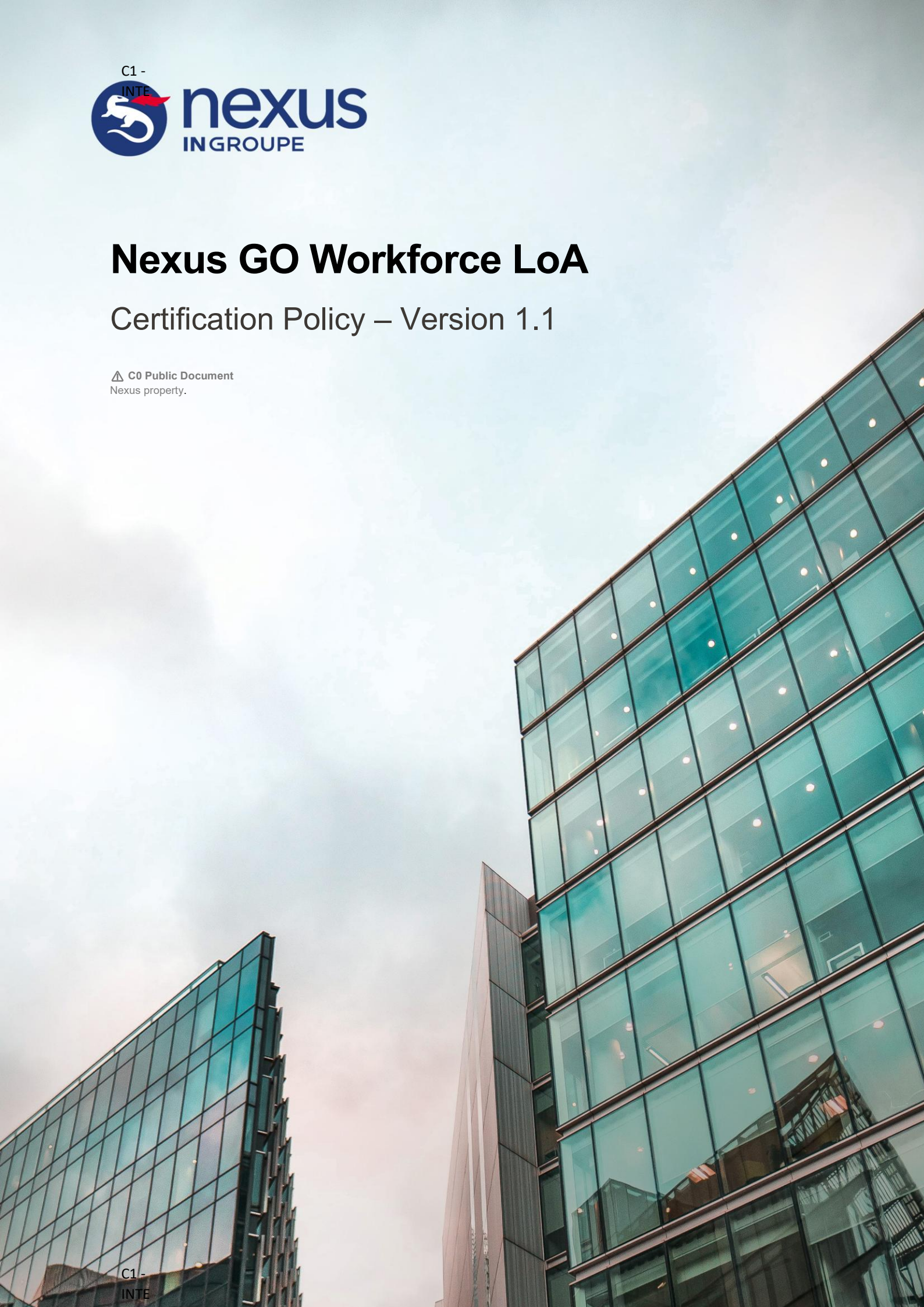
Nexus GO Workforce LoA

Certification Policy – Version 1.1



Identification of the document		
No pages: 73	**State:** Approved	**Reference:** Nexus-GO-WF-LoA-CP
Creation date: 6/24/2024	**Last updated:** 12/11/2025	**Version:** 1.1

Version history			
Version	**Author**	**Date**	**What changes were made, where**
0.1	SEALWeb	2024-06-24	Initial version (draft)
1.0	Nexus Group	2024-11-22	First Approved Version
1.1	Linh Pham – Product Owner	2025-12-10	Performed minor formatting and typographical corrections throughout the document. Updated CRL Profile section to clarify issuance frequency and validity periods. Updated CA Profiles to replace G1 with Gn across the full PKI hierarchy. Removed the LoA End-Entity Certificate section and replaced it with a reference link to the dedicated document. Reviewed and approved in governance meeting on 2025-12-11.
		Click or tap to enter a date.	
		Click or tap to enter a date.	
		Click or tap to enter a date.	

Table of Contents

1 Introduction

1.1 Overview

Technology Nexus Secure Business Solutions AB (in the following the ‘Trust Service Provider’ or ‘TSP’) operates a PKI cloud service (called ‘Nexus GO Workforce LoA’) for issuing and managing certificates intended for natural persons.

The TSP provides the ‘Nexus GO Workforce LoA’ service (briefly ‘the Service’) for its contracted Service Customers.

‘Nexus GO Workforce LoA’ is a multi-tenancy-enabled, shared cloud PKI service, and is one of several ‘Nexus GO’ cloud services. The central ‘TSP Organization’ of Nexus operates these services in a dedicated infrastructure under guidance of the following industry-standard certificate policies and technical specifications:

- [ETSI TS 319 401]
- [ETSI TS 319 411-1], Normalized Certificate Policy (NCP)
- [CEN TS 419 261]
- [BSI TR-03145-1]

The present document constitutes the certificate policy (CP) of issuing CAs from ‘Nexus GO Workforce LoA’ service that issue electronic certificates that comply with the requirements of ISO/IEC 29115 for the level of assurance 3 (LoA3).

This document describes the different levels of responsibility, security measures (technical, organizational, etc.) and certificate profiles.

The issuing CAs covered by the present CP issue two types of certificates:

- Authentication certificates, and
- Signature certificates.

In the scope of the present CP, certificates are issued exclusively to natural persons who use them (and the associated private keys) in the context of their activities in relation to the Customer Entity identified in the certificate and with which these natural persons have a contractual relationship.

The document also sets out the commitments of ‘Nexus GO Workforce LoA’ within the context of the provision of its electronic certification services for holders, in accordance with the requirements of the standards cited above.

The present document is only one of the documents issued by the TSP, which regulate the conditions of the services provided by the TSP. Further documents are the General Terms and Conditions, SLA and the individual agreements/contracts made with the Service Customer.

The content and the format of this CP complies with [RFC3647] “X.509 Public Key Infrastructure Certificate Policy Certification Practice Statement Framework” of the Internet Engineering Task Force (IETF). To strictly preserve the outline specified by [RFC 3647], section headings where the document does not impose a requirement have the statement "No stipulation".

Given the complexity of reading the CP for Certificate holders or users who are not specialists in the field, Nexus publishes Terms and Conditions document based on the PDS (PKI Disclosure Statement) defined in the ETSI EN 319411-1 standard.

1.2 Document name and identification

This document describes the different levels of responsibility, security measures (technical, organizational, etc.) and certificate profiles.

The Nexus eID service CA hierarchy consists of the following CAs:

- a Root CA named “Nexus GO eID Root CA G[n]*” and whose CP is identified by the following OID: 1.2.752.274.1.1.1,
- an Intermediate CA named “Nexus GO eID Intermediate CA G[n]*” and whose CP is identified by the following OID: 1.2.752.274.1.1.2,
- Issuing CAs implemented per Customer and named as follows: **[Customer name]** Issuing CA G[n]*.

Note on Naming Convention:

*: G[n] denotes the Generation number (e.g., G1, G2, G3, etc.). This designation is used to illustrate the evolution or versioning of the PKI chain over time.

This CP is identified in the following table by the following OIDs:

CA	Type	CP OID
[Customer name] Issuing CA G[n]	Issuing CA, dedicated to the Customer, for user certificates	1.2.752.274.1.1.3

The certificates issued by Issuing CAs are associated with the following OIDs:

Certificate profiles of [Customer name] Issuing CA G[n]	Type	CP OID
User Authentication (smartcard)	End Entity	1.2.752.274.1.2.1.1
User Signing (smartcard)	End Entity	1.2.752.274.1.2.2.1
User Authentication (Mobile ID)	End Entity	1.2.752.274.1.2.1.2
User Signing (Mobile ID)	End Entity	1.2.752.274.1.2.2.2
OCSP Signing	End Entity	1.2.752.274.1.2.4

1.3 PKI participants

1.3.1 Certification authorities

The CA is responsible for providing certificate management services throughout their lifecycle (generation, distribution, renewal, revocation) and relies on a technical infrastructure known as the Public Key Infrastructure (PKI). The CA’s services are the result of different functions that correspond to the different stages of the life cycle of key pairs and certificates.

The PKI is based on the following functional services:

- **Key pair generation:** This service generates the key pair for future Holders and provides the public key to be certified to the certificate generation service
- **Generation of certificates:** This service generates electronic certificates for future Holders based on information provided by the registration authority.
- **Revocation:** This service processes certificate revocation requests and determines the actions to be taken, including the generation of the certificate revocation list (CRL).
- **Publication:** This service provides Certificate Users (CUs) and Certificate Holders or certificate managers with the information necessary to use certificates issued by CAs (General Terms and Conditions of Use, PC, CA certificates, etc.) as well as the processing results of the certificate revocation management service (CRL).

The CA generates and revokes certificates from requests sent by the Registration Authority (see section 1.3.2). The CA implements certificate generation, certificate revocation, certificate status information, logging and audit services.

1.3.2 Registration Authorities

The Registration Authority (RA) service is used for the implementation of certificate application registration, certificate delivery, certificate revocation, logging and audit services. In particular, the role of the RA is to verify the identity of future certificate holders.

In the scope of the present CP, the role of the RA is to verify the identity of the future certificate holder. The Service Customer (including Nexus Issuing CA) takes on the RA role and can register and request certificates for End-users that are employed or contracted by the organization it serves. For the end-user to receive a user certificate, the Service Customer is responsible for the following tasks:

- Take into account and verify the information of the holder and their entity and the creation of the corresponding registration file during a first request, or during renewal,
- The activation of the certificate,
- Initiating or passing along revocation requests for certificates

1.3.3 Customers and end-users

In the scope of this CP, an end-user can only be a natural person associated to a legal person (Customer entity). This end-user uses their private key and the corresponding certificate in the context of their professional activities, i.e. their activities in relation to the Customer Entity identified in the certificate and with which she/he has a contractual relationship (employees or contractors).

The end-user shall comply with the conditions concerning him/her and defined in this CP. These conditions are included in the Terms and Conditions document that she/he explicitly accepted when applying for a certificate.

1.3.4 Relying parties

The relying parties are any application, natural person or legal entity, computer system or equipment that use an end-user's certificate in accordance with this CP.

Under this CP, the relying parties must validate the certification chain (validation of the end-user's certificate, the CA certificates and the Root CA certificate) and check the non-revocation of certificates (Holder's certificate and CA certificate) through the publication service made available to relying parties.

Relying parties of Authentication Certificates may include:

- An on-line service that uses a certificate and an authentication verification mechanism either to validate an access request made by the certificate holder as part of an access check, or to authenticate the origin of a message or data transmitted by the certificate holder,
- A user who receives a message or data and uses a certificate and an authentication verification device to authenticate its origin.

Relying parties of Signature Certificates may include:

- An on-line service that uses a certificate and signature verification mechanism to verify the electronic signature affixed to data or a message by the certificate holder,
- A user who electronically signs a document or message,
- A user who receives a message or data and uses a certificate and a signature verification mechanism to verify the electronic signature affixed by the certificate holder to that message or data.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

1.4.1.1 End-user certificates

This CP deals with key pairs and certificates corresponding to two categories of certificates intended for the end-users identified in chapter 1.3.3:

- Authentication, so that these end-users can authenticate themselves on the services made available to end-users as part of their work and
- Signature, so that these end-users can, authenticate themselves on the services made available to end-users as part of their work and electronically sign data (documents or messages) as part of dematerialized exchanges with the categories of relying parties identified in chapter 1.3.4

It is expressly understood that a certificate holder may only use their private key and certificate for authentication or signature purposes as defined in the use of their certificate. In the event of unauthorized use of a private key and its certificate by its holder, the latter could be held liable.

It is also expressly understood that the relying parties can only trust the certificate in the context of paperless exchanges with the end-user. The electronic signature provides, in addition to the guarantees of the authenticity and integrity of the data thus signed, a guarantee of the signatory's consent to the content of such data.

