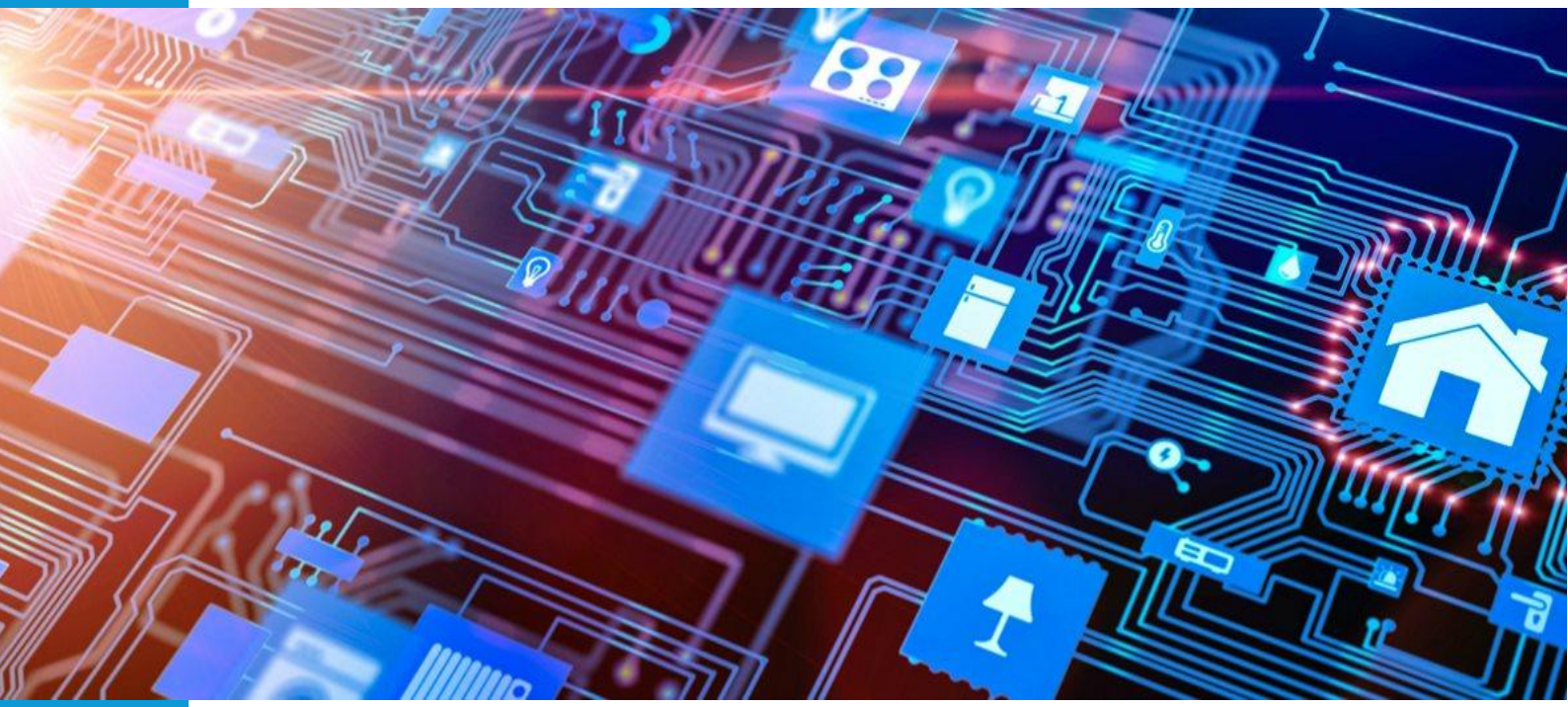
Enabling trusted identities



Nexus GO Workforce LoA

Certificate Practice Statement

Version 1.1

ISO public information

Document identification and ownership

Document issuer:	Technology Nexus Secure Business Solutions AB, Trust Service Provider (TSP) organization
Document name:	Nexus GO Workforce LoA – Certificate Practice Statement
Document version:	1.1
Date:	2025-10-23

Trust Service Provider (TSP) identity

Entity name:	Technology Nexus Secure Business Solutions AB
Company registry number:	556258-0414
Head office, postal address:	Telefonvägen 22B, 126 26 Hägersten, Sweden
Phone:	+46 8 685 45 60
General contact:	https://www.nexusgroup.com/contact/
Website:	https://www.nexusgroup.com

Contact to TSP organization

Please send any comments or queries about this document to gopki@nexusgroup.com .

Web page of the Nexus GO IoT PKI: https://pki.nexusgroup.com/

Change history

Version	Description	Affected section	Effect date	Responsible
0.1	Initial version		2022-03-02	Nexus TSP, Wallström
1.1	Updated new address of the TSP Cross referenced to CP and other documents Minor changes	Trust Service Provider (TSP) identity and Contact Section 7,8,9	2025-12-10	Linh Pham – Product Owner

Table of Contents

Document identification and ownership 2
Glossary 10
References 11
1 Introduction 12
1.1 Overview 12
1.2 Document name and identification 12
1.3 PKI participants 13
1.3.1 Certification authorities 13
1.3.2 Registration Authorities 14
1.3.3 Customers and end-users 14
1.3.4 Relying parties 14
1.3.5 Other participants 14
1.4 Certificate usage 15
1.4.1 Appropriate certificate uses 15
1.4.2 Prohibited certificate uses 15
1.5 Policy administration 15
1.5.1 Contact 15
1.5.2 Person determining CPS suitability for the policy 15
1.5.3 CPS approval procedures 16
1.6 Definitions and acronyms 16
2 Publications and repository responsibilities 17
2.1 Repositories 17
2.1.1 CPS Repository 17
2.1.2 Revocation Information Repository 17
2.1.3 Certificate Repository 17
2.2 Publication of certification information 17
2.3 Time or frequency of publication 18
2.4 Access control on repositories 18
3 Identification and authentication 19
3.1 Naming 19
3.1.1 Need for names to be meaningful 19

3.1.2 Anonymity or pseudonymity of subscribers 19
3.1.3 Rules for interpreting various name forms 19
3.1.4 Uniqueness of names 19
3.1.5 Recognition, authentication and role of trademarks 19
3.2 Initial identity validation 20
3.2.1 Method to prove possession of private key 20
3.2.2 Authentication of organization entity 20
3.2.3 Authentication of individual user 20
3.2.4 Non-verified subscriber information 20
3.2.5 Validation of authority 20
3.2.6 Criteria for interoperation 20
3.3 Identification and authentication for re-keying requests 21
3.3.1 Identification and authentication for regular re-keying 21
3.3.2 Identification and authentication for re-keying after revocation 21
3.4 Identification and authentication for revocation request 21
4 Certificate life-cycle operational requirements 22
4.1 Certificate application 22
4.1.1 Who can submit a certificate application 22
4.1.1.1 CAs 22
4.1.1.2 User certificates 22
4.1.2 Enrolment process and responsibilities 22
4.1.2.1 CAs 22
4.1.2.2 User certificates 22
4.2 Certificate application processing 23
4.2.1 Performing identification and authentication functions 23
4.2.2 Approval or rejection of certificate applications 23
4.2.3 Time to process certificate applications 23
4.3 Certificate issuance 23
4.3.1 CA actions during certificate issuance 23
4.3.2 Notification to subscriber by the CA of issuance of certificates 23
4.3.2.1 CA certificate issuance 23
4.3.2.2 Client certificate issuance 24
4.4 Certificate acceptance 24

4.4.1 Conduct constituting certificate acceptance 24
4.4.2 Publication of the certificate by the CA 24
4.4.3 Notification of certificate issuance by the CA to other entities 24
4.5 Key pair and certificate usage 24
4.5.1 Customer private key and certificate usage 24
4.5.2 Relying party public key and certificate usage 24
4.6 Certificate renewal 24
4.7 Certificate re-keying 25
4.8 Certificate modification 25
4.9 Certificate revocation and suspension 25
4.9.1 Circumstances for revocation 25
4.9.2 Who may request revocation 25
4.9.3 Procedure for revocation request 26
4.9.4 Revocation request grace period 26
4.9.5 Time within which CA must process the revocation request 26
4.9.6 Revocation checking requirement for relying parties 26
4.9.7 CRL issuance frequency 26
4.9.8 Maximum latency for CRLs 27
4.9.9 On-line revocation/status checking availability 27
4.9.10 On-line revocation checking requirements 27
4.9.11 Other forms of revocation advertisements available 27
4.9.12 Special requirements regarding key compromise 27
4.9.13 Circumstances for suspension 27
4.9.14 Who can request suspension 27
4.9.15 Procedure for suspension request 28
4.9.16 Limits on suspension period 28
4.10 Certificate status service 28
4.10.1 Operational characteristics 28
4.10.2 Service availability 28
4.10.3 Optional features 28
4.11 End of subscription 28
4.12 Key escrow and recovery 28
5 Physical, procedural and personnel security controls 29

