Defensie Materieel Organisatie
Ministerie van Defensie

Certification Practice Statement

for the Ministry of Defence Card Generation 2 (G2)

Certification Authority

Signature Page

Secretary General Directions DBB A009 *Verantwoordelijkheden en bevoegdheden Defensiepas 20171205* (Responsibilities and authorities Ministry of Defence Card) place Trust Service Provider (TSP) responsibility with the Principal Directorate of Operational Management and, in the context of this responsibility, authorise the Director of Joint IT Command (D-JIVC). The Director of Joint IT Command has placed TSP responsibility with the Head of the Generic IT & Infrastructure Department.

The Head of the Generic IT & Infrastructure (GIT&Infra) Department agrees to the content of the Certification Practice Statement (CPS) for the Ministry of Defence Card services.

A.G. van der Sanden
Head JIVC/GIT&Infra
Netherlands Ministry of Defence

Signature:

Antonius G J van der Sanden

Digitaal ondertekend door Antonius G J van der Sanden
Datum: 2020.03.09 16:37:33 +01'00'

Status	Definitive
Version	2.10.4
Date	March 1, 2020

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

2.10.1	25-07-2019	Changes following from Corrective Action Plan, update of department name.
2.10.2	25-09-2019	Changes following from CAP/PAP
2.10.3	17-10-2019	Corrections
2.10.4	01-03-2020	Preparation expiration G2 CA hierarchy

1 Introduction to the CPS

The Ministry of Defence makes an identity card (*Identiteitsbewijs Krijgsmacht*) available to its employees. This identity card contains certificates that make it possible for employees to use digital services. For this purpose, the Ministry of Defence 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). The Ministry of Defence has its own Trust Service Provider (TSP) that issues these certificates and guarantees their reliability. Ultimate TSP responsibility rests with the following organisation: Defence Materiel Organisation, Joint IT Command, Head of Generic IT & Infrastructure (DMO/JIVC/GIT&Infra).

1.1 Outline of the Certification Authority

The identity of the holder of a Ministry of Defence Card is checked during the application process, i.e. before the card is made available to the person who applied for it. The applicant must report in person. The Ministry of Defence Card is only made after the applicant has done so. The Ministry of Defence Card contains proof of identity in the form of electronic certificates. In this document, the "Ministry of Defence Card" means the Ministry of Defence Card in its entirety, i.e. both the physical and electronic components of the card.[1]

The TSP issues certificates that enable a holder of a Ministry of Defence Card to identify himself/herself ("authenticity certificate"), place an electronic signature that is recognised by law ("signature certificate") and encrypt data ("confidentiality certificate"). Type 1 and Type 2 Ministry of Defence 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 Ministry of Defence. The software (application) installed to perform activities determines which functions can actually be used.

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 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.

Generation 2 of PKI-O will expire in 2020. Therefore Generation 2 of the Ministry of Defensie Implementation will expire at March 23, 2020. After that date, all currect issued certificates at the Ministry of Defence Cards will be expired at March 23, 2020. Currently Generation 3 of PKI-O is operational and Ministry of Defence is implementing Generation 3 of it's PKI-O implementation. For Generation 3, a new CPS version 3.1 will be published. This CPS Generation 2 contains provisions to dismantle the Generation 2 infrastructure.

1.2 Purpose of and references to the Certification Practice Statement

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 Ministry of Defence Card with certificates.

[1] Only Type 1 and Type 2 Ministry of Defence Cards have certificates.

This CPS underpins the trust that holders of Ministry of Defence 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 Ministry of Defence Card, the Organisation Domain CP (G2 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: "RfC 3647: not determined for the certification services of the Ministry of Defence."

This CPS describes the way in which the requirements set out in the Organisation Domain CP (G2 hierarchy) have been met.

The Organisation Domain CP (G2 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 Ministry of Defence, 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 domain.
Signature	2.16.528.1.1003.1.2.5.2	OID of the PKI-O Certificate Policy for signature certificates in the Organisation domain.
Confidentiality	2.16.528.1.1003.1.2.5.3	OID of the PKI-O Certificate Policy for confidentiality certificates in the Organisation domain.

Table 1. G2 hierarchy – Organisation Domain CP OIDs

1.2.3 References to this CPS

This CPS is available on the TSP's website.

Internet address (link)	https://cps.dp.ca.mindef.nl/ips/cps.jsp
OID	2.16.528.1.1003.1.3.2.6

Table 2. References to this CPS

1.3 Parties involved

The TSP of the Ministry of Defence is organised within the ministry in accordance with the Secretary General Directions 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 as a whole is the sole customer 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 Ministry of Defence Cards and the relying parties. The respective roles of these parties are explained below.

1.3.1 Supplier of TSP services

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). Within the Ministry of Defence, DMO/JIVC/GIT&Infra is the TSP.

There is strict segregation between the three roles:
- ownership rests with the DMO director;
- commissioning rests with the JIVC director;
- TSP rests with C-GIT&Infra.

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

1.3.2 Registration Authority

The RA function is delegated to the operational branches of the NL-MoD according to General Directions A009. RA duties are performed by Ministry of Defence 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 Ministry of Defence Cards and publish certificates.

1.3.3 Holders of Ministry of Defence Cards

The Ministry of Defence 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 Ministry of Defence Card. In this CPS, preference has been given to the term holder of a Ministry of Defence Card.

In terms of the PKI-O, a holder of a Ministry of Defence 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 Ministry of Defence Card (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 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 parties involved

RfC 3647: not determined for the certification services of the Ministry of Defence.

1.4 Use of a certificate

Private keys issued by the TSP are always and exclusively used by holders of Ministry of Defence Cards who are acting on behalf of the Ministry of Defence. The foregoing therefore expressly excludes private use of the private keys.

