Commando Materieel en IT
Ministerie van Defensie

Certification Practice Statement

for the NL-MoD card (Nl-MoD card) Generation 3 (G3)

Certification Authority

Signature Page

Defence Security Authority A009 *Verantwoordelijkheden en bevoegdheden Defensiepas* (Responsibilities and authorities Ministry of Defence Card) places Trust Service Provider (TSP) responsibility with the Principal Directorate of Operational Management and, in the context of this responsibility, authorises the Director of Joint IT Command (D-JIVC). The Director of Joint IT Command has placed TSP responsibility to the TSP manager within its staff organisation.

The TSP manager agrees to the content of the Certification Practice Statement (CPS) for the Netherlands Ministry of Defence Card (Nl-MoD card) services.

R. (Remko) van Oostveen, BSc
TSP-manager
Netherlands Ministry of Defence

Signature:

Remko van Oostveen

Digitally signed by Remko van Oostveen
Date: 2024.08.30 13:32:31 +02'00'

Status	Definitief
Version	3.1.8
Date	29-08-2024

Contents

Version Control

Version	Date	Reason for change
0.1	10/05/2007	Initial version of the Ministry of Defence Card project
0.2	14/09/2007	Review by B.M.P. Giesbers, MSIT Review by E.E. de Vries (Chapter 6) BASTION additions incorporated
0.9	01/10/2007	Statement of applicability draft version
0.91	15/10/2007	Draft altered on the basis of findings of external auditors
0.92	28/10/2007	Draft altered on the basis of comments of the Directorate of Legal Affairs (DJZ)
0.93	12/11/2007	Draft altered on the basis of Doc11 findings
1.0	15/11/2007	Final version of CPS
1.1		Object identifier (OID) included; altered on the basis of comments of the steering group
1.2	08/04/2008	Altered on the basis of the Secretary General instructions on Roles and Responsibilities regarding Public Key Infrastructure Certification Services
1.3	02/08/2010	Additional measures in relation to guaranteeing the segregation of duties – finding of the audit of July 2010
1.4	24/11/2010	ECP2 realisation – SHA2 and RSA2048
1.5	27/12/2010	Review of information management in terms of data protection
1.6	07/02/2011	Incorporation of the findings of the certification audit of 2011
2.0	15/02/2011	Validation by KPMG; final version
2.1	04/10/2011	Alterations for the cross-certification
2.2	15/11/2011	Incorporation of comments on the alterations for the cross-certification
2.3	01/04/2012	Incorporation of the findings of the certification audit of 2012
2.4	15/08/2012	Alteration in connection with PIN letter to home address
2.5c	15/10/2013	Alteration of Appendix 2 and various links The CPS must be further altered and finalised after the reorganisation
2.6c	08/05/2014	Alterations because of the new Defence IV organisation; Joint IT Command
2.7	23/11/2016	Adaptation to the new organisation Adaptation to the new standards Adaptation to the G2 hierarchy
2.7.1	05/12/2016	Minor alteration in relation to service life of certificates for the migration to G3
2.7.2	09/01/2017	Reference to the Internet Publication System (IPS) added
2.8	13/02/2017	Findings of the audit of January 2017 were processed
2.8.1	06/07/2017	Minor changes to text
2.8.2	14/12/2017	Adaptations with regard to relocation of TSP responsibility
2.8.2a	19/02/2018	Minor textual changes and corrections. Consistency applied regarding English/Dutch version.
2.9	20/09/2018	Major changes in Key Escrow
2.9.1	24/09/2018	Minor changes
2.9.2	01-10-2018	Minor changes
2.9.3	11-10-2018	Minor changes

3.0	01-07-2019	G3 update(s) and changes following from CAP/ PAP
3.1	23-07-2019	Minor changes, update of department name.
3.1.1	25-09-2019	Minor changes following CAP/PAP
3.1.2	17-10-2019	Corrections
3.1.3	1-10-2020	6.4.2 updated CA to SDD. Several chapters: Validation through electronic means Several chapters: Corrections and/or explanatory text
3.1.4	1-2-2021	Changes following audit : - reconfiguring CPS according rfc3647 More details in stipulation about: - NL-MoD as owner and sole subscriber for NL-MoD employees (holders of the NL-MoD Card) and the overall liability for NL-MoD. - Use of certificates in combination with sensitive information - Identity validation and certificate provisioning
3.1.5	3-10-2022	Updates triggered by ETSI changes and PKIo change. Remote vetting services will not be introduced (chapter 3).
3.1.6	13-01-2023	Added frequency of monitoring review in 6.5.1 Updated 5.4.3 retention to 24 months. Minor corrections.
3.1.7	06-10-2023	Updated the text regarding the expiration of certificates related to the Certificate Revocation List (CRL). Update the text regarding the expiration of certificates related to CRL. Minor corrections.
3.1.8	27-08-2024	Editoral changes and discontinuation SMIME.

1 Introduction

The Netherlands Ministry of Defence (NL-MoD) has created an internal Trust Service Provider (TSP) bound to all legislation of Trust Service Provisioning within Europe (eIDAS) and the Netherlands (Telecomwet). NL-MoD as owner of the internal TSP is also the only subscriber of the internal TSP. NL-MoD has ordered the internal TSP to provide legally acknowledgable PKI certificates to employees, hired personnel and foreign military and civil personnel. All end-users are legally bound to the sole subscriber NL-MoD by contracts and/or by treaties. Use of NL-MoD means (including certificates where applicable) is mandatory for all NL-MoD-personnel (end-users) and NL-MoD personnel are bound legally to use NL-MoD means (including the personalized certificates) for NL-MoD purposes only. Every other use is legally prohibited. Because of this, NL-MoD is liable from the perspective of owner of the TSP ánd NL-MoD is liable for all permitted use of the personalized certificates issued by NL-MoD's TSP to all end-users.

The NL-MoD makes an identity card (*Identiteitsbewijs Krijgsmacht*) available to its employees that is mandatory (as mentioned before). This identity card contains certificates that make it possible for employees to use digital services. For this purpose, the NL-MoD complies with the standards set out in the schedule of requirements that applies to the Dutch government's public key infrastructure (PKI-O), of which Logius is the Policy Authority (PA). As mentioned before, NL-MoD has its own Trust Service Provider (TSP) that issues these certificates and guarantees their reliability. Ultimate TSP responsibility rests with the following organisation: Command Materiel and IT, Joint IT Command JIVC.

1.1 Overview

Every end user is identified and is subject to a background check before a request for a NL-MoD card can be accepted. During the application process, the identity of the end user of the NL-MoD card is checked again. For this, the end user has to report in person.All information (including the end users NL-MoD emailadress) is entered by automated means. Specific information (like given name, surname, etc) is checked additionally according to eIDAS and given policies by PKI-O. The NL-MoD Card contains proof of identity in the form of electronic certificates. In this document, the "NL-MoD card" means the Netherlands Ministry of Defence Card (NL-MoD card) in its entirety, i.e. both the physical and electronic components of the card.[1]

The TSP issues certificates that enable an end user of the NL-MoD card to identify himself/herself ("authenticity certificate"), place an electronic signature that is recognised by law ("qualified signature (non-repudiation) certificate") and encrypt data ("confidentiality certificate"). Type 1 and Type 2 NL-MoD cards have all three types of certificates. Type 1 cards are intended for Dutch military and civilian personnel, while Type 2 cards are intended for foreign military and civilian personnel and temporary personnel who have been hired from outside the NL-MoD. The software (application) installed to perform activities determines which functions can actually be used.

- Authentication and non-repudiation certificates are allowed to be used for all sensitivity levels for integrity, authentication and non-repudiation in all networks.
- Confidentiality certificates are allowed for protection of information classified up to Netherlands Restricted across an unsecure network (including international equivalents).
- Confidentiality certificates are allowed for Community of Information separation up to Netherlands Secret information within an adequate protected network (including international equivalents).

[1] Only Type 1 and Type 2 NL-MoD cards have certificates.

The TSP is a participant in the PKI-O. The PKI-O is a system of agreements that makes general and large-scale use of legally valid electronic signatures possible and facilitates remote identification and confidential communication. Radiocommunications Agency Netherlands (Rijksinspectie Digitale Infrastructuur) monitors compliance with the regulations that the TSP must observe in the context of legally valid electronic signatures. Moreover, the TSP is a certified service provider. This certification is confirmed each year on the basis of an audit carried out by an independent, external auditor.

Currently Generation 3 of PKI-O is operational.

This CPS version is applicable for the G3 NL-MOD implementation of PKI-O.

1.2 Document Name and Identification

The TSP's Certification Practice Statement (CPS) describes the way in which the certification services are actually performed.

1.2.1 Purpose of the Certification Practice Statement

The CPS describes the processes, procedures and control measures in place for applying for, producing, providing, managing and revoking a NL-MoD card with certificates.

This CPS underpins the trust that holders of NL-MoD cards, relying parties and other parties involved may place in the services provided by the TSP.

1.2.2 Relationship between the Certificate Policy and the CPS

The TSP is a participant in the PKI-O, which means that the TSP must comply with PKI-O regulations. These regulations are set out in the Certificate Policies (CPs) of the PKI-O. For the NL-MoD Card, the Organisation Person Domain CP (G3 hierarchy) is of importance.

Like the CPs of the PKI-O, this CPS follows the layout of Request for Comments (RfC) 3647. The "headings" of the aforementioned RfC have been included in this CPS for the sake of completeness. If headings are not relevant for this CPS, the following sentence is included: "No stipulation."

This CPS describes the way in which the requirements set out in the Organisation Person Domain CP (G3 hierarchy) have been met.

The Organisation Person Domain CP (G3 hierarchy) contains regulations for three types of certificates. The regulations for each type of certificate can be identified by means of the object identifiers (OIDs). Within the NL-MoD, we use the following identifiers.

Certificate type	Object identifier (OID)	Description
Authenticity	2.16.528.1.1003.1.2.5.1	OID of the PKI-O Certificate Policy for authenticity certificates in the Organisation Person domain.
Signature	2.16.528.1.1003.1.2.5.2	OID of the PKI-O Certificate Policy for signature certificates in the Organisation Person domain.
Confidentiality	2.16.528.1.1003.1.2.5.3	OID of the PKI-O Certificate Policy for confidentiality certificates in the Organisation Person domain.

Table 1. G3 hierarchy – Organisation Person Domain CP OIDs

1.2.3 References to this CPS

This CPS is available on the TSP's website.

Internet address (link)	https://cps.ca.pkidefensie.nl/mindef-ca-cps/
OID	2.16.528.1.1003.1.3.2.6

Table 2. References to this CPS

1.3 PKI Participants

The TSP of the Netherlands Ministry of Defence is organised within the ministry in accordance with the Defence Security Authority A009 and the Ministry of Defence Control Model (*Besturingsmodel Defensie*),[ref 2] as well as the policy making, planning and budgeting cycle included in that model.

The NL-MoD TSP is owned by NL-MoD.

The NL-MoD as a whole is the sole customer (sole subscriber) of the NL-MoD TSP.

It is not possible to acquire services from the NL MoD TSP.
The supplier of TSP services and the Registration Authority (RA) play important roles in the provision of certification services. On the user side are holders of NL-MoD cards and the relying parties. The respective roles of these parties are explained below.

1.3.1 Certification authorities

The TSP produces and publishes certificates that have been applied for based on a request of the RA. After the TSP has received a request for the revocation of a certificate, the TSP revokes the certificate and makes this revocation known by means of the Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP). Within the NL-MoD, COMMIT/JIVC TSP.

