de Staat zou kunnen schaden;
 - c. bedrijfs- en fabricagegegevens betreft, die door natuurlijke personen of rechtspersonen vertrouwelijk aan de overheid zijn meegedeeld;
 - d. persoonsgegevens betreft als bedoeld in paragraaf 2 van hoofdstuk 2 van de Wet bescherming persoonsgegevens, tenzij de verstrekking kennelijk geen inbreuk op de persoonlijke levenssfeer maakt.
2. Het verstrekken van informatie ingevolge deze wet blijft eveneens achterwege voor zover het belang daarvan niet opweegt tegen de volgende belangen:
- a. de betrekkingen van Nederland met andere staten en met internationale organisaties;
 - b. de economische of financiële belangen van de Staat, de andere publiekrechtelijke lichamen of de in artikel 1a, onder c en d, bedoelde bestuursorganen;
 - c. de opsporing en vervolging van strafbare feiten;
 - d. inspectie, controle en toezicht door bestuursorganen;
 - e. de eerbiediging van de persoonlijke levenssfeer;
 - f. het belang, dat de geadresseerde erbij heeft als eerste kennis te kunnen nemen van de informatie;
 - g. het voorkomen van onevenredige bevoordeling of benadeling van bij de aangelegenheid betrokken natuurlijke personen of rechtspersonen dan wel van derden.
3. Het tweede lid, aanhef en onder e, is niet van toepassing voorzover de betrokken persoon heeft ingestemd met openbaarmaking.
4. Het eerste lid, aanhef en onder c en d, het tweede lid, aanhef en onder e, en het zevende lid, aanhef en onder a, zijn niet van toepassing voorzover het milieu-informatie betreft die betrekking heeft op emissies in het milieu. Voorts blijft in afwijking van het eerste lid, aanhef en onder c, het verstrekken van milieu-informatie uitsluitend achterwege voorzover het belang van openbaarmaking niet opweegt tegen het daar genoemde belang.
5. Het tweede lid, aanhef en onder b, is van toepassing op het verstrekken van milieu-informatie voor zover deze handelingen betreft met een vertrouwelijk karakter.
6. Het tweede lid, aanhef en onder g, is niet van toepassing op het verstrekken van milieu-informatie.
7. Het verstrekken van milieu-informatie ingevolge deze wet blijft eveneens achterwege voorzover het belang daarvan niet opweegt tegen de volgende belangen:
- a. de bescherming van het milieu waarop deze informatie betrekking heeft;
 - b. de beveiliging van bedrijven en het voorkomen van sabotage.
8. Voorzover het vierde lid, eerste volzin, niet van toepassing is, wordt bij het toepassen van het eerste, tweede en zevende lid op milieu-informatie in aanmerking genomen of deze informatie betrekking heeft op emissies in het milieu.



Justitie Informatiesysteem Ministerie van Veiligheid en Justitie		Versie: 1.0 Datum: 15-10-2010
Project: RVS100 Versie: 1.0	Auteurs: J. J. J. J. Datum: 15-10-2010	Status: In Review Datum: 15-10-2010



doc 3



Justitiële Informatiedienst
Ministerie van Veiligheid en Justitie

RUBRICERING: DEPARTEMENTAAL VERTROUWELIJK

EAC-PKI-NL--Architectuur--Deel 2: Overzicht architectuur en infrastructuur

OID	B
Auteur	JustiD
Status	Definitief
Versie	1.0
Datum	22 november 2011
Rubricering	Departementaal Vertrouwelijk
Vastgesteld door	A
Datum vaststelling	22 november 2011

Colofon

Afzendgegevens

Justitiële Informatiedienst

Egbert Gorterstraat 6
7607 GB Almelo
Postbus 337
7600 AH Almelo
www.justid.nl

Contactpersoon

A

Projectnaam

EAC-PKI-NL

Contactpersoon: A

Auteurs

JustID

Versie overzicht

Versie	Datum	Steller	Omschrijving
1.0	22-11-2011	JustiD	Definitief

EAC-PKI-NL — Architectuur — Deel 2: Overzicht architectuur en infrastructuur

Inhoud	Pagina
1 Scope.....	9
2 Normatieve referenties.....	9
3 Termen en definities.....	9
4 Afkortingen	9
5 Architectuuroverzicht	10
5.1 Systemen.....	12
5.1.1 Systemen ten behoeve van de Signing PKI.....	12
5.1.2 Systemen ten behoeve van de Verifying PKI.....	12
5.1.3 Systemen ten behoeve van berichtenverkeer.....	14
5.1.4 Systemen ten behoeve van beheer.....	15
5.1.5 Systemen ten behoeve van beveiliging van het berichtenverkeer.....	15
5.2 Verbindingen en Informatieuitwisseling	16
5.2.1 Verbindingen met betrekking tot de NSPOC.....	16
5.2.2 Verbindingen met betrekking tot de SPOC	17
5.2.3 Verbindingen ten behoeve van de Country Signing PKI.....	18
5.2.4 Verbinding tussen IS en Terminal met Reader	18
5.2.5 Verbindingen t.b.v. de NL-SPOC-CA	18
5.2.6 Verbindingen t.b.v. de NL-CONNECT-CA.....	18
6 Scenario's	19
6.1 Signing PKI scenario's.....	19
6.2 Verifying PKI scenario's.....	23
6.3 Inspection System – Terminal met Reader scenario's.....	29
6.4 Verbindingsbeveiligingsscenario's	29
6.4.1 SPOC PKI scenario's	29
6.4.2 CONNECT PKI scenario's	31
7 Infrastructuuroverzicht	34
7.1 Storage	35
7.2 Servers	36
7.3 Ethernet switches	36
7.4 Hardware Security Module	37
7.5 Secure Services Gateway Enterprise Firewall	37
7.6 Verbindingskabels	37
A.1 Storage.....	39
A.2 Servers	39
A.3 Ethernet switches	40
A.4 Firewall	41
A.5 Verbindingskabels	41

(noot: hoofdstuk 7 en appendices moeten onder regie van JustID worden geactualiseerd)

Voorwoord

Verscheidende Nederlandse identiteitsbewijzen volgens de Wet op de identificatieplicht, zoals reisdocumenten (MRTDs) en verblijfsvergunningen (RPs), zijn inmiddels voorzien van een chip waarin document- en houdergegevens digitaal zijn opgeslagen. Dit is in overeenstemming met Europese besluiten over het toevoegen van een chip en de specificaties waaraan de chip dient te voldoen. Ook andere EU en Schengen lidstaten hebben hun paspoorten en verblijfsvergunningen voorzien van een dergelijke chip. Internationaal hebben verschillende non-EU/Schengen landen hun reisdocumenten voorzien van een chip volgens ICAO Doc 9303 die daardoor grotendeels identiek is aan de chip in Europese reisdocumenten.

Om de authenticiteit van de gegevens in de chip elektronisch te kunnen verifiëren, zijn deze gegevens digitaal ondertekend door de uitgevende instanties in de verschillende landen. Inspectiesystemen hebben de signing PKI Public Key certificaatketens behorend bij de Private Keys waarmee de gegevens ondertekend zijn nodig om de authenticiteit van de gegevens te kunnen controleren. Uitwisseling van de benodigde certificaten gebeurt bilateraal en daarnaast via de ICAO Public Key directory.

De elektronische identiteitsbewijzen kunnen in de chip naast biografische gegevens en een afbeelding van het gezicht ook een tweetal vingerafdrukken bevatten. Voor identiteitsbewijzen uitgegeven binnen de EU en Schengen is dit verplicht. Ook wordt binnen de EU/Schengen geëist dat deze meer gevoelige biometrische gegevens zijn beschermd met een extra beveiligingsmechanisme.

Het mechanisme zorgt voor veilige communicatie met de chip en toegang tot de vingerafdrukken in de chip wordt slechts gegeven aan daartoe geautoriseerde inspectiesystemen. Dit staat bekend als Extended Access Control (EAC). Wanneer een inspectiesysteem data wil uitlezen die is beveiligd met EAC, moet het inspectiesysteem zich authenticeren aan de chip en tonen dat het toegangsrechten heeft om de beveiligde data uit te lezen. Deze authenticatie is gebaseerd op zogenaamde Card Verifiable Certificates (CV certificaten), die door de chip in een identiteitsbewijs kunnen worden geverifieerd. De toegangsrechten van het inspectiesysteem staan gecodeerd in deze CV Certificates.

Nadat de terminal zich heeft geauthenticeerd op basis van CV Certificates en een Private Key, geeft de chip toegang tot gegevens waarvoor toegangsrechten in het CV Certificate zijn gecodeerd. Voor het genereren en distribueren van deze CV Certificates zijn verifying Public Key Infrastructures, ook wel EAC-PKI-NL genoemd, gespecificeerd binnen Nederland. Uitwisseling van CV Certificates en Certificate Requests met andere EU/Schengen lidstaten om ook de vingerafdrukken uit de buitenlandse identiteitsbewijzen te kunnen lezen, vindt plaats via een Single Point of Contact (SPOC).

Voor de EAC-PKI-NL is een Policy Authority (PA) opgericht. In deze PA zijn de volgende organisaties vertegenwoordigd:

- Ministerie van Veiligheid & Justitie;
- Ministerie van Buitenlandse Zaken;
- JustID.

Daarnaast kunnen eventueel andere belanghebbenden vertegenwoordigd zijn in de PA, bijvoorbeeld partijen die verantwoordelijk zijn voor de uitgifte van de identiteitsbewijzen.

Het secretariaat van de PA wordt gevoerd door de Justitiële Informatiedienst (JustID). De verantwoordelijkheid voor de uitvoering van deze PKI is belegd bij JustID. Vanuit deze verantwoordelijkheid heeft JustID ook dit document opgesteld.

Dit document is onderdeel van een serie documenten onder de algemene titel *EAC-PKI-NL — Architectuur* dat bestaat uit de volgende onderdelen:

- *Deel 1: Referentieids PKI voor EAC-PKI-NL*
- *Deel 2: Overzicht architectuur en infrastructuur*
- *Deel 3: Verbindingen*

EAC-PKI-NL — Architectuur — Deel 2: Overzicht architectuur en infrastructuur

1 Scope

Dit document beschrijft de architectuur en infrastructuur van de Public Key Infrastructures (PKIs) voor inspectie van elektronische Identiteitsbewijzen en bevat de volgende zaken

- Functioneel overzicht van de systemen, verbindingen en informatie-uitwisseling.
- Beschrijving van de verschillende scenario's binnen de EAC-PKI-NL.
- Beschrijving van de infrastructuur.

2 Normatieve referenties

[NL-A01] EAC-PKI-NL—Architectuur—Deel 1: Referentiegidis PKI voor eMRTDs.

Ten behoeve van dit document gelden de referenties zoals beschreven in [NL-A01].

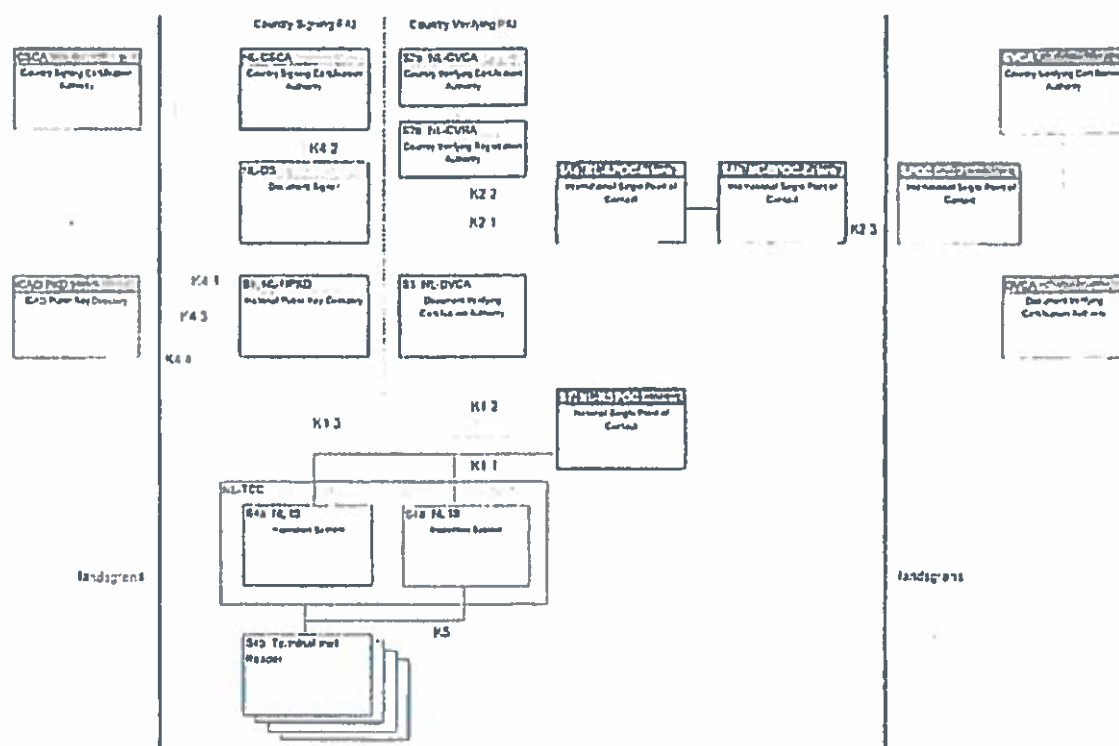
3 Termen en definities

Ten behoeve van dit document gelden de termen en definities zoals beschreven in [NL-A01].

4 Afkortingen

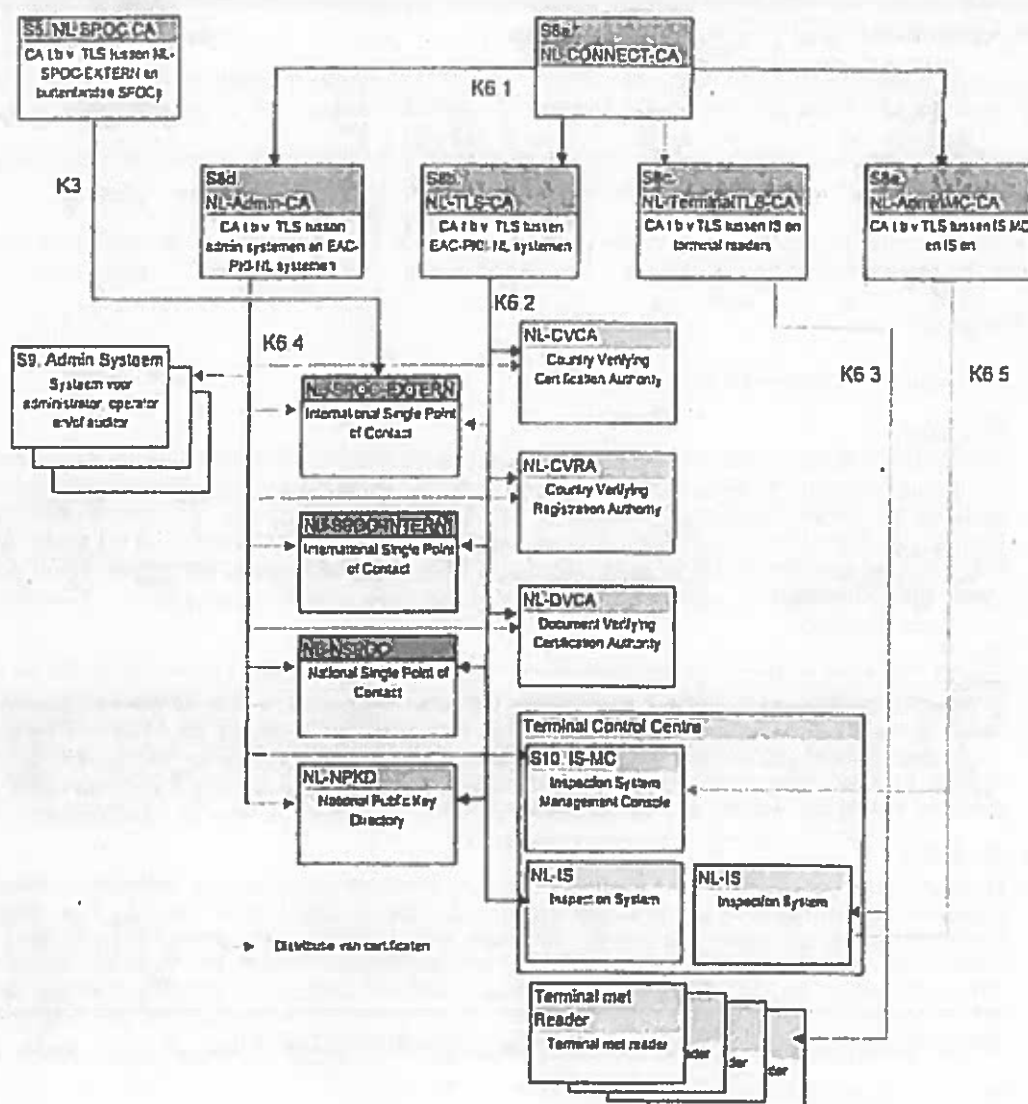
Ten behoeve van dit document gelden de afkortingen zoals beschreven in [NL-A01].

5 Architectuuroverzicht



Figuur 1 EAC-PKI-NL architectuuroverzicht

Figuur 1 geeft een overzicht van de systemen die gebruikt worden voor identiteitscontrole op basis van de chip in elektronische identiteitsbewijzen en van de verbindingen tussen deze systemen. Het middelste gedeelte van de figuur geeft de Nederlandse systemen weer. De stippellijnen geven de verdeling van de systemen aan over de Signing and Verifying PKI's. Er zijn afzonderlijke Signing PKI's voor de verschillende soorten identiteitsbewijzen (eMRTDs en eRPs) en afzonderlijke Verifying PKI's voor de verschillende soorten identiteitsbewijzen. In de figuur is voor de overzichtelijkheid echter slechts één Nederlandse Signing PKI en één Nederlandse Verifying PKI aangegeven. Voor de verschillende PKI's kunnen fysiek dezelfde systemen gebruikt worden.



Figuur 2: PKIs voor communicatiebeveiliging

Voor het beheer van de EAC-PKI-NL systemen kunnen administratoren, operators en auditors gebruik maken van Administratie Systemen (S9) waarmee de EAC-PKI-NL systemen te bereiken zijn. Het IS is niet rechtstreeks te bereiken, maar uitsluitend via het Inspectie Systeem Management Console (IS-MC) (S10.) dat zich in het Terminal Control Centre bevindt.

Om de communicatie tussen de verschillende systemen te beveiligen wordt gebruik gemaakt van Transport Layer Security (TLS) over HTTP (HTTPS). Daarvoor bestaan verschillende PKIs.

Voor het beveiligen van de communicatie tussen de NL-SPOC-Extern en buitenlandse SPOCs wordt gebruikt gemaakt van de SPOC PKI waarvoor certificaten uitgegeven worden door de NL-SPOC-CA.

Voor het beveiligen van de communicatie tussen de Nederlandse EAC-PKI-NL systemen wordt gebruikt gemaakt van de NL-TLS-PKI waarvoor certificaten uitgegeven worden door de NL-TLS-CA, een sub-CA onder de NL-CONNECT-CA.

Voor het beveiligen van de verbindingen tussen Inspectie Systemen en Terminals met Readers wordt gebruik gemaakt van de NL-Terminal-TLS-PKI waarvoor de certificaten uitgegeven worden door de NL-Terminal-TLS-CA, een sub-CA onder de NL-CONNECT-CA.

Communicatie tussen Administratie Systemen en de EAC-PKI-NL systemen wordt beveiligd door certificaten uitgegeven door de NL-Admin-CA, een sub-CA onder de NL-CONNECT-CA.

Communicatie tussen het Inspectie Systeem Management Console en de Inspectie Systemen zelf wordt beveiligd door certificaten uitgegeven door NL-AdminMC-CA onder de NL-CONNECT-CA.

Al deze systemen staan functioneel beschreven in paragraaf 5.1. De verbindingen en de communicatie tussen de systemen wordt beschreven in paragraaf 5.2.

5.1 Systemen

5.1.1 Systemen ten behoeve van de Signing PKI

NL-CSCA

Een NL-CSCA is een Certification Authority systeem van de Nederlandse Country Signer dat bovenaan de NL Country Signing PKI hiërarchie staat voor het digitaal ondertekenen van de data op de chips van Nederlandse identiteitsbewijzen. Er zijn verschillende NL-CSCAs voor de verschillende soorten identiteitsbewijzen. Een NL-CSCA geeft Certificates uit aan een of meerdere NL-DS'en. Onder één NL-CSCA kunnen meerder NL-DS'en vallen. De NL-CSCAs vallen buiten de scope van de EAC-PKI-NL en deze serie documenten.

NL-DS

Een NL-DS is een systeem van een Nederlandse Document Signer. Figuur 1 toont één NL-DS. Er kunnen meerdere Nederlandse Document Signers bestaan per NL-CSCA. Een NL-DS tekent de data op de chips van Nederlandse identiteitsbewijzen met zijn Private Key. De bijbehorende Public Key bevindt zich in een Certificate getekend door de NL-CSCA. De Terminal met Reader heeft de CSCA-DS Certificate Chain nodig voor controle van de integriteit van de data op de chip van het identiteitsbewijs. De NL-DS'en vallen buiten de scope van de EAC-PKI-NL en deze serie documenten.

S1. NL-NPKD

De NL-NPKD is de Nederlandse Nationale Public Key Directory waarin zich de nationale en internationale Certificate Chains bevinden uit de Signer hiërarchieën. De NL-NPKD bevat ook de CRLs, Masterlist en DefectList. Deze informatie hebben de Terminals met Readers nodig voor het controleren van de Nederlandse en buitenlandse identiteitsbewijzen die aangeboden worden. De NL-NPKD kan certificaten, CRLs, MasterLists en DefectLists ontvangen door middel van bilaterale uitwisseling of uit de ICAO PKD. Binnen Nederland is er één NL-NPKD. De NL-NPKD valt onder verantwoordelijkheid van Justitie. De eisen aan de NL-NPKD staan beschreven in *Systeemspecificatie NL-NPKD [NL-S1]*.

5.1.2 Systemen ten behoeve van de Verifying PKI

S2a. NL-CVCA

Een NL-CVCA is een Certification Authority systeem van de Nederlandse Country Verifier dat bovenaan een NL Country Verifying PKI hiërarchie staat voor het authenticeren van Inspectie Systemen aan elektronische identiteitsbewijzen en daarmee het uitlezen van gevoelige informatie op de chip mogelijk maakt. Een aan het CVCA Root Certificate gekoppeld Link Certificate wordt in de identiteitsbewijzen geplaatst. Er is één NL-CVCA voor reisdocumenten en één NL-CVCA voor verblijfsvergunningen. Het aantal NL-CVCAs kan indien gewenst worden uitgebreid.

Een NL-CVCA tekent de Certificates van onderliggende Document Verifiers. Dit kunnen Nederlandse en ook buitenlandse Document Verifiers zijn. Onder één NL-CVCA kunnen meerdere NL-DVCAs en buitenlandse DVCAs vallen. Een NL-CVCA ontvangt alle Certificate Requests via de bijbehorende NL-CVRA.

Een NL-CVCA plaatst Outer Signatures voor initiële NL-DVCA Certificate Requests bij buitenlandse DVCAs.

Een NL-CVCA heeft een Certificate Store waarin de volgende Certificates opgeslagen worden:

- de eigen CVCA Certificate Chain (Root en Link Certificates)

De NL-CVCAs vallen onder verantwoordelijkheid van Justitie. De NL-CVCA staat beschreven in het document *Systeemspecificatie NL-CVCA en NL-CVRA [NL-S2]*

S2b. NL-CVRA

Een NL-CVRA is een Registration Authority systeem van de Nederlandse Country Verifier. Een NL-CVRA is gekoppeld aan één NL-CVCA

Een NL-CVRA ontvangt Certificate Requests van Nederlandse en ook buitenlandse Document Verifiers via de NL-SPOC en staat die op voor goedkeuring. Een deel van de goedkeuring is geautomatiseerd. Hiertoe raadpleegt de CVRA zijn database en Certificate Store. Na de automatische goedkeuring vindt een finale handmatige goedkeuring plaats.

Een NL-CVRA heeft een Certificate Store waarin de volgende Certificates opgeslagen worden:

- de elgen CVCA Certificate Chain (Root en Link Certificates)
- door de NL-CVCA uitgegeven DVCA Certificates: deze DVCA Certificates worden opgeslagen voor controle van de Outer Signature
- buitenlandse CVCA Certificates voor verificatie van de Outer Signature bij een Initiele buitenlandse DVCA Certificate Request.

Na de finale goedkeuring stuurt een NL-CVRA de Certificate Request door naar de bijbehorende NL-CVCA voor het aanmaken van de Certificates. De NL-CVRAs vallen onder verantwoordelijkheid van Justitie. De NL-CVRA staat beschreven in het document *Systeemspecificatie NL-CVCA en NL-CVRA [NL-S2]*

S3. NL-DVCA

Een NL-DVCA is een Certification Authority systeem van de Nederlandse Document Verifier dat ook Registration Authority (RA) functionaliteit bevat. Figuur 1 toont één NL-DVCA. Er kunnen aparte NL-DVCAs zijn voor de verschillende soorten identiteitsbewijzen en per type identiteitsbewijs voor verschillende domeinen (gemeentehulzen, grenscontrole, politie, ...). In principe mag elk land slechts één DVCA per soort identiteitsbewijs hebben. Echter, onder bepaalde omstandigheden is het toegestaan om meerdere DVCAs per soort identiteitsbewijs te hebben, mits de subjectregistratie van de DVs op een gecoördineerde wijze verloopt [EU-CP].

Een NL-DVCA genereert en tekent de Certificates van onderliggende vertrouwde NL-IS'en. Initiele NL-IS Certificate Requests moeten handmatig verwerkt worden met behulp van de Registration Authority functionaliteit. Er kunnen meerdere NL-IS'en onder één NL-DVCA vallen. Ook kan één NL-IS onder meerdere NL-DVCAs vallen.

Een NL-DVCA vraagt zelf Certificates aan bij één bovenliggende NL-CVCA en bij buitenlandse CVCAs. Daarvoor plaatst een NL-DVCA een Inner en Outer Signature over een Certificate Requests. Voor de initiele Certificate Request bij de NL-CVCA plaatst een NL-DVCA de Inner Signature met de nieuw gegenereerde Private Key en is de Outer Signature leeg. Voor een initiele Certificate Request bij een buitenlandse CVCA plaatst een NL-DVCA de Inner Signature met de nieuw gegenereerde Private Key. De NL-DVCA vraagt een Outer Signature bij de NL-CVCA. Daarvoor plaatst de NL-DVCA eerst een Outer Signature over het GetOuterSignature bericht aan de NL-CVCA met de Private Key die hoort bij het door de NL-CVCA aan de NL-DVCA uitgegeven Certificate. Een NL-DVCA kan dus pas Certificate Requests naar buitenlandse DVCAs sturen als al een Certificate van de NL-DVCA ontvangen is. De NL-CVCA controleert deze Outer Signature en vervangt deze door een Outer Signature met de eigen Private Key. Voor volgende Certificate Requests wordt de Outer Signature geplaatst door de NL-DVCA met de huidige Private Key die hoort bij het door de CVCA in kwestie aan de NL-DVCA uitgegeven Certificate.

Een NL-DVCA heeft een Certificate Store waarin de volgende Certificates opgeslagen worden:

- Certificate Chains voor de NL-CVCA en buitenlandse CVCAs. Deze Certificate Chains worden door de NL-DVCA periodiek opgevraagd bij de NL-SPOC en kunnen daardoor enige latency vertonen.
- door de NL-DVCA uitgegeven NL-IS Certificates: deze NL-IS Certificates worden opgeslagen voor controle van de Outer Signature bij een Certificate Request.