1.4.1 Appropriate use of a certificate

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 Use that is prohibited

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 Ministry of Defence 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 Ministry of Defence Card.

1.5 Management of the CPS

In accordance with the Ministry of Defence Control Model,[ref 2] JIVC is tasked with TSP management. TSP responsibility rests with JIVC/ H-GIT&Infra.[ref 3].

1.5.1 Party responsible for the management of this CPS

The CPS is issued under the responsibility of the TSP.

1.5.2 Contact details

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 Conformity of the CPS with the CPs

Assessment of the conformity of this CPS with the Organisation domain (G2 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 at
https://cps.dp.ca.mindef.nl/ips/certificeringen

1.6 Abbreviations/acronyms and definitions

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

2 Publication and Electronic Storage Locations

The TSP publishes information at a number of locations on the Ministry of Defence intranet and on the internet.

2.1 Electronic storage locations

In principle, there are five locations: the general website of the Ministry of Defence on the intranet and on the internet, the Corporate Directory of the Ministry of Defence, a Ministry of Defence Publication System (DPS) and an Internet Publication System (IPS on the internet at https://certs.ca.mindef.nl/ips).

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

For the Organisation Domain CP (G2 hierarchy), see the PKI-O website at Logius.

2.2 Publication of TSP information

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

G2 Information	**INTERNET/INTRANET URLs**
CPS:	
Ministry of Defence CA – G2	https://cps.ca.mindef.nl/ips/cps.jsp
Ministry of Defence Card CA – G2	https://cps.ca.mindef.nl/ips/cps.jsp
Certificates:	
Ministry of Defence CA – G2	https://certs.ca.mindef.nl/mindef-ca-2.cer
Ministry of Defence Card CA – G2	https://certs.dp.ca.mindef.nl/mindef-ca-dp-2.cer
Certificate Revocation Lists:	
Ministry of Defence CA – G2	http://crls.ca.mindef.nl/mindef-ca-2.crl
Ministry of Defence Card CA – G2	http://crls.dp.ca.mindef.nl/mindef-ca-dp-2.crl
OCSP Online Certificate Status (intranet)	http://ocsp.dp.ca.mindef.nl:8777

Table 4. TSP information locations

2.3 Time or frequency of publication

The published TSP information is 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 to published information

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 of the holder of the Ministry of Defence Card.

3.1.1 Types of name formats

The name of the holder of the Ministry of Defence Card is always and exclusively taken from PeopleSoft, the Ministry of Defence personnel system (the source system). The name of the holder of the Ministry of Defence Card consists of characters from the Unicode Latin series. An explanation of the further content of the certificates is included in Chapter 7.

3.1.2 Meaningful names

RfC 3647: not determined for the certification services of the Ministry of Defence.

3.1.3 Anonymity or pseudonymity

Anonymity or the use of a pseudonym is not supported.

3.1.4 Rules for the interpretation of name formats

RfC 3647: not determined for the certification services of the Ministry of Defence.

3.1.5 Unicity of names

The TSP guarantees that the name of the holder of the Ministry of Defence 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 Ministry of Defence Card. This exclusiveness is achieved by adding an employee number to the name.

3.1.6 Recognition, authentication, trademarks

RfC 3647: not determined for the certification services of the Ministry of Defence.

3.2 Initial identity validation

The identity of the holder of the Ministry of Defence Card is initially validated by means of the processes described in the subsections of Section 3.2.

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 Ministry of Defence 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 the organisational identity

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

3.2.3 Authentication of the personal identity

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.

Authentication at the card provider
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 personal identity of the holder concerned.

3.2.4 Information about the certificate holder that has not been checked

RfC 3647: not determined for the certification services of the Ministry of Defence.

3.2.5 Authorisation of an application for a certificate

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 Ministry of Defence Card Management System (DBS) enforces the segregation of duties. The person who has applied for a Ministry of Defence Card may not be the person who authorises the application.

3.2.6 Criteria for interoperability

RfC 3647: not determined for the certification services of the Ministry of Defence.

3.3 Identification and authentication when a certificate is renewed

If the end of a Ministry of Defence Card's term of validity is imminent or if the Ministry of Defence 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 in the case of routine renewal

When an application for a new Ministry of Defence Card has been authorised, a new key pair is always generated and a new Ministry of Defence Card is always issued. If the end of the term of validity of a Ministry of Defence Card with certificates is imminent or if the Ministry of Defence Card is defective, the manager of the Ministry of Defence Card (not the holder of the card himself/herself) may apply for a new Ministry of Defence 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 in the case of renewal following revocation

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

3.4 Identification and authentication in the case of a revocation request

Requests for the revocation of certificates are linked to the revocation procedure that applies to Ministry of Defence Cards. Revocation requests are a regular part of the process by which replacement Ministry of Defence Cards are provided. The certificates of the old Ministry of Defence Card are revoked before the new Ministry of Defence Card is provided. The holder of the Ministry of Defence Card does not have to submit a separate request for this purpose. The Ministry of Defence Card provider signs in to the DBS using the Ministry of Defence Card and PIN.

In the event of circumstances by reason of which a Ministry of Defence 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 Ministry of Defence 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 Ministry of Defence Card in question contacts the reporting centre within the Ministry of Defence by telephone. The role of reporting centre is fulfilled by the Ministry of Defence 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 Ministry of Defence 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 *Servicecenter* and subsequently sends an email confirmation that the certificates have been revoked to the holder of the Ministry of Defence 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 Ministry of Defence, enforcing the access policy is of greater importance than the potential drawbacks of wrongly revoking Ministry of Defence Cards.