There is strict segregation between the three roles:
- ownership rests with the COMMIT director;
- commissioning rests with the JIVC director;
- TSP rests with Staff JIVC (dedicated officer TSP-manager).

In this context, TSP uses the services of the following subcontractors: Atos (with KPN as co-contractor) and IDEMIA.

1.3.2 Registration Authorities

The RA function is delegated to the operational branches of the NL-MoD according to General Directions A009. RA duties are performed by NL-MoD employees. The NL-MoD TSP is accountable for auditing, correction and sanctioning the RA's.

The RA processes applications for certificates. The RA collects the identifying data elements and checks and records these data. When necessary, the RA instructs the TSP to produce NL-MoD cards and publish certificates.

1.3.3 Subscribers

The NL-MoD Card is the carrier of the certificates and keys ("electronic proof of identity"). By definition, a certificate holder is therefore also a holder of a NL-MoD card (the end user). In this CPS, preference has been given to the term holder of a NL-MoD Card.

In terms of the PKI-O, a holder of a NL-MoD card is the person who is defined in the certificate as the holder of the private keys that are linked to the public keys included in the certificates.

The holders of the NL-MoD card are users of the certificates.
All users have been vetted on identity and trustworthiness before entering the NL-MoD and their personnel data (including an employee number (HR-number)) has been added in the NL-MoD personnel system. These users are:
- NL-MoD employees;
- NL MoD hired personnel;
- NL-MoD connected foreign military personnel bound by treaties;
- personnel of partners bound by contracts.

1.3.4 Relying parties

A relying party is any natural person or legal entity who or that is a recipient of a certificate issued by the TSP and who or that acts on the basis of trust in that certificate.

1.3.5 Other participants

No stipulation.

1.4 Certificate Usage

Private keys issued by the TSP are always and exclusively used by holders of NL-MoD cards who are acting on behalf of the NL-MoD. The foregoing therefore expressly excludes private use of the private keys.

1.4.1 Appropriate certificate uses

The TSP issues three types of certificates.

Type of certificate	Purpose
Authenticity certificate	This certificate is to be used to identify and authenticate a holder of a Ministry of Defence Card.
Signature certificate	This certificate is to be used to verify an electronic signature placed by a holder of a Ministry of Defence Card.
Confidentiality certificate	This certificate is to be used to encrypt data when communicating with a holder of a Ministry of Defence Card.

Table 3. Use of a certificate

The three types of certificates may only be used for the purpose stated in Table 3. Use of a certificate.

1.4.2 Prohibited certificate uses

Only the appropriate use of a certificate as described in Section 1.4.1 is permitted. For example the signature certificate may only be used to verify an electronic signature. Using the NL-MoD card for private transactions is prohibited.
The confidentiality certificate may not be used to store data in encrypted form. It may only be used to encrypt data when communicating with a holder of a NL-MoD Card.

1.5 Policy Administration

In accordance with the Ministry of Defence Control Model,[ref 2] JIVC is tasked with TSP management. TSP responsibility rests with JIVC staff.[ref 3].

1.5.1 Organization administering the document

The CPS is issued under the responsibility of the TSP.

1.5.2 Contact person

The contact details provided below can be used to obtain information about this CPS or the services of the TSP. Comments on this document can be directed to the same address.
Email address: defensiepas.ca@mindef.nl

1.5.3 Person determining CPS suitability for the policy

Assessment of the conformity of this CPS with the Organisation Person domain (G3 hierarchy) is part of the certification of the TSP based on an audit carried out by an independent auditor.
The TSP's statement of conformity is available on the TSP's website.

1.5.4 CPS approval procedures

Changes to the CPS are approved by the TSP manager, after consultation with the relevant stakeholders.

1.6 Definitions and Acronyms

See Appendix 1. *Abbreviations* for definitions of the abbreviations/acronyms.

2 Publication and Repository Responsibilities

The TSP publishes information at a number of locations on the NL-MoD intranet and on the internet.

2.1 Repositories

In principle, there are five locations: the general website of the NL-MoD on the intranet and on the internet, the Corporate Directory of the NL-MoD, a Ministry of Defence Publication System (DPS) and an Internet Publication System.

The NL-MoD website on the intranet, the Ministry of Defence Publication System and the Corporate Directory are within the Ministry of Defence domain and are only accessible to employees of the NL-MoD. Because of the public nature of the TSP, information is also provided on the internet. This information can be accessed through the Internet Publication System. The NL-MoD TSP publishes the compliance statement of the certifying authority on the internet site.

For the Organisation Person Domain CP (G3 hierarchy), see the PKI-O website at Logius.

2.2 Publication of certification information

The types of information and locations on the intranet and internet are stated in the table below.

G3 Information	INTERNET/INTRANET URLs
CPS:	
Ministry of Defence CA – G3	https://cps.ca.pkidefensie.nl/mindef-ca-cps/
CA Certificates:	
DomOrganisatiePersoonCA - G3	http://cert.pkioverheid.nl/DomOrganisatiePersoonCA-G3.cer
Ministry of Defence Card CA – G3	http://certs.ca.pkidefensie.nl/mindef-ca-3.cer
Certificate Revocation Lists:	
DomOrganisatiePersoonLatestCRL-G3	http://crl.pkioverheid.nl/DomOrganisatiePersoonLatestCRL-G3.crl
Ministry of Defence Card CA – G3	http://crls.ca.pkidefensie.nl/mindef-ca-3.crl
OCSP Online Certificate Status	http://ocsp.ca.pkidefensie.nl

Table 4. TSP information locations

2.3 Time or frequency of publication

The published TSP information is, publicly and internationally, available 24 hours a day, seven days a week. Measures are in place to ensure that this service is restored within 24 hours in the event of planned maintenance or malfunctions.

The availability and frequency of publication of the certificates and the certificate status information (CRL and OCSP) is described in Chapter 4 of this CPS.

2.4 Access controls on repositories

The TSP information referred to in Section 2.2 as published on the intranet is public in nature and freely accessible.

3 Identification and Authentication

This chapter describes the way in which certificate applicants are identified and authenticated during the registration procedure and the criteria that apply with respect to naming.

3.1 Naming

All certificates issued by the TSP include the name and the employee number of the holder of the NL-MoD Card.

3.1.1 Types of names

The name and employee number of the holder of the NL-MoD card is always and exclusively taken from the NL-MoD personnel system (the source system). The name of the holder of the NL-MoD card consists of characters from the West European series. When the name of the holder of the NL-MoD Card contains diacritics not supported bij the NL-MoD's personnel system, the specific character without the diacritic will be used. The employee number in the certificate will guarantee uniqueness of the holder of the NL-MoD Card. An explanation of the further content of the certificates is included in Chapter 7.

3.1.2 Need for names to be meaningful

No stipulation.

3.1.3 Anonymity or pseudonymity of subscribers

Anonymity or the use of a pseudonym is not supported.

3.1.4 Rules for interpreting various name forms

Names of persons included in the Certificate meet the requirements as stated in the Program of Requirements[2].
All names are, in principle, exactly copied from the presented identification documents. However, the name data may contain special characters that are not part of the standard character set conforming to ISO8859-1 (Latin-1). If the name contains special characters which are not part of this character set, MoD will perform a transition. MoD reserves the right to change the requested name upon registration if this is technically necessary.

3.1.5 Uniqueness of names

The TSP guarantees that the name of the holder of the NL-MoD card in the certificate is unique. This means that the distinctive name used in a certificate that has been issued can never be assigned to another holder of a NL-MoD Card. Defense has chosen not to include titles of nobility on the card and in the certificates, unless the applicant explicitly requests them.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial Identity Validation

The identity of the holder of the NL-MoD card is initially validated by means of the processes described in the subsections of Section 3.2.

[2] https://cp.pkioverheid.nl

3.2.1 Method to prove possession of private key

The key pairs are generated in a cryptographic module and loaded onto the smart card as part of the personalisation process. These steps are completed in a controlled and restricted area. The private key cannot leave the smart card. The holder of the NL-MoD card is not involved in this process and does not have to prove that he/she possesses the private key that belongs to the public key in the certificate.

3.2.2 Authentication of organization identity

The personal and organisational data for NL-MoD cards (Types 1 and 2) are always and exclusively taken from the NL-MoD personnel system (the source system). In the case of NL-MoD cards, it is not possible to submit a valid application for a certificate by manually entering data outside the NL-MoD personnel system. Because the NL-MoD personnel system is the only source system for certificate applications, it is guaranteed that the holder of a NL-MoD card has a professional link with the NL-MoD.

3.2.3 Authentication of individual identity

Authentication of personal identity is being performed before and during issuing of certificates.

3.2.3.1 Initial authentication of personal identity of all end-users is being performed before the issuing of certificates during:

- the hiring process which follows (legal) processes and that results in entering personal data into the NL-MoD's personnel system (including submitting an employee number). The processes includes checking and copying of a document issued under the Compulsory Identification Act (WID document). A foreign passport or identity card in case of foreign military or civil personnel is considered to be of equal assurance.
- the military screening process that results in a statement of trustworthiness of the employee into the specific information system.

3.2.3.2 Authentication of personal identity during the requesting of an NL-MoD Card.

Authentication of the personal identity of a holder of a Ministry of Defence Card takes place on the basis of a document issued under the Compulsory Identification Act (WID), hereinafter referred to as a "WID document", and the presence of the holder of the Ministry of Defence Card in person when the digital photograph is taken and when the Ministry of Defence Card is provided. In all cases, an RA employee checks whether the individual shown in the Ministry of Defence Card photograph or in the photograph of the identification document submitted is the same as the individual who has appeared in person. The WID document's authenticity features are also checked.

3.2.3.3 Authentication at the card provider when the NL-MoD card has to be provided.

When the Ministry of Defence Card is provided, the holder of the card must appear in person and submit the WID document used for the application. This document is used to verify the identity of the holder concerned. Note: the PIN-letter is sent to the cardholders home address. The NL-MoD Card is sent to the issuing location.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

Each application for a certificate as submitted by the card applicant is assessed to determine whether or not it may be authorised. A security check may be part of this assessment. The NL-MoD card Management System (Defensiepas Beheer Systeem: DBS) enforces the segregation of duties. The person who has applied for a NL-MoD card may not be the person who authorises the application.

3.2.6 Criteria for interoperation

No stipulation.

3.3 Identification and authentication for re-key requests

If the end of a NL-MoD Card's term of validity is imminent or if the NL-MoD card is defective, the holder of the card can submit a new application for a card to the card manager.

3.3.1 Identification and authentication for routine re-key

When an application for a new NL-MoD card has been authorised, a new key pair is always generated and a new NL-MoD card is always issued. If the end of the term of validity of a NL-MoD card with certificates is imminent or if the NL-MoD card is defective, the manager of the NL-MoD card (not the holder of the card himself/herself) may apply for a new NL-MoD Card. The application for the card shall contain the data contained in the source system. The application process shall be the same as the one completed following submission of the first application (see Section 3.2).

3.3.2 Identification and authentication for re-key after revocation

The dissemination of new keys following revocation of the certificate takes place in accordance with routine replacement (see Section 3.3.1). The CA's systems prevent previously certified keys from being certified again.

3.4 Identification and authentication for revocation request

Requests for the revocation of certificates are linked to the revocation procedure that applies to NL-MoD cards. Revocation requests are a regular part of the process by which replacement NL-MoD cards are provided. The certificates of the old NL-MoD card are revoked before the new NL-MoD card is provided. The holder of the NL-MoD card does not have to submit a separate request for this purpose. The NL-MoD card provider is identified by signing in to the DBS using the NL-MoD card and PIN.