5.1 Physical controls 29
5.1.1 Site location and construction 29
5.1.1.1 Data center environment 29
5.1.1.2 Office environment 30
5.1.1.3 Disaster recovery depots 30
5.1.2 Physical access 30
5.1.3 Power and air conditioning 31
5.1.4 Water exposures 32
5.1.5 Fire prevention and protection 32
5.1.6 Media storage 32
5.1.7 Waste disposal 32
5.1.8 Off-site backup 33
5.2 Procedural controls 33
5.2.1 Trusted roles 33
5.2.2 Number of persons required per task 34
5.2.3 Identification and authentication for each role 34
5.2.3.1 Identification and authorization in ceremonies 34
5.2.3.2 Identification and authorization at systems of the Service 35
5.2.4 Roles requiring separation of duties 35
5.3 Personnel controls 36
5.3.1 Qualifications, experience, and clearance requirements 36
5.3.2 Background Check Procedures 36
5.3.3 Training requirements 37
5.3.4 Retraining frequency and requirements 37
5.3.5 Job rotation frequency and sequence 38
5.3.6 Sanctions for unauthorized actions 38
5.3.7 Independent contractor requirements 38
5.3.8 Documentation supplied to personnel 38
5.4 Audit logging procedures 38
5.4.1 Types of events recorded 38
5.4.2 Frequency of processing log 40
5.4.3 Retention period for audit log 40
5.4.4 Protection of audit log 40

5.4.5 Audit log backup procedures 40
5.4.6 Audit collection system (internal or external) 40
5.4.7 Notification to event-causing subject 41
5.4.8 Vulnerability assessment 41
5.5 Records archival 41
5.5.1 Types of records archived 41
5.5.2 Retention period for archive 41
5.5.3 Protection of archive 42
5.5.4 Archive backup procedures 42
5.5.5 Requirements for time-stamping of records 42
5.5.6 Archive collection system (internal or external) 42
5.5.7 Procedures to obtain and verify archive information 42
5.6 Key changeover 42
5.7 Compromise and disaster recovery 43
5.7.1 Incident and compromise handling 43
5.7.2 Computing resources, software and/or data are corrupted 43
5.7.3 Entity private key compromise procedures 43
5.7.4 Business continuity capabilities after a disaster 44
5.8 CA or RA termination 44
6 Technical security controls 45
6.1 Key pair generation and installation 45
6.1.1 Key pair generation 45
6.1.2 Private key delivery to customer 45
6.1.3 Public key delivery to certificate issuer 45
6.1.4 CA public key delivery to relying parties 45
6.1.5 Key sizes 45
6.1.6 Public key parameters generation and quality checking 46
6.1.7 Key usage purposes 46
6.2 Private Key protection and cryptographic module controls 46
6.2.1 Cryptographic module standards and controls 46
6.2.2 Private key (n out of m) multi-person control 47
6.2.3 Private key escrow 47
6.2.4 Private key backup 47

6.2.5 Private key archival 48
6.2.6 Private key transfer into or from a cryptographic module 48
6.2.7 Private Key storage on cryptographic module 48
6.2.8 Method of activating the private key 48
6.2.9 Method of deactivating the private key 48
6.2.10 Method of destroying private key 48
6.2.11 Cryptographic module rating 49
6.3 Other aspects of key pair management 49
6.3.1 Public key archival 49
6.3.2 Certificate operational periods and key pair usage periods 49
6.4 Activation data 50
6.4.1 Activation data generation and installation 50
6.4.2 Activation data protection 50
6.4.3 Other aspects of activation data 50
6.5 Computer security controls 50
6.5.1 Specific computer security technical requirements 50
6.5.2 Computer security rating 51
6.6 Life cycle technical controls 51
6.6.1 System development controls 51
6.6.2 Security management controls 51
6.6.3 Life-cycle security controls 51
6.7 Network security controls 52
6.8 Time stamping 52
7 Certificate, CRL and OCSP profiles 53
8 Compliance audit and other assessments 54
9 Other business and legal matters 55

Glossary

CA	Certificate Authority: 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.
CDP	CRL Distribution Point, a service that makes revocation lists accessible to Relying Parties.
CRL	Certificate Revocation List, 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 of the issuing CA.
CPS	Certificate Practice Statement, 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.
DP	Distribution Point, a repository service which makes certificates and CRLs accessible to Relying Parties.
OCSP responder	A service that allows Relying Parties to access information about the revocation status of certificates via the standard 'Online Certificate Status Protocol'.
OID	Object Identifier, a globally unique identify of any kind of data object, data type, document.
RA	Registration Authority: the name of the organization (legal entity) and/or the technical component that performs the enrolment for certificates. Its main tasks are retrieving or capturing and verifying the identity of the certificate subject (applicant), prove possession of the key presented for the applicant.
Registration Authority	The entity responsible for issuing certificates, or signing CSRs, on behalf of a CA.
Revocation	To invalidate a certificate before its normal expiration. Revoked certificates are published to a CRL and to an online OCSP responder.
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.
TSP	Trust Service Provider; 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	A person that is a Customer employee or contractor
User certificate	A certificate issued for a subject (identified User)

References

[BSI TR-03145-1]	Secure CA operation, Part 1, Generic requirements for Trust Centers instantiating as Certification Authority (CA) in a Public-Key Infrastructure (PKI) with security level 'high', Version 1.1, 2017-03-27
[CEN TS 419 261]	Security requirements for trustworthy systems managing certificates and time-stamps, March 2015
[RFC 2119]	Key words for use in RFCs to Indicate Requirement Levels, 1997
[RFC 3647]	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003
[FIPS 140-2]	Security Requirements for Cryptographic Modules, May 2001
[FIPS 186-4]	FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013
[RFC 5280]	Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.
[RFC 5639]	Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, March 2010
[RFC 6960]	X.509 Internet Public Key Infrastructure – Online certificate Status Protocol – OCSP. June 2013.
[ETSI TS 319 401]	ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ETSI TS 319 411-1]	ETSI EN 319 411-1 V1.2.2 (2018-04); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[TSP Organization]	TSP's specification: "TSP Organization and Practices"
[TSP Training Plan]	TSP's specification: "Training Plan for the TSP Organization"
[TSP Roles]	TSP's specification: "TSP Trusted Role Descriptions"
[TSP SLA]	TSP's specification: "TSP Service Level Agreement"
[Audit Log Plan]	TSP's specification: "Nexus GO TSP - Audit Logging and Archiving Plan"
[Backup Plan]	TSP's specification: "Nexus GO TSP - Backup and Recovery Plan"
[DR Plan]	TSP's specification: "Nexus GO TSP - Disaster Recovery Plan"
[Privacy Plan]	TSP's specification: "Nexus GO TSP - Privacy Plan"
[Termination Plan]	TSP's specification: "Nexus GO TSP -Termination Plan"

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 for issuing and managing certificates for User Certificates. The marketing name of the PKI service is 'Nexus GO eID'. The TSP provides the Nexus GO eID (briefly 'the Service') for its contracted Service Customers.

Nexus GO eID is a multi-tenancy-enabled, shared cloud PKI service, and is one of the other '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 hosting environment for the online services is in ISO 27002 certified, geo-redundant data centers in Sweden. The infrastructure provider manages infrastructure (IaaS) at and below the hypervisor layer. The Nexus TSP manages the virtual networks; dedicated, co-located network appliance and HSMs, virtual network domains, virtual servers, and application software.

The Nexus GO eID service covers the registration, issuing and lifecycle management (revocation, renewal) of certificates used by employees and consultants within public sector organisations and companies (jointly called 'User certificates') primarily for communication security (authentication, encryption, integrity validation). The TSP operates the necessary PKI infrastructure including Root CA, Intermediate CAs, customer Issuing CAs, OCSP responder, CRL Distribution Point, certificate management interfaces (APIs) and web portal, for its customers.

The present Certificate Practice Statement (CPS) describes the hosting infrastructure, the CA functions, operational procedures and security rules applied in the operation of the Subordinate CAs of the Nexus Placeholder Service. Where applicable, the CPS provides a statement of compliance with respect to the [ETSI TS 319 411-1] Normalized Certificate Policy (briefly 'ETSI NCP').

Note that ETSI NCP is primarily used in conjunction with the European eIDAS regulation in relation with electronic signature and sealing services.

The content and format of the present document complies with the requirements of the RFC 3647 framework. To strictly preserve the outline specified by RFC 3647, section headings where the document does not impose a requirement have the statement "No stipulation".

Within this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in [RFC 2119].

1.2 Document name and identification

OID: 1.2.752.274.1

Nexus GO Workforce LoA – CPS for the PKI, Version 1.1

Location: https://pki.nexusgroup.com/

This document describes the **Certificate Practice Statement (CPS)** for the **Certificate Policy (CP)** defined in **Nexus-GO-WF-LoA.CP**.