4 Operational Requirements and Certificate Life Cycle

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

4.1 Applying for certificates

Applications for certificates are always linked to applications for Ministry of Defence Cards. Applications for Ministry of Defence Cards are submitted by the card manager. Holders of Ministry of Defence Cards must always be registered in the Ministry of Defence personnel system before an application can be accepted for processing.

The card manager checks whether the holder of a Ministry of Defence Card is entitled to a Ministry of Defence Card and whether the data have been recorded correctly.

The desired location at which and the date on which the card is to be provided are also recorded. Furthermore, it is stated whether or not the certificates must also be published in IPS.

A digital photograph of the holder of the Ministry of Defence Card is then added to the Ministry of Defence Card application details, which are largely taken from the Ministry of Defence personnel system. The intended holder of the Ministry of Defence Card must report to the designated photographer for this purpose. The holder of the Ministry of Defence 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 Ministry of Defence 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 Ministry of Defence personnel system. This will result in an altered application for a Ministry of Defence Card.

Applying for Generation 2 certificates will remain possible until Generation 3 becomes operational. When Generation 3 is operational, all issued Generation 2 certificates will be replaced by Generation 3 certificates by replacing all Ministry of Defence Cards. From that moment on all new initial application will be issued by Generation 3 certificates.

As of Dec 1, 2019, no applications for Generation 2 certificates are accepted. From that date, only Generation 3 applications are allowed. For Generation 3 certificates, see the CPS G3 Certification Authority Ministry of Defence.

4.1.1 Authorised certificate applicants

Applications for certificates are linked to applications for Ministry of Defence Cards, which are entered into the DBS by authorised actors.

4.1.2 Granting of mandates to certificate applicants

All Ministry of Defence employees who carry out Ministry of Defence 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 Ministry of Defence organisational units are also responsible for reviewing the list of actors and submitting authorisation requests on time.

4.2 Processing applications for certificates

Applications for certificates are always linked to applications for Ministry of Defence Cards.

4.2.1 Performing identification and authentication checks

The checks that are performed to verify the identity of the holder of a Ministry of Defence Card are described in Chapter 3 (Identification and Authentication).

4.2.2 Approving applications for certificates

The production process starts after the card authoriser has attached his/her approval to the Ministry of Defence Card application. See also Section 3.2.5.

4.2.3 Period for processing applications for certificates

The delivery period (as defined beforehand bij The Ministry of Defence) regarding a Ministry of Defence Card is subsequently laid down in the service level agreement concluded with the supplier.

4.3 Issuing certificates

Certificates are always linked to Ministry of Defence Cards.

4.3.1 Actions of the TSP when issuing certificates

Ministry of Defence Cards are received at the location at which they are provided to holders. The Ministry of Defence Cards are stored in a locked/secure space (safe/cabinet). The space in which the Ministry of Defence 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 Ministry of Defence Card. The holder of the Ministry of Defence Card must appear in person before the card provider with his/her PIN letter and WID document to obtain his/her Ministry of Defence Card. The card provider verifies the identity of the holder of the Ministry of Defence Card by means of the WID document.

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

The Ministry of Defence Card must be activated before it is handed over to the holder. To this end, the holder must enter the PIN in the presence of the card provider, after which the Ministry of Defence Card is activated and a few additional details are automatically entered into the Ministry of Defence Card.

The Ministry of Defence Card is not issued if the outcome of any one of the checks, such as the identity check, for example, is negative. The Ministry of Defence Card is also not issued if the holder does not have the right PIN or does not have an old Ministry of Defence Card, an official report or a declaration of loss.

4.3.2 Reporting the issue of certificates to the certificate holder

The certificates that belong to a Ministry of Defence Card are provided to the holder through the card itself. A Ministry of Defence Card must be activated by means of the PIN before it is handed over to its holder. The holder of a Ministry of Defence Card is also required to sign a user agreement in duplicate. This method ensures that the holder of a Ministry of Defence Card is aware of the issue of his/her certificates.

4.4 Acceptance of certificates

The certificates that belong to a Ministry of Defence Card are provided to the holder through the card itself.

4.4.1 Activities associated with the acceptance of certificates

The holder must sign the delivery receipt before he/she takes delivery of the Ministry of Defence Card. See also Section 4.3.1.

4.4.2 Publication of the certificate by the TSP

The TSP publishes the certificates internally within the Ministry of Defence in the CoDi. By default, the certificates are not published on the internet in the IPS (see Section 4.1). Users and/or their managers can request for publication on the internet.

4.4.3 TSP reporting to other parties involved regarding the issue of certificates

RfC 3647: not determined for the certification services of the Ministry of Defence, usage is not allowed for private purposes.

4.5 Key pair and use of a certificate

Private keys issued by the TSP are always and exclusively used by holders of Ministry of Defence Cards who are acting on behalf of the Ministry of Defence.

4.5.1 Use of the private keys and certificates of the certificate holder

The permitted use of the private keys and certificates of holders of Ministry of Defence Cards is described in Section 1.4.

4.5.2 Obligations of the relying parties

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 Routine renewal of the certificate

In the case of routine renewal of a Ministry of Defence Card, the manager of the Ministry of Defence Card may apply for a replacement Ministry of Defence Card. The application 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).

4.7 Renewal of the certificate and the keys

Public keys are never recertified. When an application for a new Ministry of Defence Card has been authorised, a new key pair is always generated and a new Ministry of Defence Card is always issued.

4.8 Alteration of the certificate

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

4.9 Revocation and suspension of certificates

Requests for the revocation of certificates are linked to the revocation procedure that applies to Ministry of Defence Cards.