In the event of circumstances by reason of which a NL-MoD card is revoked without a replacement being provided, for instance because of the end of employment, the regular revocation process is followed. A change to the personnel details in the NL-MoD personnel system initiates the revocation procedure.

Revocation is effected differently only in the case of theft or loss, or fraud. In the event of theft or loss, the holder of the NL-MoD card in question contacts the reporting centre within the NL-MoD by telephone. The role of reporting centre is fulfilled by the NL-MoD Service Desk (SDD). A number of unique details are used to verify the identity of the caller. If the caller is indeed the person he/she claims to be, the reporting centre staff member enters the revocation request into the DBS. The reporting centre staff member signs in to the DBS using the NL-MoD card and PIN. *During the telephone conversation itself, the reporting centre staff member confirms that the revocation request has been processed.*

The reporting centre records all requests for revocation in the incident management system and subsequently sends an email confirmation that the certificates have been revoked to the holder of the NL-MoD Card.

In the event of fraud, a revocation request can be submitted in accordance with Subsection 4.9.2.

A conscious decision was made to keep the identification and authentication process associated with a revocation request easy to complete. For the NL-MoD, enforcing the access policy is of greater importance than the potential drawbacks of wrongly revoking NL-MoD cards.

4 Certificate Life-Cycle Operational Requirements

The description of the way in which the TSP meets the operational requirements that apply to NL-MoD card processes is largely taken from the Administrative Organisation (*Administratieve Organisatie*), to which the operating instructions cards also belong.

4.1 Certificate Application

Applications for certificates are always linked to applications for NL-MoD cards. Applications for NL-MoD cards are submitted by the card manager. Holders of NL-MoD cards must always be registered in the NL-MoD personnel system before an application can be accepted for processing. Registration in the NL-MoD personnel system always implies the person has been subject to military screening (resulting in a security clearance).

The card manager checks whether the holder of a NL-MoD card is entitled to a NL-MoD card and whether the data has been recorded correctly. The desired location at which and the date on which the card is to be provided are also recorded.

A digital photograph of the holder of the NL-MoD card is then added to the NL-MoD card application details, which are largely taken from the NL-MoD personnel system. The intended holder of the NL-MoD card must report in person to the designated photographer for this purpose. The holder of the NL-MoD card must identify himself/herself by means of a WID document before a photograph may be taken.

The photographer checks the registration details of the holder of the NL-MoD card to guarantee that the digital photograph of the right person is linked to the right registration. If the registration details are inaccurate, they must first be altered in the NL-MoD personnel system. This will result in an altered application for a NL-MoD Card.

At migration point from Generation 2 towards Generation 3 certifications, the internal subscriber NL-MOD has applied for new certificates for all existing users at that point in time (from its personnel system) by automated means. At issuing, these users of the NL-MOD Cards have been authenticated by their WID documents (passport, drivers license or equivalent).

4.1.1 Who can submit a certificate application

Applications for certificates are linked to applications for NL-MoD cards, which are entered into the DBS by authorised actors.

4.1.2 Enrollment process and responsibilities

All NL-MoD employees who carry out NL-MoD card procedures as actors are trained for that purpose and, at the request of their superiors, are authorised by those who manage the DBS. The NL-MoD organisational units are also responsible for reviewing the list of actors and submitting authorisation requests on time.

4.2 Certificate Application Processing

Applications for certificates are always linked to applications for NL-MoD cards.

4.2.1 Performing identification and authentication functions

The checks that are performed to verify the identity of the holder of a NL-MoD card are described in Chapter 3 (Identification and Authentication).

4.2.2 Approval or rejection of certificate applications

The production process starts after the card authoriser has attached his/her approval to the NL-MoD card application. See also Section 3.2.5.

4.2.3 Time to process certificate applications

The delivery period (as defined beforehand by The NL-MoD) regarding a NL-MoD card is subsequently laid down in the service level agreement concluded with the supplier.

4.3 Certificate Issuance

Certificates are always linked to NL-MoD cards.

4.3.1 CA actions during certificate issuance

NL-MoD cards are received at the location at which they are provided to holders. The NL-MoD cards are stored in a locked/secure space (safe/cabinet). The space in which the NL-MoD cards are stored can only be accessed by the card provider(s).

The PIN letter is sent to the private address of the holder of the NL-MoD Card.

If the holder of the NL-MoD card already has a NL-MoD card with certificates, the previously provided NL-MoD card must be handed in. Provision of a new NL-MoD card is not possible without the return of the old NL-MoD Card. A declaration of loss is required if the old NL-MoD card is stolen or lost.

The holder of the NL-MoD card must appear in person at the card provider. The card provider verifies the identity of the holder of the NL-MoD card by means of the WID document. The card provider makes a copy of the WID and stores that secure for archiving. The NL-MoD Card will be handed to the holder of the Card.

The NL-MoD card is not issued if the outcome of any one of the checks, such as the identity check, for example, is negative. A replacement NL-MoD card is also not issued if the holder does not have an old NL-MoD Card, an official report or a declaration of loss.

At first use of the certificates it is enforced that a new pincode must be entered.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The certificates that belong to a NL-MoD card are provided to the holder through the card itself.

A NL-MoD card must be activated by means of the PIN, where it is enforced that a new pincode must be entered.

Before handed over to the holder, the holder of the NL-MoD card gets an email for receiving the Card. In that mail, the holder is informed about userregulations that are part of internal NL-MoD instructions. These instructions can be enforced by internal disciplinary measures.

Because NL-MoD is the owner of the NL-MoD TSP and because the NL-MoD is the sole subscriber of the NL-MoD TSP and because all end-users are legally bound to NL-MoD (including mandatory use of NL-MoD issued certificates where applicable) and because NL-MoD is accountable as employer, no user agreement is possible or necessary. Therefore, no user agreements for certificates exist within the working of this CPS.

4.4 Certificate Acceptance

The certificates that belong to a NL-MoD Card are provided to the holder through the card itself. Acceptance is mandatory for holders of Type 1 and 2 Ministery of Defence Cards.

4.4.1 Conduct constituting certificate acceptance

See Section 4.3.1.

4.4.2 Publication of the certificate by the CA

The TSP publishes the certificates internally within the NL-MoD in the CoDi.

4.4.3 Notification of certificate issuance by the CA to other entities.

No stipulation, usage is not allowed for private purposes.

4.5 Key Pair and Certificate Usage

Private keys issued by the TSP are always and exclusively used by holders of NL-MoD cards who are acting on behalf of the NL-MoD.

4.5.1 Subscriber private key and certificate usage

The permitted use of the private keys and certificates of holders of NL-MoD cards is described in Section 1.4.

4.5.2 Relying party public key and certificate usage

In this CPS, the obligations of relying parties, in addition to the obligations of other parties, are described in Section 9.6. Thus, a balanced overview of the liabilities and obligations of all parties involved is provided in a single chapter.

4.6 Certificate Renewal

MoD does not offer any possibility to renew PKIoverheid certificates. A request for renewal shall be treated as a request for a new certificate.

4.6.1 Circumstance for certificate renewal

No stipulation.

4.6.2 Who may request renewal

No stipulation.

4.6.3 Processing certificate renewal requests

No stipulation.

4.6.4 Notification of new certificate issuance to subscriber

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

No stipulation.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate Re-key

NL-MoD does not support re-keying.

4.7.1 Circumstance for certificate re-key

No stipulation.

4.7.2 Who may request certification of a new public key

No stipulation.

4.7.3 Processing certificate re-keying requests

No stipulation.

4.7.4 Notification of new certificate issuance to subscriber

No stipulation.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No stipulation.

4.7.6 Publication of the re-keyed certificate by the CA

No stipulation.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate Modification

Certificates always are generated only once. They are never altered.

4.8.1 Circumstance for certificate modification

No stipulation.

4.8.2 Who may request certificate modification

No stipulation.

4.8.3 Processing certificate modification requests

No stipulation.

4.8.4 Notification of new certificate issuance to subscriber

No stipulation.

4.8.5 Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6 Publication of the modified certificate by the CA

No stipulation.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate Revocation and Suspension

Requests for the revocation of certificates are linked to the revocation procedure that applies to NL-MoD cards.

4.9.1 Circumstances for revocation

Revocation of certificates that are in use takes place on a regular basis if a replacement NL-MoD card is provided. This section describes the cases in which a NL-MoD card must be revoked immediately. All other circumstances are provided for in the regular replacement process. For example, if it becomes clear that the information in the certificates is inaccurate, a new NL-MoD card with new certificates is applied for. The certificates in use are revoked prior to the issue of this new NL-MoD Card.

Immediate revocation of the NL-MoD card occurs in the following cases:

- the subscriber (NL-MoD) states that the original application for a NL-MoD card was not permitted (this can be initiated bij the user, the holder of the NL-MOD Card; the certificate holder);
- the TSP has sufficient evidence that the private key that matches the public key in the certificate has been adversely affected or there is a suspicion that security has been compromised or there is an inherent security weakness, or that the certificate has been misused in some other way. A key is deemed to have been adversely affected in the case of:
    - unauthorised access or suspected unauthorised access to the private key;
    - loss or suspected loss of the private key;
    - theft/loss or suspected theft of the NL-MoD card key;
- the holder of the NL-MoD card fails to perform his/her obligations as set out in the CPS of the TSP or the internal regulations.
- the TSP is informed of or otherwise becomes aware of a fundamental change in the information contained in the certificate. An example of such a change is a change in the name of the certificate holder;
- the TSP determines that the NL-MoD card was not issued in accordance with this CPS of the TSP;
- the TSP determines that information in the certificate is inaccurate or misleading;
- the TSP discontinues its activities and the CRL and OCSP services are not taken over by another TSP;
- the PA of PKI-O establishes that the technical content of the certificate entails an irresponsible risk for holders of a NL-MoD card, relying parties and third parties (browser parties, for example);
- revocation is necessary because of an incident or emergency.

4.9.2 Who can request revocation

The following parties may submit a request for the revocation of a certificate:

- The subscriber (NL-MoD);
- the card provider;
- the user (holder of the NL-MOD Card);

- the TSP;
- any other party that or person who, in the opinion of the TSP, is a party or person concerned.

4.9.3 Procedure for revocation request

In addition to revocation requests associated with the issue of replacement NL-MoD cards, there are revocation requests that must be processed immediately following a notification to the reporting centre of theft, loss or fraud.

The reporting centre is available 24/7 for the purpose of processing such requests. Revocation requests communicated by telephone are processed immediately.

In the case of planned maintenance or unforeseen disruptions, revocation requests submitted through the reporting centre are executed with little or no delay ensuring that all certificates are revoked within 24 hours. A fallback scenario that is regularly tested was designed for that purpose.

The reporting centre checks, in accordance with the procedures described in Section 3.4, the identity of the party that has submitted the revocation request.

The reporting centre then enters the revocation request into the DBS and thereby initiates the revocation process. The reason for revocation is recorded in the DBS. The steps of the revocation process are as follows:

1. Based on the notification, the NL-MoD card is blocked in the DBS (”logical revocation”). This blocking automatically triggers the procedure in place for the revocation of certificates.
2. The revoked certificates are placed on the Certificate Revocation List (CRL), which is then published on the internet and internally within the NL-MoD.
3. If the holder of the NL-MoD card no longer possesses the NL-MoD Card, he/she must have an official report or a declaration of loss drawn up and submit the report or declaration to the RA.
4. NL-MoD cards that are physically handed in are deactivated and subsequently permanently destroyed in a separate procedure.

4.9.4 Revocation request grace period

The information that is provided to every holder of a NL-MoD card states that a holder must immediately report the loss or theft of his/her NL-MoD card to the reporting centre.

