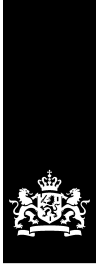

Commando Materieel en IT
Ministerie van Defensie

PDS G3 Ministry of Defence The Netherlands

PKI Disclosure Statement G3

Version	1.4
Date	3 10 2024
Status	Final

Colophon

COMMIT
JIVC

Maasland - Kantorencomplex
Coldenhovelaan 1 Maasland
3509BB Utrecht

Contact Defensiepas.Certificatie.Autoriteit@mindef.nl

Version number 1.4
Commisioned by R. (Remko) van Oostveen, BSc
Author JJ. Alders / MJ. Romeijn

Remko van Oostveen

Digitally signed by Remko van Oostveen
Date: 2024.10.16 11:15:19 +02'00'

Table of contents

1 Summary

For integrating in the Netherlands Ministry of Defence (NL-MoD) trust framework, the NL-MoD owns an internal Trust Service Provider (NL-MoD TSP) as specified in regulation (EU) no 910|2014 of the European parliament and of the council, article 2 section 1. NL-MoD TSP is fully compliant with eIDAS regulation to create a scalable and formal trust for collaboration with European and non-European partners (governments, companies and individuals).

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

The holders of the Ministry of Defence Card (NL-MoD Card) are end-users of the certificates.

All end-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.

It is not possible to acquire services from the NL MoD TSP.

The purpose of this PKI Disclosure Statement is to summarize and present the key points of the Netherlands Ministry Of Defence (NL MoD) Certificate Practice Statement (CPS) and specific conditions in a more readable and understandable format for a holder of a NL-MoD Card and relying parties that must use NL MoD certificates in their business processes.

Use of NL MoD certificates for private purposes is strictly forbidden as stated in internal policies, instructions, etc. that are automatically communicated towards the holder of the NL-MoD Card every time when receiving their NL-MoD certificates.

This PKI Disclosure Statement does not substitute or replace the NL-MoD CPS under which digital certificates are issued. Further information can be found in the CPS G3 found at https://cps.ca.pkidefensie.nl.

2 CA contact information

Questions regarding this PKI Disclosure Statement or the CPS should be directed at:
Defensiepas.Certificatie.Autoriteit@mindef.nl

3 Type of Certificates, validation procedures and certificate usage

For integrating in the Netherlands Ministry of Defence (NL-MoD) trust framework, the NL-MoD owns an internal Trust Service Provider (NL-MoD TSP) as specified in regulation (EU) no 910|2014 of the European parliament and of the council, article 2 section 1. NL-MoD TSP is fully compliant with eIDAS regulation to create a scalable and formal trust for collaboration with European and non-European partners (governments, companies and individuals).

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

The holders of the NL-MoD Card are end-users of the certificates.

All end-users have been vetted on identity and trustworthiness before entering the NL-MoD and their personal 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.

It is not possible to acquire services from the NL-MoD TSP.

3.1 Certificates

The NL-MoD TSP issues certificates that enable a user 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 NL-MoD Cards have all three types of certificates. Type 1 cards are intended for Dutch military and civilian personnel, while Type 2 cards are intended for foreign military and civilian personnel and temporary personnel who have been hired from outside the NL-MoD. The software (application) installed to perform activities determines which functions can actually be used.

3.2 Vetting

An end-user only gets his/her certificates after identification with a legal identification document. The names in the certificates represent the names in the legal identity document. Certificates are revoked when a user receives new certificates (i.e. when issuing an NL-MoD Card), leaves the NL-MoD or a compromise happened or is suspected.

3.3 Usage

The NL-MoD limits use of its certificates to strictly business purposes.

Full description of the certificates issued and their respective validation procedures are covered in the NL-MoD CPS document.

4 Limitation of the use of the reliability of certificates

The NL-MoD TSP limits the reliability and use of its certificates to all use cases where the subject operates as a holder of a NL-MoD Card and the relying party needs the certificates for a work process related to the NL-MoD. The NL-MoD TSP prohibits use of its certificates for private transactions.

5 Obligations for a holder of a NL-MoD Card

An end-user must:

- Submit accurate and complete information when applying for certificates (i.e. when applying for a NL-MoD Card).
- Exercise reasonable care to avoid unauthorized use of the card and pin/puk code.
- Only use the card for work-related activities.
- Call the service desk and ask for a revocation of their card when:
  - the card has been, potentially or actually lost, stolen or compromised.
  - the pin/puk code is revealed to others than the intended owner.
  - inaccuracy or changes to the certificate of card content, as notified to the employee.

For a more complete list of obligations, a user can refer to the policies, instructions and internal regulations he/she automatically received every time when receiving his/her (new) certificates

6 Obligations of the relying parties

Relying parties should direct their questions on when to use NL MoD certificates in their processes to their security officer.

Relying parties must perform these actions before committing to a transaction based on the NL MoD's PKI:

- Independently assess the appropriateness of the use of a certificate for any given purpose and determine that the certificate will, in fact, be used for an appropriate purpose.
- Utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations, as a condition of relying on a certificate in connection with each such operation. Such operations include:
    - identifying a certificate chain;
    - verifying the digital signatures on all certificates in the certificate chain and;
    - abort the transaction if the verification fails.

If all of the checks described above are successful, relying parties can use the certificates provided that reliance upon the certificate is reasonable under the circumstances.

7 Exclusion and liability limitation clauses

The NL-MoD accepts liability as far as they are specified in the CPS and the relying party complied with the requirements in paragraph 6, none when certificates are used in inappropriate ways or the checks in paragraph 6 have not been performed.

In specific circumstances, NL-MoD TSP will have contracts which contain explicit deviant constraints about liability.

8 Applicable agreements

A end-user always has a contractual binding with the Ministry of Defence. That can be an employment contract, a hiring contract, a delivery contract, a treaty, or any other form of binding contract. In all of those, compliance to internal NL-MoD policies, instructions and internal regulations is mandatory. On basis of these documents, all end-users are explicitly and automatically informed about their rights and obligations every time when receiving (new) certificates.

9 Reimbursement directives

Not applicable.

10 Governing Law and settlement of disputes clauses

All services concerning the certificates are governed by NL MoD policy, ABDO and Dutch law.

11 Certification

The NL-MoD is subject to a yearly compliance audit by an accredited auditor against the requirements of :

- European Union's (EU) eIDAS regulation;

- The program of requirements PKI Overheid;

- ETSI EN 319 411 -1 and ETSI EN 319 411 -2.

Proof of successful certification can be found by viewing the certificate of compliance on our website.