When Generation 3 of the NL-MOD PKI-O becomes operational, during migration towards G3 certificates, G2 certificates will automatically be revoked by the TSP. After G3 implementation, only revocation services and validation services of G2 will remain operational until G2 will expire. After expiration of G2 the last generated Revocation List (date appr March 23, 2020) will remain available

until april 30, 2020. The nextUpdate field in the last generated Revocation List will not be set to '99991231235959Z'

4.9.1 Circumstances that result in revocation

Revocation of certificates that are in use takes place on a regular basis if a replacement Ministry of Defence Card is provided. This section describes the cases in which a Ministry of Defence 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 Ministry of Defence Card with new certificates is applied for. The certificates in use are revoked prior to the issue of this new Ministry of Defence Card.

Immediate revocation of the Ministry of Defence Card occurs in the following cases:

- the subscriber (NL-MoD) states that the original application for a Ministry of Defence 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 Ministry of Defence Card key;
- the holder of the Ministry of Defence Card fails to perform his/her obligations as set out in the CPS of the TSP or the agreement that the TSP concluded with the holder of the Ministry of Defence Card;
- 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 Ministry of Defence Card was not issued in accordance with this CPS of the TSP or the agreement that de TSP concluded with the holder of the Ministry of Defence Card;
- 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 Ministry of Defense Card, relaying parties and third parties (browser parties, for example);
- revocation is necessary because of an incident or emergency.

4.9.2 Parties that may submit a revocation request

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

- the card provider;
- the holder of the 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 Revocation request procedure

In addition to revocation requests associated with the issue of replacement Ministry of Defence 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 within four 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 Ministry of Defence 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 Ministry of Defence.
3. If the holder of the Ministry of Defence Card no longer possesses the Ministry of Defence 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. Ministry of Defence Cards that are physically handed in are deactivated and subsequently permanently destroyed in a separate procedure.

4.9.4 Period within which the certificate holder must submit a revocation request

The brochure that is provided to every holder of a Ministry of Defence Card states that a holder must immediately report the loss or theft of his/her Ministry of Defence Card to the reporting centre.

4.9.5 Revocation request processing time

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

4.9.6 Compulsory checks regarding certificate status information

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.

These obligations are included in Section 9.6 of this CPS.

4.9.7 CRL frequency

The CRL is issued at least once every four hours. Each revocation results in a new CRL that is immediately published. The last CRL created will be published until April 30, 2020. The nextUpdate field in the last generated Revocation List will not be set to '99991231235959Z'

4.9.8 Maximum delay regarding 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 Online revocation/availability status check

Within the Ministry of Defence, the TSP provides an Online Certificate Status Protocol (OCSP) service. This online service makes it possible to check the status of a certificate. The OCSP server receives the availability information in the form of CRLs that are updated every 10 minutes. 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 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 Online revocation/requirements status check

RfC 3647: not determined for the certification services of the Ministry of Defence.

4.9.11 Availability of other forms of revocation/status information

RfC 3647: not determined for the certification services of the Ministry of Defence.

4.9.12 Special requirements with respect to a compromised key

RfC 3647: not determined for the certification services of the Ministry of Defence.

4.9.13 Suspension of a certificate

The Ministry of Defence 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 service

Relying parties can check the status of certificates.

4.10.1 Description of the certificate status service

Relying parties can check the validity of certificates using a CRL, both internally within the Ministry of Defence by means of the DPS and externally by means of the IPS. The OCSP service is also available within the Ministry of Defence.

4.10.2 Availability of the certificate status service

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 Ministry of Defence. 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 of the certificate status service

RfC 3647: not determined for the certification services of the Ministry of Defence.

4.11 Termination of the subscription

The Ministry of Defence Card service is not provided in the form of a subscription.

4.12 Key escrow and recovery

During the production of a Ministry of Defence Card, a copy of the private key that belongs to the confidentiality certificate of the holder of the Ministry of Defence 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 implementation

Key escrow:

The private confidentiality keys of holders of Ministry of Defence 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.

When the black box was used for the production of Generation 1 (G1) Ministry of Defence Cards, the black box was provided, on a once-only basis, with the aforementioned public G1 key of the DBS in accordance with the management procedure described above. When the black box is used for the production of Generation 2 (G2) Ministry of Defence Cards, the public G2 key of the DBS is added in accordance with the same procedure. The G1 and G2 key pairs for key escrow are generated at another Ministry of Defence site in the Hardware Security Module (HSM) of the DBS using a Key Management System (KMS). This also takes place in accordance with a key procedure under which, among other things, a shared password for the HSM must be entered by two individuals (”four eyes principle”). The two parts of the password are kept in two separate, sealed envelopes which are themselves kept in a safe at a Ministry of Defence site.

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 keys: policy and implementation

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 Ministry of Defence is documented. This documentation is classified as confidential.

5 Physical and Procedural Control Measures

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

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

5.1 Physical control measures

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

5.1.1 Sites

The registration activities and activities relating to the provisioning are performed at Ministry of Defence sites in the Netherlands and outside the Netherlands. The central DBS is in the data centre of GIT&Infra. Ministry of Defence 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 control

These measures are taken on the basis of risk analyses and security plans. The measures taken for the Ministry of Defence 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 supply and air conditioning

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

5.1.4 Water management

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

5.1.5 Protection against fire

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

5.1.6 Storage resources

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 Backups outside the location

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

5.2 Procedural control measures

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

5.2.1 Confidential roles

Within the Ministry of Defence, 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 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 confidential roles

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 Segregation 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 Ministry of Defence Card application process.

5.3 Personnel control measures

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

5.3.1 Training and experience requirements; screening 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 Security screenings

Potential Ministry of Defence 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 Ministry of Defence 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 Continuous education: frequency and requirements

RfC 3647: not determined for the certification services of the Ministry of Defence.