4.9.5 Time within which CA must process the revocation request

The processing of revocation requests up to and including publication of the updated CRL takes place within 24 hours.

4.9.6 Revocation checking requirement for relying parties

Relying parties are obliged to:

1. verify the validity of the certificate;
2. check the validity of the hierarchy within which the certificate was issued;
3. verify that the CA certificate, which is used to validate the signature under a qualified certificate, is included in the EU Trusted List of Qualified Trust Service Providers (QTSP). This is only applicable in order to rely on a signature certificate as an EU qualified certificate. These obligations are included in Section 9.6 of this CPS.

4.9.7 CRL issuance frequency

The CRL is issued at least once every four hours, with each revocation resulting in a new CRL that is immediately published. Due to bandwith restrictions revoked certificates are removed from the CRL after they have expired. MoD does not include the X.509 "ExpiredCertsOnCRL" extension as defined in ISO/IEC 9594-8/Recommendation ITU T X.509 in her CRL.

4.9.8 Maximum latency for CRLs

Although the maximum delay regarding CRLs is not further specified, it is within the confines of the maximum period of time for the processing of a revocation request as referred to in Section 4.9.5.

4.9.9 On-line revocation/status checking availability

The TSP provides an Online Certificate Status Protocol (OCSP) service. This online service makes it possible to check the status of a certificate. Pre-computed responses are not used. An OCSP response has a maximum service life of one hour.

The OCSP responder gives the following replies to a status request:
- GOOD if the certificate has been issued and has not been revoked;
- UNKNOWN if the certificate is unknown;
- REVOKED if the certificate has been revoked.

The structure of the OCSP service meets the applicable requirements set out in *IETF RfC 6960*. The OCSP service uses a certificate issued under the PKI-O hierarchy.

The availability of the OCSP service is the same as the availability of the CRL, namely 24/7. See Section 4.10.2.

4.9.10 On-line revocation checking requirements

No stipulation.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements re key compromise

A key is deemed to have been compromised in the case of:
- o unauthorised access or suspected unauthorised access to the private key;
- o loss or suspected loss of the private key;
- o theft/loss or suspected theft/loss of the NL-MoD card key;

4.9.13 Circumstances for suspension

The NL-MoD card service does not include the option of suspending the validity of certificates. Certificates are either valid or have been revoked. There is no intermediate status.

4.10 Certificate Status Services

Relying parties can check the status of certificates. MoD supports CRL and OCSP to provide revocation status, any updates to revocation status are made available to both methods. The information provided is consistant over time taking into account different delays in updating the status information.

4.10.1 Operational characteristics

Relying parties can check the validity of certificates using a CRL and/or OCSP, both internally within the NL-MoD by means of the DPS and externally by means of the IPS. The integrity and authenticity of the status information is protected by MoD.

4.10.2 Service availability

The CRL is available 24/7. In the event of disruptions to the services, availability is restored within four hours. Efforts are made to ensure the same level of availability regarding the OCSP service provided within the NL-MoD. The aim in the event of a disruption is to restore the OCSP service within four hours, even though doing so is not necessary according to PKI-O requirements.

4.10.3 Optional features

No stipulation.

4.11 End of Subscription

The NL-MoD card service is not provided in the form of a subscription.

4.12 Key Escrow and Recovery

During the production of a NL-MoD Card, a copy of the private key that belongs to the confidentiality certificate of the holder of the NL-MoD card is stored in a secure environment (”key escrow”). This is meant for future use. At the moment, there are no means in place for recovering these private keys.

4.12.1 Key escrow and recovery policy and practices

Key escrow:
The private confidentiality keys of holders of NL-MoD cards are generated by what is referred to as the black box (a cryptography box) and are immediately saved in encrypted form in the key escrow database.

The black box is connected in a secure manner to the DBS. At the moment, there are no means in place for recovering keys.

The black box uses two public keys of the DBS to encrypt the content of the key escrow database. The appurtenant private DBS keys for decrypting the content of the database are not present in the black box and are not present at the location of the managers of the black box.

Black box management:
The black box is located in a physically secure room and can only be accessed by authorised managers. Access to the building and to the room in which the black box is located is subject to the following physical security measures: a duty to report on the part of the authorised managers and the registration of these managers on arrival, and access to the black box room under escort of a security officer.

Management activities relating to the black box are subject to a key procedure under which two individuals must enter a shared password into the black box (”four eyes principle”). The two parts of the password are kept in two separate, sealed envelopes which are themselves kept in a locked cabinet in the black box room.

A protocol is drawn up following each visit to the black box room. This protocol states the time of the visit, the details of the visitors and the management activities performed in relation to the black box.

Application for and delivery of an encrypted key from key escrow
At the moment, there are no means in place for applying and/or delivering of (encrypted) private keys.

4.12.2 Session key encapsulation and recovery policy and practices

All keys are generated in the black box and in the HSM of the DBS. The use of these keys for the protection of the certification services of the NL-MoD is documented. This documentation is classified as confidential.

5 Facility, Management, and Operational Controls

The control measures described in Chapters 5 and 6 are based on various risk analyses, including the NL-MoD card risk analysis (*Risicoanalyse Defensiepas*).[Ref 1] This NL-MoD card risk analysis was carried out in accordance with the method prescribed in the NL-MoD security policy (*Defensiebeveiligingsbeleid*).

A specific risk analysis was also carried out for the NL-MoD Card. This risk analysis provides an overview of the intended, primarily technical measures that must be taken because of the threats to the NL-MoD Card. This CPS describes the main features of the control measures without compromising the confidentiality of the security measures.

5.1 Physical Security Controls

The services of the TSP are provided at different sites. The physical security measures required have been taken for all sites.

5.1.1 Site location and construction

The registration activities and activities relating to the provisioning are performed at NL-MoD sites in the Netherlands and outside the Netherlands. The central DBS is in the data centre of GIT&Infra. NL-MoD cards are produced at Idemia's business location, while the actual production of certificates takes place in KPN's data centre.

5.1.2 Physical access

These measures are taken on the basis of risk analyses and security plans. The measures taken for the NL-MoD sites meet the requirements set in the Ministry of Defence Security Policy and the associated implementing provisions. In addition, the General Security Requirements for Defence Contracts (*Algemene Beveiligingseisen voor Defensieopdrachten*, ABDO) apply to the Idemia and Atos/KPN sites.

5.1.3 Power and air conditioning

All central sites, these being data centres, have an emergency power system and a conditioned environment.

5.1.4 Water exposures

Measures have been taken at all central sites to reduce the probability of flooding.

5.1.5 Fire prevention and protection

Measures have been taken at all central sites to prevent, detect and fight fire.

5.1.6 Media storage

Storage media of the systems used are handled safely to protect the storage media against damage, theft and unauthorised access. Storage media are carefully destroyed when they are no longer required.

5.1.7 Waste disposal

Measures have been taken at all central sites to ensure that confidential waste is disposed of in a proper manner.

5.1.8 Off-site backup

Backups of the TSP's systems are regularly stored at a separate location within the data centre.

5.2 Procedural Controls

A number of procedural control measures have also been taken to maintain the TSP's services.

5.2.1 Trusted roles

Within the NL-MoD, all positions involved in the provision of TSP services are classified as confidential positions in accordance with the implementing provisions for confidential positions (*Uitvoeringsbepalingen Vertrouwensfuncties*).

5.2.2 Number of persons required per task

The TSP's services are organised such that it is not possible for one person to undermine the reliability level of the services. This protection is achieved by the segregation of duties (see Section 5.2.4) and by procedures that ensure that actions involving key material of the CAs can only be performed in the presence of several parties. This is the case when key pairs of the CAs are generated and installed, for example, and when the backup of the private key of the CAs is used.

5.2.3 Identification and authentication for each role

An employee may only fulfil a confidential role after the employee concerned has been screened and granted security clearance and has a certificate of conduct (*Verklaring Omtrent Gedrag*; see Section 5.3.2 in this regard).

Employees' rights of access are defined by an authorisation structure and implemented in the TSP's systems in accordance with this structure by means of logical access control.

5.2.4 Roles requiring separation of duties

The TSP maintains a segregation of duties between the operators ("actors") who operate the TSP's systems on a daily basis and system administrators. The duties of security officer(s), system auditor(s), system administrators and operators are also segregated.

Furthermore, segregation of duties is in place within the actors category in the Administrative Organisation to make it impossible for a single officer to independently complete every step of a NL-MoD card application process.

5.3 Personnel Controls

A number of personnel control measures have also been taken to maintain the TSP's services.

5.3.1 Qualifications, experience, and clearance requirements

De TSP deploys a sufficient number of personnel who have the professional knowledge, experience and qualifications required for the provision of certification services. Each actor must complete specific training. This training is described in greater detail in the training plan. See Section 5.3.2 for screening requirements.

5.3.2 Background check procedures

Potential NL-MoD employees may only start performing the duties of a position after a certificate of conduct (*Verklaring Omtrent Gedrag*, VOG) or a certificate of no objection (*Verklaring van Geen Bezwaar*, VGB) has been issued by the Military Intelligence and Security Service (MIVD).

Regarding NL-MoD employees of the TSP, a confidential role may only be fulfilled by an officer who holds a confidential position. Each officer who holds a confidential position is screened on a regular basis by the MIVD. A VGB is issued if the officer concerned is granted security clearance following the screening. An employee may only perform work if the outcome of the necessary security screening is positive or if he/she has received a VOG.

5.3.3 Training requirements

See Section 5.3.1.

5.3.4 Retraining frequency and requirements

No stipulation.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

An employee who performs an unauthorised act is immediately denied access to all systems of the TSP. The responsible security coordinator decides on the duration of and conditions associated with this denial of access and on the further action to be taken and sanctions to be imposed in accordance with the Ministry of Defence Civil Service Regulations/General Military Personnel Regulations (*Burgerlijk/Algemeen Militair Ambtenarenreglement Defensie*, BARD/AMAR).

5.3.7 Independent contractor requirements

The external suppliers are appropriately certified (Eidas 910/2014 ,ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 401, CEN TS-419 261) and comply with ABDO. ABDO certification is regularly checked by the MIVD. The validity of the European Telecommunications Standards Institute (ETSI) certification is assessed every six months during the SLA meetings with the suppliers.

5.3.8 Documentation supplied to personnel

The job descriptions of employees of the TSP who operate the systems as actors are provided in the Administrative Organisation and the appurtenant operating instructions cards.

5.4 Audit Logging Procedures

Events that are relevant to the quality of the certification services are automatically or manually logged in the systems and applications used to provide the services.

5.4.1 Types of events recorded

Events that are relevant to the quality of the certification services fall within the following categories:

1. Registration actions in the DBS in relation to applications for NL-MoD cards and any later changes in the registration details.
2. Events in the life cycles of the keys of the CAs and the keys produced by the TSP for holders of NL-MoD cards.
3. Events in the life cycles of certificates and CRLs, including revocation requests and the activities performed by reason of these requests.
4. Events in the life cycles of NL-MoD cards.
5. Events in the certification services infrastructure, including:
    - breaches of the systems and attempts to breach the systems;
    - logging in and logging out of system administrators;
    - actions of system administrators that are relevant to the reliability of the certification services;
    - changes to authorisations (security profiles) and accounts of actors;
    - shutting down and (re)starting of the systems;
    - error messages of the hardware or software of the systems;
    - installation of new or modified software;
    - changes of hardware;
    - actions in relation to the log files or log functionality, etc.

5.4.2 Frequency of processing log

Log files are regularly analysed in accordance with the management protocols drawn up for the certification services.