The scope includes the following Certification Authorities (CAs) and their associated Object Identifiers (OIDs) within the Nexus eID service hierarchy:

CA	Type	OID
Nexus GO eID Root CA G**[n]***	Root CA	1.2.752.274.1.1.1
Nexus GO eID Intermediate CA G**[n]***	Intermediate CA,	1.2.752.274.1.1.2
[Customer name] Issuing CA G**[n]***	Issuing CA, dedicated to the Customer, for user certificates	1.2.752.274.1.1.3

Note on Naming Convention:

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

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

Certificate profile (issued by [Customer name] Issuing CA)	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 TSP operates following CAs in a 3-tier PKI hierarchy:

- Nexus GO eID Root CA G[n] – covered by this CPS
- Nexus GO eID Intermediate CA G[n] – covered by this CPS
- Nexus GO eID [Customer Name] Issuing CA G[n] – covered by this CPS
- Additional Nexus GO eID Customer Issuing Ca G[n] – covered by this CPS

The Nexus GO eID Root CA G1 is operated on an offline platform on the premises of the TSP. The Root CA keys are stored in an HSM with multiple off-site key backups.

The Intermediate CA and below (the Intermediate CA and the Issuing CAs) are operated on a shared CA platform in the compliant, geo-redundant cloud environment of the TSP within Sweden. The certificate processes of the different CAs are logically separated and linked in an end-to-end manner from certificate management interface end points via backend service down to the HSM keys, so that a CA key can only be used by the authorized process and by the authorized interface end point.

The CA keys of Issuing CAs are stored in network HSM appliances with secure key backups. In this setup, the HSMs are shared among the Nexus and the customer-specific Issuing CAs, and clustered across the data center locations. The HSMs are under exclusive physical and logical access control of the Nexus TSP organization. The CA keys are backed up properly in both cases.

A Service Customer can opt for a customer-named Issuing CA, which are operated by the TSP in the same manner according to this CPS.

1.3.2 Registration Authorities

The Registration Authority for the CA certificates is operated by the TSP according to this CPS.

The Registration Authority for the end-user certificates is the customer, according to this CPS.

The Service Customer (including Nexus Issuing CA) 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:

- Identification and authentication of users
- Initiating or pass along revocation requests for certificates
- Approving applications for new, renewal certificates

1.3.3 Customers and end-users

All end-users will get their certificates through a Customer (or the internal Nexus RA). The Customers has a service agreement with Nexus to run their RA for them. The service agreement with the Customer covers the responsibilities and authorizations of the Customer.

The Customer RA (and Nexus internal CA) will issue certificates to Users. Users are either employees or contractors of the Customer. The User is an identified natural person.

1.3.4 Relying parties

The Relying Parties are typically other technical components that communicate with the certificate holder Device, rely on its code signature. Yet typically, the owner or operator of the relying Device typically has no contractual relationship with the TSP. Section 9.6.4 of this CPS contains the representations related to the Relying Parties' operation.

In relation with the Service, the TSP is not liable towards (owners or operators of) Relying Parties in any form. Relying Parties seeking for liabilities, need to address the Customer.

The TSP maintains its contacts with the Relying Parties mainly through its website in form of one-way information.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Certificates under this CPS are issued for the following applications:

- Root certificates: used to create Intermediate CAs
- Intermediate CAs: used to create Issuing CAs
- Issuing CAs: used to issue certificates for end-users

The public key in an end-user certificate can only be used in the same usage content as the private key was used and according to the key usage indicated in the certificate, i.e. for validation authentication data, encrypting data for the end-user, or for validating origin and/or integrity.

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

1.4.2 Prohibited certificate uses

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.

The (TSP-operated) Subordinate CA 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 CPS.

1.5 Policy administration

The present CPS document is maintained by the TSP named in the preamble if this document. The TSP organization is responsible for the drafting, registering, maintaining, and updating of the CPS.

1.5.1 Contact

Point of contact:

Nexus Group

Telefonvägen 22B

126 26 Hägersten

Sweden

gopki@nexusgroup.com

1.5.2 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.

1.5.3 CPS approval procedures

Changes in the certificate practices are first drafted in the CPS, then reviewed and approved by the Product Owner and a Compliance Officer of the TSP organization, who are responsible for service management and respectively for compliance of operation. After approval the change is implemented and at the same time, the new version of the CPS is published.

This CPS is reviewed yearly by the same roles.

Changes relevant to the delivery of the Service are explicitly communicated to the Subscriber.

1.6 Definitions and acronyms

See the Glossary on Page 10 of the present document.

2 Publications and repository responsibilities

2.1 Repositories

The CRLs of the Issuing CAs contain entries for all revoked unexpired certificates issued by the respective CA. CRLs are accessible via the HTTP address of the Distribution Point (DP) service.

The Issuing CAs provides the OCSP service. The OCSP service is available for customer-named CAs. The OCSP access method and address is asserted in the Authority Information Access extension, accessMethod=id-ad-ocsp, accessLocation=URL of the issued certificates.

Issuing CA certificates are published in the same DP repository as the respective CRLs and are accessible via HTTP protocol. Publication of the Issuing CA certificates is optional for customer-named CAs. If applicable, the respective HTTP address is contained in the IssuerAltNames extension of the issued certificates.

In addition to the DP, Nexus-named CAs, and respective CPs and CPS, are published on the public Nexus GO PKI web page, https://pki.nexusgroup.com/.

The Trust Service Provider guarantees the availability of the publishing services according to the [TSP SLA]. Upon system failure, service or other factors which are not under the control of the TSP, the TSP shall apply best endeavors to ensure that this information service is not unavailable for longer than necessary.

2.1.1 CPS Repository

The full text of this CPS is available at https://pki.nexusgroup.com/.

2.1.2 Revocation Information Repository

CRLs for the CAs are published at https://pki.nexusgroup.com/.

OCSP is the recommended method to check for certificate validity. The Nexus OCSP service is available at https://ocsp.eid.nexusgroup.com/. OCSP responses and CRLs are indirectly signed by the respective CA.

2.1.3 Certificate Repository

CA certificates are published at https://pki.nexusgroup.com/.

All issued certificates are stored in the CA system.

Certificates may also be published to other repositories if agreed with the Customer.

2.2 Publication of certification information

The Nexus GO eID Service addresses for certificate information access are the following:

- Distribution Point: http://dp.eid.nexusgroup.com/
- OCSP: http://ocsp.eid.nexusgroup.com/
- Policies, CA certificates with revocation information for CAs: https://pki.nexusgroup.com/

2.3 Time or frequency of publication

The latest versions of the relevant CP and of this CPS will be published promptly on the Nexus PKI web page https://pki.nexusgroup.com/. All earlier CP and CPS versions will be made available.

Any certificate listed in a CRL of a customer-named Issuing CA will be removed from the CRL after the certificate's expiration. Similarly, the OCSP service of the same CA cannot be used to obtain revocation information on expired certificates.

2.4 Access control on repositories

The DP, OCSP responder and the Nexus GO eID Service PKI web page can be read-accessed without authentication.

Access controls, logical and physical security measures, are implemented to prevent unauthorized persons or systems from adding, deleting, or modifying the published information.

3 Identification and authentication

This chapter describes the procedures used by the TSP to authenticate the identity and/or other attributes of an end-user Certificate prior to its issuance.

3.1 Naming

The Issuer and Subject fields of the Certificate issued by the Trust Service Provider are conform with the name format requirements of the recommendations [RFC 5280]. The TSP supports the Subject Alternative Names and Issuer Alternative Names fields located amongst the extensions.

3.1.1 Need for names to be meaningful

The subject field of the certificate identifies the entity for which the certificate was issued.

The subject name in the service certificates (i.e. certificates of CAs, indirect OCSP and CRL signers, server certificates etc.) are chosen to be meaningful for human readers.

The form is not limited, but the subject name MUST be unique. All identities and attributes are verified by validation specialists in the respective RA.

3.1.2 Anonymity or pseudonymity of subscribers

Names will be meaningful according to section 3.1.1.

3.1.3 Rules for interpreting various name forms

The interpretation of end-entity subject names is not controlled by this CPS.

3.1.4 Uniqueness of names

Subject names are unique with respect to the Certificate Holder entity (End-users, TSP service certificates, and customer-named CA certificates).

- **End-entity Uniqueness Check:** The identity and uniqueness verification of the natural person subject is performed by verifying the social security number (or equivalent identifier) as part of the registration process (see Section 1.3.2). This specific unique identifier ensures that one natural person cannot be confused with another.
- **Multiple Certificates:** While the underlying natural person subject is uniquely identified via the SerialNumber attribute, the same natural person entity **MAY** hold several certificates simultaneously (e.g., separate Authentication and Signature certificates, or certificates tied to different roles/customers) that share the same Subject Name but have different key usages and serial numbers.

See LoA-End Entity Certificate Template document for End-Entity uniqueness.

3.1.5 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

For service certificates related to CAs that are operated by the TSP and for end-entity keys generated by the Service, the keys are generated in a certified Hardware Security Module (HSM) in the secure and protected environment of the TSP, so the TSP does not have to specially verify that the Subject owns the private pair of the public key to be certified.

Possession of the private keys of external CAs and of end-entities (user certificates), which generate their own key - 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.

3.2.3 Authentication of individual user

Authentication of individual users is done by showing an approved document such as a passport, SIS approved identity card, or Swedish driver's license, in conjunction with being an employee or a contractor for the Customer (including Nexus).