Een NL-DVCA houdt bij welke IS'en bij deze NL-DVCA zijn geautoriseerd voor ontvangst van welke certificaten. Tot op het niveau van een individueel certificaat kan de DVCA een IS configureren, maar ook kunnen IS profielen worden gehanteerd. Nadat de autorisatie van de IS'en - de zogenaamde IS autorisatie - is aangepast of nadat de set beschikbare certificaten op de NL-DVCA is aangepast wordt vanuit de NL-

DVCA een SendISauthorisation bericht aan de NSPOC verstuurd waarin de NL-DVCA de IS autorisaties en de Verifier Certificate Chains kenbaar maakt

Een NL-DVCA valt onder verantwoordelijkheid van Justitie. De NL-DVCA staat beschreven in het document *Systeemspecificatie NL-DVCA* [NL-S3]

S4a. NL-IS

Een Inspectie Systeem is een systeem van de Nederlandse Document Verifier dat Nederlandse Terminals met Readers voorziet van de benodigde gegevens voor controle van elektronische identiteitsbewijzen. Onder één NL-IS kunnen meerdere Terminals met Readers vallen.

Een IS voorziet Terminals met Readers van de benodigde Signer Certificate Chains voor het controleren van de authenticiteit van de data op de chips. Het IS haalt bij de NL-NSPOC nationale en internationale Signer Certificate Chains op. Een NL-IS is slechts aan één (de) NL-NSPOC gekoppeld.

Om een Terminal met Reader toegang te verschaffen tot de gevoelige, met EAC beveiligde informatie op de chips beschikt een NL-IS over Public-Private Key Pairs met bijbehorende Verifier Certificates voor authenticatie van het geautoriseerde NL-IS aan binnen- en buitenlandse identiteitsbewijzen. Een NL-IS ontvangt de door het identiteitsbewijs gegenereerde challenge via een Terminal met Reader, tekent deze challenge met de juiste Private Key en voorziet de Terminal met Reader van de response en de bijbehorende Certificate Chain uit de Verifier PKI.

Een NL-IS vraagt Verifier Certificates met autorisatie aan bij de NL-DVs die weer geautoriseerd en gecertificeerd zijn door de CV van het land van afgifte van het Identiteitsbewijs. Een NL-IS kan onder meerdere NL-DVCAs vallen.

Een NL-IS valt onder verantwoordelijkheid van Justitie. Het NL-IS staat beschreven in *Systeemspecificatie NL-IS* [NL-S4]

S4b. Terminal met Reader

Een Terminal met Reader is een systeem dat een geautoriseerde inspecterende instantie, zoals bijvoorbeeld de KMar of de IND, gebruikt voor het controleren van elektronische identiteitsbewijzen. De Terminal met Reader leest de data van de chip en controleert deze, eventueel ook met de biometrische kenmerken van de houder. Om de integriteit van de data op de chip te kunnen controleren moet een Terminal met Reader de beschikking hebben over de Certificates uit de Document Signer hiërarchie. De Terminal met Reader ontvangt deze Signer Certificate Chains van het NL-IS waaraan het gekoppeld is. Om toegang te krijgen tot de gevoelige, met EAC beveiligde informatie op de chip, zoekt de Terminal met Reader contact met het NL-IS voor het laten ondertekenen van de door het identiteitsbewijs gegenereerde challenge en het verkrijgen van de bijbehorende Verifier PKI Certificate Chain. Een Terminal met Reader is gekoppeld aan één NL-IS, maar onder één NL-IS zullen meerdere Terminals met Readers vallen.

5.1.3 Systemen ten behoeve van berichtenverkeer

S6a. NL-SPOC-Intern

De NL-SPOC-Intern verzorgt de communicatie tussen de NL-CVRAs en CVCA's, en NL-DVCAs. Ook ontvangt de NL-SPOC-Intern via de NL-SPOC-Extern berichten van buitenlandse CVCA's en DVCAs en geeft die door aan de NL-DVCAs en NL-CVCAs en vice versa. De NL-SPOC-Intern is verantwoordelijk voor het doorsturen van DVCA Certificate Requests naar de juiste CVCA en van door een CVCA gegenereerde Certificates aan de juiste DVCA. Binnen Nederland bestaat één NL-SPOC-Intern.

Daarnaast voorziet de NL-SPOC-Intern NL-DVCAs op verzoek van de binnen- en buitenlandse CVCA Certificate Chains waarvoor de NL-DVCA geautoriseerd is. Ook voorziet de NL-SPOC-Intern NL-CVRAs op verzoek van de buitenlandse CVCA Certificate Chains. De NL-SPOC-Intern ontvangt notificaties van CVCA's over nieuwe Certificates en vraagt periodiek bij binnen- en buitenlandse CVCA's de Certificate Chains op. De NL-SPOC-Intern slaat deze Certificate Chains op in een Certificate Store. De autorisaties van de NL-DVCAs worden in de NL-SPOC-Intern bijgehouden in het configureerbare overzicht van de DV ketenautorisatie.

De NL-SPOC-Intern valt onder verantwoordelijkheid van Justitie en staat beschreven in het document *Systeemspecificatie NL-SPOC* [NL-S6]

S6b. NL-SPOC-Extern

De NL-SPOC-Extern communiceert met buitenlandse SPOCs voor het doorgeven van berichten tussen

Nederlandse DVCAs en buitenlandse CVCAs en tussen buitenlandse DVCAs en de Nederlandse CVCAs. De NL-SPOC-Extern is gekoppeld aan de NL-SPOC-Intern en geeft berichten onvangen van buitenlandse SPOCs door aan de NL-SPOC-Intern en ontvangt berichten van de NL-SPOC-Intern om door te geven aan buitenlandse SPOCs. De NL-SPOC-Extern valt onder verantwoordelijkheid van Justitie. De NL-SPOC-Extern staat beschreven in het document *Systeemspecificatie NL-SPOC* [NL-S6].

57. NL-NSPOC

De NL-NSPOC is het Nederlandse nationale systeem dat verantwoordelijk is voor informatie-uitwisseling tussen NL-IS'en en NL-DVCAs en tussen NL-IS'en en de NL-NPKD. Binnen Nederland bestaat één NL-NSPOC. Hieraan zijn meerder NL-IS'en en meerder NL-DVCAs gekoppeld. Aan één NL-DVCA kunnen meerdere NL-IS'en gekoppeld zijn en één NL-IS kunnen aan meerder NL-DVCAs gekoppeld zijn. De NL-NSPOC houdt een registratie van de koppelingen bij: de zogenaamde IS autorisatie. Vanuit elke DV wordt via een SendISauthorisation bericht aan de NSPOC de IS autorisaties en Verifier Certificate Chains kenbaar gemaakt.

De NL-NSPOC vraagt op verzoek van een IS de Signer Certificate Chains, CRLs, MasterList en DefactList op bij de NL-NPKD. De NL-NSPOC vertaalt de vraag van het IS naar een LDAP verzoek aan de NL-NPKD. De NSPOC houdt geen store aan voor deze informatie, waardoor er geen latency kan optreden.

De NL-NSPOC stuurt een Certificate Request van een NL-IS door naar de juiste NL-DVCA en het door een NL-DVCA uitgegeven Certificate naar het juiste NL-IS.

De NL-NSPOC wacht totdat er vanuit een NL-DVCA een SendISauthorisation bericht aan de NSPOC de IS autorisaties en Verifier Certificate Chains kenbaar gemaakt. Meerdere NL-DVCA kunnen zijn verbonden waarbij elk NL-DVCA een eigen lijst kenbaar maakt. De NSPOC slaat de IS autorisaties en Certificates op in de NL-NSPOC Certificate Store. Aangezien deze informatie periodiek door IS'en wordt opgevraagd, kan hier enige latency inzitten. Op verzoek van een NL-IS voorziet de NL-NSPOC het IS van de Verifier Certificate Chains waarvoor dat NL-IS geautoriseerd is. Dit is vastgelegd in het overzicht van de IS autorisaties dat op de NL-NSPOC aanwezig is.

De NL-NSPOC valt onder verantwoordelijkheid van Justitie en staat beschreven in *Systeemspecificatie NL-NSPOC* [NL-S7].

5.1.4 Systemen ten behoeve van beheer

S9. Administratie Systeem (Admin Systeem)

Om de EAC-PKI-NL systemen te beheren kunnen administrators, operators en auditors gebruik maken van Administratie Systemen. Dit zijn specifiek voor dit doel beschikbare laptops of PCs binnen het netwerk. Met behulp van een standaard browser kunnen de systemen beheerd worden.

S10. Inspectie Systeem Management Console

De Inspectie Systemen kunnen rechtstreeks vanuit een Admin Systeem beheerd worden, maar de voorkeur is ze te beheren via het Inspectie Systeem Management Console (IS-MC). Dit kan zowel lokaal als remote gebeuren. Het IS-MC wordt door operators van JustID gebruikt om de dagelijkse werkzaamheden op de IS'en uit te voeren. Per Terminal Control Centre (TCC) is er één IS-MC.

5.1.5 Systemen ten behoeve van beveiliging van het berichtenverkeer

S5. NL-SPOC-CA

De NL-SPOC-CA is een Nederlandse Certification Authority die de NL-SPOC-Extern voorziet van Certificates ten behoeve van verbodingsbeveiliging (TLS) voor communicatie met buitenlandse SPOCs. De NL-SPOC-CA bevat ook de Registration Authority functionaliteit. Het NL-SPOC-CA Root Certificate moet met buitenlandse SPOCs op een veilige manier (offline) uitgewisseld worden. De NL-SPOC-CA valt onder verantwoordelijkheid van Justitie en staat beschreven in *Systeemspecificatie NL-SPOC-CA* [NL-S5].

S8a. NL-CONNECT-CA

De NL-CONNECT-CA is een Nederlandse Certification Authority die boven een aantal sub-CAs staat die de systemen binnen de NL-EAC-PKI voorzien van Certificates ten behoeve van verbodingsbeveiliging (TLS). De NL-CONNECT-CA bevat ook Registration Authority functionaliteit. De NL-CONNECT-CA voorziet in een gemeenschappelijke Certificate Policy en Policy Authority voor de onderliggende sub-CAs. Onder de NL-CONNECT-CA vallen vier sub-CAs. De NL-CONNECT-CA voorziet de Public Keys van deze sub-CAs van

een Certificate. Het Root Certificate van de NL-CONNECT-CA wordt niet verspreid naar de systemen binnen de EAC-PKI-NL om de verschillende domeinen gescheiden te houden. De NL-CONNECT-CA en onderliggende sub-CAs staan beschreven in *Systeemspecificatie NL-CONNECT-CA* [NL-S8].

De NL-Connect-CA is een stand alone machine, die niet direct gekoppeld is met andere systemen. Handmatig worden de certificaten op gegevensdragers geladen.

S8b. NL-TLS-CA

De NL-TLS-CA voorziet de EAC-PKI-NL systemen, namelijk NL-NPKD, NL-CVRA, NL-DVCA, NL-IS, NL-SPOC-Intern, NL-SPOC-Extern en NL-NSPOC van Certificates ten behoeve van verbindingsbeveiliging (TLS). De NL-TLS-CA bevat ook Registration Authority functionaliteit. Het (Self-Signed) Root Certificate van de NL-TLS-CA moet op een veilige manier (offline) beschikbaar gesteld worden aan de EAC-PKI-NL systemen zodat die systemen met behulp van dit Certificate de TLS Client en Server Certificates voor onderlinge communicatie kunnen controleren. De NL-TLS-CA houdt geen CRL bij aangezien de aangesloten systemen geen mogelijkheid hebben de CRL op te vragen.

S8c. NL-TerminalTLS-CA

De NL-TerminalTLS-CA voorziet de IS'en en de Terminals met Readers van Certificates ten behoeve van verbindingsbeveiliging (TLS). De NL-TerminalTLS-CA bevat ook Registration Authority functionaliteit. Het (Self-Signed) Root Certificate van de NL-TerminalTLS-CA moet op een veilige manier (offline) beschikbaar gesteld worden aan de IS'en en Terminals met Readers zodat die systemen met behulp van dit Certificate de TLS Client en Server Certificates voor communicatie tussen IS en Terminal met Reader kunnen controleren. De NL-TerminalTLS-CA houdt geen CRL bij aangezien de aangesloten systemen geen mogelijkheid hebben de CRL op te vragen.

S8d. NL-Admin-CA

De NL-Admin-CA voorziet de EAC-PKI-NL systemen (behalve het IS) en de beheersystemen van Certificates ten behoeve van verbindingsbeveiliging (TLS). De NL-Admin-CA geeft derhalve TLS Certificates uit aan NL-NPKD, NL-CVRA, NL-DVCA, NL-SPOC-Intern, NL-SPOC-Extern, NL-NSPOC, Admin Systemen en IS-MC. De NL-Admin-CA bevat ook Registration Authority functionaliteit. Het (Self-Signed) Root Certificate van de NL-Admin-CA moet op een veilige manier (offline) beschikbaar gesteld worden aan deze systemen zodat de systemen met behulp van dit Certificate de TLS Client en Server Certificates voor communicatie tussen beheersystemen en EAC-PKI-NL systemen en tussen de beheersystemen onderling kunnen controleren. De NL-Admin-CA houdt geen CRL bij aangezien de aangesloten systemen geen mogelijkheid hebben de CRL op te vragen.

S8e. NL-AdminMC-CA

De NL-AdminMC-CA voorziet IS-MC en de IS'en van Certificates ten behoeve van verbindingsbeveiliging (TLS). De NL-AdminMC-CA bevat ook Registration Authority functionaliteit. Het (Self-Signed) Root Certificate van de NL-AdminMC-CA moet op een veilige manier (offline) beschikbaar gesteld worden aan IS-MC en IS'en zodat deze systemen met behulp van dit Certificate de TLS Client en Server Certificates voor communicatie tussen IS-MC en IS kunnen controleren. De NL-AdminMC-CA houdt geen CRL bij aangezien de aangesloten systemen geen mogelijkheid hebben de CRL op te vragen.

De systeemspecificaties van de onder Justitie vallende systemen geven een overzicht van de interne processen die deze systemen moeten ondersteunen en van de beveiligingsseisen aan de systemen.

5.2 Verbindingen en informatieuitwisseling

In Figuur 1 en Figuur 2 zijn de verbindingen tussen de systemen genummerd. Het gaat om de volgende verbindingen:

5.2.1 Verbindingen met betrekking tot de NSPOC

K1.1. NL-IS – NL-NSPOC

Tussen NL-NSPOC en NL-IS wordt de volgende informatie uitgewisseld.

- Certificate Requests van NL-IS naar NL-DVCA
- Certificates van NL-DVCA naar NL-IS
- Certificate Chain Requests van NL-IS bij NL-NSPOC
- Certificate Chains van NL-NSPOC naar NL-IS
- Aanvragen van Signer Certificates, CRL Signer PKIs, MasterLists en DefectLists door NL-IS bij NL-NPKD
- Signer Certificates, CRLs Signer, MasterLists en DefectLists van de NL-NPKD naar NL-IS

- Notificatie dat nieuwe Signing Certificate Chains, CRLs Signing PKI, MasterLists en DefectLists beschikbaar zijn van NL-NSPOC naar NL-IS

De informatie-uitwisseling tussen NL-NSPOC en NL-IS staat beschreven in *Koppelvlakspecificatie – Deel 1.1: NSPOC - IS* [NL-K01.1].

K1.2. NL-NSPOC – NL-DVCA

Tussen de NL-DVCA en de NL-NSPOC wordt de volgende informatie uitgewisseld:

- Certificate Requests van de IS'en naar NL-DVCA
- Certificates van NL-DVCA naar de IS'en
- Certificate Chains van NL-DVCA naar NL-NSPOC (via SendSauthorisation)
- IS authorisations van NL-DVCA naar NL-NSPOC

De informatieuitwisseling tussen NL-DVCA en NL-NSPOC staat beschreven in *Koppelvlakspecificatie – Deel 1.2: DVCA - NSPOC* [NL-K01.2].

K1.3. NL-NSPOC – NL-NPKD

Tussen NL-NSPOC en NL-NPKD wordt de volgende informatie uitgewisseld:

- Opvragen van Signer Certificates, CRLs Signer PKIs, MasterLists en DefectLists door NL-IS bij NL-NPKD
- Signer Certificates, CRLs Signer PKIs, MasterLists en DefectLists van NL-NPKD naar NL-IS
- Notificatie dat nieuwe Signing Certificate Chains, CRLs Signing PKI, MasterLists en DefectLists beschikbaar zijn van NL-NPKD naar NL-NSPOC

De informatieuitwisseling tussen NL-NSPOC en NL-NPKD staat beschreven in *Koppelvlakspecificatie – Deel 1.3: NPKD - NSPOC* [NL-K01.3].

5.2.2 Verbindingen met betrekking tot de SPOC

K2.1. NL-DVCA – NL-SPOC-Intern

Tussen de NL-SPOC-Intern en NL-DVCA wordt de volgende informatie uitgewisseld:

- Certificate Requests van de NL-DVCA bij de NL-CVRAs en via de NL-SPOC-Extern bij buitenlandse CVCA's
- Certificates van de NL-CVRAs en Certificates van buitenlandse CVCA's via de NL-SPOC-Extern naar de NL-DVCA
- Certificate Chain Requests van de NL-DVCA bij de NL-SPOC-Intern
- Certificate Chains van de NL-SPOC-Intern naar de NL-DVCA

K2.2. NL-SPOC-Intern – NL-CVRA

Tussen NL-CVRA en NL-SPOC wordt de volgende informatie uitgewisseld:

- Certificate Requests van binnenlandse en buitenlandse DVs bij de NL-CVRAs
- Certificates van de NL-CVRAs naar de DVs
- Certificates van buitenlandse CVCA's naar de NL-CVRAs
- Certificates van de NL-CVRAs naar buitenlandse CVCA's
- Certificate Chain Requests van de NL-SPOC-Intern bij de NL-CVRAs
- Certificate Chains van de NL-CVRAs naar de NL-SPOC-Intern
- DV authorisations van NL-CVRA naar NL-SPOC

K2.3. NL-SPOC-Extern – buitenlandse SPOC

Tussen de NL-SPOC-Extern en buitenlandse SPOC wordt de volgende informatie uitgewisseld:

- Certificate Requests van NL-DVCAs bij buitenlandse CVCA's
- Certificate Requests van buitenlandse DVCAs aan de NL-CVRAs
- Certificates van de NL-CVRAs naar buitenlandse DVs
- Certificates van buitenlandse CVCA's naar NL-DVCAs
- Certificates van de NL-CVRAs naar buitenlandse CVCA's
- Certificates van buitenlandse CVCA's naar de NL-CVRAs

De verbinding en informatie-uitwisseling tussen de nationale SPOC en buitenlandse SPOCs moet voldoen aan CSN 36 9791 v1.0 [EU-SPOC] zoals vastgesteld in Beschikking C(2009) 7476 van de Commissie van de Europese Gemeenschappen [EC-C2009-7476].

5.2.3 Verbindingen ten behoeve van de Country Signing PKI

- K4.1. NL-NPKD – NL-CSCA
(voorlopig buiten scope van dit document)
- K4.2. NL-DS – NL-CSCA
(buiten scope van dit document)
- K4.3. NL-NPKD – buitenlandse CSCA
(voorlopig buiten scope van dit document)
- K4.4. NL-NPKD – ICAO PKD
(voorlopig buiten scope van dit document)

5.2.4 Verbinding tussen IS en Terminal met Reader

- K5. NL-IS – Terminal met Reader
Tussen een NL-IS en een Terminal met Reader wordt de volgende informatie uitgewisseld:
 - Verzoek tot Signing Certificate Chains, CRLs Signing PKI, MasterLists en DefectLists van Terminal met Reader aan het NL-IS
 - Signing Certificate Chains, CRLs Signing PKI, MasterLists en DefectLists van NL-IS naar Terminal Reader
 - Verzoek tot Verifying Certificate Chain van Terminal Reader naar NL-IS
 - Verifying Certificate Chains van NL-IS naar Terminal Reader
 - Verzoeken voor het tekenen van de door een Identiteitsbewijs gegenereerde challenge voor Terminal Authenticatie van Terminal Reader naar NL-IS
 - Met NL-IS Private Key getekende challenge voor Terminal Authenticatie van NL-IS naar Terminal Reader
 - Notificatie dat nieuwe Signing Certificate Chains, CRLs Signing PKI, MasterLists en DefectLists beschikbaar zijn van NL-IS naar Terminal Reader

5.2.5 Verbindingen t.b.v. de NL-SPOC-CA

- K3. NL-SPOC-CA – NL-SPOC-EXTERN
De NL-SPOC-CA voorziet de NL-SPOC-EXTERN offline van Certificates

5.2.6 Verbindingen t.b.v. de NL-CONNECT-CA

- K6.1 NL-CONNECT-CA – Sub-CAs
De NL-CONNECT-CA voorziet de sub-CAs offline van Certificates. De Certificates worden handmatig vanaf een gegevensdrager in de sub-CAs geladen
- K6.2. NL-TLS-CA – EAC-PKI-NL systemen
De NL-TLS-CA voorziet de EAC-PKI-NL systemen offline van Certificates. De Certificates worden handmatig vanaf een gegevensdrager in de daartoe betreffende EAC-PKI-NL systemen geladen.
- K6.3. NL-TerminalTLS-CA – NL-IS'en & Terminals met Readers
De NL-TerminalTLS-CA voorziet de NL-IS'en en Terminals met Readers offline van Certificates. De Certificates worden handmatig vanaf een gegevensdrager in de daartoe betreffende EAC-PKI-NL systemen geladen
- K6.4. NL-Admin-CA – EAC-PKI-NL systemen
De NL-Admin-CA voorziet de EAC-PKI-NL systemen (m.u.v. NL-IS), de IS-MCs en de Admin Systemen offline van Certificates. De Certificates worden handmatig vanaf een gegevensdrager in de daartoe betreffende EAC-PKI-NL systemen geladen
- K6.5. NL-AdminMC-CA – IS & IS-MC
De NL-AdminMC-CA voorziet de NL-IS'en en IS-MCs offline van Certificates. De Certificates worden handmatig vanaf een gegevensdrager in de daartoe betreffende EAC-PKI-NL systemen geladen.

De verbindingen tussen de Nederlandse systemen staan beschreven in *EAC-PKI-NL – Architectuur – Deel 3 Verbindingen* [NL-A03]. Voor de verbindingen tussen de NL-SPOC en buitenlandse SPOCs geldt [CSN 36 9791]

6 Scenario's

6.1 Signing PKI scenario's

Binnen de Signing PKI erkennen we de volgende scenario's

1. Root Certificate van de NL-CSCA wordt binnen de kaders van de van toepassing zijnde CP/CPS initieel aangemaakt en gedistribueerd naar NL-NPKD, ICAO PKD, ICAO PKD deelnemers en eventueel naar andere buitenlandse PKDs
 - a. NL-CSCA Certificate wordt via veilige weg gedistribueerd naar NL-NPKD.
 - b. NL-NPKD controleert het Self-Signed Certificate met behulp van de Public Key uit het Certificate.
 - c. Indien deze controle positief uitvalt, slaat de NL-NPKD het NL-CSCA Certificate op voor gebruik.
 - d. NL-CSCA Certificate wordt persoonlijk door een aangewezen vertegenwoordiger van de NL-NPKD afgeleverd bij het ICAO PKD Operations Centre in Montreal, Canada en via bilateraal overeengekomen diplomatieke weg gedistribueerd naar alle ICAO PKD deelnemers.
 - e. NL-CSCA Certificate wordt eventueel via diplomatieke weg gedistribueerd naar andere buitenlandse partijen.
2. Root Certificate van buitenlandse CSCA wordt initieel gedistribueerd naar NL-NPKD.
 - a. NL-NPKD ontvangt buitenlands CSCA Root Certificate via bilateraal overeengekomen diplomatieke weg. De partij waarvan dit CSCA Root Certificate ontvangen wordt staat nog niet vast. Dit kan de buitenlandse CSCA of NPKD zijn of de NL-CSCA.
 - b. NL-NPKD controleert het Self-Signed Certificate met behulp van de Public Key uit het Certificate.
 - c. Indien deze controle positief uitvalt, slaat NL-NPKD het buitenlands CSCA Certificate op voor gebruik.
3. Root Certificates van buitenlandse CSCAs worden door NL-NPKD opgehaald bij ICAO PKD via CSCA MasterLists.
 - a. NL-NPKD downloadt van de ICAO PKD de CSCA MasterList van een vertrouwd land waarvan het reeds beschikt over het CSCA Certificate.
 - b. NL-NPKD controleert met behulp van het CSCA Certificate van het vertrouwde land de handtekening over de CSCA MasterList.
 - c. Indien deze controle positief uitvalt, controleert NL-NPKD van alle gewenste buitenlandse Self-Signed CSCA Certificates uit de CSCA MasterList het Certificate met behulp van de Public Key uit het betreffende Certificate.
 - d. Indien deze controles positief uitvallen, slaat NL-NPKD de gewenste buitenlandse CSCA Certificates op voor gebruik.
4. NL-CSCA Link Certificate wordt binnen de kaders van de van toepassing zijnde CP/CPS aangemaakt en gedistribueerd naar NL-NPKD, ICAO PKD en eventueel buitenlandse PKDs
 - a. NL-CSCA Link Certificate wordt gedistribueerd naar NL-NPKD. NL-NPKD controleert vervolgens het Certificate met behulp van de huidige Public Key. Als deze controle positief uitvalt, slaat NL-NPKD het NL-CSCA Link Certificate op voor gebruik.
 - b. NL-CSCA Link Certificate wordt door NL-NPKD elektronisch gedistribueerd naar ICAO PKD. ICAO PKD controleert daarna het Certificate met de huidige (vorige) Public Key. Indien deze controle positief uitvalt, publiceert ICAO PKD het NL-CSCA Link Certificate. NL-NPKD leest NL-CSCA Link Certificate van ICAO PKD en controleert het. Indien controle negatief uitvalt, informeert NL-NPKD ICAO PKD hierover.

- c. NL-CSCA Link Certificate wordt eventueel elektronisch gedistribueerd naar andere buitenlandse partijen (buitenlandse NPKDs).
- 5 Link Certificate van buitenlandse CSCA wordt gedistribueerd naar NL-NPKD.
- a NL-NPKD ontvangt buitenlands CSCA Link Certificate. De partij waarvan dit CSCA Link Certificate ontvangen wordt slaat nog n'et vast. Dit kan de buitenlandse CSCA of NPKD zijn of de NL-CSCA
 - b NL-NPKD controleert buitenlands CSCA Link Certificate met Public Key uit huidige buitenlands CSCA Certificate
 - c Indien de controle positief uitvalt, slaat NL-NPKD het Certificate op voor gebruik.
- 6 Link Certificates van buitenlandse CSCAs worden door NL-NPKD opgehaald bij ICAO PKD.
- a NL-NPKD downloadt van de ICAO PKD de gewenste buitenlandse CSCA Link Certificates.
 - b NL-NPKD controleert deze buitenlandse CSCA Link Certificates met de Public Keys uit de huidige buitenlandse CSCA Certificates.
 - c Indien deze contro'es positief uitvallen, slaat NL-NPKD de Certificates op voor gebruik.
- 7 Certificate van NL-DS wordt binnen de kaders van de van toepassing zijnde CP/CPS initieel aangemaakt door de NL-CSCA en gedistribueerd naar NL-NPKD, ICAO PKD en eventueel buitenlandse PKDs.
- a NL-NPKD ontvangt NL-DS Certificate van NL-CSCA
 - b NL-NPKD controleert het nieuwe NL-DS Certificate met het huidige NL-CSCA Certificate
 - c. Indien deze controle positief uitvalt, slaat de NL-NPKD het Certificate op voor gebruik.
 - d NL-NPKD distribueert het NL-DS Certificate naar de ICAO PKD die het (na eventueel enkele controles uitgevoerd te hebben) publiceert
 - e NL-DS Certificate wordt eventueel gedistribueerd naar andere buitenlandse partijen (buitenlandse NPKDs).
- 8 Certificate van NL-DS wordt vernieuwd en gedistribueerd
- Dit proces verloopt identiek aan het aanmaken en distribueren van een initieel DS Certificate
- 9 Certificate van buitenlandse DS wordt gedistribueerd naar NL-NPKD
- a NL-NPKD ontvangt buitenlands DS Certificate. De partij waarvan dit DS Certificate ontvangen wordt staat nog niet vast. Dit kan de buitenlandse CSCA of NPKD zijn of de NL-CSCA
 - b NL-NPKD controleert buitenlands DS Certificate met Public Key uit huidige buitenlands CSCA Certificate
 - c. Indien de controle positief uitvalt, slaat NL-NPKD het Certificate op voor gebruik.
- 10 NL-NPKD haalt buitenlandse DS Certificates op bij ICAO PKD.
- a NL-NPKD downloadt van de ICAO PKD de gewenste buitenlandse DS Certificates
 - b NL-NPKD controleert deze buitenlandse DS Certificates met de Public Keys uit de buitenlandse CSCA Certificates.
 - c Indien deze controles positief uitvallen, slaat NL-NPKD de Certificates op voor gebruik.
- 11 Certificate van de NL-NPKD List Signer wordt binnen de kaders van de van toepassing zijnde CP/CPS initieel aangemaakt door de NL-CSCA en gedistribueerd naar de NL-NPKD.
- a NL-NPKD maakt Key Pair aan in de eigen HSM tijdens Key Ceremony.