5.4.3 Retention period for audit log

The archiving system retains the archived audit log files for a period of at least seven years. Events in the certification services infrastructure will be retained for 24 months. The last log files of the preceding Generation 2 infrastructure and certificates are archived until 1st of april 2027.

5.4.4 Protection of audit log

Event-related information contained in the audit log files is protected against unauthorised parties by means of physical and logical access control resources.The integrity of the audit log files that are collected by the collection system is safeguarded by means of the digital signatures required with respect to such files.

5.4.5 Audit log backup procedures

A differential backup of audit log files is made on a daily basis as standard practice. Full backups are made each week.

5.4.6 Audit collection system (internal vs. external)

The collection system of audit log files is positioned in the GIT&Infra data centre.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

The TSP carries out further investigation if the analysis of the log files indicates that a security incident has occurred.

5.5 Records Archival

The TSP archives relevant information pertaining to events, data, files and forms.

5.5.1 Types of records archived

At a minimum, the following information is archived:
- audit log files;
- CRLs and certificates issued;
- documentation, such as this CPS;
- documents submitted during the application procedure;
- correspondence with the parties involved.

5.5.2 Retention period for archive

Like the information archived in printed form (WID), information archived in electronic form is retained for at least seven years.

5.5.3 Protection of archive

The TSP maintains an appropriate system of measures to protect the archived information in accordance with the Personal Data Protection Act and the Ministry of Defence security policy (*Defensiebeveiligingsbeleid*). This system includes, among others, the following measures:
- the logging and CRLs are archived in encrypted form;
- the logging is archived in redundant form;
- the CRLs and certificates are intrinsically secure in terms of authenticity and integrity;
- when archiving takes place, the TSP audit trail is electronically signed;

- only a select group of officers have access to the archive.

5.5.4 Archive backup procedures

A differential backup of audit log files is made on a daily basis as standard practice. Full backups are made each week.

No backup is made of information archived in printed form.

5.5.5 Requirements for time-stamping of records

The log records are provided with the date and time of the processing system on which the action was performed. The processing systems are synchronised in accordance with the Network Time Protocol (NTP).

5.5.6 Archive collection system (internal or external)

The archiving system consists of two physical components. One of these components is in the GIT&Infra data centre and the other is in the KPN data centre.

5.5.7 Procedures to obtain and verify archive information

The archiving system and other archives of importance to the certification services can only be accessed by authorised officers.

5.6 Key Changeover

The Certification Authority's signing key is generated and installed in KPN's data centre in accordance with a plan that is drawn up in advance.

5.7 Compromise and Disaster Recovery

The TSP has a number of procedures for resolving disruptions in the certification services.

5.7.1 Incident and compromise handling procedures

Incidents can be reported to the NL-MoD Service Desk (SDD) and are handled in accordance with the normal incident management procedures.

If an incident is expected to escalate, an emergency is reported to the emergencies manager. At that time, the decision may be made to put the emergency plan of the CA[Ref 4] into effect.

If the CA's private key is compromised, the event is deemed to be an emergency. In such a situation, the TSP will at least take the following action:

- the TSP will inform relying parties and holders of NL-MoD cards as soon as possible by publishing information about the situation on the NL-MoD intranet;
- the TSP will immediately revoke the certificates concerned and publish on the applicable ARL/CRL;
- the TSP will inform the Policy Authority of PKI-O of the emergency and further developments in that regard.
- The TSP will inform the Netherlands Supervisory Body: Rijksinspectie Digitale Infrastructuur (RDI) of the emergency and further developments in that regard.
- The TSP will inform the Conformity Assessment Body of the emergency and further developments in that regard.

5.7.2 Computing resources, software, and/or data are corrupted

In the context of incident management and the TSP's emergency plan,[Ref 4] recovery takes place in the IT environment. This process includes the option of continuing the provision of certification services at fallback locations.

5.7.3 Entity private key compromise procedures

If the keys of holders of NL-MoD cards are compromised, revocation requests are submitted as described in Section 4.9. A new NL-MoD card can be applied for following revocation. The holder will receive new keys as a result of this new application.

5.7.4 Business continuity capabilities after a disaster

See the TSP's emergency plan[Ref 4] and underlying documents at GIT&Infra.

5.8 CA or RA Termination

One of the reasons to stipulate the termination of TSP services is about bankruptcy of the TSP and because of this, the TSP cannot continue its obligations towards subscribers, users, relying parties and/or the law. By nature, the Kingdom of the Netherlands nor its Ministry of Defence can become bankrupt. Continuïng of services therefore is guaranteed. Because of this, no arrangements are in place for the eventuality of the State of the Netherlands becoming financially incapable of continuing the certification services. See also the provisions set out in "9.2 Financial responsibility and liability".

If a voluntarily decision is made to discontinue the certification services for other reasons, the TSP will take measures to continue the minimally required services for at least six months after the time at which the certification services are terminated. During these six months MoD will guarantee the integrity and availability of the last CRL.
Deliberately (see above), no measures are taken nor planned to transfer obligations to other parties, but shall hand over all information to archiving services of the Netherlands Ministery of Defence.

The TSP will take all reasonably possible measures to limit damage to the owner and sole subscriber (NL-MoD), holders of NL-MoD cards and relying parties.

Specific activities will include at least the following:
1. informing the holders of NL-MoD cards, relying parties and other parties with which agreements have been concluded about the intended termination of services;
2. inform the Netherlands Supervisory Body Rijksinspectie Digitale Infrastructuur (RDI) about the intended termination;
3. terminating the authorisations of subcontractors involved on behalf of the TSP in the provision of certification services, also in terms of rendering external links inoperative;
4. revoking all valid certificates;
5. issuing and publishing at the corresponding CRL Distribution Point a last CRL with a nextUpdate field value of "99991231235959Z".
6. putting the private keys of the Certification Authorities (CAs) out of operation;
7. retaining registration information, audit log files and CRLs in accordance with the applicable requirements.

6 Technical Security Controls

See the introductory text of Chapter 5.

All of the TSP's systems that support security-sensitive processes of the certification services are in compliance with NPR-CEN/TS 419261 Security requirements for trustworthy systems managing certificates and time-stamps.

The Hardware Security Modules (HSMs) used for the certification services are in compliance with Federal Information Processing Standard Publication 140-2 (FIPS 140-2). This compliance guarantees, among other things, that cryptographic material cannot be altered during storage, use and transport without such alteration being noticed.

6.1 Key Pair Generation and Installation

When generating key pairs, the TSP uses secure, FIPS 140-2 certified resources.

6.1.1 Key pair generation

The keys of the TSP and holders of NL-MoD cards are centrally generated.
These keys are generated in a FIPS 140-2-certified HSM. The signature algorithm SHA256RSA is used for NL-MoD cards issued under the G3 hierarchy. The hash algorithm used is SHA256.

6.1.2 Private key delivery to subscriber

The PIN is sent separately in the form of a PIN-letter to the private address of the holder of the NL-MoD Card. The letter is marked as personal.

The NL-MoD card is personally handed over to its holder at a NL-MOD location.

6.1.3 Public key delivery to certificate issuer

No stipulation.

6.1.4 CA public key delivery to relying parties

The CA's public keys are signed by the PA of PKI-O, which guarantees the integrity and origin of the public keys. The public keys are made available to relying parties in the form of certificates of the TSP through the

G3 hierarchy:

DomOrganisatiePersoonCA - G3	http://cert.pkioverheid.nl/DomOrganisatiePersoonCA-G3.cer
Ministry of Defence Card CA – G3	http://certs.ca.pkidefensie.nl/mindef-ca-3.cer

See Chapter 2.2.

6.1.5 Key sizes

The following key lengths apply:

- the length of the CA's key pairs is 4096 bits, asymmetric RSA;
- the length of the key pairs of the holder of the NL-MoD card is 2048 bits, asymmetric RSA.

6.1.6 Public key parameters generation and quality checking

The public key is generated in accordance with the requirements as described for the Organisation Person Domain CP (G3 hierarchy) and that apply to the cryptographic products concerned. These products comply with CEN/TS 419261.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

The certificates, including the key pairs that belong to them, are solely intended for the purposes described in Section 1.4 of this CPS. The purposes for which a key may be used are included in the certificate (see Section 7.1 in this regard).

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Measures have been taken to ensure the security of keys and modules.

As part of the QSCD lifecycle management, the TSP will periodically let the card issuer and personalizer check the QSCD certification status. The TSP will implement a replacement QSCD in a timely manner through regular management processes, prior to the expiry of the current QSCD certification. In the event of early and unexpectedly faster expiry of the QSCD certification, the TSP will revoke certificates that have not yet expired, inform the parties involved and make an alternative available as soon as possible.

6.2.1 Cryptographic module standards and controls

The cryptographic data are stored in an HSM for operational use. The HSM meets the requirements set out in FIPS 140-2.

6.2.2 Private key (n out of m) multi-person control

The four eyes principle is technically enforced when key pairs of the CA are generated and installed and when the backup of the private key of the CA is used. At least three individuals are required for these tasks. Each of these individuals has his/her own part of the key material on a smart card. See Section 6.2.4.1.

6.2.2.1 Escrow of private keys of the TSP

The private key of the CA is not held in escrow.

6.2.2.2 Escrow of private keys of certificate holders

The TSP holds the private key of the confidentiality certificate of all NL-MoD cards in escrow. These copies are currently not used. See Section 4.12 in this regard.

6.2.2.3 Backups of private keys of the TSP

A backup is stored in several encrypted parts in cryptographic modules and appurtenant storage devices.

A backup can only be used if three of the five designated officers are present with their part of the key and the associated PIN.

6.2.2.4 Backups of private keys of certificate holders

The TSP makes a backup of the private confidentiality key of all NL-MoD cards and holds this backup in escrow.

6.2.2.5 Archiving of private keys of the CA

The private signature key of the CA is archived in a FIPS 140-2-certified HSM. Technical and organisational measures have been taken to ensure that the archived key cannot be used again.

6.2.2.6 Archiving of the private keys of certificate holders

Private keys of signature and authenticity certificates of holders of NL-MoD cards are never archived. Technical and organisational measures have been taken to make it impossible to archive these keys.

The private key of the confidentiality certificate of a holder of a NL-MoD card is held in key escrow.

6.2.3 Private key escrow

The keys of holders of NL-MoD cards are placed in the cards immediately after they have been generated. The private key does not leave the NL-MoD card after that time. The private confidentiality key is held in key escrow. There is no possibility of Escrow of Private Keys related to Signature Certificates and Authentication Certificates.

6.2.3.1 Storage of private keys in cryptographic modules

The private keys of holders of NL-MoD cards are stored in those cards. The NL-MoD card is manufactured in accordance with Commission Implementing Decision (EU) 2016/650 using ISO/IEC 15408 (Common Criteria) processes on NEN/EN 419211 protection profile(s) (EAL4+).

The status of the QSCD certification will be monitored until the end of the validation period. When the status is modified, NL-MoD will choose for a newer (same type) or other certified QSCD.

6.2.3.2 Method used to activate the private keys

The private keys of the CA are only activated by a key ceremony and the officers who must be present to complete this ceremony. The TSP ensures a careful procedure in a secure environment.

At first use, the holder of the NL-MoD Card has to activate the QSCD with the PIN sent in the PIN-letter. At activation of the QSCD, the user is forced to enter a new PIN for be”ing able to activate the private keys. The new PIN must be entered to activate the private keys of a NL-MoD Card. These keys must be activated for each session.

6.2.3.3 Method used to deactivate the private keys

In certain situations as defined by the TSP, the private keys of the CA are deactivated in accordance with the due care procedures that apply to such deactivation. The emergency plan of the TSP[Ref 4] is put into effect if security has been compromised. See Section 5.7.