The TSP allows for two levels of assurance. Assurance Levels three and four requires a face to face meeting with an authorized and trained person RA operator, according to ISO/IEC 29115. Certificate renewals also require a face to face meeting, this is a requirement for level four assurance. Assurance level four certificates may be issued to secure tokens such as smartcards, hardware security tokens, and mobile devices.

3.2.4 Non-verified subscriber information

All information included in certificates issued by the CA is verified.

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 service certificates for customer-named CAs.

3.2.6 Criteria for interoperation

Not applicable.

3.3 Identification and authentication for re-keying requests

3.3.1 Identification and authentication for regular re-keying

Re-keying is not being done, the previous certificate connected to the end-user is revoked and a new key-pair is used for the new certificate issuance. There for the identification process follows according to issuance of certificate.

3.3.2 Identification and authentication for re-keying after revocation

Re-keying is not being done, the previous certificate connected to the end-user is revoked and a new key-pair is used for the new certificate issuance. There for the identification process follows according to issuance of certificate.

3.4 Identification and authentication for revocation request

Revocation requests shall be authenticated to ensure both the identity of the requester and their authority to revoke the certificate.

Revocation may be initiated by:

1. **The certificate holder (self-service):** The certificate holder may request revocation through an authenticated online channel using their active e-ID with a level of assurance equivalent to that used during certificate issuance.
2. **Authorized representatives within the subscriber organization:** Human Resources Managers and Operations Managers are authorized, as specified in the CP, to request revocation of certificates belonging to their employees.

When revocation is initiated by an authorized representative, the Card Officer performs the blocking on their behalf. Verification of the authorized requester may be completed through:

- A digitally signed request submitted to card administration, authenticated using a LoA3 e-ID issued by the organization, or
- A personal visit presenting a signed form accompanied by a valid physical ID.

All revocation events shall be logged and auditable in accordance with operational security procedures.

4 Certificate life-cycle operational requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application

4.1.1.1 CAs

An Issuing CA certificate application can by submitted by an authorized Nexus employee or an authorized representative of the Customer that has made an agreement to host their CA with Nexus.

4.1.1.2 User certificates

When a certificate is requested by an end-user, it is required that the ordering organisation is a Customer of Nexus with which the end-user has a contractual relation. A certificate request can be submitted by a Customer that acts as the RA, an employee or other individual contracted by a Customer organisation (User).

Authorised TSP personnel can also submit certificate applications.

4.1.2 Enrolment process and responsibilities

“Enrolment”, “registration”, and “application processing” refer to the same process in this CPS. The enrolment process is in the lone responsibility and control of the Customer. The Customer is responsible for:

- secure management of the access credentials for authentication at the Service Interface: TLS keys and certificates, factory CA keys and certificates,
- assurance of the existence of uniqueness of Device identities,
- assurance of correctness of the requested subject attributes,
- assurance of the authorization of the request, i.e. no request with unauthorized content can be submitted,
- the public key sent in the certificate request to the certificate service to correspond to the certificate holder Device indicated in the requested subject name, and
- secure, tamper-protected (tamper-proof or tamper-evident) storage of the private key in the Device.

4.1.2.1 CAs

The Application is made and signed by a Nexus employee.

4.1.2.2 User certificates

The Customer Organisation is bound to registration policies and service agreement with Nexus. The enrolment and renewal of a User certificate is handled by the RA operated on behalf of the Customer or Nexus.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

In accordance with section 3.2.

Certificate requests (synonym for 'certificate application') are processed by the Service Interface.

4.2.2 Approval or rejection of certificate applications

The RA will approve a certificate application if it meets the requirements of validation and identification. All other certificate applications will be rejected.

The end-user will be informed on why the certificate application was rejected and on how to proceed to be approved.

For CA approvals, the TSP approves or rejects CA applications.

4.2.3 Time to process certificate applications

Certificate requests will be processed for the CAs within a reasonable time frame.

User certificate requests is applied for through the Service Interfaces and will be processed automatically when the request is submitted.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The issuance of CA certificates or related service certificates for Service-internal use is performed in security ceremonies by TSP trusted personnel.

4.3.2 Notification to subscriber by the CA of issuance of certificates

Not applicable to CA or related service certificates for CA operated by the TSP.

If a certificate request (application) is successfully processed, the Service Interface returns the certificate instantly in the response to the request. The Subscriber is NOT notified via any other channel.

4.3.2.1 CA certificate issuance

The CA of the Service issues the certificates for end-entities in automated process. It:

- validates the requested subject name and key parameters, if such rules are defined for the customer-named Issuing CA,
- inserts the issuer name and other fixed contents according to the certificate profile definition, and additional CA parameters
- signs the certificate with the help of the private key of the customer-named Issuing CA.

4.3.2.2 Client certificate issuance

The issuing CAs (i.e. the customer-named Issuing CAs) make the certificate available to the end-user when the certificate request has been processed.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The Customer is considered to have accepted the certificate when:

- When the Customer start using the certificates key pair, or
- One calendar month is passed from the certificate issuance date, or
- When the user certificate has been delivered to the user.

4.4.2 Publication of the certificate by the CA

CA certificates are published in the CA repository in accordance with section 2.1.3.

4.4.3 Notification of certificate issuance by the CA to other entities

Not applicable. Other entities are not notified.

4.5 Key pair and certificate usage

4.5.1 Customer private key and certificate usage

Public key usage settings for end user certificates are aligned with their application and agreed with the Customer. Primary usages are defined in Section 1.4.1.

Users MUST use the private key and corresponding certificate according to the key usages indicated in the certificate. Proper key usage is in the responsibility of the Customer, who controls the certificate. The end user agreement SHOULD oblige the end user (owner, operator) of the certificate to use the certificate according to the intended purpose. The Customer should protect the private key from unauthorized use, and if the private key is compromised it should be revoked immediately.

4.5.2 Relying party public key and certificate usage

Relying Parties MUST use the public key and corresponding certificate according to the key usages indicated in the certificate. The Customer is responsible for handling the agreements with Relying Parties.

4.6 Certificate renewal

Certificate renewal is possible when a certificate is renewed with a new private and public key pair. Other attributes may be changed during the renewal process.

4.7 Certificate re-keying

Not applicable

4.8 Certificate modification

Certificate modification (synonym for certificate replacement) are processed as initial certificate requests as described in section 4.1 – 4.4.

In the renewal process, the subject or extension of the certificate may be changed, as described in section 4.6.

CAs and end-users MAY own several certificates with the same subject name, but with different keys.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A CA certificate or a service certificate related to a CA may be revoked, when:

- it becomes obsolete due to re-keying of the certificate (revocation reason ‘superseded’),
- it becomes obsolete due to termination of the respective CA (revocation reason ‘cessationOfOperation’), or
- its private key is compromised or is suspect being compromised (revocation reason ‘cAcompromise’ or ‘keyCompromise’).

An end-user certificate may be revoked, when:

- it becomes obsolete due to re-keying of the certificate (revocation reason ‘superseded’),
- it becomes obsolete due to User is no longer affiliated with the Customer (revocation reason ‘cessationOfOperation’),
- the User certificate is detected to misbehave, so that its operation or its use in the target application needs to be terminated (revocation reason ‘cessationOfOperation’), or
- its private key is compromised or is suspect being compromised (revocation reason ‘keyCompromise’).

4.9.2 Who may request revocation

The Customer MAY request revocation of the respective customer-named CA.

The Customer MAY request revocation of end-entity certificates via the Service Interface.

Optionally, the authorized end user of a User certificate MAY request the revocation of the end-user certificate from the Customer or the trusted supplier of the Customer, e.g. via a support hotline. This process MUST be handled by the Customer. The Service Interface assumes proper authorization of the revocation request submitted by the Customer.

4.9.3 Procedure for revocation request

The revocation of CA certificates or related service certificates for Service-internal use is performed in security ceremonies by TSP trusted personnel.

The Service Interface revokes end-user certificates in automated process. It:

- authenticates the request by means of a user certificate issued for the Customer,
- checks if the certificate is valid (not expired and not revoked), and
- revokes the certificate in the CA database.

In the Service setup, revocations immediately appear in the CRL and/or OCSP.

4.9.4 Revocation request grace period

Revocation requests SHOULD be submitted by the Customer as promptly as possible after the cause event within an appropriate time reasonable in view of the risks of misuse of a compromised end-user key.

4.9.5 Time within which CA must process the revocation request

The Service Interface and the respective CA process the revocation request within a reasonable time frame after receiving it. The revocation is published in the next regular CRL or in an immediate CRL, as described in Section 4.9.4.

4.9.6 Revocation checking requirement for relying parties

There are stipulations by this CPS for Relying Parties. Relying Parties check the revocation status via CRL or OCSP as suitable for the application. This CPS does not define requirement on the method and timing of revocation check. It is in the responsibility of the Customer to define these rules according to the risk related to a late detection of a certificate revocation by the Relying Party. On the other hand, the frequency and method of publication of revocation information by customer-named CA are chosen by the Customer of in consideration of the same risk in agreement with the TSP.