1.4.1.2 CA and component certificates

The CA has only one key pair and the corresponding certificate is attached to a higher-level CA (CA hierarchy) except for Root CA.

Root CA's key pair is used to sign the certificates of Intermediate CAs and Certificate Revocation Lists (CRLs) it issues. This key pair is used exclusively for this purpose.

The Intermediate CA's key pair is used to sign the certificates of Issuing CAs and Certificate Revocation Lists (CRLs) it issues. This key pair is used exclusively for this purpose.

The 'Nexus GO Workforce LoA' CA keys are used according to common practice to sign certificates, CRLs and OCSP responses.

1.4.2 Prohibited certificate uses

1.4.2.1 End-user certificates

It is prohibited to use the certificates issued by the TSP other than the appropriate usages set out in section 1.4.1 and agreed with and approved by the TSP.

This means that the CA cannot, under any circumstances, be held liable for any use of the certificates it issues other than that provided for in this CP.

The CA undertakes to enforce these restrictions on potential certificate holders and relying parties of such certificates. To this end, the CA publishes the Term and Conditions document (T&C) intended for them. In particular, the issuing of the certificate to an end-user is subject to the explicit acceptance of these T&C (indicated in the application form that the end-user must sign).

1.4.2.2 CA and component certificates

The CA and component certificates and the associated private keys are not used for other purposes than mentioned in Section 1.4.1 and are not used prior to the disclosure of the CA certificate and this CP.

1.5 Policy administration

1.5.1 Organization administering the document

This CP is the responsibility of Nexus.

1.5.2 Contact

Point of contact:

Nexus Group

Telefonvägen 22B

126 26 Hägersten

Sweden

gopki@nexusgroup.com

1.5.3 Person determining CPS suitability for the policy

The TSP Compliance Officer is responsible for determining the suitability of the practices described in the CPS (and other supplementary documents that are subordinate to the CPS) with this CP.

1.5.4 CPS approval procedures

The certification practices are approved by the TSP following an approval process established by Nexus.

This CP, the CPS and the suitability are reviewed yearly by the TSP Compliance Officer in order to:

- Ensure compliance with the security standards expected by applications that reference end-user certificates,
- Update the list of applications concerned by the CP,
- Adapt to technological developments.

1.6 Definitions and acronyms

1.6.1 Acronyms

ARL	Authority Revocation List
CA	Certificate Authority
CDP	CRL Distribution Point
CRL	Certificate Revocation List
CP	Certificate Policy
CPS	Certification Practice Statement
DP	Distribution Point, a repository service which makes certificates and CRLs accessible to Relying Parties.
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
LR	Legal reprensentative
OCSP responder	Online Certificate Status Protocol
OID	Object Identifier
RA	Registration Authority
TSP	Trust Service Provider

1.6.2 Definitions

Activation data: Data values, other than keys, that are necessary to operate the cryptographic modules or the elements they protect and that must be protected (e.g. a PIN, a passphrase, etc.).

Certificate: an entity's public key, as well as other information, the forging of which is made impossible by encrypting it with the private key of the issuing certification authority [ISO/IEC 9594-8; ITU-T X.509]. The certificate contains identification information of the owner of the key pair.

Certificate Authority (CA): the name of the organization (legal entity) and/or the technical component that performs the issuing of certificates. Its main task is to sign the certificate containing the presented subject and key information in a secure process, to keep the CA key secret and control its use.

Compromise: A proven or suspected breach of a security policy, during which unauthorised disclosure or loss of control of sensitive information may have occurred. For private keys, a compromise is the loss, theft, disclosure, modification, unauthorised use, or other compromise of the security of this private key.

CRL Distribution Point (CDP): a service that makes revocation lists accessible to Relying Parties.

Certificate Revocation List (CRL): a list of certificate revocation events (each record containing at least the certificate identifier, revocation reason and time stamp) signed and published by the CA.

Certificate Practice Statement (CPS): the type of this document describing the Trust Service Provider's practices, its provisions towards and the responsibilities of the Service Customer and of other parties.

Cryptographic modules: A set of software and hardware components used to implement a private key to enable cryptographic operations (signature, encryption, authentication, key generation, etc.). For a CA, the cryptographic module is an evaluated and certified hardware cryptographic resource (FIPS or common criteria), used to store and implement the CA private key.

Disaster Recovery Plan: A plan defined by a CA to restore all or part of its PKI services after they have been damaged or destroyed as a result of a disaster, within a time frame defined in the PC package.

Distribution Point (DP): a repository service which makes certificates and CRLs accessible to Relying Parties.

Electronic certificate validation: a checking operation to ensure that the information contained in the certificate has been verified by a certification authority (CA) and is still valid. Validation of a certificate includes, among other things, checking its validity period, its status (revoked or not), the identity of CAs and verification of the certification chain. The validation of an electronic certificate requires prior approval of the certificate from the Root authority (self-signed certificate).

Key ceremony: A procedure by which a CA dual key is generated and/or its public key certified.

Key pairs: Pair of asymmetric keys, consisting of a public key and the corresponding private key.

OCSP responder: A service that allows Relying Parties to access information about the revocation status of certificates via the standard 'Online Certificate Status Protocol'.

Object Identifier (OID): a globally unique identify of any kind of data object, data type, document.

Private key: key of the asymmetric key pair of an entity to be used only by that entity [ISO/IEC 9798-1].

Public key: key of the asymmetric key pair of an entity that can be made public. [ISO/IEC 9798-1].

Public Key Infrastructure (PKI): This is the infrastructure required to produce, distribute, manage and archive keys, certificates and Certificate Revocation Lists.

Revocation: To invalidate a certificate before its normal expiration. Revoked certificates are published to a CRL and to an online OCSP responder.

RSA: public key cryptographic algorithm invented by Rivest, Shamir, and Adleman.

Secret Holder: persons who hold activation data related to the implementation of a CA's private key using a cryptographic module.

Security policy: a set of rules issued by a security authority relating to the use, provision of security services and facilities [ISO/IEC 9594-8; ITU-T X.509].

Service Agreement: The collection of relevant contract documents describing the business agreement between Service Customer and TSP.

Service Customer: The organization (legal entity) closing the service agreement with the TSP entity.

Trust Service Provider (TSP): an acronym for the service provider, who operates the PKI service.

TSP Organization: The internal organizational unit inside the TSP entity, which is responsible for the design, implementation, and the operation of the PKI Service.

User / End-user: A person that is a Customer employee or contractor

User certificate: A certificate issued for a subject (identified User)

Validity period of a certificate: The validity period of a certificate is the period during which the CA guarantees that it will maintain information regarding the validity status of the certificate. [RFC 5280]. Outside this period (before the valid-from date and after the valid-to date), the certificate is deemed invalid.

2 Publications and repository responsibilities

2.1 Repositories

Nexus is responsible for publishing 'Nexus GO Workforce LoA' service information.

The information to be published for relying parties and end-users is available at the following web address: https://pki.nexusgroup.com/.

Certificate status information is published at the distribution points indicated in the profiles of issued certificates (see chapter 7). You can find the CRLs here: http://dp.eid.nexusgroup.com/.

The publication of these elements is automated for the CRLs signed by the Issuing CA and the Intermediate CA. It is manual for the CRL (called also ARL) issued by the Root CA.

A second method for verifying the certificates status is available through an OCSP service available at this address: http://ocsp.eid.nexusgroup.com/.

2.2 Publication of certification information

The following documents are published at https://pki.nexusgroup.com/ and accessible for end-users and relying parties:

- The present CP,
- The CPS,
- The Term & Conditions,
- CA certificates (of all CAs in the hierarchy),
- OCSP responder certificates
- Revocation lists

Nexus does not publish details that it considers sensitive or even confidential in its CP/CPS.

2.3 Time or frequency of publication

The publication timeframes and frequencies depend on the information:

- For information related to a CA (new version of the CP, T&C, etc.), the information is published whenever necessary in order to ensure, at all times, consistency between the published information and the CA's actual commitments, means and procedures.
- For the CA's certificates, they are disseminated prior to any issuing of certificates and/or of corresponding CRLs within an interval of 24 hours.

The deadlines and frequencies for publishing certificate status information and the availability requirements for the systems publishing them are described in chapters 4.9 and 4.10.

The publication systems are available 7 days a week and 24 hours a day.

2.4 Access control of repositories

All information published for end-users and relying parties (CP, CPS, T&C, CA certificates, CRLs, OCSP responders) is freely accessible for reading.

Access to publishing systems for editing (adding, deleting or modifying published information) is strictly limited to the authorized internal functions, through logical and physical access control.

3 Identification and authentication

3.1 Naming

3.1.1 Types of names

The names used in certificates issued by ‘Nexus GO Workforce LoA’ comply with the specifications of standard [X.500]. In each certificate conforming to standard [X.509], the issuing CA (issuer) and the end-user (subject) are identified by a "Distinguished Name" (DN) in UTF8String.

3.1.2 Need for names to be meaningful

3.1.2.1 Naming CA

The Root CA is identified by its DN, as follows:

DN Attributes	Value
country (C)	SE
organisationName (O)	NEXUS
commonName (CN)	Nexus GO eID Root CA G[n]

The Intermediate CA is identified by its DN, as follows:

DN Attributes	Value
country (C)	SE
organisationName (O)	NEXUS
commonName (CN)	Nexus GO eID Intermediate CA G[n]

The Issuing CAs are identified by their DN, as follows:

DN Attributes	Value
country (C)	SE
organisationName (O)	NEXUS
commonName (CN)	**[Customer Name]** Issuing CA G[n]

3.1.2.2 Naming end-users

The *subject* field DN of the certificates issued by the Issuing CA identifies the end-user certificate.

DN Attributes	Attribute name	Value
C	*countryName*	This field MUST contain the country code for the Subject's organization as listed in the official records. In ISO3166 format. Source: Companies Registration Office and Central Bureau of Statistics
O	*organizationName*	This field MUST contain the Subject's full legal organization name as listed in the official records. Source: Companies Registration Office and Central Bureau of Statistics
OI	*organizationIdentifier*	This field MUST contain the Subject's full legal organization number as listed in the official records in the following format: XXXXXXXXXX. Source: Companies Registration Office and Central Bureau of Statistics
CN	*commonName*	This field MUST contain the Subject's common name which is a combination of Given Name and Surname
SN	*surName*	This field MUST contain the first Subject's surname. Source: provided by customer but must comply with SPAR
GN	*givenName*	This field MUST contain the Subject's marked Given Name IF it exists OR All Given Names of the subject if marking of Given Name is absent and First Names exists This field is empty if Given Name and First Names are absent Source: provided by customer but must comply with SPAR
SerialNumber	*SerialNumber*	This field MUST contain the Subject's full Swedish social security number (or equal) Social Security Number will be given in the following format: YYYYMMDDXXXX This field guarantees the uniqueness of the end-user's DN within the CA.

3.1.3 Anonymity or pseudonymity of subscribers

The Issuing CA do not issue a certificate with an anonymous identity or a pseudonymous identity.

3.1.4 Rules for interpreting various name forms

All characters are in UTF8String or PrintableString format.

The rules for interpreting the different name forms are defined with the Customer in the CPS.

3.1.5 Uniqueness of names

The uniqueness of the subject is ensured by the field “SerialNumber” attribute present in the DN and containing the Subject’s full Swedish social security number (or equal).

3.1.6 Recognition, authentication and role of trademarks

Subject names in service certificates of customer-named CAs and in end-entity certificates MUST respect registered trademarks and business ethics.

The CA cannot be held liable for any unlawful use by the certificate end-users and customers of trademarks, well-known trademarks and distinctive signs, as well as domain names.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The key pair generation is triggered by the RA in the presence of the end-user and carried out directly on the user's equipment.

The possession of the private keys is ensured by the applied certificate request protocols, which verify the proof-of-possession signature created by the private key to be certified.

3.2.2 Authentication of organization entity

The entity of the Customer, which is named in certificates, is identified by the TSP by means of common commercial method, e.g. a company registry.

The Customer entity enters into a commercial relationship with the TSP and becomes a RA for the ‘Nexus GO Workforce LoA’ service and is authorized to issue certificates to its employees and contractors.

As part of the RA role, the Customer entity is responsible for verifying the identity of future holders before issuing certificates to them.

3.2.3 Authentication of individual user

The registration of an end-user relies exclusively on information provided by the Customer or provided by the end-user and collected by the Customer.

In both cases, the information is verified by the RA.

The identification and authentication of the end-user are confirmed by the RA during the physical face-to-face meeting during which the keys and certificate are generated on the end-user's equipment.

The identity of the end-user is verified by checking a valid official identity document including a picture of the end-user (passport, SIS approved identity card, or Swedish driver's license).

The conditions for issuing a certificate to an end-user are as follows:

- the user must be an employee or a contractor of the Customer,
- their identity must be checked and validated by the RA.

3.2.4 Non-verified subscriber information

Certificates issued by Issuing CA do not contain any unverified identity information.