Deactivation of the private keys of a holder of a NL-MoD card is linked to the process by which NL-MoD cards are withdrawn, certificates are revoked and, if appropriate, NL-MoD cards are physically destroyed.

6.2.3.4 Method used to destroy the private keys

The private keys of the CA and NL-MoD cards are rendered inoperative and, if appropriate, destroyed in such a manner as to ensure that they can no longer be used.

6.2.3.5 Requirements that apply to the NL-MoD card as a cryptographic module

The NL-MoD card is manufactured in accordance with Commission Implementing Decision (EU) 2016/650 using ISO/IEC 15408 (Common Criteria) processes on NEN/EN 419211 protection profile(s) (EAL4+).

6.2.4 Private key backup

No backup will be made of the Private Keys associated with subject Certificates.

6.2.5 Private key archival

Private keys of Certificates are not archived.

6.2.6 Private key transfer into or from a cryptographic module

The only allowed transfer operation of private keys is between the blackbox of Idemia and the QSCD.

6.2.7 Private key storage on cryptographic module

Private keys are generated in the Idemia blackbox and transferred into the QSCD. After transfer the keys are removed from the blackbox (except the confidentiality keys which are held in key-escrow 6.2.3).

6.2.8 Method of activating private key

The private keys can only be activated directly by the subjects (pin), the procedure of which is described in the "Handboek Administratieve Organisatie".

6.2.9 Method of deactivating private key

See Section 4.9.

6.2.10 Method of destroying private key

No stipulation

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

This section provides information about the archiving of public keys and arrangements in place regarding service life.

6.3.1 Public key archival

Public keys are archived by the TSP and stored in a physically secure environment for at least seven years following the end of the period of validity of the associated certificates.

6.3.2 Certificate operational periods and key pair usage periods

The service life of a CA's key pairs and certificates never exceeds the service life of the CA that is higher in the hierarchy and is a maximum of ten years.

The service life of NL-MoD cards, certificates and keys issued is set at three years.

6.4 Activation Data

The following measures have been taken to minimise the likelihood of NL-MoD card activation data being compromised.

6.4.1 Activation data generation and installation

The activation data, the PIN and PUK, are prepared and distributed in a secure manner.

6.4.2 Activation data protection

The PIN is made known to the holder of the NL-MoD card by means of a PIN letter that is sent to the private address of the applicant. Measures have been taken to ensure that third parties cannot covertly become aware of the PIN (the PIN cannot be read if the PIN letter is in the envelope, for example). The PUK is not made known to the holder of the NL-MoD Card. It is securely stored by the CA.

The holder of the NL-MoD card is personally responsible for protecting the PIN after he/she has received it.

The holder of the NL-MoD card has to activate the Card on initial use and then is forced to enter a new PIN.

A NL-MoD card is blocked if an incorrect PIN is entered five times. The holder of the card must contact the SDD to have the card unblocked. The unblocking procedure includes technical and procedural security measures to ensure that the PUK cannot be used by unauthorised parties. The procedure, which also includes the segregation of duties, is described in the Administrative Organisation.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

The TSP takes adequate measures to safeguard availability, integrity and exclusivity.

6.5.1 Specific computer security technical requirements

Computer systems are secured against unauthorised access and other threats in an appropriate manner. A risk analysis and a security measures implementation plan (IBP) are available for the NL-MoD card service. Reliability levels are defined in detail with suppliers and laid down in service level agreements (SLAs).

The configuration of the TSPs systems is checked regulary for changes which violate the TSPs security policies. The maximum interval between two checks is 1 week.

The CA keys are used for digitally signing certificates, Certificate Revocation Lists (CRLs), and the Online Certificate Status Protocol (OCSP) signer, as specified in this CPS.
To ensure the integrity and confidentiality of CA keys, appropriate security measures are implemented, including the use of hardware security modules (HSMs) and strict access control mechanisms.
CA keys are generated following strict procedures.These procedures include generating keys on secure systems and using cryptographic methods compliant with applicable standards.
Each certificate issued by the CA is digitally signed using the corresponding CA key. The digital signature verifies the authenticity and integrity of the certificate.

6.5.2 Computer security rating

The systems and data of the TSP are classified on the basis of current regulations and policy and/or additional Risk Management. This classification is regularly assessed and altered if necessary. A number of systems must also meet CEN/TS 419261. See Section 9.3.

6.6 Life Cycle technical controls

The TSP ensures that software, during its entire life cycle, cannot be modified without such modification being noticed.

6.6.1 System development controls

The TSP has outsourced system development to ABDO-certified subcontractors. These subcontractors develop and test systems in accordance with quality and test plans. The TSP carries out acceptance tests in accordance with test plans that are drawn up in advance.

The TSP safeguards system development by, among other measures, using separate environments for testing, acceptance and production purposes, and by adhering to processes in place for version control and change management.

6.6.2 Security management controls

The security settings of hardware and software are documented in, among other things, control protocols. The National Audit Service (ADR) of the Netherlands and/or the Internal IT Audit Service checks these settings during the partial, rotational audits carried out in the context of the annual audit programme.

6.6.3 Life cycle security controls

The security of the TSP's hardware and software is regularly audited. Such audits result in an opinion regarding the level of security and, if necessary, in recommendations.

6.7 Network Security Controls

Network security measures that guarantee the availability, integrity and exclusivity of the data have been implemented.

Communication over public networks between systems of the TSP takes place in confidential form. The links between the public networks and the TSP's networks are protected by stringent security measures. The links comply with Ministry of Defence framework D401 *Koppelingen met defensienetwerken* (links with Ministry of Defence networks).

6.8 Time-stamping

Time stamping is not used in the certification services provided.

7 Certificate, CRL, and OCSP Profiles

The certificate profiles, CRL profiles and OCSP profiles are described in full in the document *Certificaat en CRL-profielen MinDef PKIo TSP* (TSP Ministry of Defence PKI-O certificate and CRL profiles).

This chapter does not deal comprehensively with certificate, CRL and OCSP profiles because the profiles used by the NL-MoD were compiled in accordance with the PKI-O profiles as prescribed in the Organisation Person Domain CP (G3 hierarchy) and the Services CP. The profiles determine which information is included in the certificates as standard. This information relates to the CA that issues the certificates, the holder of the NL-MoD Card, the algorithms used and so on. The prescribed PKI-O profiles provide for a degree of discretion. An explanation is provided where this discretion has resulted in choices of potential importance to holders of NL-MoD cards or relying parties. This is the case, for example, with respect to the description of personal data in the certificates.

This chapter describes certificate profiles, CRL profiles and OCSP profiles. These profiles are numbered for Figure 1. In the context of the NL-MoD Card, they are as follows:

1. Staat der Nederlanden Root (SdN) CA-G3: this is the root CA that is governed, owned and operated by Ministry of Internal Affairs/Logius. It is the self-signed Root CA for the entire PKI-O Generation 3. This SdN Root CA-G3 signes the existing intermediate SdN [Domain] CA-G3. The certificate profile of this CA is determined by the Ministry of Internal Affairs/Logius (PKI-O), which is also responsible for the associated CRL profile.
2. Staat der Nederlanden Organisatie Persoon CA-G3: This is the intermediate domain CA for services in the Organization-Person domain. This intermediate domain CA-G3 is governed, owned and operated by Ministry of Internal Affairs/Logius. This intermediate CA is signed by the SdN Root CA-G3. This intermediate CA-G3 signes existing issuing CA's for this domain like the Ministerie van Defensie PKIoverheid Organisatie Persoon CA-G3. The certificate profile of this CA is determined by the Ministry of Internal Affairs/Logius (PKI-O), which is also responsible for the associated CRL profile.
3. Ministerie van Defensie PKIoverheid Organisatie Persoon CA-G3: This is the Issuing CA for the NL-MoD Card that contains 3 certificates. This issuing CA is governed, owned and operated by the Netherlands Ministry of Defence. This issuing CA is signed by the SdN Organisatie Persoon CA-G3. This issuing CA signs the end-user certificates (authenticity, signature and confidentiality) of the holders of the Netherlands Ministry of Defence Defensiepas (the NL-MoD Card). The certificate profile of this CA is determined by the Ministry of Internal Affairs/Logius (PKI-O), which is also responsible for the associated CRL profile and OCSP profile.
4. The Ministry of Defence Card (NL-MoD Card) contains three end-user certificates (authenticity, signature and confidentiality). The certificate profiles of the end-user certificates is the responsibility of the Ministry of Defence.

Figure 1 shows the CA hierarchy for the G3 hierarchy. The NL-MoD card certificates are also shown at the lowest level.

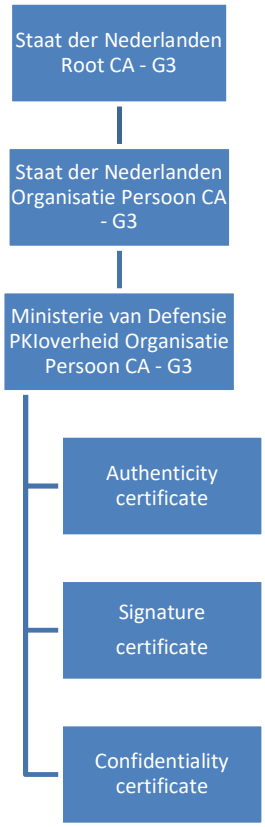

Figure 1. CA hierarchy

The locations at which the CRLs and the OCSP service can be found are stated in Section 2.2.

7.1 Certificate Profile

The certificate profiles of the 'Staat der Nederlanden Root CA – G3' and the 'Staat der Nederlanden Organisatie Persoon CA – G3' were determined by PKI-O. These certificate profiles are available at www.pkioverheid.nl.

PKI-O is also responsible for the certificate profile of the 'Ministerie van Defensie PKIoverheid Organisatie Persoon CA – G3' (Figure 1).

The certificate profile of the 'Ministerie van Defensie PKIoverheid Organisatie Persoon CA – G3' (Figure 1), on the other hand, is the responsibility of the Ministry of Defence (Figure 1).

The composition of the certificates of holders of NL-MoD cards for authenticity, signature and confidentiality (Figure 1) is of direct importance to holders of NL-MoD cards and relying parties. The main elements of these three types of certificates are the same.
They differ in terms of the key usage value, which indicates whether the private key included in the certificate may be used for the signature (non-repudiation), confidentiality (keyEncipherment, dataEncipherment) or authenticity (digitalSignature).

The name of the CA in these certificates is 'Ministerie van Defensie PKIoverheid Organisatie Persoon CA – G3'.

In all certificates the countrycode is "NL" which stands for "The Netherlands".

See Subsection 6.3.2 for the period of validity of the certificates.

After the period of three years has elapsed, users receive new NL-MoD cards with new G3 certificates that are valid for three years.

The amount of personal data on the NL-MoD card and in the certificates is limited for privacy reasons, since certificates are intended for wide distribution.

The personal data in the certificates are as follows: the given names, surname and email address of the holder of the NL-MoD card augmented with an employee number. This number makes the name unique. The work-related employee number separates the professional domain from the private one.

7.1.1 Version number(s)

The MoD Certificates are structured according to the PKI X.509 v3 standard.

7.1.2 Certificate extensions

All certificates are configured per Regulation (EU) No. 910/2014, ETSI EN
319 411-1/411-2 and Program of Requirements PKIoverheid. All other fields and extensions in the certificates are set in accordance with RFC 5280.

7.1.3 Algorithm object identifiers

MoD uses RSA encryption with SHA-2 algorithm and keys having the length at least of 2048 bits.