4.9.7 CRL issuance frequency

Nexus-named CAs publish revocation information via CRLs. Customer-named CAs also publish revocation information via CRLs in the same manner.

The CRL validity is indicated in the CRL's nextUpdate field. The issuing frequency is chosen to be shorter to provide some reserve time for issuing before CRL expiry.

The default CRL validity and issuance frequency for the different CAs is defined below:

Entity	CRL validity period	Issuing frequency
Nexus GO eID Root CA G1	18 months + 30 days	12 months (or immediately)
Nexus GO eID Intermediate CA G1	1 month + 10 days	1 month (or immediately)

Entity	CRL validity period	Issuing frequency
Nexus eID Issuing CA G1	1 week	1 day (or immediately)
Customer-named Issuing CA G1	1 week	1 day (or immediately)

These default validity and operation periods are applied to all Nexus or Customer named CAs. They are designed to provide a latency of at most 1 day for publication of a revocation event.

IMPORTANT!

After a certificate listed in a CRL expires, it will be removed from later-issued CRLs after the certificate's expiration. (The OCSP responder may respond accordingly with 'good' after expiry of the certificate.) Accordingly, Relying Parties cannot verify after the expiry date if a certificate was revoked.

4.9.8 Maximum latency for CRLs

CRLs of Intermediate and Issuing CAs are published automatically and instantly after having been signed by the respective CA key (or optionally by the indirect CRL signer key).

4.9.9 On-line revocation/status checking availability

Intermediate and Issuing CAs publish revocation information via OCSP.

In the Service setup, revocations immediately appear in the CRL and/or OCSP. OCSP is supplied with revocation information in form of the CRL.

4.9.10 On-line revocation checking requirements

There are stipulations by this CPS for Relying Parties. The same considerations apply as for CRLs as described in Section 4.9.6.

4.9.11 Other forms of revocation advertisements available

Not applicable.

4.9.12 Special requirements regarding key compromise

The TSP will notify affected Customers of an actual or suspected CA private key compromise using commercially reasonable efforts. The same applies to the compromise of the indirect CRL and OCSP signer keys.

4.9.13 Circumstances for suspension

Suspension of CA certificates is not supported.

End-user certificates may be temporarily suspended, being "onhold".

4.9.14 Who can request suspension

Suspension of CA certificates is not supported.

The RA can request a temporary suspension of end-users certificates, "onhold".

4.9.15 Procedure for suspension request

Suspension of CA certificates is not supported.

The RA identifies the token or user to suspend, and then requests a suspension of that token or user. If the user is suspended, all its tokens will also be suspended.

4.9.16 Limits on suspension period

Suspension of CA certificates is not supported.

4.10 Certificate status service

4.10.1 Operational characteristics

Certificate status services are available for CAs in three forms, as described in Sections 4.9.7, 4.9.9 and 4.9.11:

- CRLs are available via the Distribution Point (see Section 2.2)
- OCSP, and
- Nexus GO PKI web page.

4.10.2 Service availability

Certificate status services are available 24x7 with scheduled quarterly maintenance slots according to the agreement with the Customer.

The Nexus GO PKI web page is operated without an SLA and is not in the scope of the Service Agreement.

4.10.3 Optional features

Not applicable.

4.11 End of subscription

The Service Customer or the TSP can terminate the Service Agreement according to the Terms and Condition of the agreement. The technical process is described in Section 5.8.

4.12 Key escrow and recovery

Key escrow and recovery are not supported in relation to the Issuing CAs.

5 Physical, procedural and personnel security controls

5.1 Physical controls

5.1.1 Site location and construction

The CA and RA operations are conducted in secure hosting facilities in Sweden, which meet the requirements of Security and Audit Requirements.

5.1.1.1 Data center environment

The Service is operated in data centers in the Sweden with ISO 27002 compliant physical and logical protection. (Other regions are planned and will be announced in this CPS, when applicable.) All equipment (servers, firewalls, switches, load balancers, HSMs) and data (payload CA data, CA configuration data, infrastructure code, system and audit logs, certificate requests, etc.) are operated in these environments; with exceptions listed later in this clause. All Service components (except disaster recovery backup storage) operate in at least two data centers with similar protection level. The data centers have a distance of at least 10 km.

All exterior walls of the data centers are pre-cast or masonry block, concrete or material of equivalent strength and penetration resistance. Windows, doors, and other openings are protected against intrusion by mechanisms such as intruder-/burglar-resistant glass, bars, glass-break detectors, or motion or magnetic contact detectors.

The network and server equipment of the Service are located in a separate room or cage with exclusive access of the infrastructure provider, a subcontractor of the TSP entity. The HSMs are located in a separate closed, locked and sealed HSM rack with exclusive access of the trusted personnel of the TSP. Activation data is held separately, i.e. is not stored in the data centers.

The TSP has implemented policies and procedures to ensure that a high level of security is maintained in the physical environment in which the Service equipment is installed. In particular:

- The Service network is isolated by means of entry firewalls from the Internet. All Service nodes are virtualized, and the virtual machines are connected via virtual firewalls of the cloud environment.
- The data centers (as well as the administrative office environment, see below) is protected by at least two physical perimeters with increasing security (e.g. fence, building, room or cage; respective building, office, ceremony room);
- HSMs are stored in a separate closed, locked and sealed rack within the data center physical environment (room or cage). Only trusted persons of the TSP Organization have access to the HSM rack. CA key backups are stored as encrypted files on the backend servers of the Service on multiple data center sites. The key backup contains the CA keys of all Service Customers. The decryption key is stored in the HSMs. Backups of HSM activation data and administration credentials (smart cards) are not stored in the data centers. They are stored in sealed envelopes in the secure operational depot within the ceremony room, and respectively in disaster recovery depots. By organization rules, the HSM racks and the security depots are always accessed in protocolled ceremonies under multiple trusted persons' control.

The security techniques employed are designed to resist a large number and combination of different forms of attack. The mechanisms include:

- perimeter alarms, reinforced walls and motion detectors in the data centers; perimeter alarms and closed-circuit surveillance of server rooms; video logging of accesses to the dedicated area (room or cage within the data center, where also the HSM rack is located) of the infrastructure provider; metal curtains in the ceremony room; intrusion-safe security depot.
- badge to enter and leave the data center facilities and the dedicated physical area in the data center and in the office environment.

The data center provider uses authorized personnel to continually monitor the data center facility on a 7 x 24 x 365 basis. The facility is never left unattended.

5.1.1.2 Office environment

The office environment is separate from the data center environment. The office environment operates the following equipment and data:

- administration workstation,
- credentials of operative accounts (password letters, smart cards),
- activation data for HSMs (smart cards)
- other trusted equipment (smart card readers, data transfer storage media, log writer PC, printer, scanner etc.),
- paper-based logbooks, inventories, and trusted personnel's authorization letters.

These equipment and data are held in a physically secure and access-controlled ceremony room and operative depot on the office premises of the TSP.

5.1.1.3 Disaster recovery depots

Disaster recovery copies of following data are held in secure cloud storage off-site from the operation data centers and of the office premises:

- credentials of disaster recovery accounts (password letters, smart cards),
- disaster recovery copy of CA keys (in encrypted form on durable medium),
- disaster recovery activation data for HSMs (smart cards).
- electronic copies of paper-based logbooks, inventories, and trusted personnel's authorization letters.

5.1.2 Physical access

Equipment and data of the Service is always protected from unauthorized access. The physical security mechanisms for equipment comprise:

- Data center facilities are monitored manually and electronically 24x7x365 for unauthorized intrusion. An access log is maintained separately from the TSP's ceremony logs.

- The closed HSM rack is locked and sealed with security seal providing temper protection and detection. HSM activation data (smart cards) are stored in security sealed envelopes in the locked physically secure depots. Access to the HSM rack is possible, by organizational rule, only in protocolled ceremonies under multiple trusted persons' control.
- Removable media are stored in security sealed envelopes in the locked physically secure depots. Paper documents (logbooks, inventories, authorization letters) containing sensitive plain-text information are store in the locked physically secure depots.
- Secure areas are always entered in protocolled ceremonies under multiple trusted persons' control. By organizational rule, it is ensured that any individual entering secure areas who is non-authorized on a permanent basis is not left without supervision by an authorized employee.
- The access log is maintained continuously and inspected periodically.
- The data centers as well as the administrative office environment is protected by at least two physical perimeters with increasing security (e.g. fence, building, room or cage; respective building, office, ceremony room);
- The HSMs can be physically accessed in the HSM rack by organizational rule of the data center provider in escort of the data center's security personnel. By organizational rule of the TSP organization, the HSM racks are accessed only in protocolled ceremonies under multiple trusted persons' control.

A security check of the facility housing equipment (HSM rack, ceremony room and the security depots) is carried out if it is to be left unattended. At a minimum, the check verifies at the time of the leaving the facility that:

- the equipment in the HSM rack is in a state appropriate for the current mode of operation;
- for off-line components, all equipment (e.g. administration PC) is shut down or - for a ceremony break - locked;
- any security containers (tamper-proof envelope, security depot) are properly secured;
- physical security systems (e.g. door locks, vent covers, electricity) are functioning properly;
- the area is secured against unauthorized access, i.e. rack door, ceremony room door, security depot door is locked and – if applicable - sealed.