3.2.5 Validation of authority

The existence of the Service Agreement with the Customer is the precondition and at the same time the evidence of authorization for issuing certificates for customer-named Issuing CAs.

3.2.6 Criteria for interoperation

Not applicable.

3.3 Identification and authentication for re-keying requests

The Issuing CA do not issue a new certificate for a previously issued key pair. Renewal requires the generation of a new key pair and a new certificate application.

3.3.1 Identification and authentication for regular re-keying

Checks relating to current renewal shall be carried out in accordance with the initial certificate application procedure (see chapter 3.2).

3.3.2 Identification and authentication for re-keying after revocation

Checks relating to the renewal of a key pair after revocation of the certificate are carried out in accordance with the initial certificate application procedure (see chapter 3.2).

3.4 Identification and authentication for revocation request

Requests for revocation of a certificate shall give rise to verification of the identity of the applicant and verification of their authority in relation to the certificate to be revoked.

The following persons have the authority to request blocking employees' e-IDs:

1. Human Resources Manager in the organization
2. Operations Manager in the organization

The card officer performs blocking on behalf of an authorized person; verification of authorized identity can be done at:

1. Via signed request addressed to card administrators (signed PDF document) based on LoA3 e-ID issued by the organization.
2. Via personal visit with a signed form and identification based on a valid physical ID

4 Certificate life-cycle operational requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application

The certificate request comes from an end-user belonging to an organization which is a Nexus Customer entity and acts as an RA.

The end-user is therefore either an employee or a contractor in relationship with Customer entity and registered as a resident in Sweden at the time of the request.

4.1.2 Enrolment process and responsibilities

All operations relating to the issuance of a certificate are carried out from the portal made available to the Customer by Nexus.

Prior to any certification request, end-user information (holders and future holders) is provided by the Customer and imported into the portal according to the Customer's technical means (e.g. integration into the Customer's Active Directory, integration into the Customer's HR application, or import via CSV file, etc.). For a certificate, only the first name, last name, Social Security Number and email address are used.

Then, a certificate request follows the following steps:

1. **Integrate Users**: The user who needs a card must first be imported from the customers AD or LDAP directory to GO Workforce LoA
2. **LoA3 Card Order**: To order a card the user needs to visit an administrator with the role qualified operator, bringing a valid ID.
3. **F2F ID Check**: The operator checks the ID for validity. E.g. for Swedish passports or Swedish national IDs, the operator can do this at https://etjanster.polisen.se/egid/giltighetskontroll/. If the ID is valid the operator will scan the ID and upload it to GO Workforce LoA. If the ID is not valid, the card will not be ordered. This deviation should also be reported to HR.
4. **Swedish resident check**: After step 3 there will be an automatic check to SPAR (Statens personadressregister). For this check to work the users SSN (personnummer or samordingsnummer) is used. The purpose of the check is to verify that the user is registered as a resident in Sweden. If this returns false, then the card will not be ordered.

5. **Approve Order**: Approval is needed for the order to be produced. It must also be done by a qualified operator but not by the same operator who executed step 2-4.
    a. If approved the card order will be sent to Nexus.
    b. If not approved the card will, of course, not be ordered.
6. **Launch card production**: After the job has run, which creates the orders in Nexus GO Cards production portal, the card order arrives at Nexus production centre in Stockholm.
7. **Card delivery**: After production, the card is delivered to the customer, and the card data will be sent back to GO Workforce LoA. This includes the ICCSN (Integrated Chip Card Serial Number), which uniquely identifies the card.
    a. When the card arrives at the customer, an administrator needs to manually change the status of the card to “received”.
8. **Send OTP via email**: The action in step 7 triggers an S/MIME encrypted email to be sent to the user containing an OTP (One Time Password).
9. **Activate card**: To activate the card, the user needs to visit an administrator with the role qualified operator, bringing the same ID as in step 2.
10. **F2F ID Check:** The administrator compares the ID with the image which was uploaded to GO Workforce LoA in step 3. If the ID differs from the image, then the activation must not be done.
11. **Enter OTP**: For the activation process to proceed the OTP, which was received by the user in step 8, must first be entered.
12. **Provision LoA3 Certificates**: The administrator will then enter the card into a card reader. The cards ICCSN (Integrated Chip Card Serial Number) is read, to verify that the correct card has been inserted in the card reader. If the wrong card has been inserted by the administrator, then the activation process will not continue but can be restarted.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The RA performs the following processing operations:

- Checking the identity of the end-user (“natural person” identification)
- Checking the consistency of the supporting documents provided
- Checking with SPAR that the end-user is registered as a resident in Sweden

4.2.2 Approval or rejection of certificate applications

If the certificate request is rejected, the RA shall inform the end-user. A notification of rejection is made by email.

If the certificate request is accepted, the end-user is informed by email.

4.2.3 Time to process certificate applications

The RA and the end-user must schedule an appointment for the certificate generation and the delivery of the equipment containing the certificate.

The technical operation of issuing certificates is carried out when the equipment is issued (e.g. smartcard, etc.).

Case of certificate issuing on a smart card:

For a certificate stored in a smartcard, once the certificate request has been validated:

- The certificate request is transmitted to the pre-personalization center
- The pre-personalization center carries out the graphic personalization of cardholder
- The pre-personalization center sends:
  - The card (blocked and devoid of any key) to the RA
  - Card production report to the portal.
- From the portal, once the pre-personalized card is received, the RA validates receipt of the card which triggers the transmission of activation codes to cardholders.

The transmitted card does not contain any keys or certificates. Certificates are issued when the card is handed over to the Holder.

From there, the RA and the end-user must schedule an appointment for the certificate generation and the delivery of the smartcard containing the certificate.

Case of certificate issuing on Mobile ID:

For a validated certificate stored in Mobile ID:

- The pre-requisite is that the end-user already has a smartcard – then the issuance of Mobile ID is done with ID exchange via the self-service portal by end-user without RA interaction.
- RA has the ability to issue a Mobile ID from the portal after the certificate request has been validated.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Following validation of the request by the RA, the CA initiates the process of generating and preparing the elements for the end-user: creation of the medium (card).

The card is transmitted to the RA and the latter triggers the certificate issuance process:

- Upon receipt of the end-user's card, the RA confirms receipt and triggers the sending of an email to the end-user containing:
  - An activation code (in the form of OTP) necessary to trigger the personalization of the card. The RA cannot have access to this activation code
  - The applicable Terms & Conditions,

The RA and the end-user then meet face-to-face to issue the certificates and hand over the card to the end-user.

- The RA verifies the identity of the end-user

- The RA inserts the end-user's card on their personalization station and launches the personalization of the card
- The activation code is entered by the end-user to authorize the launch of the personalization of the card
- The key pair is generated on the card and the certificate request (Certificate Signing Request) is transmitted to the CA
- During the personalization process, the end-user initializes the PIN code of their card

At the end of the generation of the key pairs and certificates, the content of the certificates, the Terms & Conditions and a declaration of delivery of the card to the Holder are displayed on the screen.

The end-user can accept or refuse the certificates,

Once consent has been obtained, the RA gives the card to the end-user.

4.3.2 Notification to subscriber by the CA of issuance of certificates

No notification needed.

The certificates are issued in the presence of the end-user.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

For a certificate issued on a smartcard and Mobile ID:

The Customer is considered to have accepted the certificate when the user certificate has been issued on the user’s equipment and it has been handed to them.

The certificates generated following the personalization of the card are presented to the end-user for acceptance. It is the end-user's responsibility to check the consistency of the information contained in the certificate (for example the email address) before any use.

The end-user can accept or refuse the certificates presented.

Acceptance of certificates by the end-user is collected by a check box.

In the event of explicit refusal of certificates by the end-user, the certificates are revoked by the CA.

The trace of certificate acceptance is kept by the CA.

4.4.2 Publication of the certificate by the CA

Certificates issued by the CA under this CP are not published.

4.4.3 Notification of certificate issuance by the CA to other entities

Not applicable.

4.5 Key pair and certificate usage

4.5.1 Customer private key and certificate usage

End-user must strictly adhere to the authorized uses of the key pairs and certificates. Otherwise, they could be held liable.

The authorized use of the key pair and the associated certificate are also indicated in the certificate itself, via the extensions concerning the use of the keys.

The use of the end-user's private key and associated certificate is strictly limited to the service defined by the OID from its policy (see section 1.4.1.1).

4.5.2 Relying party public key and certificate usage

See previous section and section 1.4.

Relying parties must strictly adhere to the authorized uses of certificates. Otherwise, they could be held liable.

4.6 Certificate renewal

In accordance with [RFC3647], the notion of "certificate renewal" refers to the issue of a new certificate for which only the validity dates are changed, all other information is identical to the previous certificate (including the public key).

Under this CP, there can be no certificate renewal without renewal of the corresponding key pair.

4.7 Certificate re-keying

4.7.1 Possible causes for changing a key pair

The key pairs must be periodically renewed in order to minimize the possibility of cryptographic attacks. Thus, the end-user's key pairs, and the corresponding certificates, will be renewed at least before their end of life as defined in section 6.3.2.

The end-user's key pairs may be renewed in advance, following the revocation of the end-user's certificate. The various reasons for revocation are described in 4.9.1.

The change of key pair results in the change of certificate.

4.7.2 Origin of a new certificate request

The request for a new certificate may be made at the initiative of the end-user.

The end-user is notified by email of the expiry of their certificate at least 1 month before the end of the validity of the certificate.

4.7.3 Procedure for processing a new certificate request

Processing of an application for a new certificate shall be carried out under the same conditions and in accordance with the same procedures as the initial application. (see section 4.2 above).

4.7.4 Notification to the holder of the drawing up of the new certificate

For any renewal: the CA notifies the end-user under the conditions of section 4.3.2.

4.7.5 Procedure for accepting the new certificate

Any renewal shall be carried out under the conditions of section 4.4.1.

4.7.6 Publication of the new certificate

See section 4.4.2.

4.7.7 Notification by the CA to other Entities of the issue of the new certificate

See section 4.4.3.

4.8 Certificate modification

In accordance with [RFC 3647], the modification of a certificate corresponds to changes in information without changing the public key, other than only the modification of validity dates.

This operation is not authorized by this CP. In the event of a change in information, a new certificate must be issued with the generation of a new key pair and the revocation of the old certificate.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

4.9.1.1 End-user certificates

The reasons for revoking an end-user's certificate are as follows:

- compromise, suspicion of compromise, theft, loss of private key,
- theft, loss or irreversible malfunction of the equipment,
- the end-user's information contained in their certificate no longer complies with the identity or use provided for in the certificate, before the end of the validity of the certificate,
- non-compliance by the end-user with the applicable terms and conditions for using the certificate,
- non-compliance by the end-user with their obligations under the CP,

- error detected in the registration application,
- non-acceptance of the certificate by the end-user after its issue,
- the end-user or an authorized entity requests the revocation of the certificate (in particular in the case of destruction or alteration of the private key of the end-user and/or its equipment),
- death of the end-user, departure of the Customer entity, termination of the Customer entity's activity,
- revocation of the CA certificate.

When one of the above circumstances occurs and the CA becomes aware of it (it is informed of it or it obtains the information during one of its verifications, particularly when issuing a new certificate), the certificate concerned is revoked.

4.9.1.2 CA and component certificates

The reasons for revoking a certificate of a PKI component are as follows:

- cessation of activity of the entity operating the component,
- compromise, suspicion of compromise, theft, loss of the means of reconstituting the component's private key (loss of the main secret, loss of the activation code and loss of more than two shared secrets),
- non-compliance with the CA's CP (detected during a negative compliance audit),
- change in PKI component,
- obsolescence of cryptography with respect to DIGG requirements.

4.9.2 Who may request revocation

4.9.2.1 End-user certificates

The persons authorized to request the revoking of a Holder certificate are as follows:

- The end-user in whose name the certificate was issued,
- The Legal Representative of the Customer entity to which the end-user belongs,
- Authorized entity of the Customer entity such as Human Resources represented by the HR manager,
- The CA issuing the certificate,
- A component of CA (the RA).

Note: The end-user is informed of the person/entities authorized to make a request to make a revocation request of their certificate.

4.9.2.2 CA and component certificates

The revocation of the CA certificate can only be decided by the entity responsible for the CA or by the judicial authorities via a court decision.

The revocation of the other component certificates is decided by the entity operating the component concerned, which shall inform the CA without delay.

4.9.3 Procedure for revocation request

4.9.3.1 End-user certificates

The requirements for identifying and validating a revocation request are described in section 3.4.

A revocation request may be submitted:

- By meeting the RA,
- Through the SELF-SERVICE portal.

The following information should at least be included in the request for revocation of the certificate:

- Identity of the end-user whose certificate is to be revoked,
- Identity of the applicant,
- Information necessary to identify the certificate to be revoked unequivocally (e.g. serial number, etc.)