5.3.5 Job rotation: order and frequency

RfC 3647: not determined for the certification services of the Ministry of Defence.

5.4 Disciplinary process

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).

5.4.1 Requirements that external suppliers must comply with

The external suppliers are appropriately certified (ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 401) 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.

5.4.2 Job descriptions

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.

5.5 Audit log 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.

5.5.1 Type of information 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 Ministry of Defence 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 Ministry of Defence 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 Ministry of Defence 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.

5.5.2 Frequency with which audit log files are handled

Log files are regularly analysed in accordance with the management protocols drawn up for the certification services. After expiration of the CA repetitive log file handling will be stopped. Log files will be archived for possible later investigations.

5.5.3 Retention period of the audit log files

The archiving system retains the archived audit log files for a period of at least seven years.

5.5.4 Protection of the audit log files

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.

5.5.5 Backup procedures of the audit log files

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

5.5.6 Position of the collection system of audit log files

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

5.5.7 Notification to the party that caused a logged event

RfC 3647: not determined for the certification services of the Ministry of Defence.

5.5.8 Analysis of the audit log files

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

5.6 Archiving procedures

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

5.6.1 Type of information 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.

5.6.2 Retention period of the archive

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

5.6.3 Protection of the 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.

5.6.4 Backup procedures of the archive

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.

5.6.5 Requirements that apply to time stamping of the log 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).

5.6.6 Position of the collection system of the archive files

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.

5.6.7 Procedures for consulting the archive

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

5.7 Procedures for renewing the TSP key

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.

5.8 Disruptions and continuity

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

5.8.1 Procedures for handling incidents and disruptions

Incidents can be reported to the Ministry of Defence 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 Ministry of Defence Cards as soon as possible by publishing information about the situation on the Ministry of Defence intranet;
- the TSP will immediately revoke the certificates concerned and publish on the applicable CRL;
- the TSP will inform the Policy Authority of PKI-O of the emergency and further developments in that regard.
- The TSP will inform Agentschap Telecom (AT) of the emergency and further developments in that regard.
- The TSP will inform the audit organisation of the emergency and further developments in that regard.

5.8.2 IT environment recovery procedures

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 fall back locations.

5.8.3 Recovery procedures in the case of compromised keys of certificate holders

If the keys of holders of Ministry of Defence Cards are compromised, revocation requests are submitted as described in Section 4.9. A new Ministry of Defence Card can be applied for following revocation. The holder will receive new keys as a result of this new application.

5.8.4 Business continuity plan

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

5.9 Termination of TSP services

One of the reasons to stipulate the terminiation 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 Defense 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 were terminated. Deliberatly (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 Defense.

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

Specific activities will include at least the following:
1. informing the holders of Ministry of Defence Cards, relying parties and other parties with which agreements have been concluded about the intended termination of services;
2. inform the supervisory body Agentschap Telecom (AT) 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. putting the private keys of the Certification Authorities (CAs) out of operation;
6. retaining registration information, audit log files and CRLs in accordance with the applicable requirements.

6 Technical Security

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 CWA 14167-1, Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements and/or 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 Generating and installing key pairs

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

6.1.1 Generation of key pairs

The keys of the TSP and holders of Ministry of Defence Cards are centrally generated.
These keys are generated in a FIPS 140-2-certified HSM. The signature algorithm SHA256RSA is used for Ministry of Defence Cards issued under the G2 hierarchy. The hash algorithm used is SHA256.

6.1.2 Transfer of private key to the certificate holder

The Ministry of Defence Card is personally handed over to its holder at the location duly designated for the purpose. The PIN is sent separately in the form of a PIN letter to the private address of the holder of the Ministry of Defence Card. The letter is marked as personal.

6.1.3 Transfer of public key to the CA

RfC 3647: not determined for the certification services of the Ministry of Defence.

6.1.4 Transfer of the public key of the TSP 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

G2 hierarchy:
https://certs.ca.mindef.nl/mindef-ca-2.cer
and
https://certs.dp.ca.mindef.nl/mindef-ca-dp-2.cer

See Chapter 2.2.

6.1.5 Key lengths

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 Ministry of Defence Card is 2048 bits, asymmetric RSA.

6.1.6 Generation of the public key: key material and quality control

The public key is generated in accordance with the requirements as described for the Organisation Domain CP (G2 hierarchy) and that apply to the cryptographic products concerned. These products comply with CWA 14167-1 and/or CEN/TS 419261.

6.1.7 Purposes of key use [X.509 v3]

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 Control measures regarding private keys and cryptographic modules

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

The TSP will monitor the validity of the sscd at least on an annual interval. Also for this reason, TSP shall discuss the validity with it's vendors during service level meetings, tactical meetings and/or strategic meetings. TSP shall initiate renewal or replacement.

6.2.1 Current standards

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 Four eyes principle

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.

6.2.3 Escrow of private keys

Not all keys of the TSP are held in escrow.

6.2.3.1 Escrow of private keys of the TSP

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

6.2.3.2 Escrow of private keys of certificate holders

The TSP holds the private key of the confidentiality certificate of all Ministry of Defence Cards in escrow. These copies are currently not used. See Section 4.12 in this regard.

6.2.4 Backups of private keys

Backups are made of the private keys of the CAs of the Ministry of Defence.

6.2.4.1 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.

6.2.4.2 Backups of private keys of certificate holders

The TSP makes a backup of the private confidentiality key of all Ministry of Defence Cards and holds this backup in escrow.

6.2.5 Archiving of private keys

Not all private keys of the TSP are archived.

6.2.5.1 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.