7.1.4 Name forms

See Section 3.1

7.1.5 Name constraints

All certificates are configured to meet the applicable requirements.

7.1.6 Certificate policy object identifier

The applicable Certificate policies can be identified througt the OIDs as described in Section 1.2.2.

7.1.7 Usage of Policy Constraints extension

No stipulation

7.1.8 Policy qualifiers syntax and semantics

MoD issues certificates with a policy qualifier within the Certificate Policies extension.
This extension contains a CPS pointer qualifier that points to the CPS

7.1.9 Processing semantics for the critical Certificate Policies

No stipulation

7.2 CRL Profile

The Certificate Revocation List (CRL) is a list of revoked certificates. The OCSP services includes such a list. At the NL-MoD, this status information only includes the certificate serial number and the date of revocation. A reason for the revocation is expressly not included in the CRLs.

The profile of the CRL for the Ministry of Defence CA is determined by PKI-O, which also publishes this CRL.

The TSP publishes one CRL, the CRL in which the status of the certificates of the holders of NL-MoD cards can be checked.

The CRL profile was prepared in accordance with the Organisation Person Domain CP (G3 hierarchy) of PKI-O.

Furthermore, the date and time of issue and the period of validity of the CRL are stated. The period of validity of the CRL for certificates of holders of NL-MoD cards is 24 hours.

7.2.1 Version number(s)

MoD issues X.509 version 2 CRLs.

7.2.2 CRL and CRL entry extensions

NL-MoD complies with the requirements outlined in the PoR of Logius PKIo. Specifically, our Certificate Revocation Lists (CRLs) include the extension values in the Extensions fields as detailed in Section 7.2.2.

7.3 OCSP Profile

In terms of PKI-O, the certificate profile of the Online Certificate Status Protocol (OCSP) signer is a certificate of the service certificate for authenticity type. This certificate was prepared in accordance with the Services CP (OID 2.16.528.1.1003.1.2.2.4).

The Common Name of the OCSP-service is *OCSP-responder Ministerie van Defensie CA Defensiepas* (OCSP responder, Ministry of Defence, NL-MoD card CA).

OCSP provides a list of revoked certificates that can be consulted internally within the NL-MoD by means of the DPS and externally by means of the IPS.

7.3.1 Version number(s)

The OCSP Responder conforms to RFC 6960.

7.3.2 OCSP extensions

NL-MoD complies with the requirements as stipulated in the PoR of Logius PKIo Section 7.3. Specifically, all OCSP responses:
Are compliant with the RFC 6960 OCSP response profile, and
Do not contain fields and extensions other than those described or referenced under this section.

8 Compliance Audit and Other Assessment

The certification services of the TSP of the NL-MoD were certified by BSI on the basis of the framework defined by ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 and ETSI EN 319 403-1, and complies with PKI-O.

The conformity certificates of the most recent audits are available at the electronic storage location of the NL-MoD. The TSP also complies with the PKI-O's system of standards as set out in the program of requirements (see https://cp.pkioverheid.nl/).

The TSP of the Ministry of Defence is registered as certified service provider according to Regulation EU 910/2014 eIDAS by the Netherlands Supervisory Body: Rijksinspectie Digitale Infrastructuur.

The quality of the NL-MoD card service is also regularly audited by the National Audit Service (ADR) of the Netherlands and/or internal IT audit Sevices in the context of the annual audit programme. The ADR's audit is more broadly audited than the audit based on the framework defined by ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 403-1 and PKI-O. Whereas the ETSI audit focuses mainly on the legal validity of the electronic signature, the ADR audit focuses more generally on control of the risks associated with providing a NL-MoD card with certificates. Complementary internal checks are carried out at the locations at which NL-MoD cards are provided. These checks are aimed at ascertaining whether the NL-MoD organisational units are performing the Registration Authority (RA) duties in accordance with the standard. Information management staff members report the findings of these checks to TSP management.

Under the name *Defensiepas* (NL-MoD Card), the processing of personal data in the context of the NL-MoD card service is reported to the Data Protection Officer of the NL-MoD.

As part of the QSCD lifecycle management, the TSP will periodically let the card issuer and personalizer check the QSCD certification status and shall take appropriate measures in case of modification of this status.

Due to the fact that the Ministry of Defence CA is technically capable of producing S/MIME certificates, NL-MoD will make sure that the CA is compliant with the latest version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates. However as of 2-09-2024 NL-MoD does not produce S/MIME certificates.

8.1 Frequency or circumstances of assessment

As a qualified Trust Service Provider in The Netherlands, MoD is annually audited to assess compliance with ETSI EN 319401, ETSI EN 319411-1, ETSI EN 319411-2, eIDAS, CA/Browser Forum – Netsec/SMIME, Program of Requirements PKIoverheid and national law & regulations.

8.2 Identity/qualifications of assessor

Audits are performed by an external certified auditor.

8.3 Assessor's relationship to assessed entity

The assessor performing the audit is an independent third party.

8.4 Topics covered by assessment

The scope of the audit covers all requirements from the standards for the Trust Service Provider component services:
- Registration Service

- Certificate Generation Service
- Dissemination Service
- Revocation Management Service
- Revocation Status Service
- Subject Device Provision Service

with subjects as:
- Organisation and Compliance
- Risk assessment
- Policies, Practices, Terms and Conditions
- Key Management and Cryptographic Controls
- Trustworthy Systems and Device Certifications
- Logical Access Control
- Network and System Security
- Logging and Monitoring
- Asset management, Change Management, Incident management
- Human Resource Security
- Physical Security
- Business Continuity and TSP Termination

8.5 Actions taken as a result of deficiency

In case of a deficiency, MoD addresses this nonconformity in a Corrective Action Plan (CAP) in accordance with the Trust Service Provider Conformity Assessment requirements ETSI EN 319 403-1. In the CAP the actions and planning are documented to resolve the nonconformity.

9 Other Business and Legal Matters

9.1 Fees

No fees are included in this CPS.

9.1.1 Certificate issuance or renewal fees

No stipulation.

9.1.2 Certificate access fees

No stipulation.

9.1.3 Revocation or status information access fees

No stipulation.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

No stipulation.

9.1.6 Financial responsibility

See Section 9.2

9.2 Financial Responsibility

The TSP has taken adequate measures to cover the liability associated with the certification services. The recoverability of liability claims concerning these services is guaranteed by the financial position of the NL-MoD and, in a broader context, the State of the Netherlands (central government).

9.2.1 Insurance coverage

The NL-MoD has not taken out separate insurance for the certification services, since, in accordance with government policy, the State of the Netherlands does not insure itself.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiallity of business information

A risk analysis of the entire NL-MoD card service was carried out. This analysis resulted in a security measures implementation plan (IBP). See *Risicoanalyse Defensie* (Ministry of Defence risk analysis).

9.3.1 Scope of confidential information

The IBP specifies the way in which different types of information must be protected. This plan is confidential.

9.3.2 Information not within the scope of confidential information

The information used in the context of the NL-MoD card service is not classified or protectively marked.

9.3.3 Responsibility to protect confidential information

Responsibility for the protection of confidential information rests in the first instance with the process model owner, the Principal Director of Organisational Management (HDBV). D-JIVC as process model holder and the TSP are responsible in the second instance.

9.4 Privacy of Personal Information

The processing of personal data in the context of the NL-MoD card service is compliant with the General Data Protection Regulation EU 2016/679 (GDPR). The processing and the details of it are reported to the Data Protection Officer of the NL-MoD.

In the event that the information included in this chapter regarding the processing of personal data is contrary to the GDPR, this contrariety is unintended and the GDPR always prevails over this CPS.

Information about the processing of personal data is included in the instructions that is provided to every holder of a NL-MoD card and is written in internal regulations of the NL-MoD.

9.4.1 Privacy plan

An analysis of the processing of personal data was carried out. The considerations and findings are set out in the *Privacyanalyse rapportage* (privacy analysis report).

9.4.2 Information treated as private

Table 5 provides an overview of the most important personal data. The personal data type is specified in the first column. The following columns indicate where the datum is placed, i.e on the NL-MoD Card, in Certificates or in the NL-MoD card Management System (DBS). The purpose of this table is to provide an impression of the personal data used. The table does not constitute a set of instructions for the syntax of these data.

Personal data	Card	Certificate	DBS
Surname	x	x	x
Prefixes	x	x	x
Given names	x	x	x
Email address		x	x
Date of birth	x		x
Sex	x		x
Passport photograph	x		x
Employee number	x	x	x
Employment end date			x
Number and type of citizen identity document			x

Home address			x

Table 5. Overview of NL-MoD card personal data

The personal data are largely taken from the personnel system of the NL-MoD.
The purposes of processing personal data for the NL-MoD card can be summarised as follows:

1. facilitating the operating processes regarding guard duties, security, the granting of access and access checks by means of the NL-MoD Card, including authorisations;
2. by means of the NL-MoD Card, using public key infrastructure functions, namely:
   a. an electronic signature;
   b. confidentiality by encrypting data;
   c. identification and authentication;
3. managing the life cycle of NL-MoD cards, certificates and cryptographic keys. This life cycle starts with the application for NL-MoD cards, certificates and keys, proceeds through a number of phases and ends with revocation and putting out of operation.
4. Legal archiving requirements.

9.4.3 Information not deemed private

The published data of certificates can be readily consulted within the NL-MoD. The information provided regarding published and revoked certificates is limited to that stated in Chapter 7.

9.4.4 Responsibility to protect private information

An important starting point of the General Data Protection is that a body is always responsible for the processing of data. In certain cases, this body can be held liable by law for situations that are contrary to the law. In terms of the government of the Netherlands, this body is always the administrative body involved within the meaning of the General Administrative Law Act. At central government level, the individual ministers are deemed to be the responsible parties. For the NL-MoD, this party is therefore the Minister of Defence.

9.4.5 Notice and consent to use private information

Holders of NL-MoD cards have a right to inspect their personal data and to have these data corrected.

During the registration process, holders of NL-MoD cards are given the opportunity to inspect their personal data and suggest corrections. Corrections are processed through the personnel system of the NL-MoD.

9.4.6 Disclosure pursuant to judicial or administrative process

Release of information to investigating officers
If information that is not intended for publication is stored for the NL-MoD card service and this information is requested by a duly authorised investigating officer in the context of a criminal or disciplinary investigation, the information in question is released by the NL-MoD following the handing over of a legally valid demand.

Release of information for civil proceedings
If information that is not intended for publication is stored for the NL-MoD card service and this information is requested in the context of civil proceedings, the NL-MoD releases this information if, in the opinion of the TSP, compelling reasons do not militate against the provision of the information referred to. The NL-MoD card holder concerned is informed in advance of the provision of information.

9.4.7 Other information disclosure circumstances

With the exception of the cases referred to in Section 9.4.6 above, no certificates or other recorded data that belong to holders of NL-MoD cards are released to parties outside the NL-MoD without the express permission of the NL-MoD card holder concerned and the TSP.

Within the NL-MoD, certificates or other recorded data that belong to holders of NL-MoD cards are released subject to the condition that such release takes place for the purposes of data processing specified in Section 9.4.2.

9.5 Intellectual Property Rights

This CPS is the property of the State of the Netherlands (Ministry of Defence). Unaltered copies of this CPS may be distributed and published without permission provided that the source is acknowledged.

Ownership rights, including intellectual property rights, to the certificates and the NL-MoD card remain vested in the State of the Netherlands (Ministry of Defence) also after issue.

The NL-MoD guarantees to holders of NL-MoD cards that the certificates and NL-MoD cards issued by the TSP, including the associated documentation, do not infringe intellectual property rights vested in suppliers.