Once the request has been authenticated and checked, the revocation of the corresponding certificate is processed, and the new status of the certificate is communicated to the certificate status information service.

The request for revocation of an end-user certificate is processed either by the holder himself or by the RA.

The applicant, the end-user (if not the applicant) and the end-user's Customer entity are informed of the revocation of the end-user's certificate.

4.9.3.2 CA and component certificates

In the event of revocation of one of the certificates in the certification chain, the CA shall inform all affected end-users as soon as possible and by any means (and if possible, in advance) that their certificates are no longer valid.

4.9.4 Revocation request grace period

The end-user must immediately request the revocation of their certificate as soon as a cause for revocation as defined in section 4.9.1 is identified. Otherwise, the request must be made by the Legal Representative or by an authorized entity within the Customer entity to which the end-user is attached.

4.9.5 Time within which CA must process the revocation request

4.9.5.1 End-user certificates

By default, a revocation request is processed urgently.

The CA shall process revocation requests as soon as possible after receipt, preferably immediately, and within less than 24 hours. This period refers to the time between receipt of the authenticated revocation request and the provision of revocation information (through CRLs and OCSP service) to relying parties.

The revocation service is available 7 days a week and 24 hours a day.

The CA guarantees a maximum downtime by service interruption (failure or maintenance) of the revocation management function of 1 hour and a maximum total downtime of 4 hours per month.

4.9.5.2 CA and component certificates

The revocation of the certificate of a PKI component is carried out immediately upon detection of an event described in the possible causes of revocation.

The revocation of a CA signature certificate (signature of certificates, CRL/ARL) is carried out immediately, particularly if the private key is compromised.

4.9.6 Revocation checking requirement for relying parties

Relying parties are required, before using it, to check the status of the certificates of the entire corresponding certification chain by consulting the appropriate LCR and LAR or by using the OCSP service.

4.9.7 CRL issuance frequency

The frequency of generating a CRL depends on the CA that generates it.

Below are the characteristics of the CRLs (ARLs) generated by the Root CA:

Entity	CRL validity period	Issuing frequency
Nexus GO eID Root CA G**[n]***	18 months + 30 days	12 months (or immediately after a revocation)

Below are the characteristics of the CRLs (ARLs) generated by the Intermediate CA:

Entity	CRL validity period	Issuing frequency
Nexus GO eID Intermediate CA G**[n]***	1 month + 10 days	1 month (or immediately after a revocation)

Below are the characteristics of the CRLs generated by the Issuing CA:

Entity	CRL validity period	Issuing frequency
[Customer Name] Issuing CA G**[n]***	1 week (7 days)	1 day (or immediately after a revocation)

For the Issuing CA, a new CRL is generated and published at least every 24 hours. The CA does not implement the CRL delta mechanism. In the event of revocation of an end-user certificate, the CRL is immediately generated.

4.9.8 Maximum latency for CRLs

For Root CA:

After being generated, the CRL (ARL) is published within a maximum of 24 hours.

For Intermediate CA:

After being generated, the CRL (ARL) is published within a maximum of 30 minutes.

For Issuing CA:

After being generated, the CRL is published within a maximum of 30 minutes.

4.9.9 On-line revocation/status checking availability

The 'Nexus GO Workforce LoA' service provides an OCSP (Online Certificate Status Protocol) response service available and accessible at the address cited in section 2.1.

The response time of the OCSP responder to a status request is less than 10 seconds.

4.9.10 On-line revocation checking requirements

See section 4.9.6.

4.9.11 Other forms of revocation advertisements available

Not applicable.

4.9.12 Special requirements regarding key compromise

For end-user certificates, entities authorized to make a revocation request are required to do so without delay after becoming aware that the private key has been compromised.

For CA and component certificates, the revocation information following the compromise of the private key will be relayed to affected Customers and relying parties (e.g. by email, on the Nexus website and possibly by other means if necessary).

4.9.13 Circumstances for suspension

The suspension of certificates is not authorized under this CP.

4.9.14 Who can request suspension

The suspension of certificates is not authorized under this CP.

4.9.15 Procedure for suspension request

The suspension of certificates is not authorized under this CP.

4.9.16 Limits on suspension period

The suspension of certificates is not authorized under this CP.

4.10 Certificate status service

4.10.1 Operational characteristics

The CA provides relying parties the information allowing them to verify and validate, prior to its use, the status of a certificate and the entire corresponding certification chain (up to and including the Root CA), also to verify the signatures of the certificates in the chain, the signatures guaranteeing the origin and integrity of the CRLs (and ARLs) and the status of the certificate of the Root CA

As a reminder, the CRLs and OCSP responses issued within the PKI are signed as follows:

- The CRL (ARL) are signed by the same Root CA that the one used to sign CA certificates,
- The CRL (ARL) are signed by the same Intermediate CA that the one used to sign Issuing CA certificates,
- The CRL are signed by the same Issuing CA that the one used to sign end-user certificates.
- The OCSP responses are signed by an OCSP certificate issued by the same CA certificate that the one used to sign end-user certificates.

The certificate status information provides relying parties a free consultation mechanism for CRLs (ARLs) in V2 format and an accessible OCSP responder.

The distribution points of the CRL are indicated in the certificate profiles described in section 7 of this document.

The access point of the OCSP responder is indicated in section 2.1 and in the certificate profiles described in section 7 of this document.

Note: Revocation status information is available beyond the validity period of the certificates. The CRLs does not contain the serial numbers of certificates that expired after their revocation.

4.10.2 Service availability

The certificate status information service is available 24 hours a day, 7 days a week. For specific details regarding availability please refer to Nexus Support and Maintenance Description.

4.10.3 Optional features

Not applicable.

4.11 End of subscription

In the event of the termination of a contractual, hierarchical or regulatory relationship between the CA and the Customer prior to the end of the validity of its end-user's certificates, for one reason or another, the certificates are revoked.

4.12 Key escrow and recovery

Private keys associated with end-user's authentication and signature certificates cannot be held in escrow.

CA keys shall not, under any circumstances, be held in escrow.

5 Physical, procedural and personnel security controls

5.1 Physical controls

5.1.1 Site location and construction

The PKI's operating sites comply with current regulations and standards as well as any specific requirements in the event of risks such as earthquakes or explosions (proximity to a factory area or chemical warehouses, etc.).

5.1.2 Physical access

The PKI resources and information used in its implementation are installed in an operating room, access to which is controlled and restricted to authorized persons only.

The access control system ensures the traceability of access to the areas where PKIs are hosted. Outside business hours, security is standard through the use of physical and logical intrusion detection methods. If unauthorized persons are required to enter operating rooms, they shall be handled by an authorized person who shall ensure their supervision. These persons shall be accompanied at all times by authorized personnel.

The machines are installed within a trusted perimeter that respects the separation of trusted roles as provided for in this CP. This security perimeter ensures that the functions and information hosted on the machines are only accessible to people with recognized and authorized trusted roles.

5.1.3 Power and air conditioning

Power protection and air conditioning generation systems shall be implemented to ensure the availability and continuity of the services provided, in particular the revocation management service and the certificate status information service.

The equipment used to provide the services is operated in accordance with the conditions defined by their suppliers and/or manufacturers.

5.1.4 Water exposures

The systems are installed in such a way that they are not sensitive to flooding and other liquid spills and flows.

5.1.5 Fire prevention and protection

In order to ensure the availability of the PKI's computer systems, systems for generating electricity and protecting electrical installations are implemented. The characteristics of the power supply and air conditioning equipment make it possible to comply with the conditions of use of PKI equipment as defined by their suppliers.

5.1.6 Media storage

The various information involved in the PKI's activities is identified and their security needs defined (in terms of confidentiality, integrity and availability). The CA maintains an inventory of this information and has put in place measures to prevent the compromise and theft of this information.

In particular, the media (paper, hard disk, USB keys, CDs, etc.) containing this information are managed in accordance with the defined security needs: protection against theft, damage and unauthorized access, etc.

5.1.7 Waste disposal

Information media are destroyed at the end of their life.

The procedures and means of destruction shall be in accordance with the level of confidentiality of the relevant information.

5.1.8 Off-site backup

The operator shall perform off-site backups to enable rapid recovery of PKI services following the occurrence of a disaster or event that seriously and permanently affects the performance of its services, in accordance with the CA's undertakings in terms of availability, in particular for revocation management services and certificate status information.

Information backed up off-site shall comply with the requirements of this CP for the protection of the confidentiality and integrity of such information.

Backup and recovery functions are performed by ad-hoc trust roles in accordance with procedural security measures.

5.2 Procedural controls

5.2.1 Trusted roles

People are aware of and understand the implications of the operations for which they are responsible. Persons in a trusted role shall not have any conflict of interest that could affect the impartiality of operations within the PKI.

The CA's trusted roles are classified into 5 groups:

- **Security Officer** - The Security Officer is responsible for the implementation of the PKI security policy. S/he manages physical access controls to system equipment. S/he is authorized to examine the archives and is responsible for analyzing event logs in order to detect any incident, anomaly, attempted compromise, etc.
- **Application Manager** - The Application Manager is responsible for the implementation of the PKI CP at the level of the application for which s/he is responsible. Their responsibility covers all the functions rendered by this application and the corresponding performance.
- **Operating manager** - The operating manager ensures that the systems are maintained in fully operational working condition. S/he is responsible for the start-up, configuration and technical maintenance of the component's IT equipment. S/he provides the technical administration of the component's systems and networks.
- **Operator** - An operator within a component of the PKI performs, as part of their responsibilities, the operation of applications for the functions implemented by the component.
- **Controller or auditor** - their role is to regularly check the compliance of the implementation of the functions provided by the component with the CP and the component's security policies. The auditor is appointed by the TSP.

In addition to these trusted roles, the CA has defined the role of Secret Share Holder. The Secret Share Holder is responsible for ensuring the confidentiality, integrity and availability of the share entrusted to him/her. More internal role descriptions can be found in Nexus internal documents for the TSP organization.

5.2.2 Number of persons required per task

The number and type of roles and persons that must be present (as persons involved or witnesses) may be different depending on the type of operations performed.

For reasons of availability, each task must be able to be performed by at least two people.

Sensitive functions (e. g. key ceremonies) are distributed over several people for security reasons.

5.2.3 Identification and authentication for each role

Each entity operating a component of the PKI shall have the identity and authorizations of any of its staff working within the component verified before assigning them a role and the corresponding rights, in particular:

- that their name be added to the access control lists of the entity hosting the component concerned by the role,
- that their name be added to the list of persons authorized to physically access these systems,
- where applicable and depending on the role, that an account be opened in their name in these systems,
- potentially, that cryptographic keys and/or a certificate be issued to it to fulfil its role in the PKI.
- These checks are in accordance with the component's security policy.

Each assignment of a role to a member of the PKI staff shall be notified in writing. This role is clearly mentioned and described in their job description.

5.2.4 Roles requiring separation of duties

Several roles may be assigned to the same person, as long as the accumulation of roles does not compromise the safety of the functions implemented. For trusted roles, however, it is recommended that the same person

does not hold more than one role and at least the following requirements for non-accumulation are met. The responsibilities associated with each role are in accordance with the security policy of the component concerned.

With regard to trust roles, the following accumulations are prohibited:

- security manager and operations manager/operator
- controller and any other role
- operations manager and operator.

More internal role segregation can be found in Nexus internal documents for the TSP organization.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

Each person who works in the CA is subject to a confidentiality clause with respect to their employer. It is also verified that the powers of these persons correspond to their professional skills.

Anyone involved in PKI certification procedures is informed of their responsibilities for PKI services and procedures related to system security and personnel checking.

Management personnel have the appropriate expertise and are familiar with safety procedures.

5.3.2 Background Check Procedures

The CA shall use all legal means at its disposal to ensure the honesty of the staff required to work within the component. This check is based on a background check of the person (employee outside the probationary period). It is specifically checked that each person has not been convicted of a criminal offence (i.e. extract from the criminal record) in contradiction with their powers.

Persons are subject to a specific authorization (with provisions in their employment contract) and their task is defined in relation to their need to know.

Persons in a trusted role shall not have any conflict of interest that could affect the impartiality of their tasks.

These checks are carried out prior to assignment to a trusted role and reviewed regularly (at least every 3 years).

5.3.3 Training requirements

Personnel are trained in the internal software, hardware and operating and security procedures that they implement and must comply with, corresponding to the component in which they operate. Members of staff are aware of and understand the implications of the operations for which they are responsible.

5.3.4 Retraining frequency and requirements

The staff concerned shall receive adequate information and training prior to any changes in systems, procedures, organization, etc., depending on the nature of these changes.

5.3.5 Job rotation frequency and sequence

Not applicable.

5.3.6 Sanctions for unauthorized actions

Sanctions are provided for actions not authorized by the policies and procedures established by the CP and the internal processes and procedures of the PKI, either through negligence or which are carried out maliciously.