6.2.5.2 Archiving of the private keys of certificate holders

Private keys of signature and authenticity certificates of holders of Ministry of Defence 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 Ministry of Defence Card is held in key escrow.

6.2.6 Transfer of the private keys from and to cryptographic modules

The keys of holders of Ministry of Defence Cards are placed in the cards immediately after they have been generated. The private key does not leave the Ministry of Defence Card after that time. The private confidentiality key is also held in key escrow.

6.2.7 Storage of private keys in cryptographic modules

The private keys of holders of Ministry of Defence Cards are stored in those cards. The Ministry of Defence Card is manufactured in accordance with the CWA 14169 standard for smart cards (SSCDs, or secure signature creation devices of the type "EAL 4+").

The G2 Ministry of Defense Cards do not contain a QSCD. They are implemented before eIDAS and NEN-EN 419211. The used SSCD is certified with no end-date of certification.

6.2.8 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.

The appropriate PIN must be entered to activate the private keys of a Ministry of Defence Card. These keys must be activated for each session.

6.2.9 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 Ministry of Defence Card is linked to the process by which Ministry of Defence Cards are withdrawn, certificates are revoked and, if appropriate, Ministry of Defence Cards are physically destroyed.

6.2.10 Method used to destroy the private keys

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

6.2.10.1 Requirements that apply to the Ministry of Defence Card as a cryptographic module

The Ministry of Defence Card is manufactured in accordance with the CWA 14169 standard for smart cards (SSCDs, or secure signature creation devices of the type "EAL 4+").

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 Archiving of public keys

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 Service life of certificates and keys

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 Ministry of Defence Cards, certificates and keys issued from 01 April 2012 is set at three years. The Ministry of Defence is migrating to third-generation PKI-O. As a result, after 22 March 2017, the Ministry of Defence will issue certificates that are valid for a shorter period of time than the three years referred to above. The service life of the certificates will never extend beyond 22 March 2020. The period of validity will again be three years as soon as the G3 certificates become available.

6.4 Activation data

The following measures have been taken to minimise the likelihood of Ministry of Defence Card activation data being compromised.

6.4.1 Generation and installation of activation data

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

6.4.2 Protection of activation data

The PIN is made known to the holder of the Ministry of Defence 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 Ministry of Defence Card. It is securely stored by the CA.

The holder of the Ministry of Defence Card is personally responsible for protecting the PIN after he/she has received it.

A Ministry of Defence Card is blocked if an incorrect PIN is entered five times. The holder of the card must contact the CA 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

RfC 3647: not determined for the certification services of the Ministry of Defence.

6.5 Control measures regarding computer systems

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

6.5.1 Technical security 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

Ministry of Defence Card service. Reliability levels are defined in detail with suppliers and laid down in service level agreements (SLAs).

6.5.2 Assignment of security level

The systems and data of the TSP are classified on the basis of a risk analysis and current regulations and policy. This classification is regularly assessed and altered if necessary. A number of systems must also meet the CWA 14167-1 requirements for trustworthy systems and or CEN/TS 419261. See Section 9.3.

6.6 Control measures regarding technical life cycle

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

6.6.1 Control measures for system development

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 Control measures regarding security management

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

6.6.3 Classification of the security level

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 control measures

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 CSP* (CSP 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 Ministry of Defence were compiled in accordance with the PKI-O profiles as prescribed in the Organisation Domain CP (G2 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 Ministry of Defence 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 Ministry of Defence 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 Ministry of Defence Card, they are as follows:

1. Ministry of Defence CA: this is a CA that only issues the certificate of the subordinate CA. The certificate profile (Figure 1 (1)) of this CA is determined by PKI-O, which is also responsible for the associated CRL profile (Section 7.2);
2. Ministry of Defence, Ministry of Defence Card CA: this is a CA that issues the certificates of holders of Ministry of Defence Cards. A certificate profile has been prepared for this CA's own certificate (Figure 1 (2)). If this CA's own certificate is revoked, the revocation is recorded on a CRL, for which a profile has been adopted (Section 7.2);
3. Ministry of Defence Card certificate profiles: these are the profiles of the certificates of holders of Ministry of Defence Cards for authenticity, signature and confidentiality (5). Revoked certificates are made known by means of a CRL and through an OCSP service. A CRL profile (6) and an OCSP profile (Section 7.3) have been prepared.

Figure 1 shows the CA hierarchy for the G2 hierarchy. The Ministry of Defence Card certificates are also shown at the lowest level.

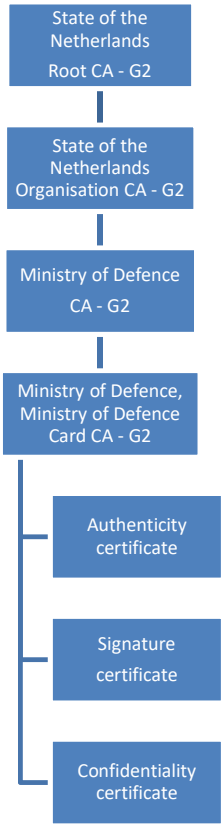

Figure 1. CA hierarchy

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

7.1 Certificate profiles

The certificate profiles of the State of the Netherlands Root CA certificate and the State of the Netherlands Organisation CA certificate 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 Ministry of Defence CA certificate (Figure 1).

The certificate profile of the Ministry of Defence Card CA (Figure 1), on the other hand, is the responsibility of the Ministry of Defence CA (Figure 1).

The composition of the certificates of holders of Ministry of Defence Cards for authenticity, signature and confidentiality (Figure 1) is of direct importance to holders of Ministry of Defence 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 Certificatie Autoriteit Defensiepas – G2* (Ministry of Defence, Ministry of Defence Card Certification Authority - G2 hierarchy).