At a minimum, the check verifies at the time of the next access of the facility that:

- the equipment in the facility (HSM rack, ceremony room, security depot) is in untampered and unchanged state;
- any security containers (tamper-proof envelope, security depot) are in untampered state;
- locks are in locked state, security seal are intact and match the seal number in the ceremony log of the last access.

5.1.3 Power and air conditioning

The operational data center facilities are equipped with reliable access to electric power to ensure operation with no or minor failures. Uninterruptible power supply provides power in the event of external

power failure for the sake of smooth shutdown of the Service equipment in the event of a lack of power. The facilities are equipped with heating/ventilation/air-conditioning systems to maintain the temperature and relative humidity of the equipment within operational range.

5.1.4 Water exposures

The operational data center facilities are protected in a way that minimizes impact from water exposure. No water or soil pipes are present in the rooms where the Service is deployed.

5.1.5 Fire prevention and protection

The TSP's operational data centers are operated in line with fire safety requirements. The data centers are equipped with fire and smoke detectors as well as manual and automatic fire extinguishers. The location of manual fire extinguishers and escape routes are indicated in high visibility locations. Storage media is protected in the same manner as other equipment.

Backups of critical system data are stored in the alternate data center and is therefore protected in the same way as the system itself.

5.1.6 Media storage

Operational storage media used for the Service are operated inside data centers and are therefore protected from damage, theft and unauthorized access. The hosting platform includes automatic functions for protection against obsolescence and deterioration of media in the period for which records have to be retained.

Paper as storage media is used only for ceremony logbooks, inventories, and authorization letter. These are stored in the operative security depot. Paper is obsolescence-free. Deterioration protection is provided by the electronic backups on optical medium.

All items of storage equipment (e.g. magnetic and flash memory disks) are managed by the infrastructure provider to ensure that any sensitive data and licensed software are removed or securely overwritten prior to disposal or re-use.

Paper-based material is destroyed in shredder in ceremonies. Flash memory devices (USB memory sticks, SSD discs) are destroyed in ceremonies by demounting and drilling through the memory chip(s). Optical media (DVD, BluRay) are cut in many parts and disposed at several places. Hard disks are not used. Smart cards are destroyed in ceremonies by drilling through the chip, and/or run through a smart card shredder. Passwords are reset, and the corresponding password letters are shredded in ceremonies.

Assets associated with information and information processing facilities is identified and an inventory of these assets is maintained. The inventory is maintained in electronic and paper-based forms.

5.1.7 Waste disposal

All items of storage equipment (e.g. magnetic and flash memory disks) are managed by the infrastructure provider to ensure that any sensitive data and licensed software are removed or securely overwritten prior to disposal or re-use.

Before disposal, storage media is destroyed securely using mechanisms described in Section 5.1.6.

Before removing from operation, all private keys in HSMs are erased using the HSM's native management mechanisms. Then the security domain is removed from the HSM, which will affect erasing the key encryption key of the domain.

5.1.8 Off-site backup

Full back-ups of virtual machines and data sufficient to recover from system failure, are made at least after Service deployment and after each new key-pair generation. Back-up copies of essential business information (key pair and CRL) and software are made regularly. Adequate back-up facilities are provided to ensure that all essential business information and software can be recovered following a disaster or media failure. Backup arrangements for individual systems are regularly tested to ensure that they meet the requirements of the business continuity plan. Full backup copies of virtual machines are stored in at least two data centers. The backup copy is stored in the operational data centers, i.e. with physical and procedural controls as the operational environment. Additionally, database content with certificate data is stored in off-site backup storage in encrypted form.

Backup data are subject to the same access requirements as the operational data. Offsite backup data is encrypted. In the event of complete loss of data, the information required for putting the Service into operation shall be completely recovered from the backup data.

Private CA key material is backed up using the native backup mechanisms of the HSM. CA key backups are stored as encrypted files on the backend servers of the Service on multiple data center sites. The key backup contains the CA keys of all Service Customers. The decryption key is stored in the HSMs. CA key backup data can only be recovered by another HSM within the same security domain. The HSM administration credentials (smart cards) needed to recover the CA keys are in exclusive control of TSP Security Officers on smart cards.

5.2 Procedural controls

This section describes the implementation of requirements for roles, duties, and identification of personnel. The TSP maintains a security organization according to the requirements of the [ETSI TS 319 411-1] NCP policy.

5.2.1 Trusted roles

Employees and contractors who are assigned trusted roles are considered 'trusted persons'. Persons seeking to become trusted persons by obtaining a trusted position are background-checked according to the HR policies of the TSP.

Only trusted persons have access to or control authentication or cryptographic operations that may affect in the Service:

- the validation of information in certificate applications;
- the acceptance, rejection or other processing of certificate applications, revocation requests or renewal requests;
- the issuance or revocation of certificates, including personnel having access to restricted portions of its repository or the handling of subscriber information or requests.

The trusted roles are aligned with [ETSI TS 319 411-1] and include:

- Compliance Officers
- Depot Officers
- Security Officers
- System Administrators
- Security Auditor
- Registration Officers
- Support Officers (including the general role of Revocation Officers)

5.2.2 Number of persons required per task

The TSP practices segregation of duties based on trusted roles and ensures that multiple trusted persons are required to perform sensitive tasks. The roles and related practices comply to [ETSI TS 319 411-1] and apply the practices according to the following clauses.

Policy and control procedures are in place to ensure separation of duties based on job responsibilities. Importantly, the roles Security Officer, System Administrator and Security Auditor are segregated. The most sensitive tasks, such as access to and the management of CA cryptographic hardware (HSM) and its associated key material, are performed by Security Officers. These tasks require the authorization of 2 of N Security Officers, which is enforced by technical means.

Physical and logical access to HSMs is possible only by multiple trusted persons throughout its lifecycle, from incoming receipt, inspection, configuration, installation in the data center environment, activation to final logical and/or physical destruction. Once an HSM is installed in the data center environment, access to the containing locked private rack is possible only by a System Administrator on order of a Service Delivery Manager (the service owner).

5.2.3 Identification and authentication for each role

All persons assigned a trusted role are identified and authenticated prior to any tasks to be performed in the Service. The trusted persons are identified and authenticated based on an official identity document (ID card or passport). The identity data is captured and archived on the Authorization Letters. Authorization Letters are part of the paper-based Ceremony Logbook and are stored under physical control in a secure depot (a security closet) under Depot Officer's control of the key(s).

The TSP verifies and confirms the identity and authorization of all personnel seeking to become trusted persons before they are:

- issued with their access devices and granted access to the required facilities;
- given electronic credentials to access and perform specific functions in the Service.

5.2.3.1 Identification and authorization in ceremonies

Tasks that involve manual administration steps or the usage of trusted equipment (e.g. administration workstation, card readers), are performed in ceremonies under multiple persons control. At the beginning of each ceremony, the participating officers verify the identity of the other officers based on an official identity document with photo and verify their authorization to act in the claimed role on basis of the Authorization Letter of the person.

5.2.3.2 Identification and authorization at systems of the Service

Depending on availability of authentication mechanisms, the following methods are used:

- System Administrators:
  - authentication with strong random-generated passwords (min. 16 characters),
  - 2-factor authentication with SSH client certificate with strong passphrase (min. 16 characters), or
  - 2-factor authentication with mobile SMS.
- Security Officers: exclusively smart card based 2-factor authentication.
- Operative accounts and authentication credentials are always person-related and are in personal possession.
- Disaster recovery (DR) accounts are pseudonymous (e.g. “Security Officer DR#1”). The credentials are stored sealed in remote, secure DR Depots under physical control of Depot Officers.

5.2.4 Roles requiring separation of duties

Roles requiring separation of duties include (but are not limited to):

- the acceptance or rejection of registration requests and other processing of CA certificate applications are tasks of Registration Officers;
- the acceptance or rejection of revocation requests are tasks of Support Officers (including the role of Revocation Officers, revocation of certificates issued by Customer Issuing CAs via Support is not being used in the Service, the Customer is responsible for User certificates);
- the generation, issuing and destruction of a CA certificate are tasks of Security Officers.

The above three trusted roles are segregated.

Segregation of duties are enforced by organizational procedures: The Compliance Officers authorize trusted persons to act in trusted roles and enforce the role segregation rules. Individuals use one single identity, which is their personal identity as recorded in the official document and/or the HR database.

The part of the Service concerned with subject identification, validation, registration, certificate generation and revocation management for a (and under a) Nexus-named CA are direct employees or contractors of the TSP (Nexus), who have no affiliation in other organizations. They are furthermore independent for their decisions relating to the establishing, provisioning, maintaining, and suspending of services in line with the applicable certificate policies. In particular, staff in trusted roles is free from any commercial, financial and other pressures that might adversely influence trust in the Service.