5.3.7 Independent contractor requirements

The staff of external service providers working on the premises and/or on the components of the PKI shall also comply with the requirements of this section 5.3. This is reflected in appropriate clauses in contracts with these service providers.

5.3.8 Documentation supplied to personnel

As a minimum, each staff member have adequate documentation regarding the operational procedures and specific tools they implement as well as the general policies and practices of the component in which they work. In particular, s/he shall be given the security policy or policies concerning him/her.

5.4 Audit logging procedures

Event logging consists of recording events manually or electronically by input or automatic generation.

The resulting files, in paper and/or electronic form, make it possible to trace and account for the operations carried out.

5.4.1 Types of events recorded

Each component operating a component of the PKI shall log, as a minimum, the events as described below in electronic form. Logging is automatic from system start-up and uninterrupted until it is shut down.

- Creation/modification/deletion of User accounts (access rights) and corresponding authentication data (passwords, certificates, etc.),
- Start-up and shutdown of computer systems and applications,
- Firewall and router logs,
- Logging events: starting and stopping the logging function, changing logging settings, actions taken following the failure of the logging function, software and hardware failures,
- Logging in/out of Users with trusted roles, and corresponding unsuccessful attempts.

5.4.1.1 Information recorded for each event

Each event record in a log contains the following fields:

- Type of event,
- Name of the executor or reference of the system that triggered the event,

- Date and time of the event,
- Result of the event (failure or success).

Depending on the type of event concerned, the following fields can be saved:

- Recipient of the operation
- Name or identifier of the applicant for the operation or reference of the system making the request
- Name of persons present (if it is an operation requiring several people),
- Cause of the event
- Any information characterizing the event (for example, for the generation of a certificate, its serial number).

Logging operations are performed during the relevant process. In the case of manual entry, the entry is made, except in exceptional cases, on the same working day as the event.

5.4.1.2 Events recorded by 'Nexus GO Workforce LoA' service

Specific events to the different functions of 'Nexus GO Workforce LoA' service must also be logged:

- Receipt of a certificate request (initial and renewal)
- Validation/rejection of a certificate request
- Personalization of media and generation of activation codes
- Sending the operator card to the RA and acknowledgment of receipt
- Generation of end-user key pairs
- Generation of end-user certificates
- Personalization of the PIN code of the end-user's card
- Explicit acceptance or rejection by the end-user
- Activation of the equipment by the end-user
- Receipt of a revocation request
- Validation/rejection of a revocation request
- Events related to signature keys and CA certificates (generation, backup / recovery, destruction, etc.),
- Publication and update of CA-related information (CP, CA certificates, T&C, etc.)
- Generation and publication of CRLs
- OCSP requests and responses.

5.4.1.3 Various events

Other events are also collected. These are security events that are not automatically generated by the systems implemented:

- Physical access to sensitive areas,
- System maintenance and configuration change actions,
- Changes to staff in trusted roles,
- Actions to destroy and reset media containing confidential information (keys, activation data, passwords or end-user code, etc.).

5.4.1.4 Accountability

Accountability for an action rest with the person, organization or system that carried it out. The name or identifier of the executor is explicitly included in one of the fields of the event log.

5.4.2 Frequency of processing log

Event logs are checked and analyzed by a security manager to identify anomalies related to failed attempts at the frequency defined in section 5.4.8.

5.4.3 Retention period for audit log

Event logs are kept on site for at least 10 years. They are archived as soon as possible after their generation and at the latest within 1 month (possible recovery between the on-site storage period and the archiving period).

5.4.4 Protection of audit log

Logging is designed and implemented to limit the risk of bypassing, modifying or destroying event logs. Integrity check mechanisms are in place to detect any changes, voluntary or accidental, to these logs. The availability of event logs is protected (against loss and partial or total destruction, voluntary or not).

Systems generating event logs (except physical access control systems) are synchronized to a reliable source of UTC time (see section 6.8).

5.4.5 Audit log backup procedures

Logging is designed and implemented to limit the risk of bypassing, modifying or destroying event logs. Integrity check mechanisms are in place to detect any changes, voluntary or accidental, to these logs.

The availability of event logs is protected (against loss and partial or total destruction, voluntary or not).

The event dating system associates all archives with an archive generation date.

The definition of the sensitivity of event logs depends on the nature of the information contained. It may lead to a need for confidentiality protection.

5.4.6 Audit collection system (internal or external)

The log collection system may be internal or external to the components of the PKI. The system ensures the collection of archives while respecting the level of security relating to data integrity, availability and confidentiality.

5.4.7 Notification to event-causing subject

The TSP chooses not to notify the event responsible of the recording of an event.

5.4.8 Vulnerability assessment

Each entity operating a component of the PKI is able to detect any attempt to violate the integrity of the component in question.

Event logs are checked at least once per business day to identify anomalies related to failed attempts.

The logs are analyzed in their entirety once a day and as soon as an anomaly is detected. This analysis results in a summary in which important elements are identified, analyzed and explained. The summary shows the anomalies and falsifications found.

A reconciliation between the different RA and CA event logs is performed at least once a month, in order to verify the concordance between dependent events and thus help to reveal any anomalies.

In addition, a vulnerability scan is periodically carried out as part of an intrusion test campaign. The preferred method for performing these intrusion tests is a technical audit performed by a qualified information systems security audit service provider.

The vulnerabilities detected during these regular or spot checks are analyzed to identify and assess their possible consequences and impacts. Depending on the criticality of the impact, an action plan is implemented to mitigate these vulnerabilities.

5.5 Records archival

5.5.1 Types of records archived

The data archived at the level of each component is as follows:

- Software and configuration files for each component,
- The certification policy and certification practice statement,
- Certificates, CRLs and OCSP responses as issued or published,
- Certificate application records including the identity documents of the end-users, and their parent company where applicable,
- Event logs of the different components of the PKI.

5.5.2 Retention period for archive

5.5.2.1 Certificates and CRLs issued by the CA

The retention period for certificates and CRLs issued by the CA, as well as for CA certificates and ARLs, is 10 years after their expiry.

5.5.2.2 OCSP responses

OCSP responses are archived for at least three months after their expiry.

5.5.2.3 Events logs

The event logs as addressed in section 5.4 is 10 years after their generation.

5.5.3 Protection of archive

Throughout the entire period of their conservation, the archives:

- Are protected in terms of integrity,
- Are accessible only to authorized persons,
- Can be reviewed or used,
- Are audited and tested regularly (access, readability, exploitation and the absence of format distortion depending on the archiving media)

5.5.4 Archive backup procedures

The TSP is responsible for implementing and maintaining the necessary measures to ensure the integrity and availability of the archives as required in this CP.

The CPS describes the procedure for saving archives. The level of protection of backups is at least equivalent to the level of protection of archives.

5.5.5 Requirements for timestamping of records

Section 6.8 specifies the dating and time-stamping requirements.

5.5.6 Archive collection system (internal or external)

The system ensures the collection of archives while respecting the level of security of the archives as required by section 5.5.3.

5.5.7 Procedures to obtain and verify archive information

The archives are retrievable within less than 2 working days, knowing that only the CA can access all archives (as opposed to an entity operating a component of the PKI that can only retrieve and consult the archives of the component in question).

5.6 Key changeover

The life span of the CA certificate is determined according to the validity period of the associated private key, in accordance with the security cryptographic recommendations for key lengths, including the recommendations of the relevant national or international authorities.

The CA may not generate certificates whose life span exceeds the validity period of its CA certificate. Therefore, the CA key pair is renewed no later than the expiry date of the CA certificate minus the life span of the certificates issued.

As soon as a new private key is generated for the CA, only that key is used to generate new Holder certificates. The previous CA certificate remains valid to validate the certification path of the old certificates issued by the previous CA private key, until the expiry of all Holder certificates issued using this key pair.

In addition, the CA changes its key pair and the corresponding certificate when the key pair ceases to comply with cryptographic security recommendations regarding key size or if it is suspected it is compromised.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling

Each entity acting on behalf of the PKI implements incident reporting and incident handling procedures. This is achieved through awareness raising and staff training and through the analysis of event logs.

In the case of a major incident, such as loss, suspicion of compromise, compromise, or theft of the CA private key, the initiating event is the recognition of this incident at the level of the component concerned, which immediately informs the CA. A major incident scenario must be dealt with as soon as it is received and the publication of information on the revocation of the certificate, if necessary, is made in the greatest urgency, or even immediately, by any useful or available means. If any of the algorithms, or associated parameters, used by the CA or its end-users become insufficient for its remaining intended use, then the CA shall notify all end-users and third-party Certificate Users with whom the CA has entered into agreements. In addition, all the certificates concerned shall be revoked.

In accordance with regulatory requirements, the National Supervisory Body (DIGG) will be informed of any security incidents affecting the CA and its services within 24 (twenty-four) hours.

5.7.2 Computing resources, software and/or data are corrupted

Each component of the PKI has a business and service continuity plan that addresses the availability requirements of the various PKI functions resulting from this CP, the CA's commitments with respect to the functions related to the publication and revocation of certificates.

This continuity plan is tested at least once a year and corrective measures, if any, are implemented.

5.7.3 Entity private key compromise procedures

The case of compromise of an infrastructure key or component check is treated in the component's continuity plan as a disaster.

In the event of compromise of a CA key, the corresponding certificate is immediately revoked as specified in section 4.9.

In addition, the CA meets the following commitments:

- Immediately stop using the key of the compromised component,
- Inform without delay: all end-users, Customer entities with which the CA has entered into agreements and relying parties,

- Indicate without delay that certificates and revocation status information issued using this CA key may no longer be valid.
- Notify DIGG of the compromise,
- If necessary, file a complaint with the competent authorities.

5.7.4 Business continuity capabilities after a disaster

The various components of the PKI have the necessary resources (technical, organizational and human) to ensure the continuity of their activities in accordance with the requirements of this CP (see section 5.7.2).

5.8 CA or RA termination

One or more components of the PKI may have to cease their activity or transfer it to another entity for various reasons.

The CA takes the necessary steps to cover the costs of meeting these minimum requirements in the event that the CA is bankrupt or for other reasons is unable to cover these costs on its own, to the extent possible, within the constraints of applicable bankruptcy legislation.

The transfer of activity is defined as the end of activity of a component of the PKI that does not affect the validity of certificates issued prior to the transfer and the resumption of that activity organized by the CA in collaboration with the new entity. The new entity guarantees an adequate level of trust, the maintenance of financial guarantees and continuity of service (including archiving, maintenance of confidentiality, interoperability of certificates, etc.).

Termination of activity is defined as the end of activity of a component of the PKI that affects the validity of certificates issued prior to the termination in question. Thus, the certificates issued will be revoked without delay and the entities informed of the revocation of the certificates.

In the event of cessation of activity, the CA or, if this is not possible, any entity substituted by a law, regulation, court decision or agreement previously concluded with such entity, shall ensure the revocation of certificates and the publication of ARLs/CRLs in accordance with the undertakings made in the CP.

In the event of a transfer of activity, the CA notifies the Certificate end-users in the event that the proposed changes may affect the undertakings made and shall do so at least within one month. It will also provide information to the administrative authorities.

In the event of cessation of activity, the CA shall notify the Certificate end-users within one month. It will also provide information to the administrative authorities.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 End-user keys generated by the End-user (decentralized)

For a key generation on a smartcard:

The personalization operation of the end-user's card, including in particular the generation of the end-user's key pair, is triggered by the RA in presence of the end-user.

The end-user’s key pair is generated on the card intended for the end-user.

For a key generation on Mobile ID:

The personalization operation of the end-user's Mobile ID, including in particular the generation of the end-user's key pair, is triggered by the RA in presence of the end-user or via ID exchange from the self-service portal.

The end-user’s key pair is generated on the mobile id intended for the end-user.

6.1.1.2 End-user keys generated by the CA (centralized)

Not applicable.

6.1.1.3 CA and component keys

The generation of the key pairs associated with the CA certificate takes place during a key ceremony using a hardware cryptographic resource certified FIPS 140-2 level 2 (or higher) or certified Common Criteria EAL4+.

Key ceremonies are conducted under the control of at least three persons in trusted roles (master of ceremonies and witnesses, at least external to the CA). Witnesses shall provide objective and factual evidence of the conduct of the ceremony in relation to the script previously approved by the CA.

Following their generation, the secret shares (activation data) are given to previously designated activation data Holders who are authorized by the CA to perform this trusted role. Regardless of the form (paper, magnetic media or confined to a smart card or USB key), a holder may not hold more than one CA secret share at any one time. Each secret share is implemented by its holder.

Information about private keys of other PKI system components is described in the CPS.

6.1.2 Private key delivery to end-user

For a key generation on a smartcard:

The end-user's private key is generated by the end-user's card during an operation which is triggered by the RA and validated by the end-user via his activation code.