- b. NL-NPKD maakt X 509V3 Certificate Request voor de Public Key.
- c. NL-NPKD stuurt deze Certificate Request naar de NL-CSCA.
- d. NL-CSCA controleert de Certificate Request en indien deze controle positief uitvalt, maakt de NL-CSCA een Certificate aan voor de NL-NPKD List Signer Public Key.
- e. NL-CSCA stuurt Certificate naar de NL-NPKD.
- f. NL-NPKD controleert Certificate met CSCA Certificate.
- g. Indien deze controle positief uitvalt, slaat NL-NPKD Certificate op voor gebruik.
- h. NL-NPKD neemt List Signer Certificate op in MasterList.
- i. NL-NPKD List Signer Certificate wordt door NL-NPKD eventueel gedistribueerd naar andere buitenlandse partijen (buitenlandse NPKDs).
- j. Noot: mogelijk worden verschillende List Signers gespecificeerd (voor MasterList en voor DefectList). De procedure is identiek.

12. Certificate van de NL-NPKD List Signer wordt vernieuwd en gedistribueerd.

Dit proces verloopt identiek aan het aanmaken en distribueren van een initieel NL-NPKD List Signer Certificate.

Noot: mogelijk worden verschillende List Signers gespecificeerd (voor MasterList en voor DefectList). De procedure is identiek.

13. CRL wordt door de NL-CSCA gemaakt en gedistribueerd naar NL-NPKD, ICAO PKD en/of buitenlandse PKDs.

Er kunnen verschillende redenen zijn om een CRL aan te maken.

- a. Indien vastgesteld wordt dat een Private Key behorend bij een door de NL-CSCA uitgegeven Certificate mogelijk gecompromitteerd is, wordt de NL-CSCA hiervan via diplomatische weg op de hoogte gesteld. De NL-CSCA moet dan binnen een beperkte vastgestelde tijd een nieuwe CRL uitgegeven.
- b. Daarnaast wordt periodiek een nieuwe CRL uitgegeven.

Het uitgeven van een nieuwe CRL omvat de volgende stappen:

- c. De NL-CSCA plaatst ingetrokken Certificates waarvan de geldigheidstermijn nog niet verlopen is op de CRL.
- d. De NL-CSCA voegt datum en tijd toe aan de CRL.
- e. NL-CSCA tekent de CRL met haar Private Key.
- f. De CRL met handtekening wordt gedistribueerd naar NL-NPKD.
- g. NL-NPKD controleert vervolgens de handtekening met behulp van het CSCA Certificate.
- h. Als deze controle positief uitvalt, slaat NL-NPKD de CRL op voor gebruik.
- i. De CRL wordt elektronisch gedistribueerd naar ICAO PKD.
- j. ICAO PKD controleert de handtekening met behulp van het CSCA Certificate.
- k. Indien deze controle positief uitvalt, publiceert ICAO PKD de CRL.
- l. De CRL wordt eventueel elektronisch gedistribueerd naar andere buitenlandse partijen (buitenlandse NPKDs).

14. CRL van buitenlandse CSCA wordt gedistribueerd naar NL-NPKD.

- a. NL-NPKD ontvangt buitenlandse CRL. De partij waarvan deze CRL ontvangen wordt staat nog niet vast. Dit kan de buitenlandse CSCA of NPKD zijn of de NL-CSCA.

- b. NL-NPKD controleert handtekening over de CRL met de Public Key uit het buitenlands CSCA Certificate.
- c. Indien de controle positief uitvalt, slaat NL-NPKD de CRL op voor gebruik

15. NL-NPKD haalt CRLs op bij ICAO PKD

- a. NL-NPKD downloadt van de ICAO PKD de gewenste buitenlandse CRLs
- b. NL-NPKD controleert deze buitenlandse CRLs met de Public Keys uit de buitenlandse CSCA Certificates.
- c. Indien deze controles positief uitvallen, slaat NL-NPKD de CRLs op voor gebruik

16. CSCA Certificates voor nationaal gebruik wordt door NL-NPKD geautoriseerd (bv de NL-NSPOC

- a. Wanneer een nieuw CSCA Root Certificate beschikbaar is wordt door de NL-NPKD beslist of deze wordt opgenomen in de lijst met geautoriseerde Certificaten voor nationaal gebruik. Wanneer een Certificaat verloopt wordt door de NL-NPKD beslist of deze wordt verwijderd in de lijst met geautoriseerde Certificaten voor nationaal gebruik
- b. De NL-NPKD maakt de geautoriseerde CSCA Certificates beschikbaar voor de NSPOC
- c. De NL-NPKD stuurt indien urgent een notificatie naar de NL-IS'en v a de NSPOC.

17. CRL's voor nationaal gebruik wordt door NL-NPKD geautoriseerd (bv de NL-NSPOC

- a. Wanneer een nieuwe CRL beschikbaar is wordt door de NL-NPKD beslist of deze wordt opgenomen in de lijst met geautoriseerde CRLs voor nationaal gebruik.
- b. De NL-NPKD maakt de geautoriseerde CRLs beschikbaar voor de NSPOC
- c. De NL-NPKD stuurt indien urgent een notificatie naar de NL-IS'en via de NSPOC

18. MasterList voor nationaal gebruik wordt door NL-NPKD aangemaakt en gedistribueerd naar NL-NSPOC

- a. Wanneer een nieuw CSCA Root Certificate beschikbaar is wordt door de NL-NPKD beslist of deze wordt opgenomen in de MasterList voor nationaal gebruik. Wanneer een Certificaat verloopt wordt door de NL-NPKD beslist of deze wordt verwijderd in de MasterList voor nationaal gebruik. Na het besluit maakt de NL-NPKD een nieuwe MasterList door het CSCA Certificate toe te voegen aan de lijst met vertrouwde certificaten.
- b. De NL-NPKD voegt datum en tijd toe aan de MasterList en het List Signer Certificate
- c. De NL-NPKD List Signer tekent de MasterList met zijn Private Key.
- d. De NL-NPKD maakt de MasterList beschikbaar voor de NSPOC
- e. De NL-NPKD stuurt indien urgent een notificatie naar de NL-IS'en via de NSPOC

19. MasterList voor ICAO wordt door NL-NPKD aangemaakt en eventueel gedistribueerd naar ICAO PKD

- a. De NL-NPKD maakt een selectie uit de beschikbare (geaccepteerde) certificaten en maakt een nieuwe MasterList met vertrouwde certificaten
- b. De NL-NPKD voegt datum en tijd toe aan de MasterList en het List Signer Certificate
- c. De NL-NPKD List Signer tekent de MasterList met zijn Private Key
- d. De NL-NPKD distribueert de nieuwe MasterList elektronisch naar de ICAO PKD
- e. ICAO PKD controleert de handtekening over de MasterList met behulp van het List Signer en CSCA certificaat
- f. Indien deze controle positief uitvalt, publiceert ICAO PKD de MasterList

20. DefectList voor nationaal gebruik wordt door NL-NPKD aangemaakt.

- a. Wanneer een nieuw defect bekend is wordt door de NL-NPKD beslist of deze wordt opgenomen in een nieuwe DefectList aan met daarin het defect.
- b. De NL-NPKD voegt datum en tijd toe aan de DefectList en het List Signer Certificate.
- c. De NL-NPKD List Signer tekent de DefectList met zijn Private Key.
- d. De NL-NPKD stuurt een notificatie naar de NL-IS'en via de NSPOC.

21. IS vraagt Signer Certificates, CRLs, MasterList of DefectList op bij NL-NPKD via NL-NSPOC.

- a. IS ontvangt notificatie over nieuw beschikbare Signer Certificates, CRLs, MasterList of DefectList of IS besluit zelfstandig data op te vragen.
- b. IS vraagt Certificates, CRLs, MasterList of DefectList op bij NL-NPKD via NL-NSPOC.
- c. NL-NPKD stuurt Certificates, CRLs, MasterList of DefectList naar IS via NL-NSPOC.
- d. IS stuurt notificatie naar onderliggende Terminals met Readers.

6.2 Verifying PKI scenario's

Binnen de Country Verifying PKI erkennen we de volgende scenario's:

1. Root Certificate van NL-CVCA wordt binnen de kaders van de van toepassing zijnde CP/CPS initieel aangemaakt en gedistribueerd.

- a. NL-CVCA maakt Key Pair aan in de eigen HSM tijdens Key Ceremony.
- b. De Public Key wordt in een Card Verifiable Certificate geplaatst dat door de NL-CVCA zelf getekend wordt met de bijbehorende Private Key tijdens de Key Ceremony. Dit is het Self-Signed NL-CVCA Root Certificate van de EAC-PKI-NL.
- c. Het Self-Signed NL-CVCA Root Certificate kan gedistribueerd worden naar BZK om in NL-MRTDs geplaatst te worden. In de praktijk zullen uitsluitend eraan gerelateerde Link Certificates in NL-MRTDs geplaatst worden.
- d. Het Self-Signed NL-CVCA Root Certificate wordt gedistribueerd naar DG-JLS, het onderdeel van de Europese Commissie (EC) dat de gegevens van de CVCA's van de lidstaten beheert. Distributie naar DG-JLS wordt vanuit de NL-CVCA geïnitieerd en vindt plaats via diplomatieke weg.
- e. Het Self-Signed NL-CVCA Root Certificate wordt gedistribueerd naar andere landen waarvan Nederland wil dat DV's in staat zijn autorisaties aan te vragen voor het lezen van biometrische gegevens van Nederlandse Identiteitsbewijzen.

Het distribueren kan plaatsvinden via de NL-SPOC intern en NL-SPOC-Extern en buitenlandse SPOC of op een andere manier zoals via een ander netwerk of een extern opslag medium.

Wanneer gebruik gemaakt wordt van de SPOC-verbinding kan ervan uitgegaan kunnen worden dat de gebruikte SPOC PKI voldoende zekerheid biedt dat het Certificate inderdaad afkomstig is van de NL-CVCA.

Als ervan uitgegaan wordt dat dit niet voldoende zekerheid biedt of als gebruik gemaakt wordt van een andere manier van distribueren, dient de ontvangende partij de authenticiteit van het certificaat te controleren op basis van offline verkregen informatie en handmatig een beslissing te nemen over het opslaan van het Certificate voor gebruik.

- f. Het Self-Signed NL-CVCA Root Certificate wordt via de NL-SPOC-Intern ook gedistribueerd naar onderliggende Nederlandse systemen die gebruik mogen maken van de NL-CVCA. De NL-CVCA stuurt het Self-Signed NL-CVCA Root Certificate naar de NL-SPOC.

Wanneer gebruik gemaakt wordt van de SPOC-verbinding kan ervan uitgegaan kunnen worden dat de gebruikte SPOC PKI voldoende zekerheid biedt dat het Certificate inderdaad afkomstig is van de NL-CVCA.

Als ervan uitgegaan wordt dat dit niet voldoende zekerheid biedt of als gebruik gemaakt wordt van een andere manier van distribueren, dient de ontvangende partij de authenticiteit van het certificaat

te controleren op basis van offline verkregen informatie en handmatig een beslissing te nemen over het opslaan van het Certificate voor gebruik

- g. De NL-SPOC stuurt na ontvangst van een nieuw CVCA Certificate een bericht naar NL-DVCAs die vervolgens bij de CVCA een certificaat aan kunnen vragen

2 Root Certificate van buitenlandse CVCA wordt initieel gedistribueerd

- a. Een buitenslands Self-Signed CVCA Root Certificate wordt gedistribueerd naar Nederland indien het land wil dat Nederlandse DVCAs en onderliggende Nederlandse IS'en in staat zijn de biometrische gegevens van haar identiteitsbewijzen te lezen

Het distribueren van het Root Certificate kan vanuit het buitenland geïnitieerd worden, of op verzoek van Nederland of via DG-JLS.

Het distribueren kan plaatsvinden via de verbinding tussen de buitenlandse SPOC en de NL-SPOC-Extern en NL-SPOC-Intern, of op een andere manier zoals via een andere netwerkverbinding of een extern opslagmedium.

Wanneer gebruik gemaakt wordt van de SPOC verbinding kan ervan uitgegaan kunnen worden dat de gebruikte SPOC PKIs voldoende zekerheid bieden dat het Certificate inderdaad afkomstig is van de buitenlandse CVCA

Als ervan uitgegaan wordt dat dit niet voldoende zekerheid biedt of als gebruik gemaakt wordt van een andere manier van distribueren, dient de ontvangende partij de authenticiteit van het Certificate te controleren op basis van offline verkregen informatie en handmatig een beslissing te nemen over het opslaan van het Certificate voor gebruik

De NL-SPOC-Intern heeft de verantwoordelijkheid actuele CVCA certificaten te verzamelen. De CVRA heeft de verantwoordelijkheid de (distributie-)autorisaties per DV aan de NL-SPOC-Intern kenbaar te maken. Op basis van deze autorisatie reageert / distribueert de NL-SPOC-Intern CVCA certificaten

- b. De NL-SPOC-Intern stuurt na ontvangst van een nieuw CVCA Certificate een bericht naar hiertoe geautoriseerde NL-DVCAs die bij de CVCA een certificaat aan kunnen vragen

3 NL-DVCA vraagt Certificate Chains op bij NL-SPOC-Intern

- a. Een NL-DVCA kan bij de NL-SPOC-Intern CVCA Certificate Chains (CVCA Root en Link Certificates) opvragen waarvoor de NL-DVCA autorisatie heeft. Dit kunnen Certificate Chains van meerdere DVCAs zijn, namelijk

- i. DVCAs voor verschillende soorten identiteitsbewijzen (eMRTD, eRP, ...).
- ii. vanuit zowel het binnenland en het buitenland

Een NL-DVCA zal periodiek de opvraag operatie uitvoeren en eveneens uitvoeren nadat de NL-DVCA een notificatie heeft ontvangen van de NL-SPOC-Intern over een nieuw beschikbaar CVCA certificaat

- b. Wanneer de NL-SPOC-Intern een aanvraag voor CVCA Certificate Chains ontvangt van een NL-DVCA, zoekt de NL-SPOC-Intern in het overzicht van de DV autorisatie na voor welke CVCA Certificate Chains de NL-DVCA in kwestie geautoriseerd is.
- c. NL-SPOC-Intern haalt die CVCA Certificate Chains uit de Certificate Store en stuurt ze naar de NL-DVCA.

4 Certificate van NL-DVCA wordt initieel aangemaakt door NL-CVCA en gedistribueerd

- a. NL-DVCA maakt Key Pair aan in elgen HSM tijdens Key Ceremony
- b. NL-DVCA maakt Certificate Request voor Public Key. Inner Signature is gezet met de bijbehorende Private Key. Outer Signature is leeg bij deze initiële Certificate Request.
- c. NL-DVCA stuurt deze Certificate Request naar de NL-CVRA. Dit kan plaatsvinden via de NL-SPOC-Intern, of op een andere manier, zoals via een ander netwerk, e-mail of een extern opslag medium.

- d. NL-CVRA ontvangt Certificate Request en controleert de Certificate Request volgens paragraaf 4.2.2 van [CP].
 - e. Indien de controle positief uitvalt, bepaalt NL-CVCA of NL-CVRA (nog te bepalen) de toegangsrechten tot Nederlandse eMRTDs voor de DVCA.
 - f. NL-CVCA maakt Certificate aan met toegangsrechten en ondertekent dit Certificate met de eigen Private Key.
 - g. NL-CVCA stuurt Certificate naar de NL-CVRA. De NL-CVRA stuurt Certificate via de NL-SPOC-Intern naar de NL-DVCA of op een andere manier, zoals via een ander netwerk, e-mail of een extern opslagmedium.
 - h. NL-DVCA beschikt al over of krijgt de beschikking over NL-CVCA Root Certificate en controleert het Certificate hiermee.
 - i. Indien deze controle positief uitvalt, slaat de NL-DVCA het Certificate op voor gebruik. De NL-DVCA kan dit Key Pair nu gebruiken voor het ondertekenen van Certificate Requests van onderliggende IS'en om Nederlandse paspoorten uit te lezen.
5. Certificate van NL-DVCA wordt initieel aangemaakt door buitenlandse CVCA en gedistribueerd.
- a. NL-DVCA maakt Key Pair aan in eigen HSM tijdens Key Ceremony.
 - b. NL-DVCA maakt Certificate Request voor Public Key. Inner Signature is gezet met de bijbehorende Private Key. Outer Signature is gezet met de Private Key behorend bij het door de NL-CVCA aan de NL-DVCA uitgegeven Certificate.
 - c. NL-DVCA stuurt Certificate Request naar NL-CVRA via NL-SPOC-Intern.
 - d. NL-CVRA controleert Outer Signature. De NL-CVCA voorziet Certificate Request van Outer Signature met eigen Private Key en stuurt dit aan de NL-CVRA.
 - e. NL-CVRA stuurt Certificate Request naar de desbetreffende NL-DVCA via de NL-SPOC-Intern.
 - f. NL-DVCA stuurt Certificate Request naar buitenlandse CVCA via de NL-SPOC-Intern en SPOC-verbinding of op een andere manier, zoals via een ander netwerk of een extern opslag medium.
 - g. Buitenlandse CVCA controleert de Certificate Request.
 - h. Buitenlandse CVCA neemt beslissing over toekennen van Certificate, gebaseerd op controle onder het vorige punt en op basis van offline verkregen en handmatig verwerkte informatie zoals het CP van de NL-DVCA.
 - i. Buitenlandse CVCA bepaalt toegangsrechten van NL-DVCA tot nationale eMRTDs.
 - j. Buitenlandse CVCA maakt het nieuwe DVCA Certificate aan en ondertekent dit met de eigen Private Key.
 - k. De buitenlandse CVCA stuurt het nieuwe DVCA Certificate naar de NL-DVCA via SPOC-verbinding en de NL-SPOC-Intern of op een andere manier, zoals via een ander netwerk of een extern opslag medium.
 - l. NL-DVCA beschikt al over of krijgt de beschikking over buitenlands CVCA Root Certificate en controleert hiermee het Certificate.
 - m. Indien deze controle positief uitvalt, slaat de NL-DVCA het Certificate op voor gebruik. De NL-DVCA kan dit Key Pair nu gebruiken voor het ondertekenen van Certificate Requests van onderliggende IS'en om buitenlandse paspoorten uit te lezen.
6. Certificate van buitenlandse DVCA wordt initieel aangemaakt door NL-CVCA en uitgewisseld.
- a. Buitenland stuurt Certificate Request met Inner en Outer Signature naar NL-CVRA via de SPOC-verbinding of op een andere manier, zoals via een ander netwerk of een extern opslagmedium.
 - b. NL-CVRA controleert Certificate Request volgens paragraaf 4.2.2 van [CP].
 - c. NL-CVRA neemt beslissing over toekennen van Certificate, gebaseerd op checks onder vorige punt en op basis van offline verkregen en handmatig verwerkte informatie zoals het CP van de buitenlandse DVCA.

- d. NL-CVCA of NL-CVRA (nog te bepalen) bepaalt toegangsrechten van buitenlandse DVCA tot Nederlandse eMRDs.
- e. NL-CVCA maakt Certificate en ondertekent het met de eigen Private Key.
- f. NL-CVCA stuurt het gelekende Certificate naar de NL-CVRA. De NL-CVRA stuurt het gelekende Certificate naar het buitenland via de NL-SPOC-Intern en de SPOC-verbinding of op een andere manier, zoals via een ander netwerk of een extern opslag medium

7. NL-NSPOC vraagt CVCA Certificate Chains op bij NL-DVCA

- a. De NL-NSPOC wacht totdat er vanuit een NL-DVCA in een bericht aan de NL-NSPOC de IS autorisaties en Verifier Certificate Chains kenbaar zijn gemaakt (CVCA Root en Link Certificates). Dit kunnen Certificate Chains van meerdere CVCA's zijn, namelijk CVCA's voor verschillende soorten identiteitsbewijzen (eMRP, eRP, eMRD, ...) en CVCA's uit verschillende landen

8. NL-IS vraagt Certificate Chains op bij NL-NSPOC

- a. Een NL-IS vraagt periodiek bij de NL-NSPOC CVCA-DVCA Certificate Chains op. Wanneer de NL-NSPOC een aanvraag voor CVCA-DVCA Certificate Chains ontvangt van een NL-IS, zoekt de NL-NSPOC in het overzicht van de IS autorisatie op voor welke Certificate Chains de NL-IS in kwestie geautoriseerd is.
- b. De NL-NSPOC haalt de betreffende Certificate Chains uit de Certificate Store en stuurt ze naar het NL-IS

9. Certificate van NL-IS wordt initieel aangemaakt.

- a. NL-IS heeft Certificate Chains opgevraagd bij NL-NSPOC
- b. NL-IS maakt Key Pair aan in eigen Secure Module.
- c. NL-IS maakt Certificate Request voor Public Key. Inner Signature is gezet met de bijbehorende Private Key. Outer Signature is leeg bij deze initiële aanvraag. De aanvraag betreft een aanvraag op een van de ontvangen Certificate Chains
- d. NL-IS stuurt Certificate Request via de NL-NSPOC naar de betreffende NL-DVCA via het EAC-PKI-NL netwerk of op een andere manier, zoals via een ander netwerk, e-mail of een extern opslag medium.
- e. Op basis van de Registration Authority functionaliteit binnen de NL-DVCA wordt een beslissing genomen over toekennen van een Certificate op basis van controles zoals beschreven in paragraaf 4.2.3 van [CP]
- f. NL-DVCA bepaalt de toegangsrechten van het IS tot eMRD's uit bepaald land
- g. NL-DVCA maakt het Certificate en ondertekent het met de eigen Private Key.
- h. NL-DVCA stuurt Certificate naar het NL-IS via het EAC-PKI-NL netwerk of op een andere manier, zoals via een ander netwerk, e-mail of een extern opslag medium.
- i. NL-IS beschikt al over het NL-DVCA Certificate en controleert hiermee het ontvangen Certificate
- j. Indien deze controle positief uitvalt, slaat het IS het Certificate op voor gebruik.

10. Root Certificate van NL-CVCA wordt vernieuwd en gedistribueerd

- a. NL-CVCA maakt Key Pair aan in eigen HSM tijdens Key Ceremony
- b. NL-CVCA plaatst nieuwe Public Key in Certificate en tekent dit Certificate met de huidige Private Key. Daarmee wordt het nieuwe Certificate gelinkt aan het vorige.
- c. Het nieuwe NL-CVCA Link Certificate wordt gedistribueerd naar de NL-CVRA.
- d. Het nieuwe NL-CVCA Link Certificate wordt van de NL-CVRA gedistribueerd naar BZK om in nieuw uit te geven NL-eMRDs te plaatsen

- e. Het nieuwe NL-CVCA Link Certificate wordt door de NL-CVRA geautoriseerd voor binnen- en buitenlandse DV's die een (schriftelijke) autorisatie hebben voor deze keten. Het nieuwe NL-CVCA Link Certificaat en de update van DV autorisatielijst wordt aan de NL-SPOC-Intern gedistribueerd.
- f. Het NL-CVCA Link Certificate wordt gedistribueerd naar andere landen waarvan Nederland wil dat DV's in staat zijn autorisaties aan te vragen voor het lezen van biometrische gegevens van Nederlandse identiteitsbewijzen.
Het distribueren vindt geautomatiseerd plaats via de NL-SPOC-Intern en NL-SPOC-Extern en buitenlandse SPOC op basis van de DV autorisatielijst (zie onderliggende stappen).
- g. Het NL-CVCA Link Certificate wordt via de NL-SPOC-Intern op basis van de DV autorisatielijst ook gedistribueerd naar onderliggende Nederlandse systemen die gebruik mogen maken van de NL-CVCA. De NL-CVRA stuurt het NL-CVCA-Link Certificate naar de NL-SPOC-Intern.
- h. De NL-SPOC-Intern controleert het nieuwe NL-CVCA Link Certificate met behulp van het huidige NL-CVCA Certificate en slaat indien deze controle positief uitvalt het NL-CVCA Link Certificate op in zijn Certificate Store.
- i. De NL-SPOC-Intern stuurt na ontvangst van een nieuw CVCA Certificate een notificatie bericht naar NL-DVCAs die bij de CVCA een certificaat aan kunnen vragen en naar buitenlandse SPOCs van landen die bij de NL-CVRA een certificaat aan kunnen vragen op basis van de DV autorisatielijst.
- j. De onderliggende NL-DVCAs en buitenlandse systemen vragen het nieuwe CVCA Certificate op bij de NL-SPOC en controleren het nieuwe NL-CVCA Link Certificate met behulp van het huidige NL-CVCA Certificate.
- k. Indien deze controle positief uitvalt slaan ze het nieuwe NL-CVCA Link Certificate op voor gebruik en starten ze het proces om onder dit CVCA Certificate zelf nieuwe Certificates aan te vragen.

11. Vernieuwd Root Certificate van buitenlandse CVCA wordt gedistribueerd.

- a. Het nieuwe buitenlandse CVCA Link Certificate wordt gedistribueerd via de SPOC verbinding naar de NL-SPOC-Extern en NL-SPOC-Intern indien het land wil dat Nederlandse systemen in staat zijn de biometrische gegevens van haar eMRTDs te lezen.
- b. De NL-SPOC-Intern controleert het nieuwe CVCA Link Certificate met behulp van het huidige CVCA Certificate en slaat indien deze controle positief uitvalt het CVCA Link Certificate op in zijn Certificate Store.
- c. De NL-SPOC-Intern stuurt na ontvangst van een nieuw CVCA Certificate een notificatie bericht naar NL-CVRA die de op basis van de registratie de DV autorisaties herzielt en de vernieuwde DV autorisatielijst aan de NL-SPOC-Intern stuurt.
- d. De NL-SPOC-Intern stuurt na ontvangst van de DV autorisatielijst een nieuw CVCA Certificate een notificatie bericht naar NL-DVCAs die bij de betreffende CVCA een certificaat aan kunnen vragen.
- e. De onderliggende NL-DVCAs vragen het nieuwe CVCA Certificate op bij de NL-SPOC-Intern en controleren het nieuwe NL-CVCA Link Certificate met behulp van het huidige CVCA Certificate.
- f. Indien deze controle positief uitvalt slaan ze het nieuwe CVCA Link Certificate op voor gebruik en starten ze het proces om onder dit CVCA Certificate zelf nieuwe Certificates aan te vragen.