The part of the Service concerned with subject identification, validation, registration, certificate generation and revocation management for a (and under a) customer-named CA MAY be employees or contractor of the Customer. Identification, authentication, and personnel controls are in the responsibility of the Customer and MUST fulfil the practices (including segregation) described in the CPS.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

The TSP organization has sufficient qualified personnel to operate the Service with the stated security and availability level. All staff within the TSP organization receives formal training in Public Key Infrastructure, the CA solution and the TSP organization's practices including roles and responsibilities. All TSP roles are documented in [TSP Roles] and added to individual job descriptions for members of the TSP organization. Before any individual is onboarded in the TSP organization, background checks are carried out according to the TSP's HR policy. These rules apply to both internal employees and external contracted workforce.

5.3.2 Background Check Procedures

All employed or contracted persons seeking to become trusted persons are background-checked by the TSP's HR department according to a defined process and checklist.

Background investigation of persons seeking to become a trusted person includes but is not limited to:

- confirmation of previous employment;
- a check of professional references covering their employment over a period of at least five years;
- a confirmation of the highest or most relevant educational degree obtained;
- a search of criminal records;
- financial credibility check.

The background check is repeated at least every five years as long as the person holds a trusted role.

If HR finds information that may be considered as grounds for that the individual is not suitable for employment and/or a TSP role, the individual will be rejected. The factors revealed in a background check that may be considered grounds for rejecting candidates for trusted roles or for withdrawing authorization from a trusted person include (but are not limited to) the following:

- misrepresentations made by the candidate or Trusted Person,
- highly unfavourable or unreliable professional references,
- criminal convictions, and
- indications of a lack of financial sovereignty or independence.

Reports containing background check information is evaluated by HR personnel, who takes reasonable action in the light of the type, magnitude and frequency of the behavior uncovered by the background check. Such action may include measures up to and including cancelling offers of employment made to candidates for trusted positions or terminating the employment of existing trusted persons. The use of information revealed in a background check as a basis for such action is subject to and handled by HR according to applicable law. The information is not disclosed to any other parts of the company, e.g. the TSP organization.

5.3.3 Training requirements

5.3.3.1 TSP training

The TSP organization provides their personnel with the requisite training to fulfil their responsibilities relating to Service operations competently and satisfactorily.

The internal training program is reviewed bi-yearly by the Compliance Officers and updated if necessary. The training addresses all matters that are relevant to functions performed by their personnel.

External training programs are used as appropriate, such as trainings for 3rd party security or IT products.

The training program addresses matters that are relevant to the Service environment and practices, including:

- security rules and mechanisms of the Service;
- CA software and configuration including generic PKI processes
- cloud service configuration and implementation
- all generic duties the person is expected to perform, and internal and external reporting processes and sequences;
- monitoring and support of the solution;
- incident and compromise reporting and handling;
- disaster recovery and business continuity procedures;

5.3.3.2 External training

RA will receive service specific training via e-Learning modules that has a been specifically designed by Nexus Group. The module is designed with an exam that needs to be passed to be able to access the service as an RA.

5.3.4 Retraining frequency and requirements

5.3.4.1 TSP training

Training will be carried out when new TSP systems or processes are introduced.

The persons assigned to TSP roles will be required to refresh the knowledge they have gained from training on an ongoing basis using a training environment. Training will be repeated whenever deemed necessary to ensure that they maintain the required level of proficiency to fulfil their job responsibilities competently and satisfactorily and at least every two years.

Any significant change in the Service operation will be accompanied by a training plan and the execution of the plan will be documented.

The TSP organization provide their staff with refresher training and updates to the extent and with the frequency required to ensure that they maintain the required level of proficiency to fulfil their job responsibilities competently and satisfactorily.

Individuals in trusted roles are made aware of changes in the Service operations by a Compliance Officer.

5.3.4.2 External training

For customer RA there will be a frequency of 2 years for re-examination. This needs to be passed to keep access to the service as an RA. Audit will be included here to make sure that the frequency is upheld.

5.3.5 Job rotation frequency and sequence

Not applicable.

5.3.6 Sanctions for unauthorized actions

A formal disciplinary process is defined by the HR department of the TSP, ensuring that unauthorized actions are appropriately sanctioned. Any severe unauthorized actions will result in that the TSP role is withdrawn with corresponding access rights and privileges.

5.3.7 Independent contractor requirements

The TSP may permit independent contractors to become trusted persons only under the conditions the contractors are trusted by the TSP to the same extent as if they were employees. The same qualifications, experience, and clearance requirements apply to contractors to be part of the TSP organization as above for employed personnel.

Otherwise, contractors have access to Service' secure facilities only if escorted and directly supervised by trusted persons.

5.3.8 Documentation supplied to personnel

5.4 Audit logging procedures

5.4.1 Types of events recorded

The different audit logs contain information about events as follows:

- The main and central source of security audit is the paper-based Ceremony Logbook; containing the logs of Security Ceremonies of the Service conducted by trusted personnel to deploy components or to perform security-relevant changes in the Service.
- The CA software audit log, containing all actions using CA keys, i.e. certificate and CRL issuing, revocation, CA and key management, changes of CA's policy configurations, CA user management; This audit log also contains all actions on end-entity certificates, independently of if they are initiated via the Service API or the Certificate Management Portal.
- The Certificate Management Portal's audit log, containing all actions (including approvals for certificate requests, and user and user credential management actions;
- The servers' operating system logs containing administrator access information including user management, superuser access for patching etc.;

- Log of the cloud infrastructure management portal, including changes of firewall settings, server resource scaling, backups, deployments of infrastructure code.

The audit logs record the following types of audit events, as described in the [Audit Log Plan]:

- physical facility access
- trusted roles management
- logical access
- backup management
- log management
- data from the authentication process for Subscribers or Devices (end-entities)
- acceptance and rejection of certificate requests
- Device (end-entity) registration
- HSM management
- IT and network management
- security management

At a minimum, each audit record includes the following (recorded automatically or manually for each auditable event):

- type of event (as from the list above);
- trusted date and time the event occurred;
- result of the event – success or failure where appropriate;
- identity of the entity and/or operator that caused the event if applicable;
- identity of the entity for which the event is addressed.

In accordance with the GDPR, the audit logs do not permit access to privacy-related data concerning Devices (end-entities). The privacy plan for the Service is described in the external document [Privacy Plan].

Each person-triggered transaction related to certificate life-cycle is logged along with timestamp, the identity of the transaction requestor, and the original request, optionally including the officer's non-repudiation digital signature. Person-triggered transactions are limited to administration tasks performed by trusted personnel. Their personal identity is not encrypted in the audit logs. The audit log is access-protected, and access is limited, in general, to Security Auditors, Compliance Officers. Operating system audit logs may be read-accessed by System Administrators.

All security audit logs, both electronic and non-electronic, are retained and made available during compliance audits.

5.4.2 Frequency of processing log

Audit logs (logbooks, digital audit trail) are reviewed by TSP-internal or external Security Auditors in response to alerts based on irregularities and incidents within the Service and in addition periodically every year.

Audit-log processing consist of a review of the audit logs and documenting in the Audit Report the reason for all significant events in an audit-log summary, which is specified described in the [Audit Log Plan]. Audit-log reviews include a verification that the log has not been tampered with, an inspection of all security-relevant log entries and an investigation of any alerts or irregularities in the logs. Actions taken on the basis of audit-log reviews are documented.

Electronic audit logs are archived at least weekly. The available disk space is continuously monitored in the Service. Paper-based audit logs are backed up in electronic form and kept offsite of the paper log.

5.4.3 Retention period for audit log

The different audit logs are backed up and/or archived, and retained according to the [Audit Log Plan]. If not otherwise stated in the separate CPS of a customer-named CA, the TSP retains audit log records for:

- at least 10 years for CA keys and certificates after the related certificate ceases to be valid (i.e. either expires or is revoked),
- at least 1 years for end entity keys and certificates after the related certificate ceases to be valid (i.e. either expires or is revoked),
- at least 10 years for system and cloud administration tasks, and actions in the DevOps process.

User-related records are retained as long as any retained audit log contains the actions performed by the user.

5.4.4 Protection of audit log

The audit log protection mechanisms are defined in the [Audit Log Plan]. The integrity and confidentiality of the audit log is guaranteed by a role-based access control mechanism. Audit logs are protected against tampering.

5.4.5 Audit log backup procedures

Backups are created for all log types, and backed-up to a secure location. Backups secured under the same rules as the originals.

Paper-based logs are scanned and backed up/archived in the same manner as the audit logs.

5.4.6 Audit collection system (internal or external)

The CA software activates the CA software audit logging process at system startup and deactivates it only at system shutdown. If audit logging processes are not available, the CA software suspends its operation.

5.4.7 Notification to event-causing subject

Events that are initiated by a trusted role holder, are logged in all audit log types with the role holder's unique identifier. Regular users of the systems are not notified on a separate channel about their activities.

5.4.8 Vulnerability assessment

The role in charge of conducting audit (Security Auditor) and roles in charge of realizing PKI system operation (Security Officer, System Administrator) in the Service explain all significant events (i.e. incidents) in an audit-log summary. Such reviews are part of the vulnerability assessment and management process and involve verifying that the logs have not been tampered with and that there is no discontinuity or other loss of audit data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Action taken as a result of these reviews is documented.