Once the card is given to the end-user, the private key is maintained under the sole control of the end-user.

For a key generation on Mobile ID:

The end-user's private key is generated by the end-user's Mobile during an operation which is triggered by the RA and validated by the end-user via his activation code.

It can also be triggered from end-user via self-service ID exchange.

Once the Mobile ID is given to the end-user, the private key is maintained under the sole control of the end-user.

6.1.3 Public key delivery to certificate issuer

The end-user's certificate request is transmitted to the CA in PKCS#10 format, which ensures the integrity of the key and authenticates the origin.

6.1.4 CA public key delivery to relying parties

The Issuing CA's public signature verification keys are distributed to relying parties in a manner that ensures their end-to-end integrity and authenticates their origin.

The Issuing CA public key is issued in a certificate signed by the Intermediate CA. The public key of the Intermediate CA is distributed in a certificate signed by the Root CA. The public key of the Root CA is distributed in a self-signed certificate.

The Issuing CA, Intermediate CA and Root CA certificates are available at the URLs listed in section 2.1 of this CP.

6.1.5 Key sizes

The recommendations of the competent national and international bodies (concerning key lengths, signature algorithms, hash algorithms, etc.) are periodically consulted to determine whether or not the parameters used in the issue of Holder and CA certificates should be modified.

6.1.5.1 End-user keys

End-user keys are at least 2048-bit RSA keys, following the WebTrust requirements.

6.1.5.2 CA and component keys

CA keys (Root CA, Intermediate CA, Issuing CA) are 4096-bit RSA keys.

CA key pairs with a complexity of less than 4096 bits for the RSA algorithm are not supported by this CP.

6.1.6 Public key parameters generation and quality checking

The equipment used for the generation of the CA and end-user key pairs are material cryptographic resources that comply with the security standards corresponding to the key pair (see section 6.1.5).

6.1.7 Key usage purposes

The use of the CA's private key and associated certificate is strictly limited to signing certificates and CRLs.

The use of the end-user's private key and associated certificate is strictly limited to the security function in question (see sections 1.4.1.1 and 4.5).

6.2 Private Key protection and cryptographic module controls

6.2.1 Cryptographic module standards and controls

6.2.1.1 CA cryptographic module

The CA cryptographic modules (for the generation and implementation of its signature keys) and OCSP responder cryptographic modules are certified FIPS 140-2 level 2 (or higher) or certified Common Criteria EAL4+.

The CA implements procedures for:

- ensuring the integrity of the cryptographic modules during storage and transport,
- ensuring that the cryptographic modules are working properly,
- ensure that operations on cryptographic modules are performed by at least two staff members in trusted roles.

6.2.1.2 Devices for protecting the secret elements of end-user

For a key pair and a certificate stored in a smartcard:

Qualified Signature Creation Devices (QSCD) are used for the protection of private keys. The smartcard models in use must be certified as QSCD and approved by Digg prior to deployment.

For a key pair and a certificate stored in Mobile ID:

Mobile ID has a layered security model that includes features such as:

- Private key security and storage with non-exportable keys.
- AES-encrypted storage of cryptographic keys, protected by user PINs.
- Support for biometrics (e.g., fingerprint and facial recognition) for additional security.
- Regular security reviews and updates to ensure the app is protected against vulnerabilities.
- Jailbreak and root detection to ensure the app runs in a safe environment.
- Secure communication channels using HTTPS and certificate pinning.

More details are available on the public documentation page for Mobile ID.

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

This section deals with the control of the CA private key for export/import out of/into the cryptographic module. The generation of the key pair is treated in section 6.1.1, the activation of the private key in section 6.2.8 and its destruction in section 6.2.10.

The checking of private CA signature keys is carried out by trusted personnel (Secret Holders) and implements a secret sharing tool (3 operators out of 5 must authenticate themselves).

6.2.3 Private key escrow

No private keys associated with certificates are held in escrow.

6.2.4 Private key backup

CA private keys are the subject of backup copies, either in a cryptographic module achieving the same level of security as those stipulated in the section 6.2.1.1, or outside a cryptographic module but in this case in encrypted form and with an integrity check mechanism. The corresponding encryption offers a level of security equivalent to or greater than the storage within the cryptographic module and, in particular, is based on an algorithm of a key length and with an operating mode capable of resisting attacks by cryptanalysis for at least the lifespan of the key thus protected.

The encryption and decryption operations are carried out inside the cryptographic module in such a way that the CA private keys are never in the clear outside the cryptographic module.

End-user private keys are not backed up by the CA.

6.2.5 Private key archival

Under any circumstances, CA private keys are not archived.

The end-user private keys are not archived under any circumstances by the CA or any of the components of the PKI.

6.2.6 Private key transfer into or from a cryptographic module

6.2.6.1 End-user keys

If the CA generates the end-user's private key outside the end-user's device, the transfer of the end-user’s private key in the card is carried out in accordance with the requirements of section 6.1.1.2.

6.2.6.2 CA and component keys

CA keys are generated, activated and stored in hardware cryptographic resources.

When not stored in hardware cryptographic resources or during their transfer, CA private keys are encrypted by the AES algorithm (FIPS 197). A CA private key cannot be decrypted without the use of a hardware cryptographic resource and the presence and authentication of several persons holding trusted roles.

6.2.7 Private Key storage on cryptographic module

CA private keys stored in hardware cryptographic resources are protected with the same level of security as the one with which they were generated.

6.2.8 Method of activating the private key

6.2.8.1 End-user private keys

For a key pair and a certificate stored in a smartcard:

The end-user defines their PIN code during the card personalization operation.

Activation of end-user' private keys requires entry of the card's PIN code, under the exclusive control of the end-user.

The device used is such that the end-user’s private key can only be activated upon presentation of a PIN code.

During a signature operation, after the card has calculated the signature, the card invalidates the “PIN code submitted” status. This mechanism requires the PIN code to be entered systematically for each signature calculated by the card.

The device is blocked after several unsuccessful attempts to enter the PIN code. This mechanism protects the device in the event of a PIN code search by an unauthorized third party.

For a key pair and a certificate stored in Mobile ID:

The end-user defines their PIN code during the Mobile ID personalization operation.

Activation of end-user' private keys requires entry of the Mobile ID PIN code, under the exclusive control of the end-user.

The device used is such that the end-user’s private key can only be activated upon presentation of a PIN code.

During a signature operation, after the Mobile ID has calculated the signature, the Mobile ID invalidates the “PIN code submitted” status. This mechanism requires the PIN code to be entered systematically for each signature calculated by the Mobile ID.

The device is blocked after several unsuccessful attempts to enter the PIN code. This mechanism protects the device in the event of a PIN code search by an unauthorized third party

6.2.8.2 CA and component private keys

CA private keys can only be activated in the cryptographic module with a minimum of 3 people in trusted roles (Secret Holders) and who hold activation data for the CA in question.

6.2.9 Method of deactivating the private key

6.2.9.1 End-user private keys

For a key pair and a certificate stored in a smartcard:

Deactivation of the private key is the end-user's responsibility.

To ensure deactivation of the private key, the end-user removes the card from the workstation or logs off of their system after use.

For a key pair and a certificate stored in Mobile ID:

Deactivation of the private key is the end-user's responsibility.

To ensure deactivation of the private key, the end-user removes the Mobile from the mobile device.

6.2.9.2 CA and component private keys

Hardware cryptographic resources in which CA keys have been activated shall not be left unattended or accessible to unauthorized persons. After use, hardware cryptographic resources are disabled. Cryptographic resources are then stored in a secure area to prevent unauthorized handling by roles that are not highly authenticated.

Furthermore, the deactivation of CA private keys in a cryptographic module is automatic as soon as the module's environment changes: shutdown or disconnection of the module, disconnection of the operator, etc.

6.2.10 Method of destroying private key

6.2.10.1 End-user private keys

For a key pair and a certificate stored in a smartcard:

After the card issuance, the end-user is the only one who can destroy the private key (by deleting the keys with the manufacturer’s software or by physical destruction of the card).

For a key pair and a certificate stored in Mobile ID:

After the Mobile ID issuance, the end-user is the only one who can destroy the private key (by deleting the keys with the mobile operating systems function).

6.2.10.2 CA and component private keys

CA private keys are destroyed when they are no longer in use or when the certificates to which they correspond have expired or been revoked. The destruction of a private key involves the destruction of backup copies, activation data and the deletion of the cryptographic resource containing it, so that no information can be used to find it. The destruction of a CA private key is carried out in the presence of witnesses and is recorded in a report.

6.2.11 Cryptographic module rating

6.2.11.1 CA cryptographic module

The cryptographic modules used by the CAs and the OCSP responder are evaluated at EAL4+ level or certified FIPS 140-2 level 2 (or higher).

Private keys of Subordinate CAs, and their indirect OCSP and CRL signers are generated, stored, and operated in FIPS 140-2 level 2 or Common Criteria EAL 4+, or higher, compliant Hardware Security Modules. A specific protection profile is not required.

6.2.11.2 Devices for protecting the secret elements of end-user

For a key pair and a certificate stored in a smartcard:

Devices issued by the CA are assessed at EAL4+ level.

The CA monitors devices certification.

For a key pair and a certificate stored in Mobile ID:

6.3 Other aspects of key pair management

6.3.1 Public key archival

The public keys of the CA and the end-user are archived as part of the archiving of the corresponding certificates.

6.3.2 Certificate operational periods and key pair usage periods

The Root CA certificate is valid for 30 years. The life span of the corresponding key pair is equivalent, i.e. also 30 years. The Root CA certificate expires after the end of the Intermediate CA certificate it issues.

The Intermediate CA certificate is valid for 30 years. The life span of the corresponding key pair is equivalent, i.e. also 30 years. The Intermediate CA certificate expires after the end of the Issuing CA certificate it issues.

The Issuing CA certificate is valid for 15 years. The life span of the corresponding key pair is equivalent, i.e. also 15 years. The Issuing CA certificate expires after the end of the end-user certificates it issues.

The end-user certificates covered by this CP have a maximum validity period of 5 years. The life span of the key pairs is equivalent, i.e. also 5 years max.

6.4 Activation data

6.4.1 Activation data generation and installation

6.4.1.1 Generation and installation of activation data corresponding to the CA private key

CA private key activation data is generated during key ceremonies (refer to section 6.1.1.3). The activation data is automatically generated according to a Shamir threshold scheme (type M (3) of N (5)). In all cases, the activation data is given to its Holders after generation during the key ceremony. Holders of Activation Data are persons authorized for this trusted role.

6.4.1.2 Generation and installation of activation data corresponding to the end-user private key

For a key pair and a certificate stored in a smartcard:

The end-user's private keys are generated on the card at the time of delivery.

The activation code (in the form of an OTP code) is sent by email directly to the end-user.

During the card issuance session, the user must define a PIN code which he must keep secret and under his sole control.

For a key pair and a certificate stored in Mobile ID:

The end-user's private keys are generated on the Mobile device at the time of delivery.

The activation code is presented on the RA’s computer screen after ID identification of the end-user has been made.

When ID exchange identification via self-service is used, then the activation code is shown directly for end-user.

During the Mobile ID issuance session, the user must define a PIN code which he must keep secret and under his sole control.

6.4.2 Activation data protection

6.4.2.1 Protection of activation data corresponding to the CA private key

The activation data which is generated for the CA cryptographic modules is protected in integrity and confidentiality until delivery to their recipient. This recipient is then responsible for ensuring its confidentiality, integrity and availability.

Activation data is protected from disclosure by a combination of cryptographic and physical access control mechanisms. Holders of activation data are responsible for their management and protection. An activation data holder cannot hold more than one activation data from the same CA at the same time.

6.4.2.2 Protection of activation data corresponding to the end-user private key

For a key pair and a certificate stored in a smartcard:

The activation code allowing the end-user's card personalization operation to be triggered is sent to the end-user by email.

The card PIN code is initialized by the end-user during the personalization operation.

End-users are responsible for the confidentiality of their PIN codes, so that only they can use the private key. In the event of a suspected loss of confidentiality, the end-users undertake to modify these PIN codes.

For a key pair and a certificate stored in Mobile ID:

The Mobile ID PIN code is initialized by the end-user during the personalization operation.

End-users are responsible for the confidentiality of their PIN codes, so that only they can use the private key. In the event of a suspected loss of confidentiality, the end-users undertake to modify these PIN codes.

6.4.3 Other aspects of activation data

Not applicable.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The following functions are provided by the operating system, or by a combination of the operating system, software and physical protective mechanisms.

A component of a PKI includes the following functions:

- Strong identification and authentication of trusted roles (physical and logical access),
- Management of access rights based on profiles respecting the least privilege principle,
- Management of user sessions (disconnection after a period of inactivity, management of file access rights),
- Prohibition of the reuse of objects,
- Requires the use of cryptography for communications,
- Ensures the rigorous separation of tasks,
- Protection against computer viruses,
- Protection of the network against illegal intrusion,
- Performs security monitoring to ensure that security patches are regularly applied to IT systems and that critical vulnerabilities are addressed within 48 hours,
- Provides self-protection of the operating system,
- Audit function.