12. Certificate van NL-DVCA wordt vernieuwd door NL-CVCA.

- a. NL-DVCA maakt nieuw Key Pair aan in eigen HSM tijdens Key Ceremony.
- b. NL-DVCA maakt Certificate Request voor Public Key. Inner Signature is gezet met de bijbehorende Private Key. Outer Signature is gezet met huidige Private Key.
- c. NL-DVCA stuurt deze Certificate Request naar de NL-CVRA via de NL-SPOC-Intern.
- d. NL-CVRA ontvangt Certificate Request en controleert dit volgens paragraaf 4.2.2 van [CP].
- e. Indien de controles positief uitvallen, biedt de NL-CVRA het Certificate Request aan aan de NL-CVCA en tekent NL-CVCA het Certificate met de eigen Private Key.
- f. NL-CVCA stuurt Certificate naar de NL-CVRA. NL-CVRA stuurt Certificate via de NL-SPOC-Intern naar de NL-DVCA.

- g NL-DVCA controleert het Certificate met behulp van het NL-CVCA Certificate
- h Indien deze controle positief uitvalt, slaat de NL-DVCA het Certificate op voor gebruik.

13 Certificate van NL-DVCA wordt vernieuwd door buitenlandse CVCA.

- a NL-DVCA maakt nieuw Key Pair aan in eigen HSM tijdens Key Ceremony.
- b NL-DVCA maakt Certificate Request voor Public Key. Inner Signature is gezet met de bijbehorende Private Key. Outer Signature is gezet met de huidige Private Key
- c NL-DVCA stuurt deze Certificate Request naar de buitenlandse CVCA via de NL-SPOC-Intern en de SPOC verbinding.
- d Buitenlandse CVCA ontvangt Certificate Request en controleert deze
- e Buitenlandse CVCA bepaalt de toegangsrechten voor de NL-DVCA tot nationale eMRTDs, zodat de rechten in het Certificate geplaatst kunnen worden.
- f Buitenlandse CVCA maakt het Certificate en tekent dit Certificate met de eigen Private Key.
- g Buitenlandse CVCA stuurt het Certificate naar de NL-DVCA via de SPOC verbinding en de NL-SPOC-Intern.
- h NL-DVCA controleert het Certificate met behulp van het buitenlandse CVCA Certificate.
- i Indien deze controle positief uitvalt, slaat de NL-DVCA het Certificate op voor gebruik

14 Certificate van buitenlandse DVCA wordt vernieuwd door NL-CVCA.

- a Buitenlandse DVCA stuurt Certificate Request naar NL-CVCA via SPOC-verbinding en NL-SPOC-Intern. Hierbij dient de Inner Signature gezet te zijn met de nieuwe Private Key en de Outer Signature met de vorige Private Key.
- b NL-CVCA controleert de Certificate Request volgens paragraaf 4.2.2 van [CP]
- c NL-CVCA of NL CVCA (nog te bepalen) bepaalt toegangsrechten voor de buitenlandse DVCA tot Nederlandse eMRTDs, zodat de rechten in het Certificate geplaatst kunnen worden.
- d NL-CVCA maakt het Certificate en ondertekent het met de eigen Private Key
- e NL-CVCA stuurt Certificate naar NL-CVRA. NL-CVRA stuurt Certificate naar de buitenlandse DVCA via de NL-SPOC-Intern en de SPOC-verbinding

15 Certificate van NL-IS wordt vernieuwd

- a NL-IS maakt Key Pair aan in eigen Secure Module.
- b NL-IS maakt Certificate Request voor Public Key. Inner Signature is gezet met de bijbehorende Private Key. Outer Signature is gezet met een huidige geldige Private Key in de trust-relatie NL-IS ↔ NL-DVCA. Deze Certificate Request is voor het uitlezen van eMRTDs uit één specifiek land en voor een specifiek type document.
- c NL-IS stuurt Certificate Request naar de NL-DVCA via de NL-NSPOC
- d NL-DVCA controleert de Certificate Request volgens paragraaf 4.2.3 van [CP]
- e NL-DVCA bepaalt toegangsrechten voor IS tot eMRTDs van bepaald land, zodat de rechten in het Certificate geplaatst kunnen worden
- f NL-DVCA maakt het Certificate en tekent het met de eigen Private Key.
- g NL-DVCA stuurt Certificate naar het IS via het EAC-PKI-NL netwerk
- h NL-IS controleert het Certificate met behulp van het NL-DVCA Certificate
- i Indien deze controle positief uitvalt, slaat het NL-IS het Certificate op voor gebruik

6.3 Inspection System – Terminal met Reader scenario's

1. Terminal met Reader vraagt Signing Certificate Chains, CRLs, MasterList of DefectList op bij NL-IS
 - a. Terminal met Reader ontvangt notificatie van NL-IS over nieuwe Signer Certificates, CRLs, MasterList of DefectList of besluit zelfstandig data op te vragen
 - b. Terminal met Reader vraagt Signer Certificates, CRLs, MasterList of DefectList op bij NL-IS.
 - c. NL-IS stuurt Certificates, CRLs, MasterList of DefectList naar Terminal met Reader.
 - d. Terminal met Reader controleert Certificates, CRLs, MasterList of DefectList door het controleren van de handtekening
 - e. Indien deze controle positief uitvalt, slaat Terminal met Reader data op voor gebruik
2. Terminal met Reader voert Terminal Authenticatie uit.
 - a. Terminal met Reader heeft trust'points uit elektronisch identiteitsbewijs gelezen.
 - b. Terminal met Reader vraagt Verifying Certificate Chain op basis van primary trust point op bij NL-IS
 - c. NL-IS stuurt gevraagde Certificate Chain naar Terminal met Reader. Indien Certificate Chain niet beschikbaar is laat NL-IS dit weten aan Terminal met Reader.
 - d. Indien Certificate Chain niet beschikbaar is, vraagt Terminal met Reader Verifying Certificate Chain op basis van secondary trust point op bij NL-IS. Indien Certificate Chain niet beschikbaar is laat NL-IS dit weten aan Terminal met Reader.
 - e. Terminal met Reader biedt Certificate Chain aan aan elektronisch identiteitsbewijs.
 - f. Terminal met Reader vraagt Challenge aan elektronisch identiteitsbewijs.
 - g. Terminal met Reader stuurt Challenge naar NL-IS voor ondertekening.
 - h. NL-IS tekent Challenge met Private Key.
 - i. NL-IS stuurt getekende Challenge naar Terminal met Reader.
 - j. Terminal met Reader biedt getekende Challenge aan aan elektronisch identiteitsbewijs.

6.4 Verbindingsbeveiligingsscenario's

6.4.1 SPOC PKI scenario's

Binnen de SPOC PKI erkennen we de volgende scenario's:

1. Root Certificate van NL-SPOC-CA domein wordt Initieel aangemaakt en gedistribueerd.
 - a. NL-SPOC-CA maakt Key Pair aan in de eigen HSM tijdens Key Ceremony.
 - b. Public Key wordt in Certificate geplaatst dat door de NL-SPOC-CA zelf getekend wordt met de bijbehorende Private Key. Dit is het Self-Signed Root Certificate van het SPOC-CA domein.
 - c. Dit Self-Signed SPOC-CA Root Certificate wordt gedistribueerd naar de NL-SPOC-Extern en buitenlandse SPOCs van landen waarvan Nederland wil dat de landen in staat zijn EAC-PKI gegevens met Nederland uit te wisselen..
Het distribueren kan plaatsvinden via een netwerkverbinding of op een andere manier zoals via e-mail of een extern opslag medium.
 - d. De ontvangende partijen controleren de authenticiteit van het Certificate op basis van offline verkregen informatie en nemen handmatig een beslissing over het opslaan van het Certificate voor gebruik.

2 Root Certificate van buitenlandse SPOC-CA wordt initieel gedistribueerd naar NL-SPOC-Extern.

- a Het buitenlandse Self-Signed SPOC-CA Root Certificate wordt gedistribueerd naar de NL-SPOC-Extern. Voor sommige landen is dit het CSCA Certificate.

Het distribueren van het Root Certificate kan gebeuren via een netwerkverbinding of op een andere manier zoals via e-mail of een extern opslag medium.

- b De NL-SPOC controleert de authenticiteit van het Certificate op basis van offline verkregen informatie en neemt handmatig een beslissing over het opslaan van het Certificate voor gebruik.
- c Indien deze controle positief uitvalt, slaat de NL-SPOC-Extern het Certificate op voor gebruik.

3 TLS Client en Server Certificates van NL-SPOC-Extern worden initieel aangemaakt

De TLS Client en Server Certificates voor de NL-SPOC-Extern worden uitgegeven door de SPOC-CA en zullen gebruikt worden bij het opzetten van een TLS verbinding met/door de NL-SPOC-Extern. Uitwisseling van de TLS certificaten van de NL-SPOC-Extern met buitenlandse SPOCs hoeft niet vooraf plaats te vinden, omdat dit reeds gebeurd is voor het Root Certificate van de SPOC-CA.

4 TLS Client en Server Certificates van buitenlandse SPOC worden initieel aangemaakt

Dit proces valt geheel onder verantwoordelijkheid van het buitenland. De TLS Client en Server Certificates van de buitenlandse SPOC zullen gebruikt worden bij het opzetten van een TLS verbinding met de NL-SPOC-Extern. Uitwisseling van de TLS certificaten met de NL-SPOC-Extern hoeft niet vooraf plaats te vinden, omdat dit reeds gebeurd is voor het Root Certificate van de buitenlandse SPOC-CA.

5 Root Certificate van NL-SPOC-CA domein wordt vernieuwd.

Er kunnen verschillende redenen zijn om het NL-SPOC-CA Certificate te vervangen:

- a Het Certificate is (bijna) verlopen. Er wordt een nieuw Self-Signed Root Certificate aangemaakt. Dit Certificate wordt gedistribueerd naar buitenlandse SPOCs op dezelfde manier als het initiële Certificate gedistribueerd is. Dit staat beschreven in [CSN 36 9791]. Binnen Nederland kan ervoor gekozen worden het nieuwe NL-SPOC-CA Root Certificate te distribueren door middel van TLS met gebruik van de huidige SPOC PKI en af te zien van een handmatige beslissing op basis van offline verkregen informatie.
- b De Private Key is gecompromitteerd. In dit geval zal het oude Certificate ingetrokken worden (offline communicatie en handmatig verwijderen van Certificate bij de relying parties) en dient opnieuw initiële uitwisseling plaats te vinden met alle deelnemende partijen.

Nadat de onderliggende systemen op de hoogte zijn gebracht van het nieuwe Root Certificate moeten al deze systemen een nieuw Certificate aanvragen voor hun eigen Public Keys. Dit zal gepaard gaan met het opnieuw genereren van Key Pairs.

6 Certificate van buitenlandse SPOC-CA wordt vernieuwd

Het nieuwe Self-Signed Root Certificate zal gedistribueerd worden naar de NL-SPOC op dezelfde manier als het initiële Certificate gedistribueerd is. Dit staat beschreven in [CSN 36 9791]. De NL-SPOC controleert de authenticiteit van het Certificate op basis van offline verkregen informatie en neemt handmatig een beslissing over het opslaan van het Certificate voor gebruik.

7 TLS Client en Server Certificates van NL-SPOC-Extern worden vernieuwd

Dit proces verloopt geheel identiek aan het initieel aanvragen van TLS Client en Server Certificates.

8 TLS Client en Server Certificates van buitenlandse SPOC worden vernieuwd

Dit proces valt geheel onder verantwoordelijkheid van het buitenland. Het TLS Client of Server Certificate van de buitenlandse SPOC zal gebruikt worden bij het opzetten van een TLS verbinding met de NL-SPOC.

Zodra de NL-SPOC-Extern geconfronteerd wordt met het nieuwe buitenlandse SPOC TLS Certificate zal de NL-SPOC-Extern dit controleren met behulp van het buitenlandse SPOC-CA Root Certificate.

9. CRL wordt aangemaakt door NL-SPOC-CA.

Er kunnen verschillende redenen zijn om een CRL aan te maken:

- a. Indien vastgesteld wordt dat een Private TLS Key van de NL-SPOC-Extern mogelijk gecompromitteerd is, wordt de NL-SPOC-CA hiervan via diplomatieke weg op de hoogte gesteld. De NL-SPOC-CA moet dan binnen 72 uur een nieuwe CRL uitgeven voor het domein.
- b. Daarnaast wordt periodiek een nieuwe CRL uitgegeven.

Het uitgeven van een nieuwe CRL omvat de volgende stappen:

- c. De NL-SPOC-CA plaatst ingetrokken TLS Certificates waarvan de geldigheidsstermijn nog niet verlopen is op de CRL.
- d. De NL-SPOC-CA voegt datum en tijd toe aan de CRL.
- e. De NL-SPOC-CA tekent de CRL met de Private Key van het domein.
- f. De NL-SPOC-CA stelt de CRL beschikbaar om opgevraagd te worden. De CRL is beschikbaar op een URL die aangegeven is in het Root Certificate.

10. NL-SPOC vraagt CRL van buitenlands systeem op.

- a. De NL-SPOC ontvangt een notificatie van een nieuwe CRL en vraagt de CRL op of de NL-SPOC-CA besluit zelfstandig de CRL te controleren die is gepubliceerd op de URL zoals opgenomen in het buitenlandse SPOC Certificate.
- b. De NL-SPOC-CA ontvangt de CRL en controleert de handtekening.
- c. Indien deze controle positief uitvalt, verwerkt de NL-SPOC de informatie in de CRL.

11. Root Certificate van NL-SPOC-CA domein wordt ingetrokken.

Indien vastgesteld wordt dat de Private Key van de NL-SPOC-CA mogelijk gecompromitteerd is, worden alle systemen binnen het domein hiervan via diplomatieke weg op de hoogte gesteld. Voor de NL-SPOC-Extern betekent dit dat ook buitenlandse SPOCs waarmee het Root Certificate is uitgewisseld op de hoogte gebracht worden. De systemen zullen het Certificate verwijderen en geen gebruik meer maken van met de Private Key getekende TLS Certificates en CRLs. Zodra een nieuw NL-SPOC-CA Root Certificate beschikbaar is, zal de NL-SPOC-Extern nieuwe TLS Client en Server Certificates aanvragen.

12. Root Certificate van buitenlandse SPOC-CA wordt ingetrokken.

Indien vastgesteld wordt dat de Private Key van een buitenlandse SPOC-CA mogelijk gecompromitteerd is, zal de NL-SPOC hier via diplomatieke weg van op de hoogte gesteld worden. De NL-SPOC verwijdt het ingetrokken buitenlandse SPOC-CA Root Certificate.

6.4.2 CONNECT PKI scenario's

De scenario's binnen de CONNECT PKI voor de verschillende sub-CAs zijn identiek. Daarom gelden de hieronder beschreven scenario's voor alle sub-CAs.

1. Root Certificate van NL-CONNECT-CA domein wordt initieel aangemaakt en gedistribueerd.

- a. NL-CONNECT-CA maakt Key Pair aan tijdens Key Ceremony.

- b. Public Key wordt tijdens Key Ceremony in Certificate geplaatst dat door de NL-CONNECT-CA zelf gelekend wordt met de bijbehorende Private Key. Dit is het Self-Signed Root Certificate van het CONNECT-CA domein
- c. Dit Self-Signed CONNECT-CA Root Certificate wordt gedistribueerd naar de sub-CAs. Het distribueren kan plaatsvinden via een netwerkverbinding of op een andere manier zoals via e-mail of een extern opslagmedium
- d. De sub-CAs controleren de authenticiteit van het Certificate op basis van offline verkregen informatie en nemen handmatig een beslissing over het opslaan van het Certificate voor gebruik.

2. Certificates van Sub-CAs worden initieel aangemaakt en gedistribueerd

- a. Sub-CA maakt Key Pair aan tijdens Key Ceremony.
- b. Public Key wordt in Certificate Request geplaatst die naar de NL-CONNECT-CA gestuurd wordt. Het distribueren kan plaatsvinden via een netwerkverbinding of op een andere manier zoals via e-mail of een extern opslagmedium
- c. Op basis van de Registration Authority (RA) functionaliteit binnen de NL-CONNECT-CA wordt de authenticiteit van de Certificate Request gecontroleerd met behulp van offline verkregen informatie en wordt handmatig een beslissing genomen over het tekenen van het Certificate
- d. Indien de beslissing positief uitvalt, tekent de NL-CONNECT-CA het Certificate met haar Private Key.
- e. NL-CONNECT-CA stuurt het Certificate naar de Sub-CA.
Dit kan plaatsvinden via een netwerkverbinding of op een andere manier zoals via een extern opslagmedium
- f. De Sub-CA controleert het Certificate met behulp van het NL-CONNECT-CA Root Certificate
- g. Indien deze controle positief uitvalt, slaat de Sub-CA het Certificate op voor gebruik en distribueert de Sub-CA haar Certificate naar onderliggende NL-systemen. Dit kan plaatsvinden via een netwerkverbinding of op een andere manier zoals via e-mail of een extern opslagmedium
- h. De NL-systemen controleren het Certificate met behulp van offline verkregen informatie. De NL-systemen beschikken niet over het NL-CONNECT-CA Root Certificate.
- i. Indien deze controle positief uitvalt slaan de NL-systemen het Sub-CA Certificate op voor gebruik

3. TLS Client en Server Certificates van NL-systemen worden initieel aangemaakt

- a. Sub-CA maakt Certificate en Private Key aan en stuurt deze naar het NL-systeem. Dit kan plaatsvinden via een netwerkverbinding of op een andere manier zoals via een extern opslagmedium
- b. NL-systeem controleert het Certificate met behulp van het Sub-CA Certificate
- c. Indien deze controle positief uitvalt, slaat het NL-systeem Private Key en Certificate op voor gebruik

4. Root Certificate van NL-CONNECT-CA domein wordt vernieuwd

Er kunnen verschillende redenen zijn om het NL-CONNECT-CA Certificate te vervangen

- a. Het Certificate is (bijna) verlopen
- b. De Private Key is gecompromitteerd. In dit geval zal het oude Certificate ingetrokken worden (offline communicatie en handmatig verwijderen van Certificate bij de relying parties)

In beide gevallen wordt een nieuw Self-Signed Root Certificate aangemaakt en gedistribueerd naar de Sub-CAs. Aanmaak en distributie van het nieuwe Self-Signed Root Certificate vindt op dezelfde manier plaats als het initiële proces

Nadat de sub-CAs op de hoogte zijn gebracht van het nieuwe Root Certificate moeten deze sub-CAs een nieuw Certificate aanvragen voor hun eigen Public Keys. Dit zal gepaard gaan met het opnieuw genereren van Key Pairs

5. Certificates van sub-CAs worden vernieuwd.

Er kunnen verschillende redenen zijn om het Sub-CA Certificate te vervangen

- a. Het Certificate is (bijna) verlopen.
- b. De Private Key is gecompromitteerd. In dit geval zal het oude Certificate ingetrokken worden (offline communicatie en handmatig verwijderen van Certificate bij de relying parties).

In beide gevallen wordt een nieuw sub-CA Certificate aangemaakt en gedistribueerd naar de onderliggende NL-systemen. Aanmaak en distributie van het nieuw sub-CA Certificate vindt op dezelfde manier plaats als het initiële proces

Nadat de onderliggende systemen op de hoogte zijn gebracht van het nieuwe sub-CA Certificate moeten al deze systemen een nieuw Certificate aanvragen voor hun eigen Public Keys. Dit zal gepaard gaan met het opnieuw genereren van Key Pairs.

6. TLS Client en Server Certificates van NL-systemen worden vernieuwd.

Dit proces verloopt geheel identiek aan het initiële aanvragen van TLS Client en Server Certificates.

7. Root Certificate van NL-CONNECT-CA domein wordt ingetrokken.

Indien vastgesteld wordt dat de Private Key van de NL-CONNECT-CA mogelijk gecompromitteerd is, worden alle sub-CAs hiervan op de hoogte gesteld. De sub-CAs zullen het Certificate verwijderen en geen gebruik meer maken van met de Private Key getekende Certificates. Zodra een nieuw NL-CONNECT-CA Root Certificate beschikbaar is, zullen de sub-CAs nieuwe Certificates aanvragen.

8. Certificate van Sub-CA domein wordt ingetrokken.

Indien vastgesteld wordt dat de Private Key van een Sub-CA mogelijk gecompromitteerd is, worden alle systemen binnen het domein hiervan op de hoogte gesteld. De systemen zullen het Certificate verwijderen en geen gebruik meer maken van met de Private Key getekende TLS Certificates en CRLs. Zodra een nieuw Sub-CA Certificate beschikbaar is, zullen de systemen nieuwe TLS Client en Server Certificates aanvragen.

9. TLS Client of Server Certificate van NL-systeem wordt ingetrokken.

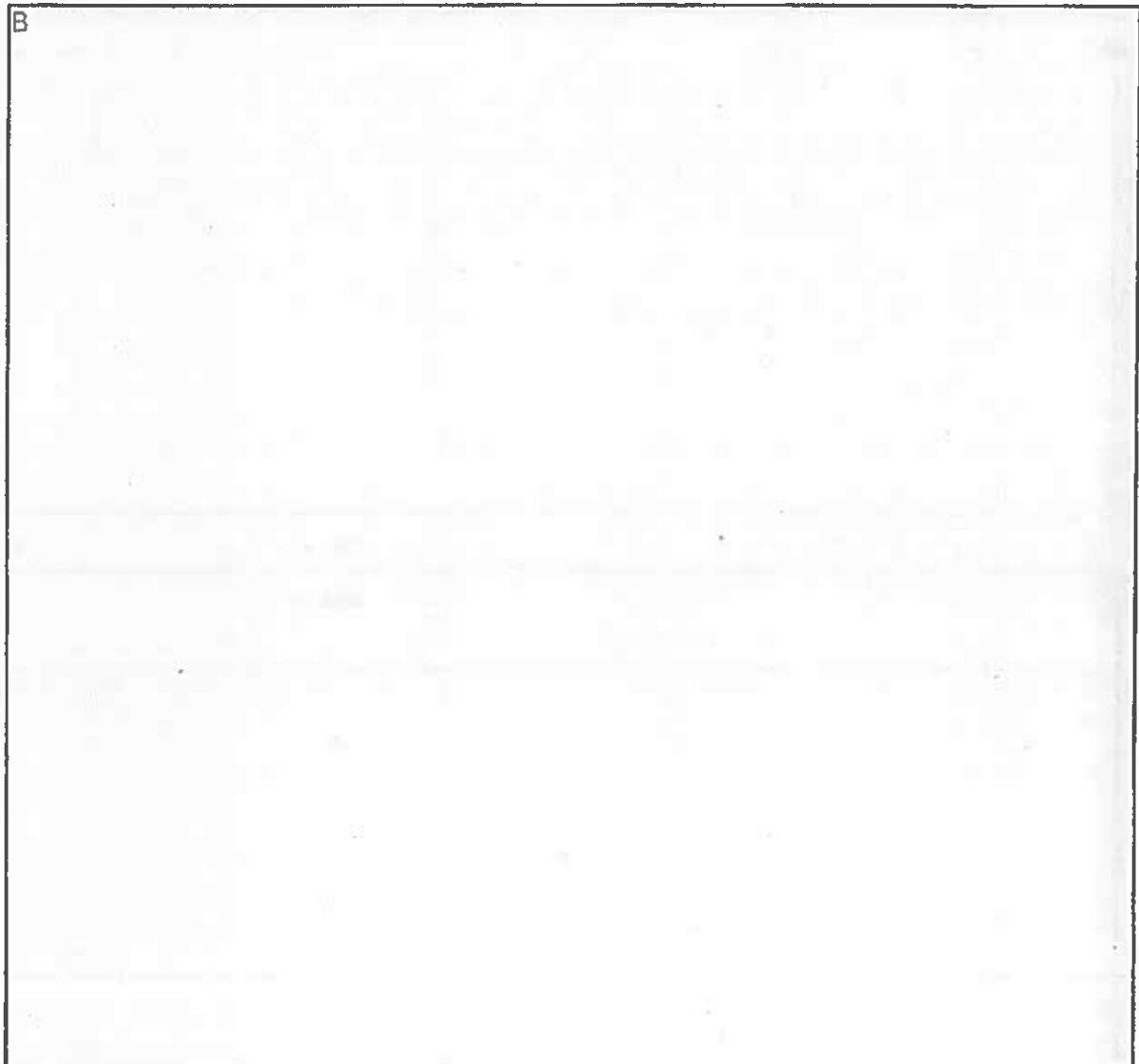
Indien vastgesteld wordt dat een TLS Private Key van een NL-systeem mogelijk gecompromitteerd is, worden Key Pair en Certificate vervangen. Behalve binnen de NL-Terminal-TLS-PKI wordt geen gebruik gemaakt van CRLs.