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

After the period of three years has elapsed, users receive new cards with new G2 certificates that are valid for three years.

The amount of personal data on the Ministry of Defence Card and in the certificates is limited for privacy reasons, since certificates are intended for wide distribution. In fact, only personal data that do not exceed risk category I, i.e. basic level, according to the AV23 guidelines of the Dutch Data Protection Authority (AP) are included.

The personal data in the certificates are as follows: the given names and surname of the holder of the Ministry of Defence 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.

7.2 CRL profiles

The Certificate Revocation List (CRL) is a list of revoked certificates. The OCSP services include such a list. At the Ministry of Defence, 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 two different CRLs, the CRL in which the revoked certificates of the issuing CA are recorded and the CRL in which the status of the certificates of the holders of Ministry of Defence Cards can be checked.

Both CRL profiles were prepared in accordance with the Organisation Domain CP (G2 hierarchy) of PKI-O.

Furthermore, the date and time of issue and the period of validity of each CRL are stated. The period of validity of the CRL for the issuing CA is 24 hours. The period of validity of the CRL for certificates of holders of Ministry of Defence Cards is also 24 hours. As of end March 22, 2020 the last CRL will have an indefinite validity. After this date, no new CRL's are created since the CA will expire at that date. The last CRL will be published until April 30, 2020.

The period of validity of the CRL of the Ministry of Defence CA is one month.

7.3 OCSP profiles

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, Ministry of Defence Card CA).

OCSP provides a list of revoked certificates that can only be consulted online within the Ministry of Defence. The OCSP will be stopped at the end of March 22, 2020.

8 Conformity Assessment

The certification services of the TSP of the Ministry of Defence were certified by BSI on the basis of the framework defined by ETSI EN 319-411-1, ETSI EN 319 411-2, ETSI EN 319 401 and ETSI EN 319 403, and complies with PKI-O model 3a, version 4.7.

The conformity certificates of the most recent audits are available at the electronic storage location of the PKI-O Policy Authority. The TSP also complies with the PKI-O's system of standards as set out in the schedule of requirements (see https://www.logius.nl/producten/toegang/pkioverheid/).

The TSP of the Ministry of Defence is registered as certification service provider at Agentschap Telecom.

The quality of the Ministry of Defence Card service is also regularly audited by the National Audit Service (ADR) of the Netherlands 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 319 411-1, ETSI EN 319 411-2, ETSI EN 319 401, ETSI EN 319 403 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 Ministry of Defence Card with certificates. Complementary internal checks are carried out at the locations at which Ministry of Defence Cards are provided. These checks are aimed at ascertaining whether the Ministry of Defence 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* (Ministry of Defence Card), the processing of personal data in the context of the Ministry of Defence Card service is reported to the Data Protection Officer of the Ministry of Defence.

9 General and Legal Provisions

9.1 Rates

No rates are included in this CPS.

9.2 Financial responsibility and liability

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 Ministry of Defence and, in a broader context, the State of the Netherlands (central government).

Regarding liability, see also Section 9.6.

9.2.1 Insurance cover

The Ministry of Defence 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

RfC 3647: not determined for the certification services of the Ministry of Defence.

9.2.3 Insurance cover or liability cover for end users

RfC 3647: not determined for the certification services of the Ministry of Defence.

9.3 Confidential (business) data

A risk analysis of the entire Ministry of Defence 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 Classification of information (confidential)

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

9.3.2 Classification of information (unclassified, not protectively marked)

The information used in the context of the Ministry of Defence Card service is not classified or protectively marked.

9.3.3 Responsibility for the protection of 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 Confidentiality of personal data

The processing of personal data in the context of the Ministry of Defence 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 Ministry of Defence.

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 brochure that is provided to every holder of a Ministry of Defence Card.

9.4.1 Personal data analysis report

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 Confidential handling of personal data

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 Ministry of Defence Card, in Certificates or in the Ministry of Defence 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 datum type	Card	Certificate	DBS
Surname	x	x	x
Prefixes	x	x	x
Given names	x	x	x
Date of birth	x		x
Sex	x		x
Passport photograph	x		x
Employee number	x	x	x
Employment end date			x
Citizen service number			x
Number and type of citizen identity document			x
Home Address			x
Private confidentiality key	x		
Public confidentiality key		x	x
Private authenticity key and signature key	x		
Public authenticity key and signature key		x	

Table 5. Overview of Ministry of Defence Card personal data

The personal data are largely taken from the personnel system of the Ministry of Defence.
The purposes of processing personal data for the Ministry of Defence 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 Ministry of Defence Card, including authorisations;
2. by means of the Ministry of Defence 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 Ministry of Defence Cards, certificates and cryptographic keys. This life cycle starts with the application for Ministry of Defence Cards, certificates and keys, proceeds through a number of phases and ends with revocation and putting out of operation.

9.4.3 Public personal data

The published data of certificates can be readily consulted within the Ministry of Defence. Publication outside the Ministry of Defence, via internet, is only permitted if the holder of the Ministry of Defence Card or his/her card manager has granted permission for such publication. The information provided regarding published and revoked certificates is limited to that stated in Chapter 7.

9.4.4 Responsibility for the protection of personal data

An important starting point of the General Data Protection Regulation 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 Ministry of Defence, this party is therefore the Minister of Defence.

9.4.5 Rights and duties of the parties involved in the processing of personal data

Holders of Ministry of Defence Cards have a right to inspect their personal data and to have these data corrected.

During the registration process, holders of Ministry of Defence Cards are given the opportunity to inspect their personal data and suggest corrections. Corrections are processed through the personnel system of the Ministry of Defence.