6.5.2 Computer security rating

When a PKI component is hosted on a platform assessed for security assurance requirements, it is used in its certified version. At least the component uses the same operating system version as the one on which the component was certified.

6.6 Life cycle technical controls

Security measures relating to the life cycles of IT systems meet the security objectives that result from the risk analysis conducted by the CA.

6.6.1 System development controls

System developments are controlled by the following measures:

- Purchase of hardware and software to reduce the possibility of a particular component being altered,
- The hardware and software developed were developed in a controlled environment, and the development process defined and documented. This requirement does not apply to commercially purchased hardware and software,
- All hardware and software must be shipped or delivered in a controlled manner allowing continuous monitoring from the place of purchase to the place of use,
- It is necessary to take care not to download malware on PKI equipment. Only applications required to perform CA activities are acquired from sources authorized by applicable CA policy. CA hardware and software are scanned for malicious code on first use and periodically thereafter,
- Hardware and software updates are purchased or developed in the same way as the originals and are installed by trusted personnel who are trained in accordance with current procedures.

6.6.2 Security management controls

The configuration of the CA system, as well as any modification or change, shall be documented and checked by the CA.

There is a mechanism in place to detect any unauthorized changes to the software or CA configuration. A formal configuration management method is used for the installation and subsequent maintenance of the PKI system. When it is first loaded, it is checked that the PKI software corresponds to the one delivered by the seller, that it has not been modified before being installed, and that it corresponds to the desired version.

6.6.3 Life-cycle security controls

With respect to the software and hardware evaluated, the CA continues to monitor the requirements of the maintenance process to maintain the level of trust.

Any significant system change of a PKI component is tested and validated before deployment. These operations are carried out by trusted personnel.

6.7 Network security controls

Interconnection to public networks is protected by security gateways configured to accept only those protocols necessary for the operation desired by the CA and to counter denial of service or intrusion attacks. In this case, the network is equipped with routers, firewalls with IPS intrusion detection system with alerting.

The CA ensures that local network components are maintained in a physically secure environment and that their configurations are periodically audited for compliance with the requirements specified by the CA.

The IT systems administration network is logically separate from the operating network.

6.8 Time stamping

There is no time stamp used by the CA but an event date that allows the CA to sequence events from the PKI system time.

Automatic or manual procedures are used to synchronize PKI system clocks with each other, at least to the nearest minute, and with respect to a reliable source of UTC time, at least to the nearest second.

7 Certificate, CRL and OCSP profiles

7.1 Certificate Profile

7.1.1 CA certificate profile

7.1.1.1 Root CA certificate profile

The fields of Root CA certificate are as follows:

Nexus GO eID Root CA	
Basic fields	**Value**
Version	2 (=version 3)
Serial Number	Defined by the PKI
Issuer	C = SE O = Technology Nexus Secured Business Solutions AB CN = Nexus GO Root CA G2
Validity	30 years
Subject	C = SE O = Technology Nexus Secured Business Solutions AB CN = Nexus GO Root CA G[n]*
Subject Public Key Info	4096 bits
Signature Algorithm	SHA-512 With RSA Encryption

The extensions of Root CA certificate are as follows:

Extensions	Criticality	Value
Authority Key Identifier	N	Identifier of the Root CA public key
Basic Constraints	O	Basic constraints: SubjectType=CertAuthority PathLengthConstraint=2
Certificate Policies	N	Certificate strategies: All issuing strategies https://pki.nexusgroup.com/
CRL Distribution Points	N	ARL distribution point: URL= http://dp.eid.prod.go.nexusgroup.com/crl/nexus-go-root-ca-g2-ca.crl
Key Usage	O	Certificate signature Signing of the revocation list off-line Signing of the revocation list
Subject Key Identifier	N	Identifier of the CA public key

7.1.1.2 Intermediate CA certificate profile

The fields of Intermediate CA certificate are as follows:

Nexus GO eID Intermediate CA	
Basic fields	**Value**
Version	2 (=version 3)
Serial Number	Defined by the PKI
Issuer	C = SE O = Technology Nexus Secured Business Solutions AB CN = Nexus GO Root CA G[n]*
Validity	30 years
Subject	C = SE O = Technology Nexus Secured Business Solutions AB CN = Nexus GO SE Intermediate CA GN*
Subject Public Key Info	4096 bits
Signature Algorithm	SHA-512 With RSA Encryption

The extensions of Intermediate CA certificate are as follows:

Extensions	Criticality	Value
Authority Key Identifier	N	Identifier of the Intermediate CA public key

Basic Constraints	O	Basic constraints: SubjectType=CertAuthority PathLengthConstraint=1
Certificate Policies	N	Certificate strategies: All issuing strategies https://pki.nexusgroup.com/
CRL Distribution Points	N	ARL distribution point: URL= http://dp.eid.prod.go.nexusgroup.com/crl/nexus-go-se-intermediate-ca-g2.crl
Key Usage	O	Certificate signature Signing of the revocation list off-line Signing of the revocation list
Subject Key Identifier	N	Identifier of the CA public key

7.1.1.3 Issuing CA certificate profile

The fields of Issuing CA certificate are as follows:

[Customer] Issuing CA	
Basic fields	**Value**
Version	2 (=version 3)
Serial Number	Defined by the PKI
Issuer	C = SE O = Technology Nexus Secured Business Solutions AB CN = Nexus GO SE Intermediate CA G[n]
Validity	15 years
Subject	C = SE O = [Customer organization] CN = [Customer Name] Issuing CA G[n]
Subject Public Key Info	4096 bits
Signature Algorithm	SHA-256 With RSA Encryption

The extensions of Issuing CA certificate are as follows:

Extensions	Criticality	Value
Authority Key Identifier	N	Identifier of the Issuing CA public key
Basic Constraints	O	Basic constraints: SubjectType=CertAuthority PathLengthConstraint=0
Certificate Policies	N	Certificate strategies: All issuing strategies https://pki.nexusgroup.com/

CRL Distribution Points	N	CRL distribution point: URL= http://dp.eid.prod.go.nexusgroup.com/crl/[customer]-issuing-ca-g1-ca.crl
Key Usage	O	Certificate signature Signing of the revocation list off-line Signing of the revocation list
Subject Key Identifier	N	Identifier of the CA public key

7.1.2 End-user certificate profile

See LoA-End-Cert-Template.

7.2 CRL profile

The fields of CRL are as follows:

CRL profile			
Basic fields	**Value**		
Version	1 (=version 2)		
Issuer	**Root CA**	**Intermediate CA**	**Issuing CA**
	C = SE O = Technology Nexus Secured Business Solutions AB CN = Nexus GO Root CA G[n]	C = SE O = Technology Nexus Secured Business Solutions AB CN = Nexus GO SE Intermediate CA G[n]	C = SE O = [Customer organization] CN = [Customer Name] Issuing CA G[n]
This Update	Date CRL generated		
Next Update	Next publication date (Deadline for issuing the next CRL)		
Revoked certificates	List of serial numbers of revoked end-user certificates		

The extensions of a CRL are as follows:

Extensions	Criticality	Value
Authority Key Identifier	N	Contains the key identifier of the issuing CA's public key (same value as the "Subject Key Identifier" field of the Issuing CA's certificate).
CRLNumber	N	CRL serial number

7.3 OCSP profile

7.3.1 OCSP certificate profile

The fields of OCSP responder certificate are as follows:

OCSP certificate	
Basic fields	**Value**
Version	2 (=version 3)
Serial Number	Defined by the PKI
Issuer	C = SE O = [Customer organization] CN = [Customer] Issuing CA G[n]
Validity	1 year
Subject	C = SE O = [Customer organization] OI = [Identifier of the Customer Entity] CN = [OCSP service name]
Subject Public Key Info	4096 bits
Signature Algorithm	SHA-256 With RSA Encryption

The extensions of OCSP responder certificate are as follows:

Extensions	Criticality	Value
Authority Key Identifier	N	Contains the key identifier of the issuing CA's public key (same value as the "Subject Key Identifier" field of the Issuing CA's certificate).
Subject Key Identifier	N	Identifier of the OCSP responder's public key
Key Usage	O	DigitalSignature, non-repudiation
Extended Key Usage	N	OCSP Signing
Basic Constraints	N	Basic constraints: SubjectType=EndEntity PathLengthConstraint=none
Certificate Policies	N	Certificate strategies: OID = 1.2.752.274.1.2.4 URL = https://pki.nexusgroup.com/
OCSP No Check	N	Null

7.3.2 OCSP request format

The fields of OCSP request are as follows:

OCSP request	
Basic fields	**Value**
Version	1 (=version 0)
Requester Name (Optional)	Requester DN
Request List	List of certificate identifiers as defined in RFC 6960: • Hash Algorithm • Issuer Name Hash • Serial Number
Signature Algorithm	SHA-256WithRSAEncryption

The extensions of OCSP request are as follows:

Extensions	Criticality	Value
Nonce	N	Nonce value

7.3.3 OCSP response format

The fields of OCSP response are as follows:

OCSP response	
Basic fields	**Value**
Version	1 (=version 0)
Responder ID	OCSP responder DN: C = [Customer country] O = [Customer organization] OI = [Identifier of the Customer Entity] CN = [OCSP service name]
Produced At	Generalized Time
List of responses	Certificate id: • Hash Algorithm • Issuer Name Hash • Serial Number Certificate status: • Good, Revoked or Unknown • ThisUpdate • NextUpdate
Signature Algorithm	SHA-256WithRSAEncryption

The extensions of OCSP response are as follows:

Extensions	Criticality	Value
Nonce	O	Request nonce value
ArchiveCutoff	N	Response retention period value

8 Compliance audit and other assessments

8.1 Frequency or circumstances of assessment

Prior to the first commissioning of a component of its PKI or following any significant change within a component, the TSP shall also have that component checked for compliance.

The TSP also carries out a compliance check once a year of its entire PKI as part of the CA's LoA3 certification,

8.2 Identity/qualifications of assessor

The checking of a component must be assigned by the TSP to a team of auditors competent in information systems security and in the field of activity of the checked component. They are authorized, if necessary.

8.3 Assessor's relationship to assessed entity

The audit team is in no way part of the entity operating the audited PKI component, whatever that component may be, and is duly authorized to carry out the specified checks.

8.4 Topics covered by assessment

Compliance checks cover a component of the PKI (spot checks) or the entire architecture of the PKI (periodic checks) and aim to verify compliance with undertakings and practices (operational procedures, resources implemented, etc.) defined in the CA's CP.

8.5 Actions taken as a result of deficiency

Following a compliance audit, the audit team issues one of the following opinions to the TSP: "success", "failure", "to be confirmed".

According to the opinion given, the consequences of the check are as follows:

- In the event of failure, and depending on the size of the non-conformities, the audit team issues recommendations to the TSP, which may be cessation (temporary or permanent) of activity, revocation of the component certificate, revocation of all certificates issued since the last positive check, etc. The choice of the measure to be applied is made by the TSP and must comply with its internal security policies,
- In the event of a “to be confirmed” result, the TSP shall provide the component with a notice specifying the period within which the non-conformities must be resolved. Then, a “confirmation” check will verify that all critical points have been resolved,
- If successful, the TSP confirms to the audited component that it complies with the CP requirements.

8.6 Communication of results

The results of compliance checks are disclosed only and solely to the audited component and to the TSP manager. They include the component’s corrective actions already taken or in progress.

Given the confidential nature of the results, they will not be published without the authorization of all parties, nor transmitted to other persons involved without their agreement.

However, the results of compliance audits must be made available to the body responsible for the CA’s LOA3 certification.

9 Other business and legal matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

Pricing is established on the basis of a global offering of Nexus integrating a set of services including the issue and management of digital certificates and devices. This pricing, which can be reviewed annually, is defined in the general terms and conditions of service.

9.1.2 Certificate access fees

Certificates are freely accessible to relying parties.

9.1.3 Revocation or status information access fees

Certificate status and revocation information is available free of charge on the publishing server

9.1.4 Fees for other services

No special requirements.

9.1.5 Refund policy

No special requirements.

9.2 Financial responsibility

Nexus undertakes to comply with this CP. Any additional conditions not included in this document cannot be considered as an obligation of Nexus.

9.2.1 Insurance coverage

Nexus applies reasonable levels of insurance coverage and has taken out public liability insurance for the performance of its professional activity.

9.2.2 Other assets

Nexus is in a financial position to fulfil its task.

9.2.3 Insurance or warranty coverage for end-entities

Relying parties must be financially capable of carrying out their task.