7 Infrastructuuroverzicht

B

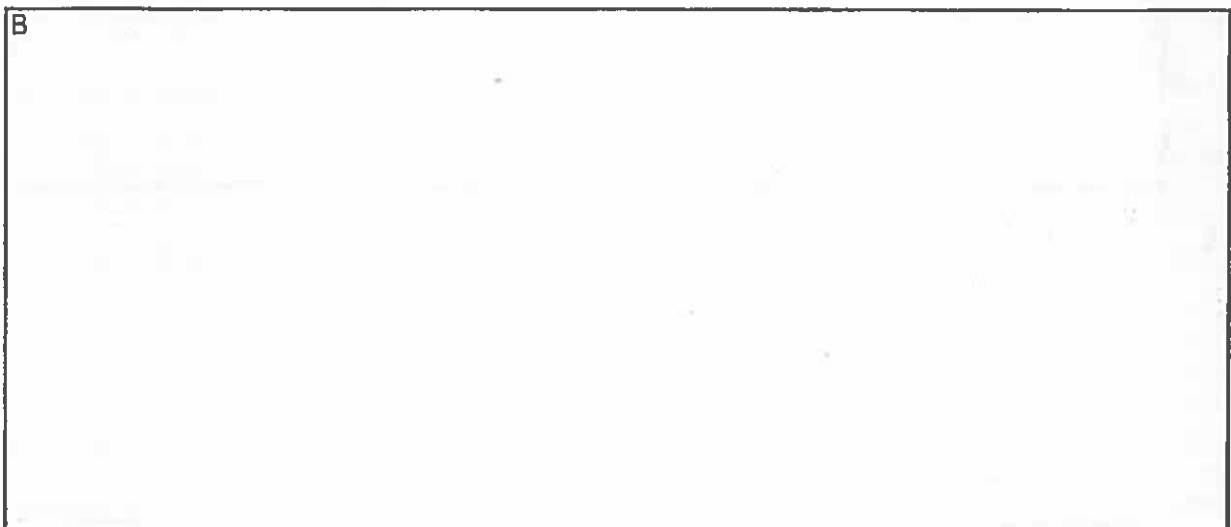


B

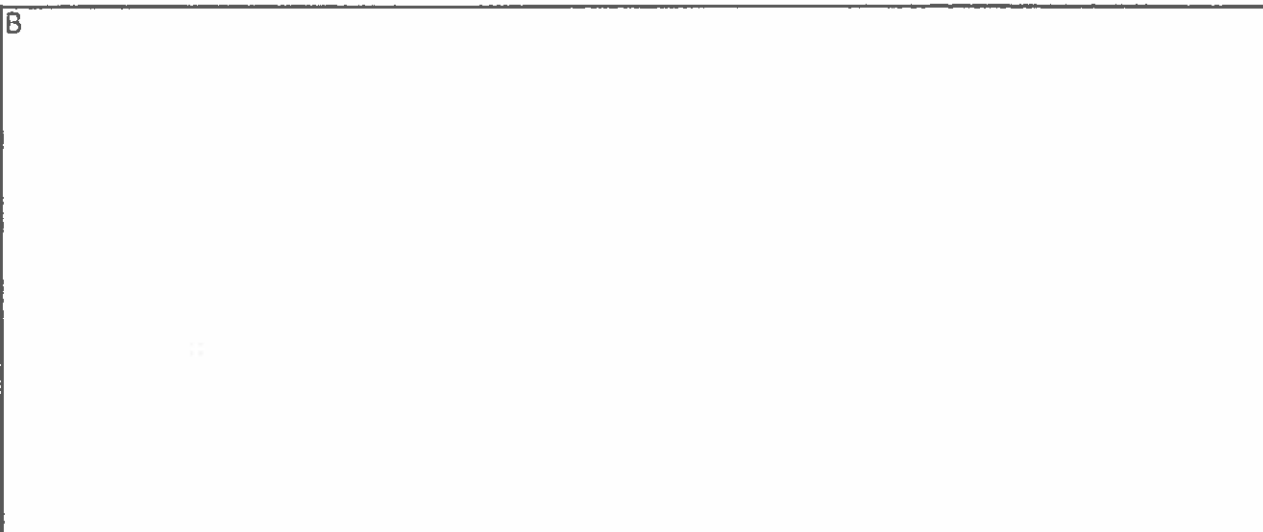
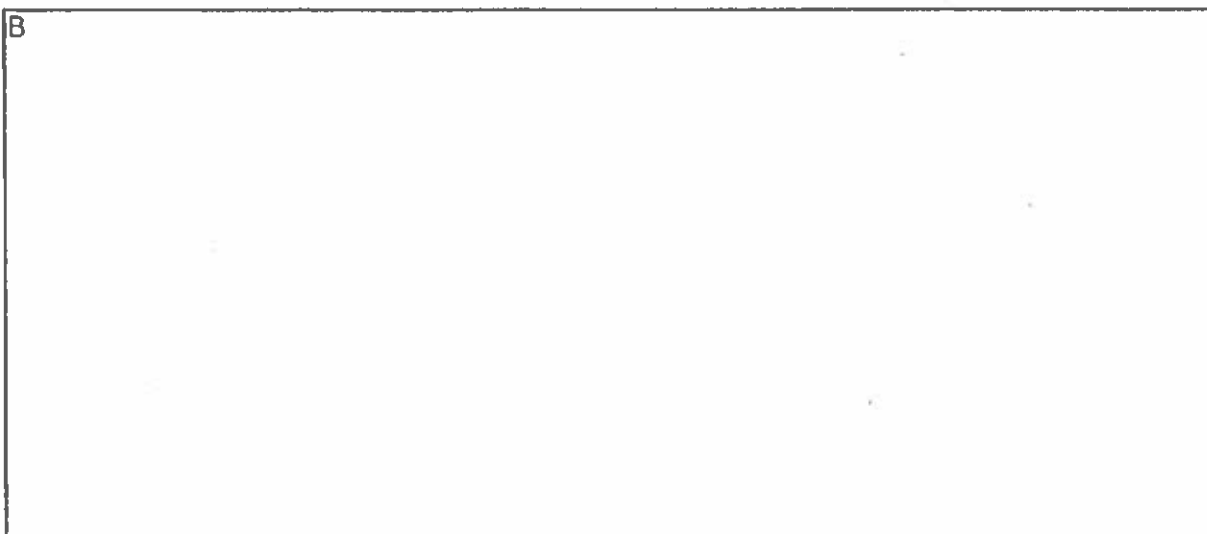


7.1 Storage

B



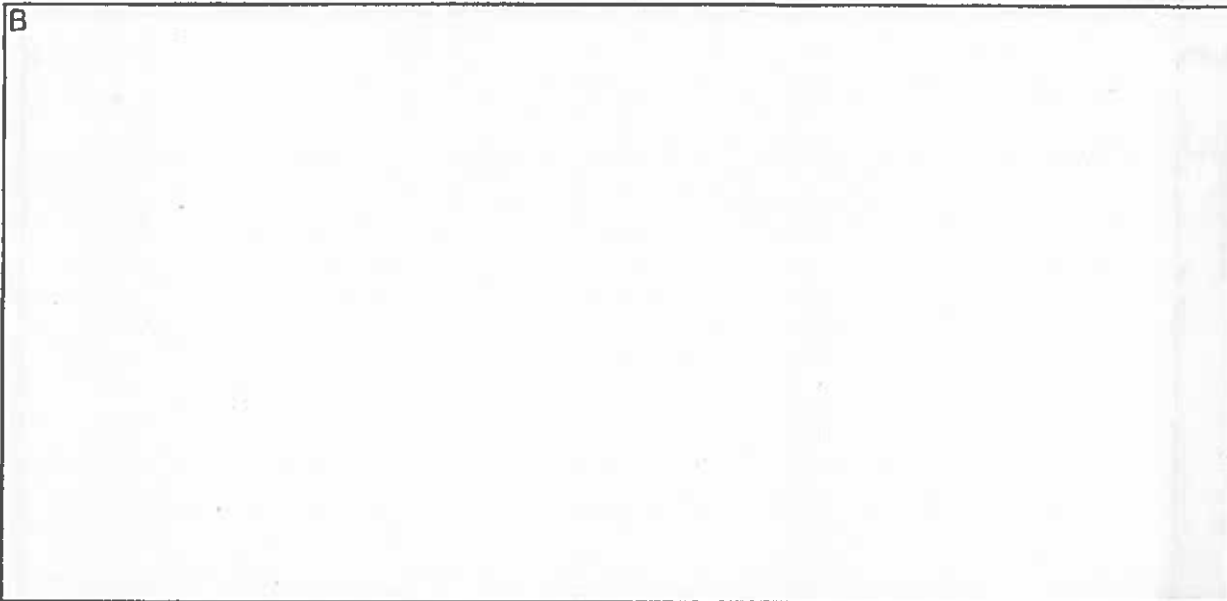
7.2 Servers



7.3 Ethernet switches



B



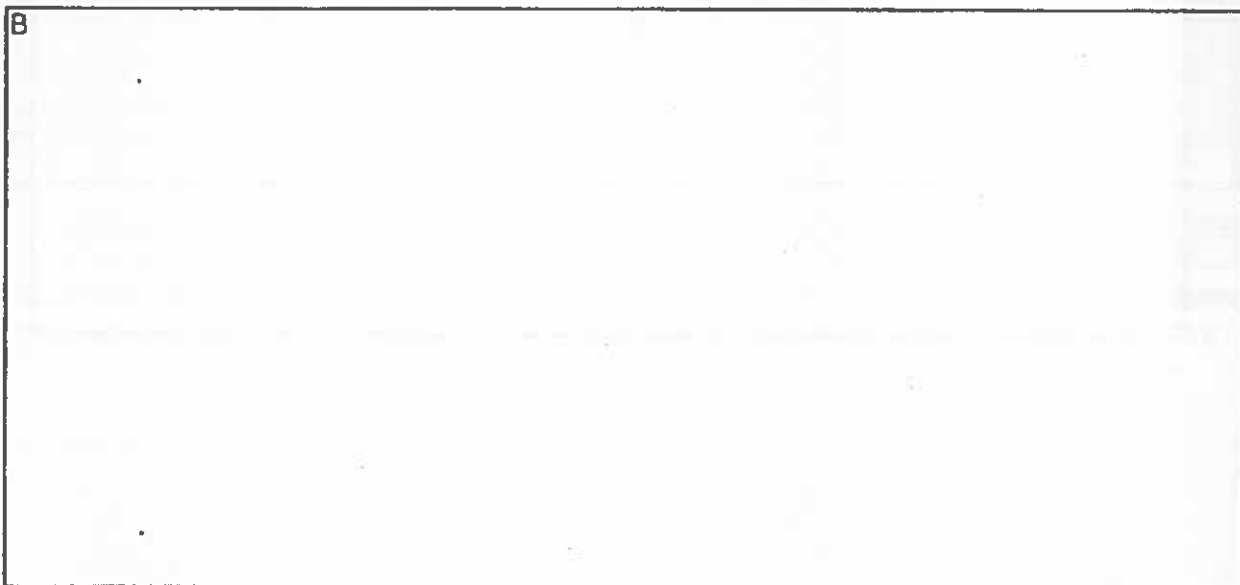
7.4 Hardware Security Module

B



7.5 Secure Services Gateway Enterprise Firewall

B

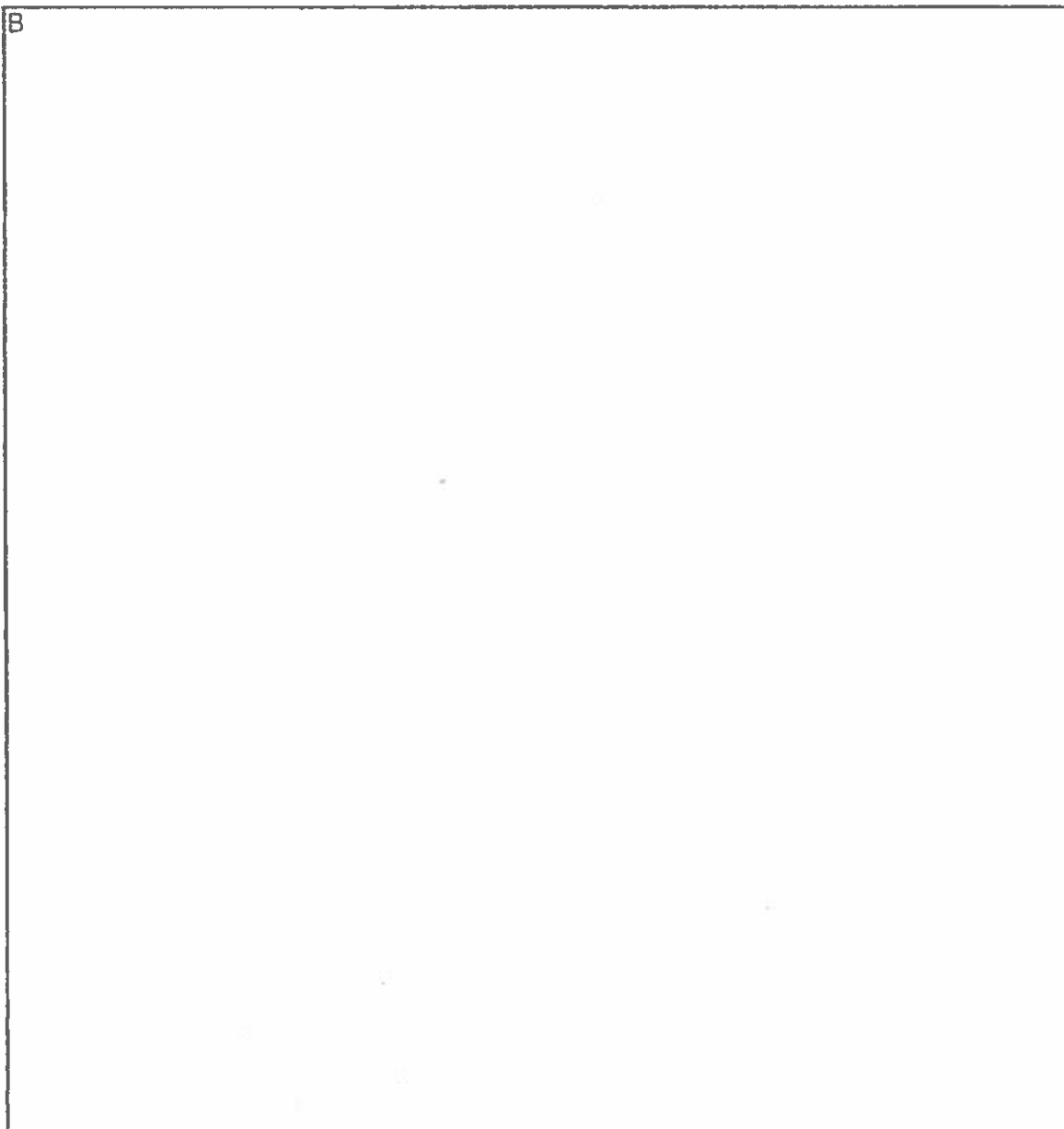


7.6 Verbindingskabels

B



B



Annex A Stukslijsten

A.1 Storage

B

Aantal	Artikel	Omschrijving
B		

B

Aantal	Artikel	Omschrijving
B		

B

A.2 Servers

B

Aantal	Artikel	Omschrijving
B		

B

Aantal	Artikel	Omschrijving
B		

B

Aantal	Artikel	Omschrijving
B		

A.3 Ethernet switches

B

Aantal	Artikel	Omschrijving
B		

B

Aantal	Artikel	Omschrijving
B		

B

A.5 Verbindingskabels

8

[illegible]

doc 4



Justitiële Informatiedienst
Ministerie van Veiligheid en Justitie

RUBRICERING: DEPARTEMENTAAL VERTROUWELIJK

EAC-PKI-NL--Architectuur--Deel 3: Communicatie

OID	B
Auteur	justID
Status	Definitief
Versie	1.0
Datum	22 november 2011
Rubricering	Departementaal Vertrouwelijk
Vastgesteld door	A
Datum vaststelling	22 november 2011



Justitiële Informatiedienst
Ministerie van Veiligheid en Justitie

Colofon

Afzendgegevens

Justitiële Informatiedienst

Egbert Gorterstraat 6
7607 GB Almelo
Postbus 337
7600 AH Almelo
www.justid.nl

Contactpersoon

T A
F

Projectnaam

PKI

Contactpersoon: A

Auteurs

JustiD

Versie overzicht

Versie	Datum	Steller	Omschrijving
1.0	22-11-2011	JustID	Definitief

EAC-PKI-NL — Architectuur — Deel 3: Verbindingen

Inhoud	Pagina
1 Scope	9
2 Normatieve referenties	9
3 Termen and definities	9
4 Afkortingen	9
5 Overzicht van verbindingen binnen de EAC-PKI-NL	10
6 Algemene communicatie eisen	12
7 SOAP en LDAP	13
7.1 SOAP Interfaces	13
7.2 LDAP interfaces	13
7.3 Berichten per Interface: Tabellen	13
7.3.1 EAC Tabel	13
7.3.2 PA tabel	14
8 Verbindingsbeveiliging	15
8.1 Eisen aan HTTPS / TLS	15
8.2 TLS certificaten	16
8.2.1 Uit te geven certificaten	16
8.2.2 Certificaatprofiel	20
8.3 Initieel aanmaken en uitwisselen van de PKI certificaten voor verbindingsbeveiliging	22
8.3.1 Opslagmedium en bestandsnaamconventie	22
8.3.2 Metadata	23
8.3.3 Beveiligingsoverwegingen	23
8.4 Intrekken van certificaten / Certificate Revocation List	23
9 Connectiviteit	24
Annex A Bijzondere lijsten	25
A.1 MasterList	25
A.2 DefectList	25

Voorwoord

Verscheidende Nederlandse identiteitsbewijzen volgens de Wet op de Identificatieplicht, zoals reisdocumenten (MRTDs) en verblijfsvergunningen (RPs), zijn inmiddels voorzien van een chip waarin document- en houdergegevens digitaal zijn opgeslagen. Dit is in overeenstemming met Europese besluiten over het toevoegen van een chip en de specificaties waaraan de chip dient te voldoen. Ook andere EU en Schengen lidstaten hebben hun paspoorten en verblijfsvergunningen voorzien van een dergelijke chip. Internationaal hebben verschillende non-EU/Schengen landen hun reisdocumenten voorzien van een chip volgens ICAO Doc 9303 die daardoor grotendeels identiek is aan de chip in Europese reisdocumenten.

Om de authenticiteit van de gegevens in de chip elektronisch te kunnen verifiëren, zijn deze gegevens digitaal ondertekend door de uitgevende instanties in de verschillende landen. Inspectiesystemen hebben de signing PKI public key certificaatkets behorend bij de private keys waarmee de gegevens ondertekend zijn nodig om de authenticiteit van de gegevens te kunnen controleren. Uitwisseling van de benodigde certificaten gebeurt bilateraal en daarnaast via de ICAO public key directory.

De elektronische identiteitsbewijzen kunnen in de chip naast biografische gegevens en een afbeelding van het gezicht ook een tweetal vingerafdrukken bevatten. Voor identiteitsbewijzen uitgegeven binnen de EU en Schengen is dit verplicht. Ook wordt binnen de EU/Schengen geëist dat deze meer gevoelige biometrische gegevens zijn beschermd met een extra beveiligingsmechanisme. Dit mechanisme zorgt voor veilige communicatie met de chip en toegang tot de vingerafdrukken in de chip wordt slechts gegeven aan daartoe geautoriseerde inspectiesystemen. Dit slaat bekend als Extended Access Control (EAC). Wanneer een inspectiesysteem data wil uitlezen die is beveiligd met EAC, moet het inspectiesysteem zich authenticeren aan de chip en tonen dat het toegangsrechten heeft om de beveiligde data uit te lezen. Deze authenticatie is gebaseerd op zogenaamde Card Verifiable Certificates (CV certificaten), die door de chip in een identiteitsbewijs kunnen worden geverifieerd. De toegangsrechten van het inspectiesysteem staan gecodeerd in deze CV certificaten. Nadat de terminal zich heeft geauthenticeerd op basis van CV certificaten en een geheime sleutel, geeft de chip toegang tot gegevens waarvoor toegangsrechten in het CV certificaat zijn gecodeerd. Voor het genereren en distribueren van deze CV certificaten zijn verifiying Public Key Infrastructures, ook wel EAC-PKI-NL genoemd, gespecificeerd binnen Nederland. Uitwisseling van CV certificaten en certificaataanvragen met andere EU/Schengen lidstaten om ook de vingerafdrukken uit de buitenlandse identiteitsbewijzen te kunnen lezen, vindt plaats via een Single Point of Contact (SPOC).

Voor de EAC-PKI-NL is een Policy Authority (PA) opgericht. In deze PA zijn de volgende organisaties vertegenwoordigd:

- Ministerie van Veiligheid en Justitie,
- Ministerie van Buitenlandse Zaken;
- JustID.

Daarnaast kunnen eventueel andere belanghebbende vertegenwoordigd zijn in de PA, bijvoorbeeld partijen die verantwoordelijk zijn voor de uitgifte van de identiteitsbewijzen.

Het secretariaat van de PA worden gevoerd door JustID. De verantwoordelijkheid voor de uitvoering van deze PKI is belegd bij de Justitiele Informatiedienst (JustID). Vanuit deze verantwoordelijkheid heeft JustID ook dit document opgesteld.

Dit document is onderdeel van een serie documenten onder de algemene titel *EAC-PKI-NL — Architectuur* dat bestaat uit de volgende onderdelen

- *Deel 1: Referentieids PKI voor EAC-PKI NL*
- *Deel 2: Overzicht architectuur en infrastructuur*
- *Deel 3: Verbindingen*

EAC-PKI-NL — Architectuur — Deel 3: Communicatie

1 Scope

Dit document beschrijft de eisen aan de verbindingen tussen de Nederlandse systemen binnen de EAC-PKI-NL (interne verbindingen). Voor de verbindingen en communicatie tussen de NL-SPOC (External webservice) en buitenlandse SPOCs (externe verbindingen) geldt [CSN 36 9791].

Dit document bevat de volgende zaken.

- Eisen aan de interne verbindingsbeveiliging (TLS)
- De bij de interne en externe verbindingsbeveiliging behorende SPOC en Connect PKI certificaten voor de Nederlandse systemen.
- Eisen aan de interne verbindingen op de netwerklaag (TCP/IP)

2 Normatieve referenties

[NL-A01] EAC-PKI-NL--Architectuur--Deel 1: Referentieids PKI voor eMRTDs

Ten behoeve van dit document gelden de referenties beschreven in [NL-A01]. Daarnaast wordt gebruikt gemaakt van de volgende referenties:

- [RFC 791] "Internet Protocol" (IPv4), RFC 791, Information Sciences Institute, University of Southern California, September 1981
- [RFC 2246] "The TLS Protocol Version 1.0", RFC 2246, Dierks, T. and C. Allen, januari 1999
- [RFC 2460] "Internet Protocol, Version 6 (IPv6)", RFC 2460, IETF, December 1998
- [RFC 2818] "HTTP over TLS" RFC 2818, E. Rescorla, mei 2000
- [RFC 3268] "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)", RFC 3268, Chown, P., juni 2002
- [RFC 4346] "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, Dierks, T. and E. Rescorla, april 2006
- [RFC 4366] "Transport Layer Security (TLS) Extensions", RFC 4366, Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and T. Wright, april 2006
- [RFC 4492] "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)", RFC 4492, Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., and B. Moeller, mei 2006
- [RFC 5246] "The Transport Layer Security (TLS) Protocol, Version 1.2", RFC 5246, Dierks, T. and E. Rescorla, augustus 2008
- [RFC 5820] "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5820, D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, mei 2008

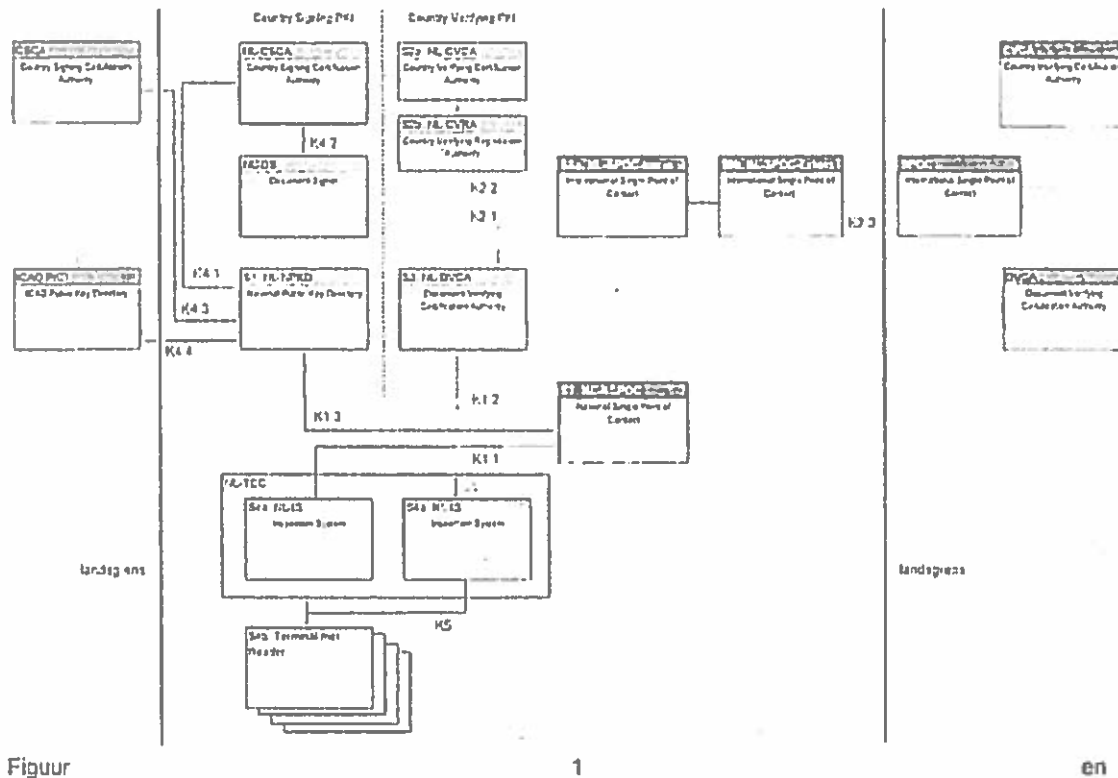
3 Termen and definities

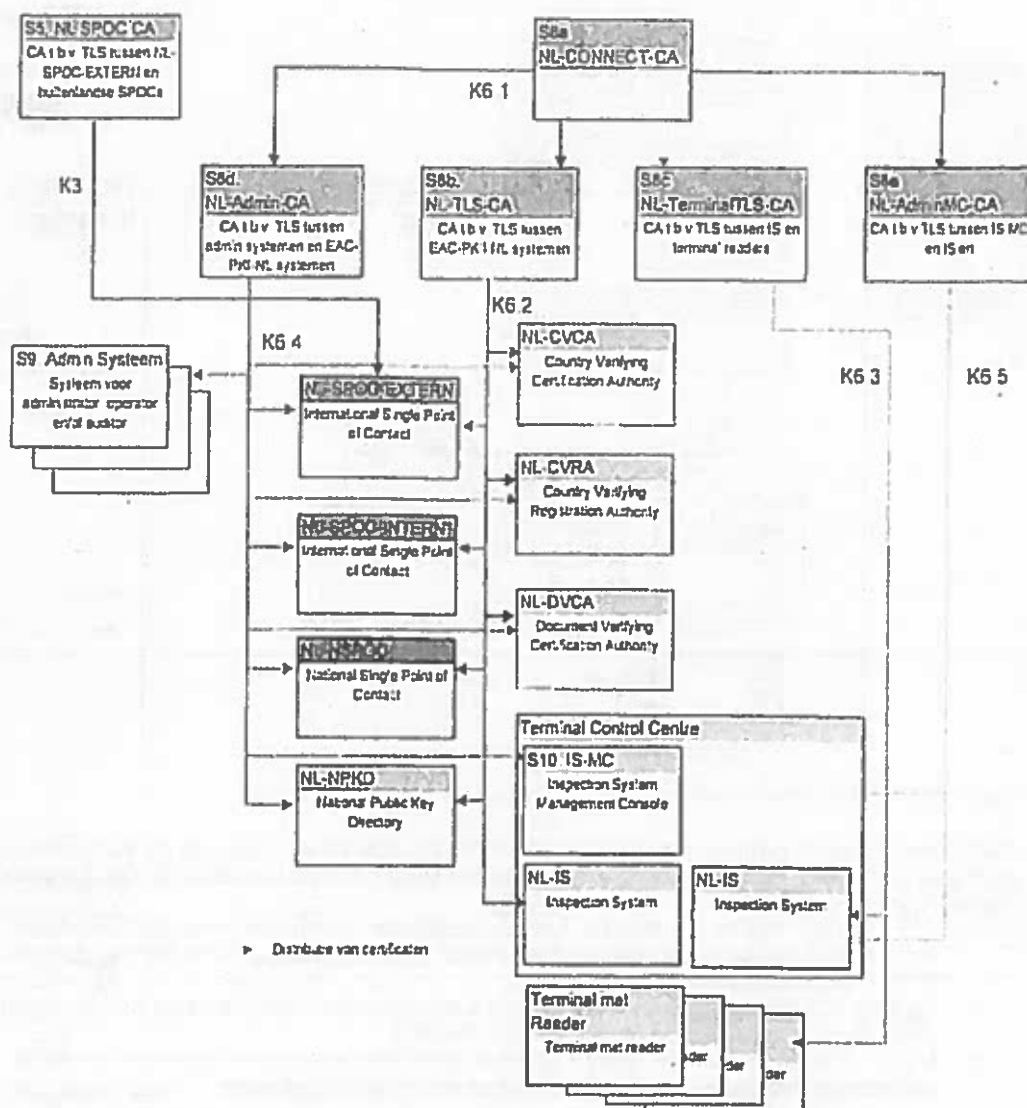
Ten behoeve van dit document gelden de termen en definities beschreven in [NL-A01].