9.4.6 Release of personal data because of legal proceedings

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

9.4.7 Other circumstances that result in the release of personal data

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 Ministry of Defence Cards are released to parties outside the Ministry of Defence without the express permission of the Ministry of Defence Card holder concerned and the CA.

Within the Ministry of Defence, certificates or other recorded data that belong to holders of Ministry of Defence 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 Ministry of Defence Card remain vested in the State of the Netherlands (Ministry of Defence) also after issue.

The Ministry of Defence guarantees to holders of Ministry of Defence Cards that the certificates and Ministry of Defence Cards issued by the TSP, including the associated documentation, do not infringe intellectual property rights vested in suppliers.

9.6 Liability and obligations

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 Ministry of Defence Cards arise from their employment relationship with or official appointment at the Ministry of Defence.

9.6.1 Liability and obligations of the Certification Authority

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 Domain CP (G2 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 Ministry of Defence Cards and relying parties determined by the Ministry of Defence;
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 Liability and obligations of RAs

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 Liability and obligations of holders of Ministry of Defence Cards

Each holder of a Ministry of Defence Card must comply with the following obligations:

1. the holder of a Ministry of Defence 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 Ministry of Defence Card must comply with the instructions communicated to him/her by the TSP at the time at which the Ministry of Defence Card is issued or on a later date;
3. the holder of a Ministry of Defence Card must provide accurate, complete and current data to the TSP, especially for the registration process;
4. the holder of a Ministry of Defence Card must protect his/her card against damage, loss or theft;
5. the holder of a Ministry of Defence Card must keep the PIN separate from the Ministry of Defence Card and treat the PIN as confidential;
6. the holder of a Ministry of Defence Card must report any actual or suspected abuse, risk of compromise, loss or theft of the Ministry of Defence Card and/or PIN code immediately to the CA. The holder of a Ministry of Defence Card must immediately discontinue his/her use of certificates and keys in these cases;
7. the holder of a Ministry of Defence 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 Liability and obligations of relying parties

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. check the authenticity of the CRL;
3. 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;
4. 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;
5. take all other precautions that can reasonably be taken by relying parties.

9.6.5 Liability and obligations of other parties involved

RfC 3647: not determined for the certification services of the Ministry of Defence.

9.7 Disclaimers

RfC 3647: not determined for the certification services of the Ministry of Defence.

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 Ministry of Defence 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 Penalty clauses

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.

9.10 Period of validity and termination of the validity of the CPS

9.10.1 Period of validity of the CPS

This CPS shall remain valid until the TSP terminates its validity. Validity of this CPS will stop at March 23, 2020. Obligations to support legal disputes will remain until 7 years after the last issued certificate.

9.10.2 Termination of the validity of the CPS

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. Because the Validity of this CPS is due to expiration of the relating CA, no stipulation on the website about ending validity is necessary. No harm can be done to subscribers or relying parties.

9.10.2.1 Consequences of termination of the CPS

RfC 3647: not determined for the certification services of the Ministry of Defence.

9.11 Communication between the parties involved

RfC 3647: not determined for the certification services of the Ministry of Defence.

9.12 Changes

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

9.12.1 Change procedure

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 of changes

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 that result in changes to OIDs

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

9.13 Dispute resolution

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 Ministry of Defence.

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 Applicable legislation

The services of the CA, this CPS and the contracts concluded by the Ministry of Defence by reason of the certification services are governed by Dutch law.

9.15 Compliance with legislation

RfC 3647: not determined for the certification services of the Ministry of Defence.

9.16 Other provisions

RfC 3647: not determined for the certification services of the Ministry of Defence.

10 Appendix 1. Abbreviations

For an exhaustive list of definitions and abbreviations of the PKI terms used, please see the PKI-O definitions and abbreviations.

This appendix includes the abbreviations used in the context of the Ministry of Defence Card service.

Abbreviation	In full
ABDO	*Algemene Beveiligingseisen voor Defensieopdrachten 2006* - General Security Requirements for Defence Contracts 2006
ADR	*Auditdienst Rijk* - National Audit Service
AO	*Administratieve Organisatie* - Administrative Organisation
AP	*Autoriteit Persoonsgegevens* - Dutch Data Protection Authority
AT	*Agentschap Telecom* - Radiocommunications Agency
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
CPS	Certification Practice Statement
TSP	Trust Service Provider
DBS	*Defensiepas Beheer Systeem* - Ministry of Defence Card Management System
DMO	Defence Materiel Organisation
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	*Informatiemanagement en Architectuur - Information Management and Architecture*
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*
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
PIN	Personal Identification Number
PUK	Personal Unblocking Key
Reh	*Richtlijn elektronische handtekeningen* - Electronic Signatures Directive
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

Wbp	*Wet bescherming persoonsgegevens* - Personal Data Protection Act
Weh	*Wet elektronische handtekeningen* - Electronic Signatures Act
Wid	*Wet op de identificatieplicht* - Compulsory Identification Act
WIK	*Werkinstructiekaart* - Operating instructions card

11 Appendix 2. Documents

This list specifies the documents referred to in this CPS.

Ref. no.	Document
1	• PKI-O dienstverlening Ministerie van Defensie, V2.3, date 18.12.2012 • 2013.03.11 Rapport Proces Risicoanalyse Defensiepas.pdf, V1.3, date 11.03.2013 • 2013.04.08 Rapport Technische Risicoanalyse Defensiepas.pdf, V1.2, date 08.04.2013
2	Besturen bij Defensie 2013 (03_bbd_2013_tcm4-1077557.pdf), 11.2013
3	Belegging TSP verantwoordelijkheid JIVC.pdf, 01-12-2017
4	Calamiteitenplan Certificatie Autoriteit versie 2.3, 12.09.2017