9.6 Representations and warranties

The structure of RfC 3647 does not provide for a description of the obligations of the parties involved. Regarding this CPS, the decision was made to include the obligations in Chapter 9 prior to a description of liabilities.

The obligations of holders of NL-MoD cards arise from their employment relationship with or official appointment at the NL-MoD.

9.6.1 CA representations and warranties

Obligations of the CA
The TSP is the party that is ultimately responsible for all aspects of the provision of certification services, including all items and services delivered by subcontractors.

More specifically, the TSP has the following obligations:
1. complying with the Organisation Person Domain CP (G3 hierarchy);
2. complying with this CPS;
3. performing all additional obligations that are stated in the certificates issued;
4. making certification services available to all categories of holders of NL-MoD cards and relying parties determined by the NL-MoD;
5. having in its possession accurately documented agreements and contractual relationships with third parties that provide the certification services;
6. in accordance with the change procedure described in Section 9.12, notifying parties in a timely manner of changes in the CPS and making the changes available to the parties involved;
7. guaranteeing that all necessary data are included in the certificate and that these data are accurate at the time of issue;
8. guaranteeing that the signatory identified in the certificate at the time of its issue was the holder of the data necessary for creating the electronic signature and that these data correspond with the information in the certificate or identity data for verification of the signature;
9. guaranteeing that all data for creating and verifying the signature can be used in a complementary manner;
10. guaranteeing that no errors will take place or incomplete data will be used during the creation and issue of certificates by the CA.

Liability of the CA

1. In principle, in its capacity as certification service provider, the TSP is liable for damage that natural persons or legal entities who or that reasonably trust in a certificate issued by the TSP and act on that basis suffer in connection with:
   a. the accuracy of all data included in the certificate at the time of its issue and for the inclusion of all data prescribed for this certificate;
   b. the fact that, on the date of issue, the person designated in the certificate as the signatory was the holder of the data necessary for creating an electronic signature, which is linked to the data in the certificate for the verification of electronic signatures;
   c. if both sets of data were generated by the TSP, the fact that the data for the creation of electronic signatures and the data for the verification of electronic signatures can be used in a complementary manner.
2. In principle, the TSP can also be held liable if it neglects to register the revocation of a certificate and update or publish the CRL and a relying party has acted in reasonable trust on the basis of the expectation of such registration.

9.6.2 RA representations and warranties

The RAs perform the services for which the TSP is responsible. The obligations of the TSP are described in the preceding section.

9.6.3 Subscriber representations and warranties

Each holder of a NL-MoD card must comply with the following obligations:

1. the holder of a NL-MoD card must comply with the requirements and procedures set out in this CPS, particularly with the requirement that the certificates issued for the holder be used only within the scope of application defined in Section 1.4 of this CPS;
2. the holder of a NL-MoD card must comply with the instructions communicated to him/her by the TSP at the time at which the NL-MoD card is issued or on a later date;
3. the holder of a NL-MoD card must provide accurate, complete and current data to the TSP, especially for the registration process;
4. the holder of a NL-MoD card must protect his/her card against damage, loss or theft;
5. the holder of a NL-MoD card must keep the PIN separate from the NL-MoD card and treat the PIN as confidential;
6. the holder of a NL-MoD card must report any actual or suspected abuse, risk of compromise, loss or theft of the NL-MoD card and/or PIN code immediately to the TSP. The holder of a NL-MoD card must immediately discontinue his/her use of certificates and keys in these cases;
7. the holder of a NL-MoD card must immediately inform the TSP if he/she discovers inaccuracies in the content of the certificates that he/she applied for.

9.6.4 Relying party representations and warranties

Those who rely on a certificate issued by the TSP are obliged to:

1. verify the validity of the certificate by means of the information published on the CRL or via the OSCP;
2. verify the signature of the certificate;
3. verify that the certificate validity period includes the current time.
4. check the authenticity of the CRL or OCSP;
5. check the validity of the hierarchy within which the certificate was issued, which means the validity of the certificates of the CAs higher in the hierarchy and of the root certificate of the State of the Netherlands;

6. verify that the CA certificate, which is used to validate the signature under a qualified certificate, is included in the EU Trusted List of Qualified Trust Service Providers (QTSP[3]). This is only applicable in order to rely on a signature certificate as an EU qualified certificate;
7. take due note of all obligations regarding use of the certificate as stated in this CPS, especially in terms of all restrictions regarding use of the certificate;
8. take all other precautions that can reasonably be taken by relying parties.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of Warranties

No stipulation.

9.8 Limitations of liability

The TSP places no restrictions on:

1. the use of the certificates issued by the TSP under this CPS within the scope defined in Section 1.4; and
2. the value of the transactions for which the certificates issued by the TSP under this CPS can be used within the scope defined in Section 1.4.

The limitations of liability included in this section are without prejudice to the operation of the Electronic Signatures Act.

The TSP's limitations of liability are as follows:

1. the TSP does not acknowledge liability for damage to natural persons or legal entities if the certificate is not used in accordance with the scope defined in Section 1.4 or if the restrictions stated in the certificate are breached;
2. the TSP does not accept liability for damage to natural persons or legal entities in the case of:
   a. damage resulting from a failure to comply with the obligations of holders of NL-MoD cards and/or relying parties described in this CPS;
   b. damage resulting from the use of a certificate after the certificate has been revoked;
3. to the extent that a relying party is deemed not to have reasonably trusted the certificate, the TSP accepts no liability towards that relying party for any form of damage suffered by him/her, even if he/she has complied with all other obligations, if the interests linked to the trust can be classified as being disproportionate relative to the level of reliability offered by the certificate;
4. the TSP may not be held liable on the grounds specified in Section 9.6.1 if the TSP can submit proof that the TSP did not act negligently.

9.9 Indemnities

To the extent that there are penalty clauses, these clauses are included in the contracts for the supply of cards and system integration concluded between GIT&Infra as a provider of CA services and subcontractors.

[3] https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/NL/8/5

9.10 Term and Termination

9.10.1 Term

This CPS shall remain valid until the TSP terminates its validity.

9.10.2 Termination

The TSP is the only party that may terminate the validity of this CPS. The TSP shall make a decision to terminate validity known on the website of the CA.

9.10.2.1 Consequences of termination of the CPS

No stipulation.

9.10.3 Effect of termination and survival

The provisions within this CPS terminate in the event of termination by MoD of its provision of PKIoverheid certificates.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

This CPS is subject to change. For example, changes in the policy recorded in the certificate policy document affect this CPS.

9.12.1 Procedure for amendment

Requests to change this CPS can be submitted by sending an email message to the central email address: Defensiepas.Certificatie.Autoriteit@mindef.nl.

Information management staff members assess and group these requests, after which the requests are submitted to TSP management.

The TSP can also initiate a change, for instance because of a change in legislation and regulations.

TSP management decides whether requests for changes are carried out. In the case of an approved request for a change, TSP also determines whether or not notification is necessary (see Section 9.12.2).

Changes to the CPS are carried out in grouped form to the greatest extent possible. Changes result in a higher version number and are reported to the relying parties.

Changes to the CPS take effect when the modified version of the CPS is published on the TSP's website.

9.12.2 Notification mechanism and period

All changes to this CPS will be made known on the TSP's website by publication of the most recent version.

9.12.3 Circumstances under which OID must be changed

In principle, changes to the CPS do not result in a change to the OID of this CPS.

9.13 Dispute Resolution Provisions

Procedure in the event of disputes
If a dispute arises concerning the interpretation of the provisions set out in this CPS or concerning the interpretation of the agreements concluded regarding certification services, a written notification can be sent as a "request for dispute resolution" to the central email address: Defensiepas.Certificatie.Autoriteit@mindef.nl.

The TSP will reply with a decision concerning the interpretation of the provisions. If this decision does not lead to a satisfactory result for all parties involved, the request will be dealt with in accordance with the procedures in force at the NL-MoD.

Procedure in the event of complaints
A complaint concerning the certification services must be submitted to the Ministry of Defence Service Desk (SDD).

9.14 Governing Law

The services of the CA, this CPS and the contracts concluded by the NL-MoD by reason of the certification services are governed by Dutch law.

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

No stipulation.

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

No stipulation.

10 Appendix 1. Abbreviations

This appendix includes the abbreviations used in the context of the NL-MoD card NL-MoD card service.

Abbreviation	In full
ABDO	*Algemene Beveiligingseisen voor Defensieopdrachten. Voorschriften voor het adequaat Beveiligen van Te Beschermen Belangen, Bijzondere Informatie in het bijzonder, die aan een partij buiten de Rijksdienst zijn toevertrouwd* – General Security Requirements for Defence Contracts. Regulations for the adequate Security of Interests to be Protected and Special information in particular that is entrusted to a party external to the civil service.
ADR	*Auditdienst Rijk* - National Audit Service
AO	*Administratieve Organisatie* - Administrative Organisation
AP	*Autoriteit Persoonsgegevens* - Dutch Data Protection Authority
BARD/AMAR	*Burgerlijk/Algemeen Militair Ambtenarenreglement Defensie* - Ministry of Defence Civil Service Regulations/General Military Personnel Regulations
BBC	*Basisvoorziening Betrouwbare Communicatie* - Basic Application for Reliable Communication
Beh	*Besluit elektronische handtekeningen* - Electronic Signatures Decree
CoDi	Corporate Directory
COMMIT	Commando Materieel en IT (Materiel and IT Command)
CPS	Certification Practice Statement
TSP	Trust Service Provider
DBS	*Defensiepas Beheer Systeem* - NL-MoD card Management System
DPS	Ministry of Defence Publication System
ETSI	European Telecommunications Standard Institute
FBO	*Functioneel Beheer Organisatie* - Information Management Organisation
FG	*Functionaris voor de Gegevensbescherming* - Data Protection Officer
FIF	*Functie Informatieformulier* - Job Information Form
GDPR	*General Data Protection Regulation* - algemene verordening gegevensbescherming
HSM	Hardware Security Module
I&A	Identification and Authentication
IA	*Interne Auditing* - Internal Auditing
IATO	Interim Approval To Operate
IBEV	*Informatiebeveiliging* - Information security
IBP	*Informatiebeveiligingsplan* - Information Security Plan
IP	*Implementatieplan* - Implementation Plan
IPS	*Internet Publicatie Systeem* - Internet Publication System
ISO	International Organization for Standardization
JIVC	*Joint InformatieVoorzieningsCommando* - Joint IT Command
MIVD	*Militaire Inlichtingen- en Veiligheidsdienst - Military Intelligence and Security Service*
NL-MoD	Netherlands Ministry of Defence
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
PIN	Personal Identification Number
PUK	Personal Unblocking Key
RDI	Rijksinspectie Digitale Infrastructuur - Radiocommunications Agency
RFC	Request For Change
SDD	*Service Desk Defensie* - Ministry of Defence Service Desk
SLA	Service Level Agreement
VGB	*Verklaring van Geen Bezwaar* - Certificate of No Objection

VMN	*Veiligheidsmachtingsniveau* - Security clearance level
Wid	*Wet op de identificatieplicht* - Compulsory Identification Act

11 Appendix 2. Documents

This list specifies the documents referred to in this CPS.

Ref. no.	Document
1	• PKI-O dienstverlening Ministerie van Defensie • Rapport Proces Risicoanalyse Defensiepas • Rapport Technische Risicoanalyse Defensiepas
2	Besturen bij Defensie
3	Belegging TSP verantwoordelijkheid JIVC
4	Calamiteitenplan Certificatie Autoriteit