4 Afkortingen

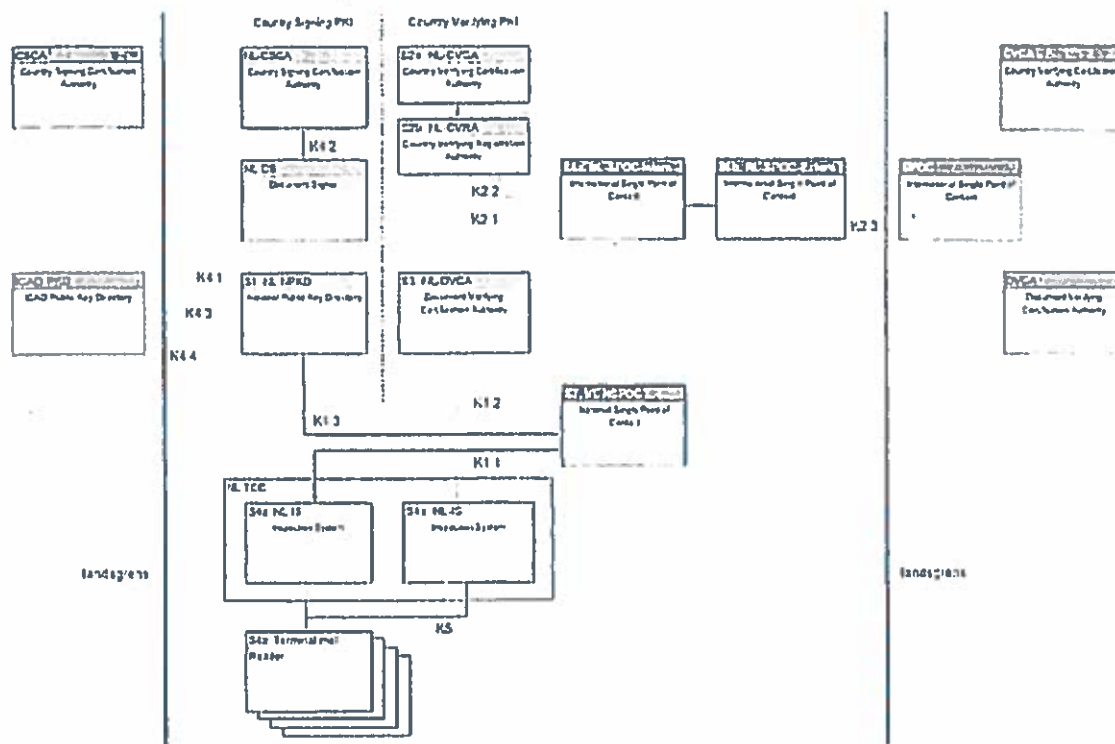
Ten behoeve van dit document gelden de afkortingen beschreven in [NL-A01].

5 Overzicht van verbindingen binnen de EAC-PKI-NL





Figuur 2 geven een overzicht van de EAC-PKI-NL. Dit document richt zich op de verbindings-eisen tussen de Nederlandse systemen genummerd van S1 t/m S10.



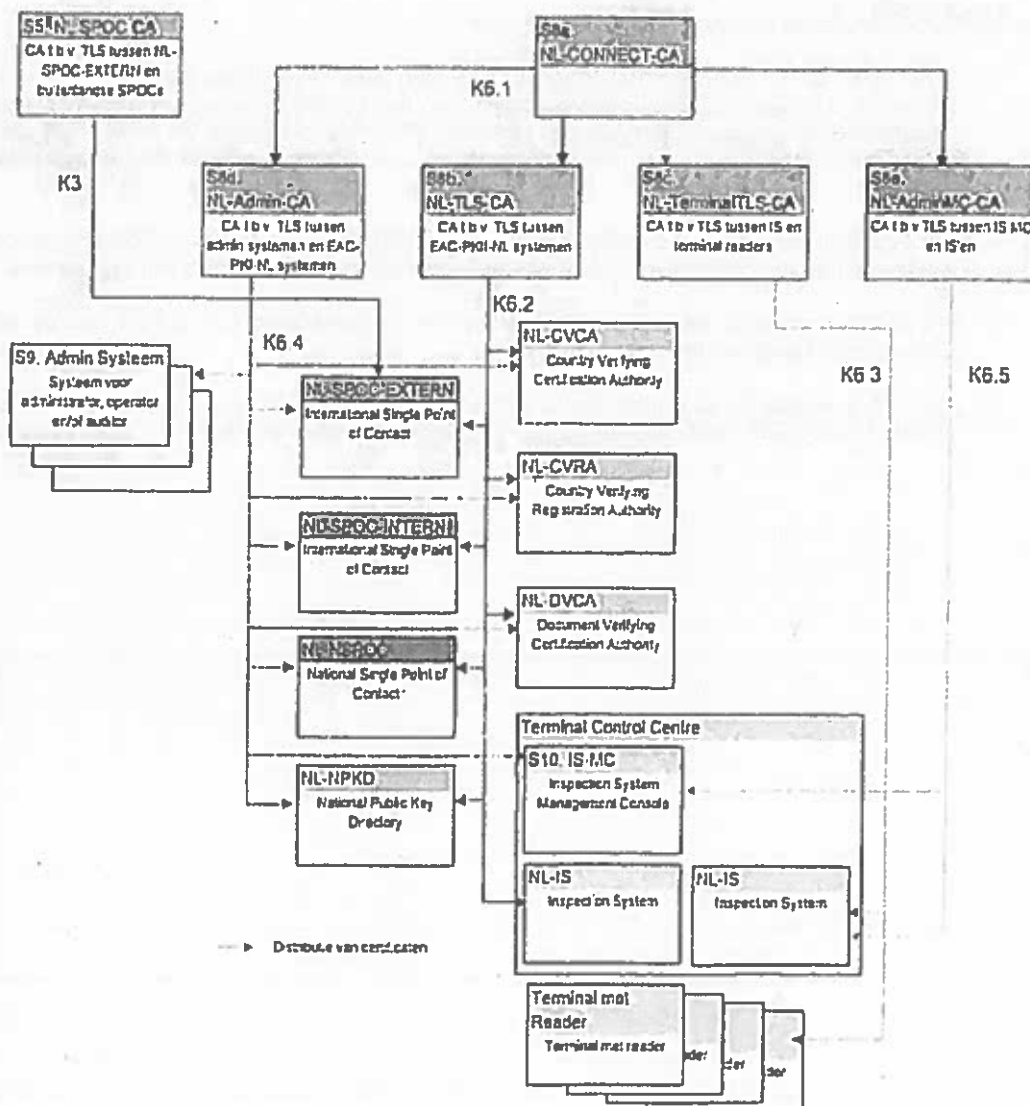
Figuur 1: Overzicht van verbindingen tussen systemen binnen de EAC-PKI-NL

Daarbij wordt gebruik gemaakt van door de NL-SPOC-CA (S5) en sub-CAs van de NL-Connect-CA (S8) uitgegeven certificaten ten behoeve van verbodingsbeveiliging (TLS, zie Hoofdstuk 8). De NL-Connect-CA is opgedeeld in vier domeinen:

- TLS domein:** binnen dit domein worden certificaten uitgegeven voor het beveiligen van de verbindingen tussen de Nederlandse EAC-PKI-NL systemen NL-CVCA, NL-DVCA, NL-IS, NL-SPOC, NL-NSPOC en de NL-NPKD.
- TerminalTLS domein:** binnen dit domein worden certificaten uitgegeven voor het beveiligen van de verbindingen tussen de NL-IS'en en Terminal Readers.
- Admin domein:** binnen dit domein worden certificaten uitgegeven voor het beveiligen van de verbindingen tussen de EAC-PKI-NL systemen en de Admin Systemen.
- AdminMC domein:** binnen dit domein worden certificaten uitgegeven voor het beveiligen van de verbindingen tussen de IS-MC en de IS'en.

De verbindingseisen zoals die in dit document beschreven worden, gelden voor de verbindingen K01.x, K02.x, K05 en K06. Dit worden interne verbindingen genoemd binnen de EAC-PKI-NL. Voor de verbinding K02.3 tussen de NL-SPOC (S6) (External webservice) en een buitenlandse SPOC gelden de verbodings- en connectiviteitseisen zoals beschreven in [CSN 36 9791]. K02.3 geeft de externe verbindingen aan waarvan in dit document sprake is. De External webservice van de NL-SPOC hoort tot het Externe SPOC domein.

De verbindingen K04.1, K04.2, K04.3 en K04.4 blijven volledig buiten scope.



Figuur 2: Overzicht van verbindingen tussen systemen binnen de EAC-PKI-NL

6 Algemene communicatie eisen

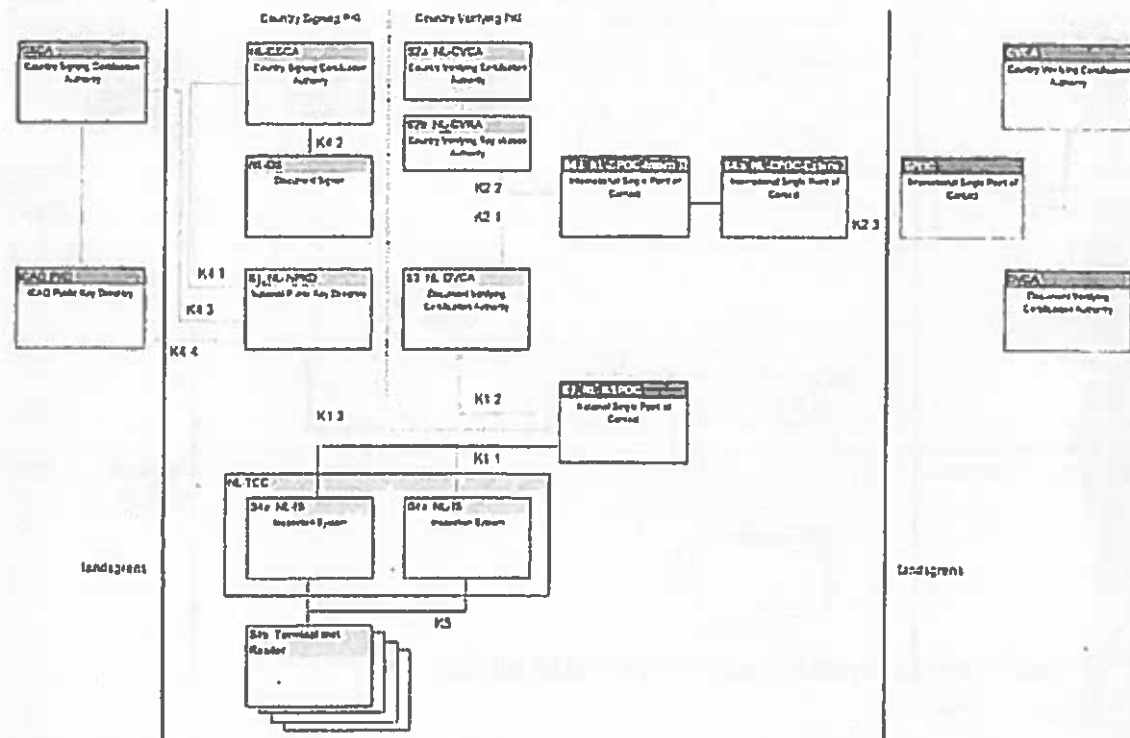
De communicatie dient te voldoen aan de volgende eisen.

- a. In het geval van handmatige afhandeling van berichten moet een systeem asynchrone communicatie gebruiken. Hierbij geeft het systeem direct na succesvolle ontvangst van het bericht een ontvangstbevestiging in de vorm van een response. Pas nadat het bericht via de bedieningsinterface is afgehandeld wordt een antwoordbericht teruggestuurd naar de verzender van het oorspronkelijke bericht.
- b. Alle berichten die worden ontvangen of verstuurd MOETEN in de log van het betreffende systeem worden geregistreerd samen met de bijbehorende (berichtverwerkings)acties van het systeem.
- c. Alle X.509 certificaten worden in de communicatie geïdentificeerd met behulp van de absolute Distinguished Name van het certificaat.
- d. Alle CRL's worden in de communicatie geïdentificeerd met behulp van de absolute Distinguished Name van het CSCA certificaat behorende bij de private sleutel waarmee de CRL is ondertekend.

7 SOAP en LDAP

7.1 SOAP Interfaces

Bij de implementatie van de interne verbindingen K01.1, K01.2, K02.2, K02.3 en K05 in

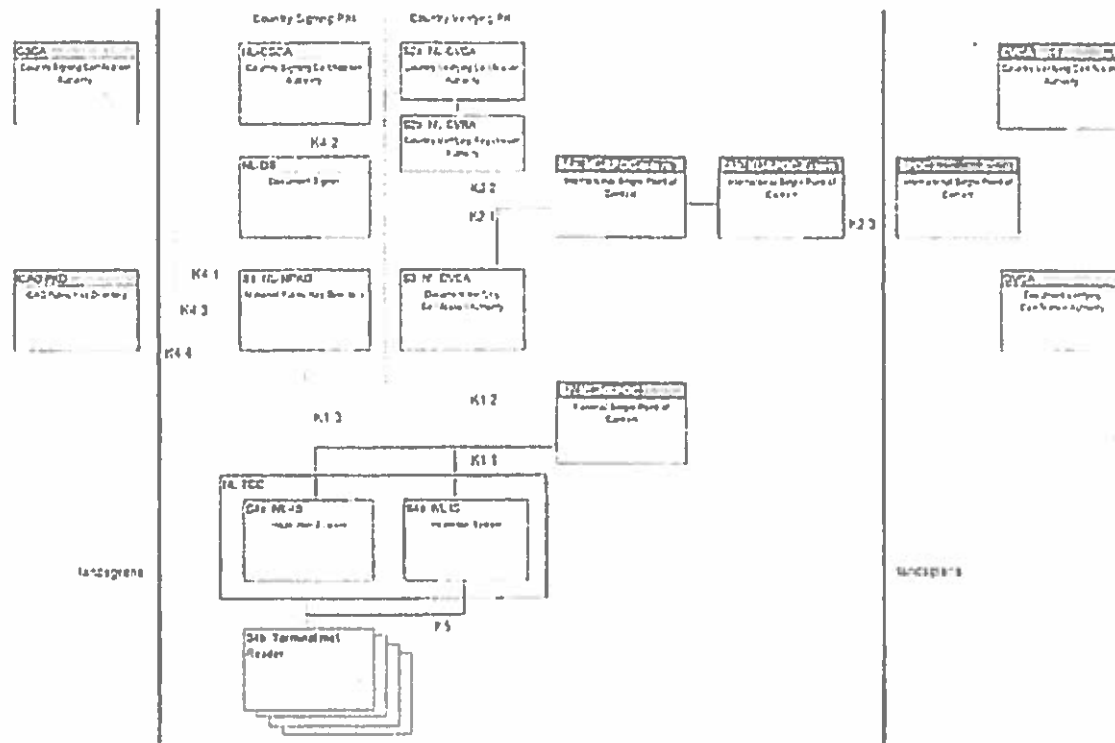


Figuur 1 wordt SOAP [SOAP] over HTTPS [RFC 2818] gebruikt. Het wordt aanbevolen dat de interne web service interfaces geïmplementeerd worden volgens [WS-I BP] en [WS-I BB]. Interface K02.1 is handmatige file transfer.

De interne SOAP communicatie voldoet aan de WSDL definities zoals beschreven in de koppelvlakspecificaties [NL-K0x].

7.2 LDAP Interfaces

Bij de implementatie van de interne verbindingen K01.3 in

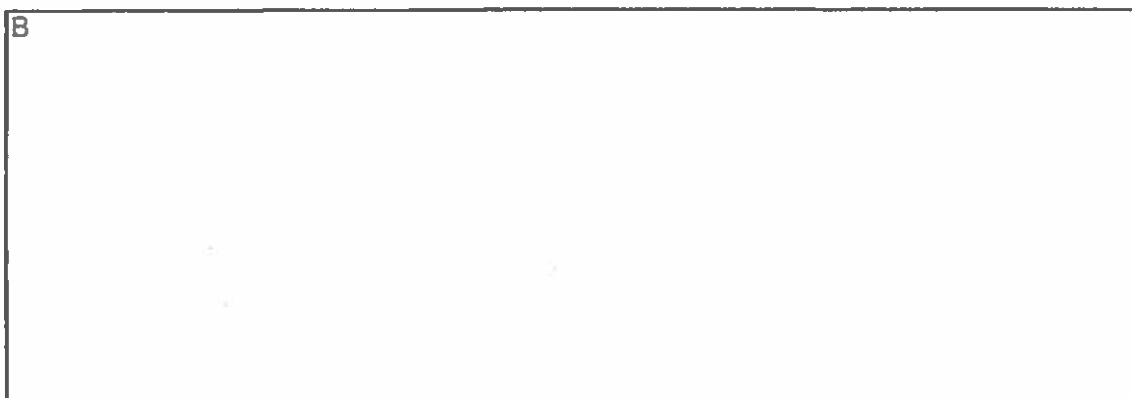


Figuur 1 wordt LDAP [LDAP] over HTTPS [RFC 2818] gebruikt

7.3 Berichten per Interface: Tabellen

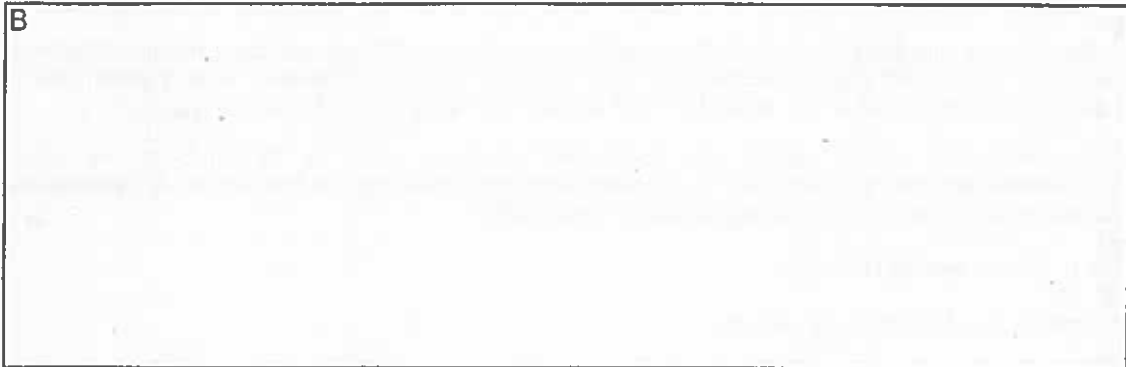
7.3.1 EAC Tabel

7.3.1.1 Server zijde per systeem



7.3.1.2 Client zijde per systeem

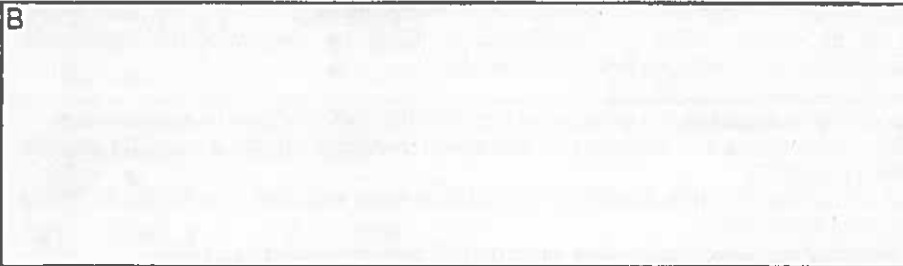
B



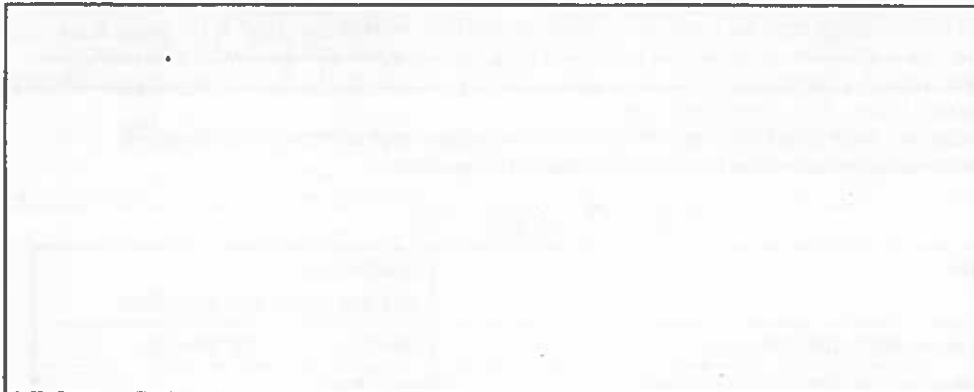
7.3.2 PA tabel

7.3.2.1 Server zijde per systeem

B



7.3.2.2 Client zijde per systeem



8 Verbindingsbeveiliging

Om de interne en externe verbindingen op transportniveau te beveiligen wordt voor alle communicatie gebruik gemaakt van HTTPS met TLS authenticatie voor zowel de client als de server. Hiervoor wordt gebruik gemaakt van de SPOC PKI voor verbinding K03.2 en de Connect PKI voor de overige verbindingen.

De SPOC PKI maakt gebruik van certificaten uitgegeven door de NL-SPOC-CA die onder verantwoordelijkheid van JustID valt.¹ De Connect PKI maakt gebruik van de Connect CA en bijbehorende sub-CAs die ook onder verantwoordelijkheid van JustID vallen.

8.1 Eisen aan HTTPS / TLS

De eisen aan HTTPS/TLS zijn als volgt:

- Twee-zijdige TLS authenticatie: zowel van de client als van de server
- Out-of-band registratie van de initiële certificaten van de CA
- Out-of-band registratie van alle systemen bij de CAs bij het aanvragen van de initiële TLS client en server certificaten
- TLS v1.0 wordt gebruikt zoals gedefinieerd in [RFC 2246], TLS 1.1 [RFC 4346] en TLS 1.2 [RFC 5246] mogen ondersteund worden via standaard TLS protocol versie onderhandeling.
- Zowel de client als de server worden geauthenticeerd op basis van asymmetrische cryptografie gebaseerd op publieke sleutels opgeslagen in X.509 certificaten.
- De TLS client voert de volgende verificaties uit:
 - Het server certificaat wordt volledig gevalideerd volgens [RFC 5280] inclusief revocation status
 - De ExtKey Usage extensie is aanwezig in het server certificaat en bevat een OID volgens paragraaf 9.1.2 van [A1].
 - De inhoud van het server certificaat subject distinguished name veld (DN) is gelijk aan de inhoud van de callerID parameter.
 In geval één van bovengenoemde verificaties faalt, moet de TLS client de verbinding afbreken.
- De TLS server voert de volgende verificaties uit:
 - de client wordt volledig geauthenticeerd gebruik makend van het certificaat
 - het client certificaat wordt volledig gevalideerd volgens [RFC 5280] inclusief de revocation status
 - de ExtKeyUsage extensie is aanwezig en bevat een OID volgens paragraaf 9.1.2 van [A1]
 - Het client certificaat distinguished name veld (DN) komt overeen met de callerID parameter
 In geval één van bovengenoemde verificaties faalt, moet het verzoek geweigerd worden met gebruik van response code HTTP 401 Unauthorized.
- Fallback naar een zwak (pre TLS) protocol wordt niet toegestaan door de interface configuratie.
- Uitsluitend de volgende algoritmen worden ondersteund en gebruikt.

Tabel 1: TLS encryptie suites

Cipher suite	Certificate and key exchange algorithm
TLS_RSA_WITH_AES_128_CBC_SHA	RSA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE_RSA
TLS_RSA_WITH_AES_256_CBC_SHA	RSA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE_RSA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE_ECDSA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE_ECDSA

¹ De SPOC PKI kan in theorie ook gebruik maken van certificaten uitgegeven door de NL-CSCA

- Binnen de scope van de TLS handshake negotiation ondersteunt de client alle TLS cipher suites gedefinieerd in Tabel 1. Zowel de server als de client ondersteunen RSA en ECDSA gebaseerde authenticatie. Het is de server toegestaan om aan de client een client certificaat te vragen van een ander type dan dat van de server. Voor de client is het toegestaan dit andere type certificaat te sturen.
- Het gebruik van ECDHE_ECDSA key agreement in de TLS handshake is in overeenstemming met de toevoegingen zoals die gedefinieerd zijn in [RFC 4492] en [RFC 4366]. Zowel de client als de server ondersteunen de van toepassing zijnde elliptische curve extensies zoals gespecificeerd in [RFC 4492] in het kader van de TLS handshake. De ondersteunde elliptische curves en EC points formaten zijn gedefinieerd in Sectie 5 van [RFC 4492]. De ondersteunde TLS cipher suites zoals gedefinieerd in Tabel 1 (welke gebruik maken van de Advanced Encryption Standard (AES) voor versleuteling), zijn in overeenstemming met de specificatie [RFC 3268].

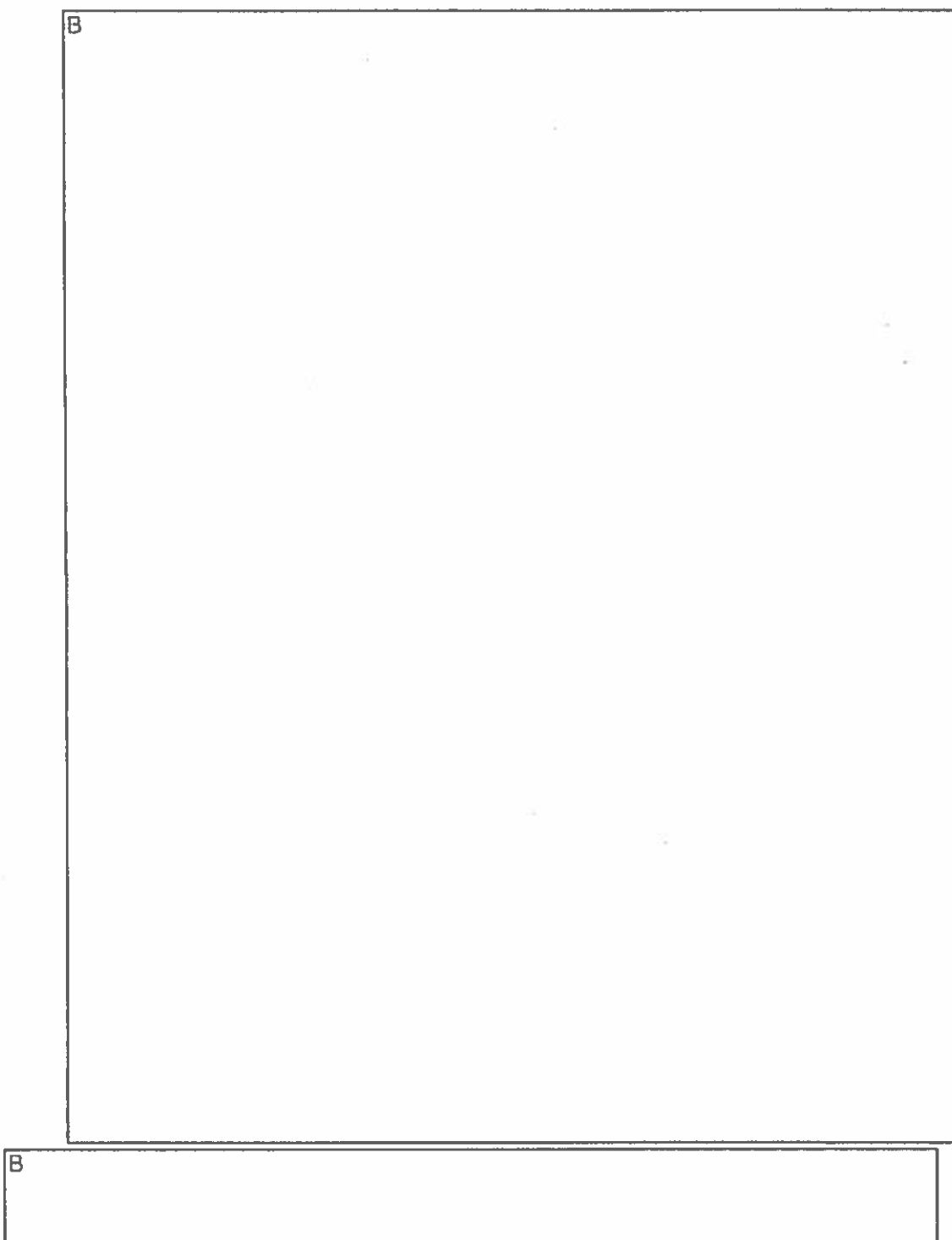
8.2 TLS certificaten

Voor communicatie tussen de NL-SPOC en buitenlandse SPOCs maakt iedere SPOC gebruik van de door de eigen SPOC-CA getekende certificaten. De andere SPOC is op de hoogte van het SPOC-CA root certificaat van het buitenland waarmee gecommuniceerd wordt. Dit betekent dat de NL-SPOC moet beschikken over het NL-SPOC-CA root certificaat van het externe SPOC domein en de SPOC-CA root certificaten van buitenlandse SPOCs waarmee gecommuniceerd wordt. Er is geen bovenliggende Europese of internationale CA.