In the event of damage for a customer caused by one of the CAs under the control of Nexus, the latter shall call upon its insurance to cover part of the customer's damage within the limit of Nexus's liability as defined in the general terms and conditions of Nexus services and herein.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

The information considered confidential shall be at least the following:

- the non-public parts of the CA CP and associated internal procedures,
- the private keys of the CA, its components and end-user certificates,
- the activation data associated with the CA private keys as well as those associated with the end-user's private keys (before such data is transmitted to the end-users),
- all the secrets of the PKI,
- the event logs of the different components of the PKI,
- the elements relating to the key ceremony, including the identity of the Secret Holders
- the causes of revocations, unless explicitly agreed by the end-user,
- the end-user's registration records,
- audit reports.

Only authorized persons may access it.

9.3.2 Information not within the scope of confidential information

Published information concerning the PKI is considered to be non-confidential and is disclosed on a need-to-know basis.

9.3.3 Responsibility to protect confidential information

The CA is required to apply security procedures to ensure the confidentiality of the information identified in section 9.3.1, in particular with respect to the permanent erasure or destruction of the media used for their storage and backup.

In addition, when these data are exchanged, the CA must ensure their integrity.

In particular, the CA is required to comply with the legislation and regulations in force on Swedish territory and European Union, in particular disclosure to judicial and/or administrative authorities. In particular, it may be required to make the registration files of the end-users available to third parties as part of legal proceedings. It must also give the end-user access to their registration file, where applicable to the RA operators in connection with the end-user's affiliated Customer entity.

9.4 Privacy of personal information

9.4.1 Privacy plan

It is understood that any collection and use of personal data by the CA and all its components is carried out in strict compliance with the legislation and regulations in force on Swedish territory and European Union GDPR (General Data Protection Regulation).

9.4.2 Information treated as private

The CA considers that the following information is personal data:

- The registration records of end-users,
- End-users certificate requests,
- Requests for revocation,
- The reasons for revocation of end-user's certificates.

9.4.3 Information not deemed as private

Any information published by the CA.

9.4.4 Responsibility to protect private information

The CA has put in place and complies with measures to protect personal data, in particular in order to guarantee its security, while respecting the principles of proportionality and transparency

9.4.5 Notice and consent to use private information

The CA undertakes to respect the purpose of the collection and processing of personal data.

In accordance with the laws and regulations in force on Swedish territory and European Union, the personal information identified in this CP must not be disclosed or transferred to a third party except in the following cases: prior consent of the data owner), judicial decision or other legal authorization.

9.4.6 Disclosure pursuant to judicial or administrative process

The CA acts in accordance with the regulations in force on Swedish territory and European Union and has procedures for disclosing personal information to judicial and administrative authorities at their express request.

9.4.7 Other information disclosure circumstances

Not applicable.

9.5 Intellectual property rights

This CP is part of the respect of intellectual and industrial property rights. The TSP retains all intellectual property rights and owns this CP, the certificates it issues and the corresponding revocation information it publishes.

9.6 Representations and warranties

The obligations common to the components of the PKI are as follows:

- to protect and guarantee the integrity and confidentiality of their secret and/or private keys as well as any activation data,
- to use their cryptographic keys (public, private and/or secret) only for the intended purposes when they are issued and with the tools specified under the conditions set by this CP and the resulting documents,
- to respect and apply the part of the CP for which they are responsible (this part must be communicated to the corresponding component),
- to submit to compliance checks carried out by the audit team mandated by the TSP and the supervisory body,
- to implement appropriate measures to correct the discrepancies detected during these compliance checks,
- to respect the agreements or contracts that bind them between themselves or to the end-users,
- to document their internal operating procedures,
- to implement the resources (technical, organizational and human) necessary to perform the services to which they commit themselves under conditions guaranteeing quality and safety,
- to implement awareness-raising and training actions,
- to set up documentation of the responsibility of each of the parties involved in question.

9.6.1 CA representations and warranties

The CA undertakes to:

- Be able to demonstrate to relying parties that it has issued a certificate for a given end-user and that the end-user has accepted that certificate in accordance with section 4.4,
- Ensure and maintain the consistency of its CP,
- Respect and ensure respect for the parts of the CPSs concerned by the various components,
- Collect Customer Entity Agreement and commitment to act as a RA as part of the 'Nexus GO Workforce LoA',
- Take all reasonable measures to ensure that its end-users are aware of their rights and use with respect to the use and management of keys, certificates or equipment and software used for the purposes of the PKI. The relationship between an end-user and the CA is formalized in a contractual or hierarchical relationship specifying the rights and obligations of the parties and in particular the guarantees provided by the CA,
- Carry out audits,
- Raise awareness among the various parties involved regarding security and the technologies used.

The TSP takes the necessary measures to cover the responsibilities related to its activities and have the financial stability and resources required to operate in accordance with this CP.

In addition, the CA acknowledges that it is liable for any duly proven fault or negligence by itself or any of its components, regardless of its nature and gravity, that would result in the reading, alteration and misuse of end-user's personal data for fraudulent purposes, whether contained in or in transit in the CA's certificate management applications.

In addition, the CA acknowledges that it has a general duty to monitor the security and integrity of certificates issued by the CA or one of its components. It is responsible for maintaining the security level of the technical infrastructure on which it relies to provide its services. Any changes that have an impact on the level of security provided must be approved by the CA's senior management.

9.6.2 RA representations and warranties

The RA's obligations are:

- Identification and authentication of the end-user,
- Checking the registration of the future end-user, validation and processing of certificate applications,
- The delivery of personalized device to the end-user,
- The secure sending of activation data to the end-user,
- Identification of the issuer of a revocation request, validation and processing of this request,
- Compliance with the CP of the issuing CA,
- Ensuring the end-user's knowledge and acceptance of their obligations (included in the Terms & Conditions document),
- Ensuring that RA operators comply with their respective obligations (relevant parts of the CP, letters of appointment, etc.).

9.6.3 Subscriber representations and warranties

The end-users are required to:

- Provide accurate and up-to-date information when applying for a certificate (initial application or renewal),
- Protect the device they have been given, their private keys and activation data,
- Comply with the conditions of use of their private key and the corresponding certificate,
- Inform the CA of any changes to the information contained in their certificate,

- Promptly apply to the RA for the revocation of their certificate upon the occurrence of any of the events listed in section 4.9.1.

9.6.4 Relying party representations and warranties

Relying parties must:

- Verify and respect the use for which a certificate has been issued,
- For each certificate in the certification chain, from the end-user's certificate to the Root CA certificate, verify the signature of the CA issuing the certificate in question and check the validity of this certificate (validity dates, revocation status),
- Verify and comply with the obligations of relying parties expressed in this CP.

9.6.5 Representations and warranties of other participants

Not applicable.

9.7 Disclaimers of warranties

The CA guarantees through its PKI services:

- Their identification and authentication through their certificate signed by the Root CA,
- The identification and authentication of end-users through the certificates it issues to them,
- Management of the corresponding certificates and certificate validity information according to this CP.

These warranties are exclusive of any other CA warranty.

It is expressly understood that the TSP cannot be held liable for any damage resulting from the fault or negligence of a Customer and/or its end-users or for any damage caused by an external event or force majeure, in particular in the event of:

- Use of the private key for a purpose other than that defined in the associated certificate,
- Using a certificate for an application other than Authorized Applications,
- Use of a certificate to guarantee an object other than the identity of the end-user,
- Use of a revoked certificate,
- Incorrect storage methods for the private key of the end-user's certificate,
- Using a certificate beyond its validity limit,
- Non-compliance with the obligations of other Stakeholders (see section 9.6.4),
- Events external to the issue of the certificate such as a failure of the application for which it can be used,
- Force majeure as defined by Swedish courts.

9.8 Limitations of liability

The CA can only be held liable in the cases listed exhaustively below:

- in the event of proven direct damage to an end-user or an application/Certificate User as a result of a breach of the procedures defined in the CP, the CA's fault must be duly proven,
- in the event of proven compromise, entirely and directly attributable to the CA.

The CA disclaims any responsibility for the use of certificates issued by it under conditions and for purposes other than those provided for in this CP and any related applicable contractual documents, in particular:

- use of a certificate for a purpose other than authentication of the end-user or protection of electronic mail,
- use of a certificate to guarantee an object other than the identity of the end-user for whom it was issued,
- use of a revoked certificate,
- use of a certificate beyond its validity limit.

The CA cannot be held liable for the consequences of delays or losses in the transmission of any electronic messages, letters, documents, and for any delays, alterations or other errors that may occur in the transmission of any telecommunications.

The CA cannot be held liable, and shall not assume any liability, for any delay in the performance of obligations or for any failure to perform obligations resulting from this CP when the circumstances giving rise to them and which could result from the total or partial interruption of its activity, or from its disorganization.

In addition to those usually retained by Swedish court and tribunal case law, labour disputes, the failure of the network or external telecommunications installations or networks are expressly considered to be force majeure or unforeseeable circumstances.

The CA disclaims any liability for indirect damages (including financial or commercial damages) which, as a result, do not give rise to any right to compensation.

In any event, any compensation that the TSP may be required to pay in respect of a proven breach of its obligations may not exceed the amount(s) specified in section 9.9 below.

9.9 Indemnities

If a proven fault of Nexus in the performance of its obligations under this CP as a CA is established and has directly caused damage, Nexus will compensate the relevant person/Customer entity within the limit defined in the service contract.

9.10 Term and termination

9.10.1 Term

The CP becomes effective on its date of validation by the TSP listed herein.

The CA CP shall remain in force at least until the end of the life of the last certificate issued under this CP.

9.10.2 Termination

The publication of a new version of this CP, may lead, depending on the changes, the need for the CA to have changes made to the associated CPs. Depending on the nature of the changes, the deadline for compliance is set in accordance with the procedures provided for by the regulations in force.

Compliance does not require the early renewal of certificates already issued, except in exceptional cases related to changes in the security requirements contained in this CP.

9.10.3 Effect of termination and survival

The clauses that remain applicable beyond the end of use of the CP are those concerning data archiving. All other obligations shall lapse and be replaced by those described in the CP(s) still in force.

9.11 Individual notices and communications with participants

In the event of a change of any kind in the composition of the PKI, the TSP undertakes:

- to have this change validated through a technical assessment no later than one month before the start of the operation, in order to assess the impacts on the level of quality and safety of the CA's functions and its various components,
- to inform the supervisory body no later than one month after the end of the operation.

The TSP undertakes to send DIGG a summary of all the changes made to the provision of its certified services on an annual basis.

9.12 Amendments

9.12.1 Procedure for amendment

The TSP reviews its CP periodically at least once a year and:

- whenever there are changes in PKI systems or internal PKI procedures that have an impact on the CP,
- whenever a significant change in industry practice or in existing legislation/regulation justifies it,
- or when the results of compliance audit checks so require (non-compliance with the standard CP).

The adoption of amendments shall be carried out under the same conditions as the adoption of the CP and in accordance with the principle of congruent forms.

In the event of a major modification of the CP, the TSP shall verify the compliance of the CP with THE standards, and the compliance of practices with this new version of the CP. The CP is only applicable after validation by the TSP.

9.12.2 Notification mechanism and period

The TSP shall give at least two months' notice to the CA components of its intention to modify its CP before making the changes and depending on the purpose of the change.

This time limit applies only to changes of substance (change of key size, change of procedure, change of certificate profile, etc.) and not to the form of the CP.

Note: spelling or typographical corrections do not require notification from the TSP.

9.12.3 Circumstances under which OID must be changed

Since the CA's OID is included in the certificates they issue, any change to this CP that has a major impact on certificates already issued must result in a change to the OID, so that Certificate Users can clearly distinguish which certificates correspond to which requirements.

However, end-user certificates and relying parties can easily identify and access on the publishing site the version of the CP under which the relevant certificate was issued by the CA. In addition to the current version of the CP, the site disseminates all the old versions, each of which clearly shows the date of publication and therefore the period over which it was in force.

9.13 Dispute resolution procedures

The TSP establish policies and procedures for the handling of complaints and the settlement of disputes from Customer entities for which it provides electronic trust services.

9.14 Governing law

The provisions of the CP are governed by Swedish law. In the event of a dispute relating to the interpretation, formation or execution of this CP and in the absence of an amicable settlement, the jurisdiction shall be that of the Courts of the Nexus registered office.

9.15 Compliance with applicable law

The policies and procedures by which the CA operates are non-discriminatory.

Nexus set up, whenever possible, means to facilitate access to its services for people with disabilities.

The laws and regulations applicable to the CP are, in particular, those indicated in section **Error! Reference source not found.**.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

All cases of force majeure usually retained by the Swedish courts are considered as force majeure, including the case of an irresistible, insurmountable and unforeseeable event.

Nexus cannot be held liable, and shall not assume any liability, for any delay in the performance of obligations or for any failure to perform obligations resulting from this CP when the circumstances giving rise to them fall within the scope of force majeure recognized by Swedish courts.