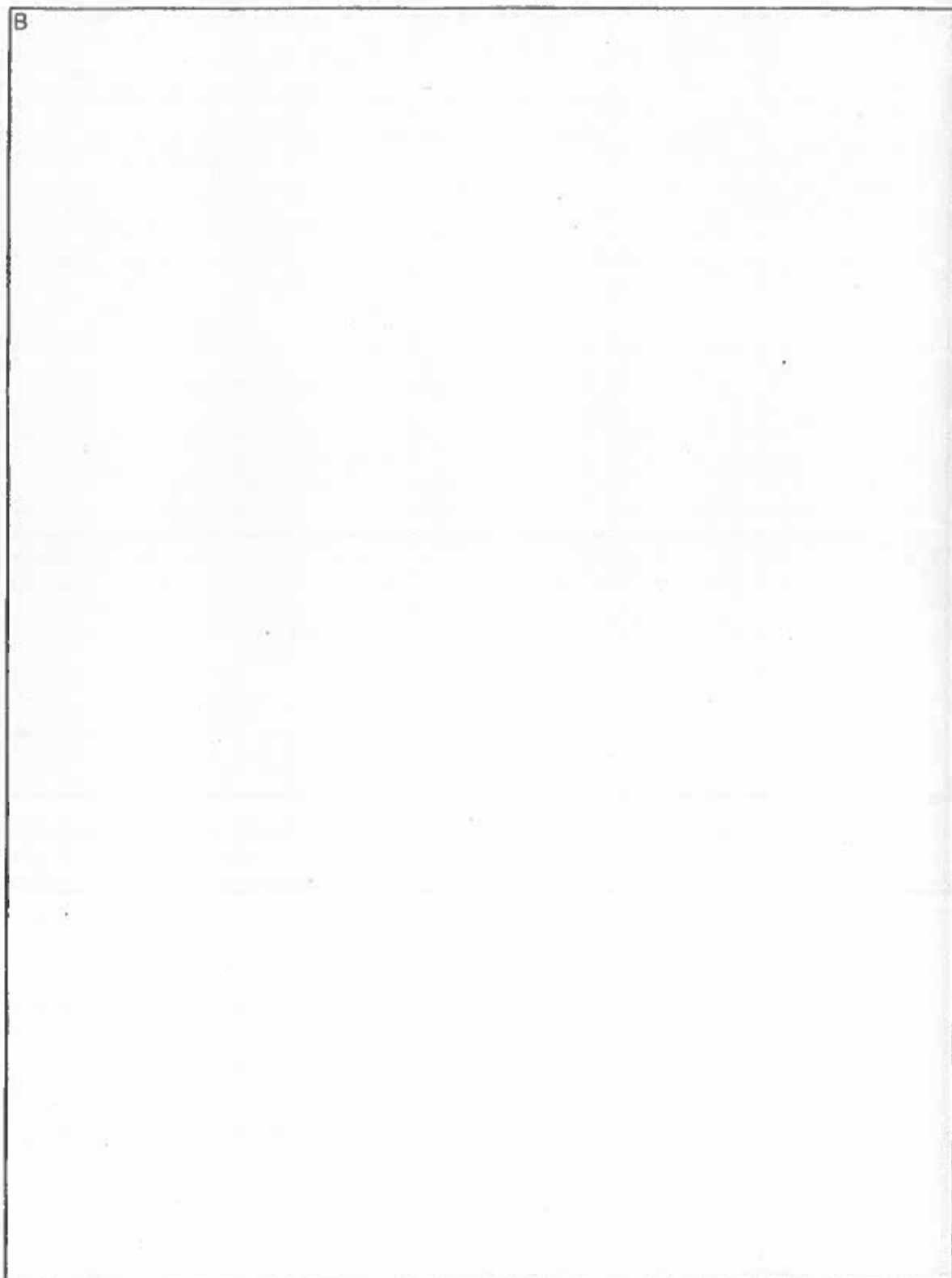
Binnen Nederland ontvangen alle systemen een of meerdere certificaatparen van de sub-CAs onder de Connect-CA. De meeste systemen maken deel uit van meer dan één domein. De Nederlandse systemen beschikken over het/de sub-CA root certificaat(en) van het/de domeinen waarvan ze deel uitmaken, niet over het Connect-CA root certificaat.

8.2.1 Uit te geven certificaten

B

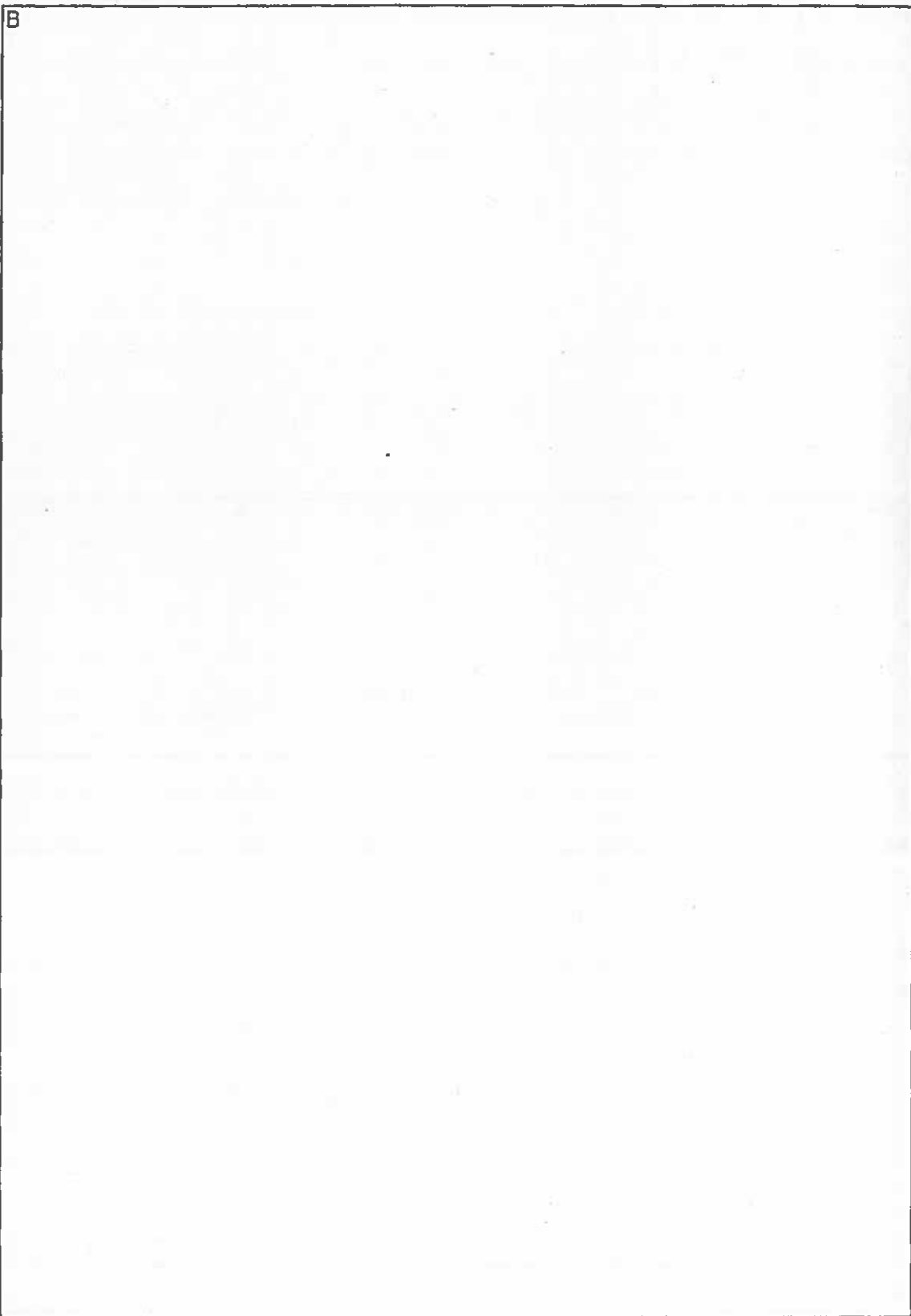


B



B

8.2.2 Certificaatprofiel



B

B

8.3 Initieel aanmaken en uitwisselen van de PKI certificaten voor verbindingsbeveiliging

B

8.3.1 Opslagmedium en bestandsnaamconventie

B

B

8.3.2 Metadata

B

8.3.3 Beveiligingsoverwegingen

B

9 Connectiviteit

De interne netwerkverbindingen zijn gebaseerd op TCP/IP.

IPv4 [RFC 791] wordt ondersteund, IPv6 [RFC 2460] mag ondersteund worden. Na 31 december 2011 wordt ook IPv6 ondersteund.

Het toewijzen van IP adressen en host-namen van systemen vindt plaats door de policy authority van de SPOC PKI.

De externe netwerkverbindingen op TCP/IP niveau moeten voldoen aan [CSN 36 9791].

Annex A Bijzondere lijsten (normatief)

A.1 MasterList

Een MasterList is een lijst met CSCA certificaten die nationaal worden vertrouwd. Voor ieder van de X.509 certificaten is het gehele certificaat opgenomen in de lijst. De Nederlandse MasterList is cryptografisch ondertekend door de List Signer module van de NL-NPKD. Voor verificatie is het betreffende List Signer certificaat opgenomen in de MasterList. Iedere keer wanneer op de NL-NPKD een CSCA certificaat als vertrouwd wordt aangemerkt, wordt een nieuwe versie van de MasterList gemaakt.

Een MasterList is geformateerd volgens RFC3369 SignedData. Hierbij wordt de inhoud van het 'eContent' element aan de hand van het onderstaande ASN.1 type MasterList gecodeerd. Hierbij wordt het ASN.1 type Certificate gebruikt zoals dat door RFC 5280 is gedefinieerd voor X.509 certificaten.

```
MasterList ::= SEQUENCE {  
    version MasterListVersion,  
    certificates SET OF Certificate  
}  
  
MasterListVersion ::= INTEGER {V0(0)}
```

A.2 DefectList

Een Defect is gedefinieerd als een productiefout die aanwezig is in een groot aantal documenten. Het intrekken van al uitgegeven documenten is onpraktisch of zelfs onmogelijk als het ontdekte defect zich bevindt in buitenlandse documenten.

DefectLists zijn ondertekende lijsten om met zulke defecten om te gaan. Defecten worden geïdentificeerd door de Document Signer Certificaten die gebruikt zijn om defecte documenten te produceren. DefectLists zijn daarom errata die niet alleen informeren over defecten maar ook corrigenda verschaffen om de fouten te herstellen waar mogelijk.

Het is mogelijk dat een document geen defect bevat hoewel het Document Signer Certificaat op de DefectList staat.

Een DefectList is geformateerd volgens BSI TR-03129, versie 1.10.



Justitiële Informatiedienst
Ministerie van Veiligheid en Justitie

doc 2

RUBRICERING: DEPARTEMENTAAL VERTROUWELIJK

**EAC-PCI-NL--Exploitatie--Deel 3.1:
NPKD Beheer**

OID	B.
Auteur	JustiD
Status	Definitief
Versie	1.2
Datum	22 november 2011
Rubricering	Departementaal Vertrouwelijk
Vastgesteld door	A.
Datum vaststelling	22 november 2011

Colofon

Afzendgegevens **Justitiële Informatiedienst**

Egbert Gorterstraat 6
7607 GB Almelo
Postbus 337
7600 AH Almelo
www.justid.nl

Contactpersoon

A

Projectnaam

EAC-PKI-NL

Contactpersoon: A

Auteur

JustID

Versie overzicht

Versie	Datum	Steller	Omschrijving
1.0	22-11-2011	JustID	Definitief

EAC-PKI-NL — Exploitatie — Deel 3: NPKD Beheer

Inhoud	Pagina
1 Scope	9
2 Normatieve referenties	9
3 Termen en definities	9
4 Afkortingen	9
5 Beheer – Fase 3	10
5.1 Starten OpenDS	10
5.2 Starten JBoss Applicatie Server	10
5.3 OpenDS Control Panel	10
5.4 NPKD Webapplicatie	11
5.4.1 Aanmelden	11
5.4.2 Module home	11
5.4.3 Module certificaten	11
5.4.4 Module CRLs	13
5.4.5 Module CRL URLs	14
5.4.6 Module Master Lists	15
5.4.7 Module landen	16
5.4.8 Module gebruikers	18
5.4.9 Module Notificaties	18
5.5 Referenties LDAP entries	19
5.5.1 Referenties Certificaat	19
5.5.2 Referenties CRL	19
5.5.3 Referenties CRL URL	19
5.5.4 Referenties Master List	19
5.5.5 Referenties Land	20
5.5.6 Referenties Gebruiker	20
Annex A	21
A.1 TLS PKI	21
A.1.1 Overzicht	21
A.1.2 Omschrijving	21
A.2 Registratie Inspectiesysteem	22
A.2.1 Benodigde gegevens	22
A.3 Interface Specificatie	22
A.4 Certificaat Validatie	24
A.5 CRL Validatie	25

Voorwoord

Verschillende Nederlandse identiteitsbewijzen volgens de Wet op de Identificatieplicht, zoals reisdocumenten (MRTDs) en verblijfsvergunningen (RPs), zijn inmiddels voorzien van een chip waarin document- en houdergegevens digitaal zijn opgeslagen. Dit is in overeenstemming met Europese besluiten over het toevoegen van een chip en de specificaties waaraan de chip dient te voldoen. Ook andere EU en Schengen lidstaten hebben hun paspoorten en verblijfsvergunningen voorzien van een dergelijke chip. Internationaal hebben verschillende non-EU/Schengen landen hun reisdocumenten voorzien van een chip volgens ICAO Doc 9303 die daardoor grotendeels identiek is aan de chip in Europese reisdocumenten.

Om de authenticiteit van de gegevens in de chip elektronisch te kunnen verifiëren, zijn deze gegevens digitaal ondertekend door de uitgevende instanties in de verschillende landen. Inspectiesystemen hebben de signing PKI public key certificaatsketens behorend bij de private keys waarmee de gegevens ondertekend zijn nodig om de authenticiteit van de gegevens te kunnen controleren. Uitwisseling van de benodigde certificaten gebeurt bilateraal en daarnaast via de ICAO public key directory.

De elektronische identiteitsbewijzen kunnen in de chip naast biografische gegevens en een afbeelding van het gezicht ook een tweetal vingerafdrukken bevatten. Voor identiteitsbewijzen uitgegeven binnen de EU en Schengen is dit verplicht. Ook wordt binnen de EU/Schengen geëist dat deze meer gevoelige biometrische gegevens zijn beschermd met een extra beveiligingsmechanisme. Dit mechanisme zorgt voor veilige communicatie met de chip en toegang tot de vingerafdrukken in de chip wordt slechts gegeven aan daartoe geautoriseerde inspectiesystemen. Dit staat bekend als Extended Access Control (EAC). Wanneer een inspectiesysteem data wil uitlezen die is beveiligd met EAC, moet het inspectiesysteem zich authenticeren aan de chip en tonen dat het toegangsrechten heeft om de beveiligde data uit te lezen. Deze authenticatie is gebaseerd op zogenaamde Card Verifiable Certificates (CV certificaten), die door de chip in een identiteitsbewijs kunnen worden geverifieerd. De toegangsrechten van het inspectiesysteem staan gecodeerd in deze CV certificaten. Nadat de terminal zich heeft geauthenticeerd op basis van CV certificaten en een geheime sleutel, geeft de chip toegang tot gegevens waarvoor toegangsrechten in het CV certificaat zijn gecodeerd. Voor het genereren en distribueren van deze CV certificaten zijn verifying Public Key Infrastructures, ook wel EAC-PKI-NL genoemd, gespecificeerd binnen Nederland. Uitwisseling van CV certificaten en certificaataanvragen met andere EU/Schengen lidstaten om ook de vingerafdrukken uit de buitenlandse identiteitsbewijzen te kunnen lezen, vindt plaats via een Single Point of Contact (SPOC).

Voor de EAC-PKI-NL is een Policy Authority (PA) opgericht. In deze PA zijn de volgende organisaties vertegenwoordigd:

- Ministerie van Veiligheid en Justitie;
- Ministerie van Buitenlandse Zaken;
- JustID.

Daarnaast kunnen eventueel andere belanghebbende vertegenwoordigd zijn in de PA, bijvoorbeeld partijen die verantwoordelijk zijn voor de uitgifte van de identiteitsbewijzen.

Het secretariaat van de PA worden gevoerd door JustID. De verantwoordelijkheid voor de uitvoering van deze PKI is belegd bij de Justitiele Informatiedienst (JustID). Vanuit deze verantwoordelijkheid heeft JustID ook dit document opgesteld.

Dit document is onderdeel van een serie documenten onder de algemene titel EAC-PKI-NL — *Exploitatie* dat bestaat uit de volgende onderdelen:

- Deel 1: *Installatie en configuratie*
- Deel 2: *EJBCA - Beheer*
- Deel 3 1: *NPKD - Beheer*
- Deel 3 2: *NSPOC - Beheer*
- Deel 3 3: *TCC/IS vaste opstelling - Beheer*

- *Deel 3.4: DVCA / DVRA - Beheer*
- *Deel 3.5: SPOC Intern en extern - Beheer*
- *Deel 3.6: CVCA / CVRA – Beheer*
- *Deel 3.7: SPOC-CA - Beheer*
- *Deel 3.8: CONNECT-CA - Beheer*
- *Deel 4 Overname CVCA en CVRA*
- *Deel 6: CVCA Risicoanalyse*
- *Deel 7: CVCA Recovery*
- *Deel 8: Beveiligingsplan*
- *Deel 9.1. Baseline beveiligingsmaatregelen inspectiesystemen vaste opstelling*
- *Deel 9.2 Baseline beveiligingsmaatregelen inspectiesystemen mobiele opstelling*
- *Deel 10. werkinstructies en formuleren EAC proces*
- *Deel 11: Configuratie Accounts*

1 Scope

Dit document geldt als handleiding voor het operationeel beheer van de NPKD.

2 Normatieve referenties

[NL-E01] EAC-PKI-NL—Exploitatie—Deel 1: Installatie en Configuratie.

Ten behoeve van dit document gelden de referenties zoals beschreven in [NL-E01].

3 Termen en definities

Ten behoeve van dit document gelden de termen en definities zoals beschreven in [NL-E01].

4 Afkortingen

Ten behoeve van dit document gelden de afkortingen zoals beschreven in [NL-E01].

5 Beheer -- Fase 3

5.1 Starten OpenDS

De OpenDS service is niet geconfigureerd om automatisch te starten wanneer het systeem opstart. Om de OpenDS service te starten en te stoppen worden de volgende commando's gebruikt. Zorg ervoor dat u deze commando's uitvoert als system user (%SYSTEM_USER_NAME%).

- Starten >
- Stoppen >

5.2 Starten JBoss Applicatie Server

De JBoss applicatie server is niet geconfigureerd om automatisch te starten wanneer het systeem opstart. Om de JBoss service te starten en te stoppen worden de volgende commando's gebruikt. Zorg ervoor dat u deze commando's uitvoert als system user (%SYSTEM_USER_NAME%).

Voor het starten/stoppen van JBoss wordt gevraagd om het root wachtwoord van het systeem (%SYSTEM_ROOT_PASSWD%). Geef dit wachtwoord in wanneer hierom gevraagd wordt.

- Starten >
- Stoppen >

JBoss is geconfigureerd met de NPKD Webapplicatie ten behoeve van het operationele beheer van de OpenDS LDAP server. Na het starten van de JBoss applicatie server is de webapplicatie beschikbaar op

5.3 OpenDS Control Panel

OpenDS bevat een control panel waarmee de server geconfigureerd kan worden. Deze tool heeft een technisch karakter en gaat uit van voldoende kennis van OpenDS en LDAP in het algemeen. Het control panel is dan ook niet geschikt om te gebruiken voor operationeel beheer.

Om het OpenDS control panel te kunnen gebruiken moet OpenDS op een beheerstation worden geïnstalleerd.

- Download OpenDS 2.2.0
- Pak OpenDS-2.2.0 zip uit op een systeem die netwerk toegang heeft tot de LDAP server op TCP/IP port
- Start OpenDS control panel
 - o Windows:
 - o Linux:
- Benodigde inloggegevens
 - o Remote Server %SYSTEM_INTERN_IP%
 - o Administration Port
 - o Bind DN %ODS_ADMIN_NAME%
 - o Password %ODS_ADMIN_PASSWD%

5.4 NPKD Webapplicatie

Dit deel beschrijft het operationeel beheer van de NPKD OpenDS LDAP server gebruikmakend van de NPKD webapplicatie.

5.4.1 Aanmelden

Voordat u succesvol kunt inloggen op de NPKD webapplicatie is het van belang dat u het juiste admin-client certificaat en private key, uitgegeven door de NL-SPOCCA, in uw browser hebt geladen. Wend u tot de handleiding van uw webbrowser naar keuze voor uitleg over het importeren van een client certificaat in uw browser.

Naast het client certificaat moet u het NL-SPOCCA certificaat in uw browser importeren als Certificate Authority.

- Ga in uw webbrowser naar
- Sommige browsers zullen u vragen het juiste client certificaat te kiezen. Mocht u fouten zien gerelateerd aan HTTPS – TLS controleer dan of de certificaten correct zijn geïmporteerd.
- Vul de volgende gegevens in op het loginformulier:
 - o Gebruikersnaam:
 - o Wachtwoord:
 - o Klik 'Aanmelden'
- Als alles goed is ziet u het hoofdscherm van de NPKD webapplicatie
- Controleer alle voorgaande stappen in geval van problemen.

5.4.2 Module home

Nadat u zich hebt aangemeld bevindt u zich op de home pagina van de applicatie. Deze pagina bevat een korte uitleg van de overige modules.

Links bovenin het scherm is aangegeven met welke credentials u bent aangemeld. Tevens vindt u hier een knop om uzelf af te melden bij het systeem.

Via de navigatiebalk kunt u navigeren naar de modules t.b.v. beheer voor certificaten, CRLs, landen en gebruikers. De navigatiebalk is op elke pagina zichtbaar.

5.4.3 Module certificaten

Binnen deze module kunt u de certificaten opgenomen in de LDAP server per land beheren.

5.4.3.1 Overzicht

Klik in de navigatiebalk op 'Certificaten' om naar de overzichtspagina van deze module te gaan.

Om alle certificaten van een land te bekijken selecteert u een land uit de lijst en klik op 'Selecteer'. Alle certificaten opgenomen in de LDAP server van het gekozen land zullen getoond worden.

5.4.3.2 Certificaat details

Om de details van een certificaat te bekijken klikt u vanuit het certificaat overzicht op de 'Details' knop uit de Actie kolom. Een nieuwe pagina met de details van het certificaat zal getoond worden.

5.4.3.3 Certificaat entry bewerken

Om velden van een certificaat entry te bewerken gaat u naar de detail pagina van het desbetreffende certificaat (zie 5.4.3.2).

Alleen de *Level of Approval* en het *Source/Origin* veld kunnen worden aangepast. Om de aanpassingen op te slaan klikt u op 'Opslaan'. U keert weer terug naar het overzicht van certificaten. De wijzigingen worden direct van kracht.

5.4.3.4 Certificaat entry verwijderen

Om het certificaat uit de LDAP server te verwijderen gaat u naar de detail pagina van het desbetreffende certificaat (zie 5.4.3.2).

Rechts onderin klikt u op 'Verwijderen'. U keert weer terug naar het overzicht van certificaten. Het certificaat zal direct uit de LDAP server worden verwijderd.

5.4.3.5 Certificaat downloaden

Om een certificaat als CERT bestand te downloaden gaat u naar de detail pagina van het desbetreffende certificaat (zie 5.4.3.2).

Links onderin klikt u op 'Download certificaat'. De inhoud van het binary veld zal nu als een CERT bestand naar uw computer gedownload worden. Uw webbrowser zal u vragen het bestand op te slaan.

5.4.3.6 Certificaat toevoegen

Om een certificaat toe te voegen aan de LDAP server gaat u naar de overzichts pagina en selecteert u het land waarvoor u een nieuw certificaat wilt toevoegen. Klik vervolgens op 'Toevoegen'. Een nieuwe pagina zal geopend worden.

Let op! Een certificaat zal slechts gepubliceerd worden in de LDAP server nadat u op 'Opslaan' klikt. Het certificaat zal pas beschikbaar worden voor de aangesloten systemen nadat de *Level of Approval* op *Approved* is gezet.

Om een certificaat te uploaden klikt u op 'Browse' en selecteert u het desbetreffende certificaat op uw computer. In het invoerveld ziet u het lokale pad staan van het juist geselecteerde certificaat. Klik 'Upload'.

Het certificaat zal nu worden gevalideerd. Als het certificaat niet bruikbaar is (bijv. onleesbaar of niet valide ASN1 structuur) zult u de mogelijkheid krijgen een ander certificaat te selecteren.

Als het certificaat bruikbaar is ziet u een nieuwe pagina met reeds ingevulde velden voor het aanmaken van een nieuw certificaat entry. Deze velden zijn overgenomen uit het certificaat en kunnen desgewenst worden aangepast. Voor een overzicht en omschrijving van de velden zie 5.5.1.

Naast de ingevulde velden is er ook een lijst met bevindingen opgenomen. Deze bevindingen komen voort uit uitgebreide validatie van het certificaat. Ondanks dat het certificaat een valide X509 ASN1 structuur bevat kunnen de bevindingen u doen besluiten het certificaat niet toe te voegen. Een bevinding hoeft geen fout in het certificaat aan te duiden. Een normale bevinding bij CSCA certificaten is bijvoorbeeld "Country Signing CA Certificate is self-signed".

Mocht u een verkeerd certificaat geupload hebben, dan kunt u op deze pagina direct een nieuw certificaat uploaden. Eventuele aanpassingen gemaakt in de velden zullen verloren gaan.

Let op dat de Common Name van een certificaat entry uniek dient te zijn. Als dit niet het geval is zal de entry niet worden toegevoegd.

Klik op 'Opslaan' om het certificaat te publiceren in de LDAP server. U keert weer terug naar het overzicht van certificaten. Het certificaat zal direct in de LDAP server gepubliceerd worden.

5.4.4 Module CRLs

Binnen deze module kunt u de CRLs opgenomen in de LDAP server per land beheren.

5.4.4.1 Overzicht

Klik in de navigatiebalk op 'CRLs' om naar de overzichtspagina van deze module te gaan.

Om alle CRLs van een land te bekijken selecteert u een land uit de lijst en klik op 'Selecteren'. Alle CRLs opgenomen in de LDAP server van het gekozen land zullen getoond worden.

5.4.4.2 CRL details

Om de details van een CRL te bekijken klikt u vanuit het CRL overzicht (zie 5.4.4.1) op de 'Details' knop uit de Actie kolom. Een nieuwe pagina met de details van het CRL zal getoond worden.

5.4.4.3 CRL entry bewerken

Om velden van een CRL entry te bewerken gaat u naar de detail pagina van het desbetreffende CRL (zie 5.4.4.2).

Alleen de *Level of Approval* en het *Source/Origin* veld kunnen worden aangepast. Om de aanpassingen op te slaan klikt u op 'Opslaan'. U keert weer terug naar het overzicht van CRLs. De wijzigingen worden direct van kracht.

5.4.4.4 CRL entry verwijderen

Om het CRL uit de LDAP server te verwijderen gaat u naar de detail pagina van het desbetreffende CRL (zie 5.4.4.2).

Rechts onderin klikt u op 'Verwijderen'. U keert weer terug naar het overzicht van CRLs. Het CRL zal direct uit de LDAP server worden verwijderd.

5.4.4.5 CRL downloaden

Om een CRL als CRL bestand te downloaden gaat u naar de detail pagina van het desbetreffende CRL (zie 5.4.4.2).

Links onderin klikt u op 'Download CRL'. De inhoud van het binary veld zal nu als een CRL bestand naar uw computer gedownload worden. Uw webbrowser zal u vragen het bestand op te slaan.

5.4.4.6 CRL toevoegen

Om een CRL toe te voegen aan de LDAP server gaat u naar de overzichtspagina en selecteert u het land waarvoor u een nieuwe CRL wilt toevoegen. Klik vervolgens op 'Toevoegen'. Een nieuwe pagina zal geopend worden.

Let op! Een CRL zal slechts gepubliceerd worden in de LDAP server nadat u op 'Opslaan' klikt.

Om een CRL te uploaden klikt u op 'Browse' en selecteert u de desbetreffende CRL op uw computer. In het invoerveld ziet u het lokale pad staan van het zojuist geselecteerde CRL. Klik 'Upload'.

De CRL zal nu worden gevalideerd. Als de CRL niet bruikbaar is (bijv. onleesbaar of niet valide ASN1 structuur) zult u de mogelijkheid krijgen een andere CRL te selecteren.

Als de CRL bruikbaar is ziet u een nieuwe pagina met reeds ingevulde velden voor het aanmaken van een nieuwe CRL entry. Deze velden zijn overgenomen uit de CRL en kunnen desgewenst worden aangepast. Voor een overzicht en omschrijving van de velden zie 5.5.2.

Naast de ingevulde velden is er ook een lijst met bevindingen opgenomen. Deze bevindingen komen voort uit uitgebreide validatie van de CRL. Ondanks dat de CRL een valide X509 ASN1 structuur bevat kunnen de

bevindingen u doen besluiten de CRL niet toe te voegen. Een bevinding heeft geen fout in de CRL aan te duiden. Een normale bevinding bij een lege CRL is bijvoorbeeld "RevokedCertificates is empty".

Mocht u een verkeerde CRL geupload hebben, dan kunt u op deze pagina direct een andere CRL uploaden. Eventuele aanpassingen gemaakt in de velden zullen verloren gaan.

Let op dat de Common Name van een CRL entry uniek dient te zijn. Als dit niet het geval is zal de entry niet worden toegevoegd.

Klik op 'Opslaan' om de CRL te publiceren in de LDAP server. U keert weer terug naar het overzicht van CRLs. De CRL zal direct in de LDAP server gepubliceerd worden.

5.4.5 Module CRL URLs

Binnen deze module kunt u de CRL URLs ten behoeve van automatische CRL update in de LDAP server beheeren. U dient eerst een land aan te maken alvorens u CRL URLs voor dat land kunt toevoegen.

5.4.5.1 Overzicht

Klik in de navigatiebalk op 'CRL URLs' om naar de overzichtspagina van deze module te gaan.

Om alle CRL URLs van een land te bekijken selecteert u een land uit de lijst en klik op 'Selecteren'. Alle CRLs URLs opgenomen in de LDAP server van het gekozen land zullen getoond worden.

5.4.5.2 CRL URL details

Om de details van een CRL URL te bekijken klikt u vanuit het CRL URLs overzicht (zie 5.4.5.1) op de 'Details' knop uit de Actie kolom. Een nieuwe pagina met de details van de CRL URL zal getoond worden.

Bovenaan de detail pagina vindt u de status van de laatste automatische update.

5.4.5.3 CRL URL entry bewerken

Een CRL URL entry kan niet worden bewerkt.

5.4.5.4 CRL URL entry verwijderen

Om de CRL URL uit de LDAP server te verwijderen gaat u naar de detail pagina van de desbetreffende CRL URL (zie 5.4.5.2).

Rechts onderin klikt u op 'Verwijderen'. U keert weer terug naar het overzicht van CRL URLs. Het CRL URL zal direct uit de LDAP server worden verwijderd.

5.4.5.5 CRL URL toevoegen

Om een CRL toe te voegen aan de LDAP server gaat u naar de overzichtspagina en selecteert u het land waarvoor u een nieuwe CRL URL wilt toevoegen. Klik vervolgens op 'Toevoegen'. Een nieuwe pagina zal geopend worden.

Voer in het veld URL de URL in van de CRL update locatie. De URL mag zowel een http // als https // URL zijn. Klik op 'Volgende'. Indien het een https // URL betreft wordt u gevraagd het TLS certificaat te accepteren alvorens door te gaan. Als u het certificaat vertrouwd klikt u op 'Volgende'. Dit certificaat zal voortaan gebruikt worden om de verbinding te valideren.

Let op! Een CRL URL zal slechts gepubliceerd worden in de LDAP server nadat u op 'Opslaan' klikt.

5.4.6 Module Master Lists

Binnen deze module kunt u de Master Lists opgenomen in de LDAP server beheren.

5.4.6.1 Overzicht

Klik in de navigatiebalk op 'MasterLists' om naar de overzichtspagina van deze module te gaan.

Alle Master Lists opgenomen in de LDAP server zullen getoond worden.

5.4.6.2 Master List details

Om de details van een Master List te bekijken klikt u vanuit het overzicht op de 'Details' knop uit de Actie kolom. Een nieuwe pagina met de details van de Master List zal getoond worden.

5.4.6.3 Master List entry bewerken

Om velden van een Master List entry te bewerken gaat nu naar de detail pagina van het desbetreffende Master List (zie 5.4.6.2).

Alleen de *Level of Approval*, *Source/Origin* en het *Department Number* veld kunnen worden aangepast. Om de aanpassingen op te slaan klikt u op 'Opslaan'. U keert weer terug naar het overzicht van certificaten. De wijzigingen worden direct van kracht.

5.4.6.4 Master List entry verwijderen

Om de Master List uit de LDAP server te verwijderen gaat u naar de detail pagina van de desbetreffende Master List (zie 5.4.6.2).

Rechts onderin klikt u op 'Verwijderen'. U keert weer terug naar het overzicht van certificaten. De Master List zal direct uit de LDAP server worden verwijderd.

5.4.6.5 Master List downloaden

Om een Master List als binary bestand te downloaden gaat u naar de detail pagina van de desbetreffende Master List (zie 5.4.6.2).

Links onderin klikt u op 'Download MasterList'. De inhoud van het binary veld zal nu als een bestand naar uw computer gedownload worden. Uw webbrowser zal u vragen het bestand op te slaan.

5.4.6.6 Master List importeren

Om een bestaande Master List te importeren in de LDAP server gaat u naar de overzichtspagina. Klik vervolgens op 'Importeren'. Een nieuwe pagina zal geopend worden.

Let op! Een Master List zal slechts gepubliceerd worden in de LDAP server nadat u op 'Opslaan' klikt. De Master List zal pas beschikbaar worden voor de aangesloten systemen nadat de *Level of Approval* op *Approved* is gezet en het *Department Number* op is gezet.

Om een Master List te uploaden klikt u op 'Browse' en selecteer de desbetreffende Master List op uw computer. In het invoerveld ziet u het lokale pad staan van de zojuist geselecteerde Master List. Klik 'Upload'.

De Master List zal nu worden gevalideerd. Als de Master List niet bruikbaar is (bijv. onleesbaar of niet valide ASN1 structuur) zult u de mogelijkheid krijgen een andere Master List te selecteren.

Let op dat de Common Name van een Master List entry uniek dient te zijn. Als dit niet het geval is zal de entry niet worden toegevoegd.

Klik op 'Opslaan' om de Master List te publiceren in de LDAP server. U keert weer terug naar het overzicht van Master Lists.

5.4.6.7 Master List samenstellen

Om een nieuwe Master List samen te stellen gaat u naar de overzichtspagina. Klik vervolgens op 'Samenstellen'. Een nieuwe pagina zal geopend worden.

Op deze pagina ziet u alle certificaten momenteel gepubliceerd in de LDAP server. Selecteer de certificaten die u op de aan te maken Master List wilt plaatsen.

U kunt een bestaande Master List in de LDAP server gebruiken als template voor de nieuwe Master List. Kies hiervoor een Master List in het 'Template' veld en klik op 'Selectie aanpassen'. De betreffende certificaten uit de Master List zullen nu geselecteerd worden.

Klik op 'Volgende' om de Master List te genereren. Een nieuwe pagina zal geopend worden.

Op deze nieuwe pagina vindt u de aangemaakte Master List in base 64 notatie.

B

B

Klik op 'Download MasterList' om de Master List naar uw computer te downloaden. Uw webbrowser zal u vragen het bestand op te slaan.

Wanneer u deze Master List voorzien heeft van een handtekening kunt u de Master List in de LDAP server importeren (zie 5.4.6.6).

5.4.7 Module landen

Binnen deze module kunt u de landen opgenomen in de LDAP server beheren. U dient eerst een land aan te maken alvorens u certificaten en CRLs voor dat land kunt toevoegen.

5.4.7.1 Overzicht

Klik in de navigatiebalk op 'Landen' om naar de overzichtspagina van deze module te gaan.

Alle landen die opgenomen zijn in de LDAP server komen voor in het overzicht.

5.4.7.2 Landen details

Om de details van een land te bekijken klikt u vanuit het landen overzicht (zie 5.4.7.1) op de 'Details' knop uit de Actie kolom. Een nieuwe pagina met de details van het land zal getoond worden.

5.4.7.3 Land entry bewerken

Om velden van een land entry te bewerken gaat nu naar de detail pagina van het desbetreffende land (zie 5.4.7.2).

Alle velden van deze entry kunnen aangepast worden behalve de Common Name. Om de aanpassingen op te slaan klikt u op 'Opslaan'. U keert weer terug naar het overzicht van landen. De wijzigingen worden direct van kracht.

5.4.7.4 Land entry verwijderen

Om een land uit de LDAP server te verwijderen gaat u naar de detail pagina van het desbetreffende land (zie 5.4.7.2).

Rechts onderin klikt u op 'Verwijderen'. U keert weer terug naar het overzicht van landen. Het land zal direct uit de LDAP server worden verwijderd. Let op! Alle eventuele gekoppelde certificaten en CRLs zullen direct worden verwijderd.

5.4.7.5 Land toevoegen

Om een land toe te voegen aan de LDAP server gaat u naar de overzichtspagina (zie 5.4.7.1). Klik vervolgens op 'Toevoegen'. Een nieuwe pagina zal geopend worden.

Voer de landcode en een omschrijving (volledige naam) in voor het land dat u wilt toevoegen. Voor een overzicht en omschrijving van de velden zie 5.5.5.

Klik op 'Opslaan' om de het land toe te voegen aan de LDAP server. U kunt nu certificaten en CRLs toevoegen aan het zojuist aangemaakte land.

5.4.8 Module gebruikers

Binnen deze module kunt u de gebruikers die toegang hebben tot de LDAP server van de NPKD beheren.

5.4.8.1 Overzicht

Klik in de navigatiebalk op 'Gebruikers' om naar de overzichtspagina van deze module te gaan

Alle gebruikers die toegang hebben tot de LDAP server komen voor in deze lijst

5.4.8.2 Gebruikers details

Om de details van een gebruiker te bekijken klikt u vanuit het gebruikersoverzicht (zie 5.4.8.1) op de 'Details' knop uit de Actie kolom. Een nieuwe pagina met de details van de gebruiker zal getoond worden.

5.4.8.3 Gebruiker entry bewerken

Om velden van een entry te bewerken gaat nu naar de detail pagina van de desbetreffende gebruiker (zie 5.4.8.2).

Alle velden van deze entry kunnen aangepast worden behalve de Common Name. Om de aanpassingen op te slaan klikt u op 'Opslaan'. U keert weer terug naar het overzicht van gebruikers. De wijzigingen worden direct van kracht.

5.4.8.4 Gebruiker entry verwijderen

Om een gebruiker uit de LDAP server te verwijderen gaat u naar de detail pagina van de desbetreffende gebruiker (zie 5.4.8.2).

Rechts onderin klikt u op 'Verwijderen'. U keert weer terug naar het overzicht van gebruikers. De gebruiker zal direct uit de LDAP server worden verwijderd en zal vanaf dat moment geen toegang meer hebben tot de LDAP server.

5.4.8.5 Gebruiker toevoegen

Om een gebruiker toe te voegen aan de LDAP server gaat u naar de overzichtspagina (zie 5.4.8.1). Klik vervolgens op 'Toevoegen'. Een nieuwe pagina zal geopend worden.

Voor de gegevens in van de gebruiker die u wilt toevoegen. Voor een overzicht en omschrijving van de velden zie 5.5.6.

Klik op 'Opslaan' om de gebruiker toe te voegen aan de LDAP server. De gebruiker kan vanaf nu toegang krijgen tot de LDAP server.

5.4.9 Module Notificaties

Binnen deze module kunt u notificaties versuren naar de aangesloten NSPOC. De NSPOC zal na het ontvangen van een notificatie de bijbehorende acties ondernemen.

Selecteer de type notificaties die u wilt versturen en klik op 'Verstuur notificaties'.

De notificaties zullen direct worden verstuurd. De status zal worden getoond in uw webbrowser.

5.5 Referenties LDAP entries

5.5.1 Referenties Certificaat

Veld webapplicatie	Veld LDAP	Omschrijving
Common Name	cn	Common Name – naam van certificaat
Serial Number	sn	Serial Number
Level of Approval	levelOfApproval	Goedkeuring t b.v. zichtbaarheid voor gebruikers (0 = onzichtbaar, 1 = zichtbaar).
Publish date	publishDate	Datum van publicatie in LDAP
Registration date	registrationDate	Datum van registratie in LDAP
Fingerprint	fingerprint	SHA1 fingerprint van het certificaat veld
Subject Key Identifier	subjectKeyIdentifier	Subject Key Identifier uit het certificaat
Certificate	certificate	Binary veld bevat het certificaat.
Source/Origin	Source	Tekstuele beschrijving van herkomst

5.5.2 Referenties CRL

Veld webapplicatie	Veld LDAP	Omschrijving
Common Name	cn	Common Name – naam van CRL
Issuer	issuer	Issuer van CRL
Level of Approval	levelOfApproval	Goedkeuring t b v. zichtbaarheid voor gebruikers (0 = onzichtbaar, 1 = zichtbaar).
CRL Number	crlNumber	Crl number
Publish date	publishDate	Datum van publicatie in LDAP
This update	thisUpdate	thisUpdate veld uit de CRL
Next update	nextUpdate	nextUpdate veld uit de CRL
Fingerprint	fingerprint	SHA1 fingerprint van het cri veld.
CRL encoded	crl	Binary veld bevat de CRL.
Registration date	registrationDate	Datum van registratie in LDAP
Source/Origin	Source	Tekstuele beschrijving van herkomst

5.5.3 Referenties CRL URL

Veld webapplicatie	Veld LDAP	Omschrijving
Common name	cn	Common name van URL
Update URL	updateUrl	URL van CRL update locatie
Description	description	Omschrijving
Trusted Certificate	trustedCertificate	X.509 certificaat voor https verbindingen
Registration date	registrationDate	Datum van registratie in LDAP

5.5.4 Referenties Master List

Veld webapplicatie	Veld LDAP	Omschrijving
Common Name	cn	Common name van Master List entry
Fingerprint	fingerprint	SHA1 fingerprint van de master list veld.
Source/Origin	Source	Tekstuele beschrijving van herkomst
Registration date	registrationDate	Datum van registratie in LDAP
Publish date	publishDate	Datum van publicatie in LDAP
Level of Approval	levelOfApproval	Goedkeuring t b.v. zichtbaarheid voor gebruikers (0 = onzichtbaar, 1 = zichtbaar).
Department Number	departmentNumber	De master list wordt uitgeleverd aan aangesloten systemen met hetzelfde Department Number.

5.5.5 Referenties Land

Veld webapplicatie	Veld LDAP	Omschrijving
Country	c	Tweecijferige country code
Description	description	Omschrijving (volledige naam van het land)

5.5.6 Referenties Gebruiker

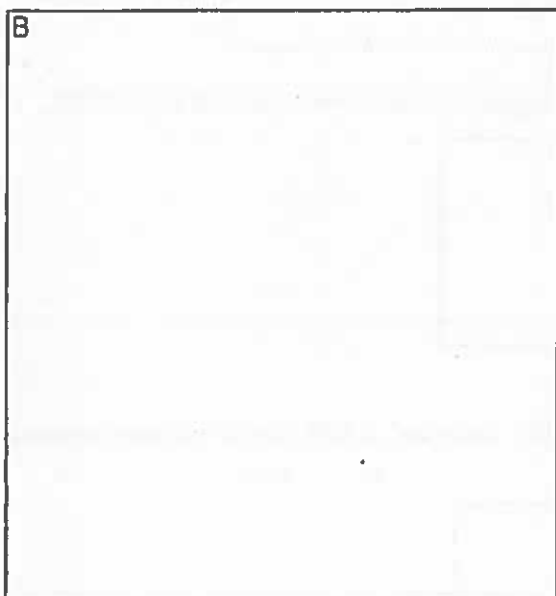
Veld webapplicatie	Veld LDAP	Omschrijving
CN	cn	Common name – naam van gebruiker
SN	sn	Serial Number
Department Number	departmenNumber	Mogelijkheid tot categoriseren van gebruikers, momenteel bestaat alleen de categorie IS voor Inspectiesystemen.
Given Name	givenName	Deze naam dient overeen te komen met de Common Name uit het IS TLS certificaat. Op basis van dit veld worden clients geautoriseerd.

Annex A

A.1 TLS PKI

De beveiliging van de NPKD is zo ingesteld dat connecties alleen worden toegestaan als de client (het inspectiesysteem) zich kan autoriseren met een certificaat dat uitgegeven is onder de NL-SPOC-CA. De NPKD is in deze afhankelijk voor de werking van de beveiliging. Alle certificaten dienen een unieke Subject CN te bevallen. B De naamgeving binnen de NL-SPOC-CA moet zodanig ingericht worden dat alle Subject CN's uniek zijn.

A.1.1 Overzicht



A.1.2 Omschrijving

Zoals te zien in het overzicht is de NL-SPOC-CA het enige systeem dat certificaten uit kan geven. Alle andere entiteiten als de NL-NPKD en de Inspectie Systemen dienen een certificaat te hebben met bijbehorende private key om onderlinge communicatie mogelijk te maken.

De NL-NPKD zal het NL-SPOC-CA certificaat vertrouwen. Alle entiteiten die een TLS connectie opbouwen met een certificaat (met private key) uitgegeven door de NL-SPOC-CA zullen geaccepteerd worden. Echter, om gegevens uit de NL-NPKD te kunnen opvragen / downloaden zal de Subject CN uit het entiteit certificaat gecontroleerd worden. De NL-NPKD registreert deze gegevens. Entiteiten waarvan de Subject CN als geaccepteerd staat binnen de NL-NPKD zullen in staat zijn gegevens te opvragen / downloaden.

Voor de NPKD is het dus van groot belang dat de entiteiten een uniek Subject CN in hun client certificaat hebben.

In NL-NPKD ontwikkel fase 1,2 en 3 zal er GEEN CRL controle plaatsvinden. Entiteiten die op de NL-SPOC-CA CRL terecht komen dienen handmatig verwijderd te worden. Het blijft voor deze entiteiten echter wel mogelijk om een TLS verbinding op te zetten. Dit komt door een beperking van OpenDS.

In NL-NPKD ontwikkel fase 4 zal de CRL controle als "nice to have" opgenomen worden.

A.2 Registratie Inspectiesysteem

Voordat een inspectiesysteem toegang kan krijgen tot de NPKD moet het inspectiesysteem zich registreren bij de NPKD Admin. Voor succesvolle registratie zijn onderstaande gegevens benodigd

A.2.1 Benodigde gegevens

Om zich te registreren heeft een entiteit de volgende gegevens nodig

- B
-
-
-

Na registratie heeft een entiteit de volgende gegevens nodig om succesvol te verbinden met de NL-NPKD.

- B
-
-
-

A.3 Interface Specificatie

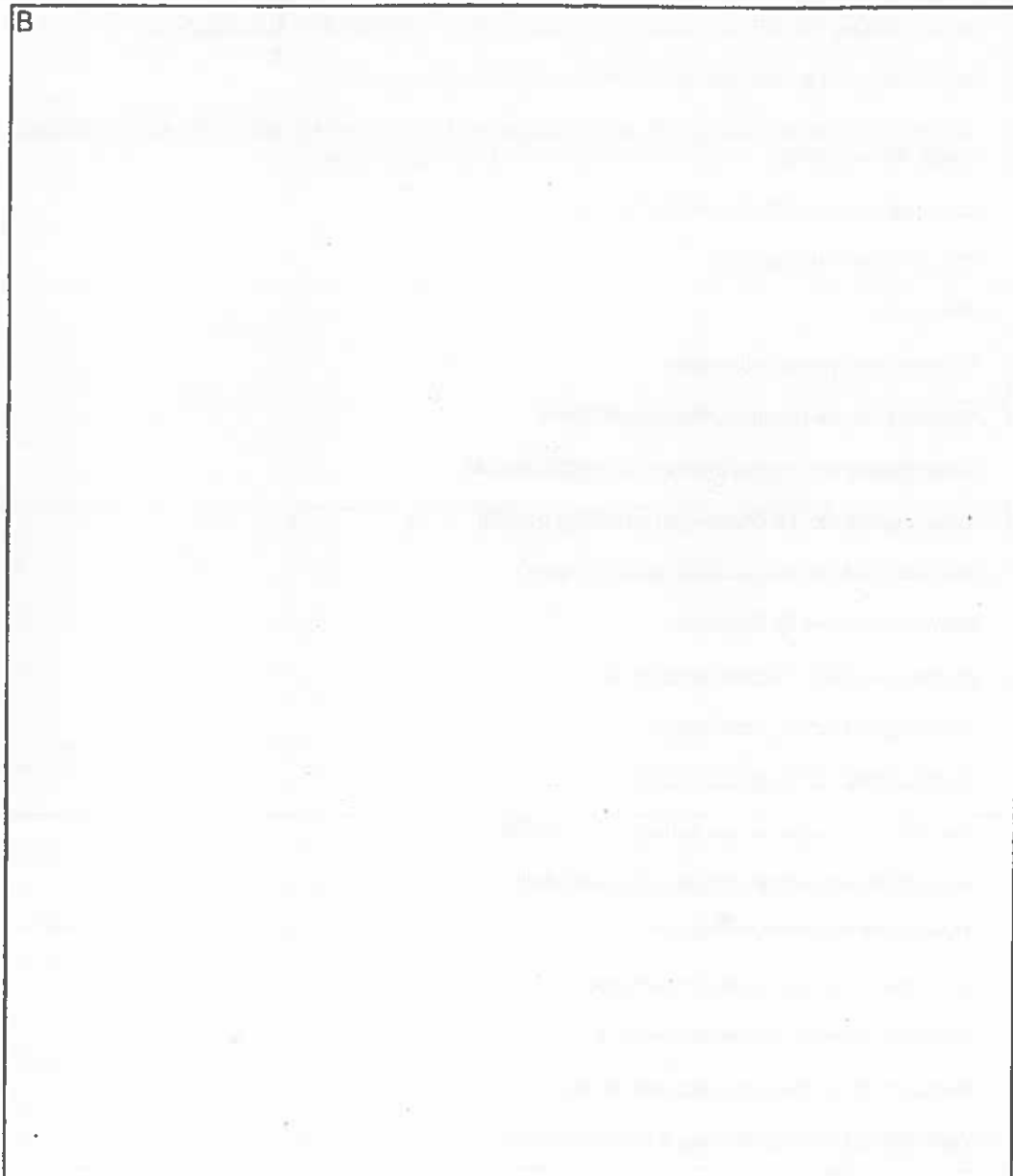
Om initieel een verbinding te kunnen maken met de LDAP server van de NPKD zijn de volgende gegevens benodigd

- B
-
-
-

De LDAP server ondersteunt de volgende commando's uit het LDAPv3 protocol

- StartTLS (verplicht)
Deze operatie is verplicht alvorens andere operaties uit te voeren, de server en de client bieden beiden hun TLS-certificaat aan. Na deze operatie is de verbinding beveiligd d.m.v. TLS
- Bind, verplicht
Deze operatie is verplicht alvorens andere operaties uit te voeren. Met deze administratieve operatie wordt bepaald voor welke andere operaties de client geautoriseerd is om uit te kunnen voeren. Tevens wordt bepaald voor welke data de client geautoriseerd is om op te vragen.
- Search
Met de search operatie kan de client data opvragen uit de LDAP.
- Abandon
De client annuleert een uitstaande operatie
- Unbind
Afmelden bij de server.

Om correcte Search commando's te kunnen uitvoeren is kennis van de LDAP hiërarchie vereist. Hieronder staat een representatie (LDIF) van de structuur van de LDAP server. De bovenste twee entries zijn de enige vaste entries in de server. De overige entries zijn dynamisch, afhankelijk van de toegevoegde landen, certificaten en CRLs.



A.4 Certificaat Validatie

Bij het toevoegen van een CSCA en DS certificaat aan de NPKD worden de volgende controle en validatiestappen uitgevoerd. Op basis van deze controle zal een certificaat niet automatisch worden afgewezen. Bevindingen worden gerapporteerd aan de NPKD-Admin.

- Is het certificaat parsable als een correct X 509 certificaat (DER/ASN1) - BouncyCastle
- Komt de KeyUsage overeen met ICAO Doc 9303 Part 1 Volume 2 A 1.2
- Op basis van het keyCertSign uit de KeyUsage word bepaald of het een CSCA of DS certificaat betreft. Als keyCertSign = true dan gaat het om een CSCA certificaat
- Aanwezigheid van signature algorithm OID.
- Aanwezigheid van signature.
- Version = 3.
- Aanwezigheid van serial number.
- Aanwezigheid van Issuer Distinghuised Name.
- Aanwezigheid van begindatum van de validity periode.
- Aanwezigheid van einddatum van de validity periode.
- Aanwezigheid van Subject Distinghuised Name.
- Aanwezigheid van de Public Key.
- Aanwezigheid van SubjectPublicKeyInfo.
- Aanwezigheid van IssuerUniqueID.
- Aanwezigheid van SubjectUniqueID.
- Voor DS, aanwezigheid van AuthorityKeyIdentifier.
- Voor CSCA, aanwezigheid SubjectKeyIdentifier.
- Afwezigheid van PolicyMappings.
- Afwezigheid van SubjectAlternativeName.
- Afwezigheid van IssuerAlternativeName.
- Afwezigheid van SubjectDirectoryAttributes.
- Voor CSCA, aanwezigheid van BasicConstraints.
- Voor DS, afwezigheid van BasicConstraints.
- Afwezigheid van NameConstraints.
- Afwezigheid van PolicyConstraints.
- Afwezigheid van ExtendedKeyUsage.
- Afwezigheid van InhibitAnyPolicy.

- Afwezigheid van FreshestCRL.
- Afwezigheid van PrivateInternetExtensions.
- Aanwezigheid van keyidentificer uit AuthorityKeyIdentifier.
- Aanwezigheid van keyidentificer uit SubjectKeyIdentifier.
- Voor CSCA, ca = TRUE (BasicConstraints).
- Voor CSCA, 0 <= PathLenConstraint <= 1 (BasicConstraints)
- Voor CSCA, controle handtekening (self signed)
- Controle op onbekende extension OIDs.

A.5 CRL Validatie

Bij het toevoegen van een CRL aan de NPKD worden de volgende controle en validatiestappen uitgevoerd. Op basis van deze controle zal een CRL niet automatisch worden afgewezen. Bevindingen worden gerapporteerd aan de NPKD-Admin.

- Is de CRL parsable als een correcte X.509 CRL (DER/ASN1) - BouncyCastle.
- Aanwezigheid SignatureAlgorithm.
- Aanwezigheid SignatureValue.
- CRL version = 2.
- Aanwezigheid Issuer.
- Aanwezigheid ThisUpdate.
- Aanwezigheid NextUpdate.
- Aanwezigheid RevokedCertificates
- Aanwezigheid AuthorityKeyIdentifier
- Aanwezigheid CRLNumber
- Afwezigheid IssuerAltName
- Afwezigheid DeltaCRLIndicator
- Afwezigheid IssuingDistributionPoint
- Afwezigheid FreshestCRL
- Afwezigheid CRLReason
- Afwezigheid HoldInstructionCode
- Afwezigheid InvalidityDate
- Afwezigheid CertificateIssuer
- Controle op onbekende extension OIDs.