The following vulnerability management measures are performed by the TSP:

- implement organizational and/or technical detection and prevention controls to protect the servers as well as the administration workstations against viruses and malicious software;
- document and follow a vulnerability correction process that addresses the identification, review, response and remediation of vulnerabilities;
- undergo or perform a vulnerability scan:
    - after any system or network changes determined by the TSP as significant for the Service; and
    - at least once a month, on public and private IP addresses identified by the TSP as part of the Service,
- undergo a penetration test on the PKI's systems on at least annual basis and after infrastructure or application upgrades or modifications determined by the TSP as significant for the Service;
- for online systems, record evidence that each vulnerability scan and penetration test was performed by a person or entity (or collective group thereof) with the skills, tools, proficiency, code of ethics and independence necessary to provide a reliable vulnerability or penetration test;
- track and remediate vulnerabilities in line with enterprise cybersecurity policies and risk mitigation methodology.

5.5 Records archival

5.5.1 Types of records archived

All audit logs mentioned in Section 5.4.1. are retained as backup or as a separate archive for their retention period.

5.5.2 Retention period for archive

The retention period for any audit log archive is defined to meet the minimal retention time of the respective audit log, as defined in Section 5.4.3.

In addition to audit log, the TSP retains the following documentation for a minimum of 10 years after any certificate based on that documentation ceases to be valid (i.e. either expires or is revoked):

- PKI audit documentation
- CPS documents
- contract between TSP and external CAs of the same PKI, if applicable (e.g. with a customer-operated Root CA)
- CA and system certificates of the Service
- certificate request records from/to an external CAs of the same PKI, if applicable
- other data or applications sufficient to verify archive contents
- documents exchanged between TSP and compliance auditors

5.5.3 Protection of archive

The same practices apply as for the protection of audit logs, see Section 5.4.4

5.5.4 Archive backup procedures

Archives are regularly transferred to several online archives and backed up regularly to offline archives as well.

5.5.5 Requirements for time-stamping of records

All records in audit logs are time-stamped in UTC.

5.5.6 Archive collection system (internal or external)

Not applicable. There is no archive collection system in the Service.

5.5.7 Procedures to obtain and verify archive information

The archives are accessible only for trusted System Administrators of the TSP. Cryptographic checksums are used to verify integrity of the archives.

A System Administrator verifies the integrity of the archive information before it is restored. Integrity validation is based and controlling the cryptographic checksum (hash) of the archive against the independently logged checksum.

Availability and integrity of archives will be tested at least every 12 months.

5.6 Key changeover

Key pairs will be retired from service and the end of their respective maximum lifetimes in accordance with section 6.3.2.

New CA key pairs are generated in accordance with section 6.1.

A new set of CA key pairs is created at least three months before the expiration time for the existing CA keys.

5.7 Compromise and disaster recovery

The TSP systems and the operation practices are designed to mitigate the risk of a compromise of the Service to a minimum. The effects of the disaster are mitigated with a multiple of backups. For the case of a compromise or a disaster, appropriate processes are in place, as described in the following subsections.

5.7.1 Incident and compromise handling

The TSP continuously monitors their equipment in order to detect potential hacking attempts or other forms of compromise. In such an event, the TSP shall investigate in order to determine nature and degree of damage. The measures are described in [TSP SLA].

Incident and compromise handling, and business continuity are covered by the [Recovery Plan].

If the personnel responsible for the management of the Service detect a potential hacking attempt or other form of compromise, they will investigate to determine the nature and degree of damage. The personnel responsible for the management of the Service, assess the scope of potential damage to determine whether the Service needs to be rebuilt, whether only some certificates must be revoked and/or whether the PKI component has been compromised. In addition, the TSP determines which services are to be maintained and how, in accordance with the business continuity plan. In the event of a PKI component being compromised, the TSP alerts / notifies the Customer and external CAs within the same PKI.

5.7.2 Computing resources, software and/or data are corrupted

If a disaster is discovered that prevents the proper operation of the Service, the TSP will investigate if:

- the private key has been compromised;
- if the redundancy of the systems allows continuing operation on all sites;
- if other site(s) can continue the operation without interruption; or
- if the Service must be suspended.

Defective hardware is replaced as quickly as possible, and the procedures described in sections 5.7.3 and 5.7.4 are applied.

The corruption of computing resources, software and/or data will be reported to affected Subscriber and any external CA within the same PKI within 24 hours for the highest levels of risk. All events are included in the periodic report of the Service.

5.7.3 Entity private key compromise procedures

If a CA key is compromised, lost, destroyed, or suspected of being compromised, the TSP will:

- suspend the operation of affected CA instance;
- revoke the certificate of the compromised CA, if possible; or notify external CAs within the same PKI within 24 hours;
- investigate the ‘key issue’ and notify affected external CAs and Customer;

5.7.4 Business continuity capabilities after a disaster

The TSP implements, tests and maintains a disaster recovery plan [Backup and Recovery Plan] designed to mitigate the effects of any natural or human-made disaster. Such plans address the restoration of information systems services and key business functions.

After an incident that requires changes in the TSP practices to mitigate the same risk in future, the practices and the present CPS will be updated accordingly.

When the compromised Service is unable to operate any longer, the compromised Service will cease its functions with immediate notification to the Customer and affected external CAs.

5.8 CA or RA termination

The TSP or the Customer can terminate the Service Agreement with official notice to the other party according to the General Terms and Conditions for Services of the TSP. Upon the Customer or TSP announcing termination of the Service Agreement, for each customer-named CA, which is still valid and according to an agreed time schedule following actions will be taken:

- The customer-dedicated instance of the certification service is closed, so that no new certificates can be issued.
- The Service may be operated for the other service ports (revocation, OCSP, DP) for a time period as agreed by the parties. The full service fee is charged in this period.

If the Customer terminates the Service, a termination plan will be created with the purpose of minimizing the impact for all involved parties.

In the event of termination of the Service, the TSP is responsible for keeping all relevant records according to the retention times defined in Section 5.4.3 and 5.5.2. A handout of records can be agreed with the Customer.

Detailed information regarding the organization of a CA termination, for example, Crl procedure for last CRL can be found in Zeta eID Termination plan.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

Private keys of all CAs, and their indirect OCSP and CRL signers are generated, stored, and operated in tamper-protected HSMs or – only in case of customer-named issuing CA – tamper-resistant cryptographic units (such as USB HSM). Keys are not exportable at all or are exportable only in encrypted form with proper control of the encryption key. Keys for the Root CA is stored in an offline-system with separate offline HSMs. The HSMs are certified for FIPS 140-2 level 2 or higher and be qualified by EAL4+. This is performed per procedure of the TSP, which includes Key Ceremony with detailed logging to provide traceability.

Private keys of other PKI system components (TLS server and client keys and certificates, log signer keys and certificates) are generated, stored, and operated in the operating systems or the application protected software certificate store.

The design and implementation of the component holding the Device private keys is in the responsibility of the Subscriber, who is at the same time liable for damages due to key compromise of Device keys.

End user keys CAN be generated on the user device such as a smartcard or Nexus SmartID mobile app in a compatible mobile device.

6.1.2 Private key delivery to customer

End-users private keys are generated on the users equipment, such as a smartcard, security hardware token, TPM chip in a computer, or Nexus SmartID mobile app. The end-users are responsible for the generation of the private keys used in their PKCS#10 requests.

A signed certificate is signed by the CA and returned to the Customer via a TLS-secured protocol.

The Service CA does not generate private keys for end-users.

6.1.3 Public key delivery to certificate issuer

The end-user public key is returned in form of the end-user certificate to the Customer or the certificate holder Device in response to the certificate request.

6.1.4 CA public key delivery to relying parties

CA public keys are delivered to Relying Parties by publishing the CA certificates in the Distribution Point, one the Repository's services (see Section 2.2).

6.1.5 Key sizes

The Root CA key size is RSA 4096 bits.

Subordinate CA keys are at least RSA 4096 bits.

User-certificates are at least RSA 2048 bits, following the WebTrust requirements.

6.1.6 Public key parameters generation and quality checking

Public key parameters (algorithm and length) for CAs and PKI system component are pre-configured in the CA software according to Section 6.1.5.

Public key parameters (algorithm and key size) in end-user certificates are verified to be in line with this CPS before their inclusion in a certificate.

The Service also checks for weaknesses of the keys in the PKCS#10 request.

6.1.7 Key usage purposes

Public key usage settings for certificates of CAs and PKI system components are pre-configured in the CA software according to X.509 v3.

Public key usage settings for end entity certificates are aligned with their application and agreed with the Customer. Primary usages are defined in Section 1.4.1.

End-user certificates are issued according to this CPS and may include the following key usages:

Application	**Key usage**
Identification/authentication	Digital Signature
Encryption	Key encipherment, Data encipherment
Digital signature validation	Non-repudiation

6.2 Private Key protection and cryptographic module controls

6.2.1 Cryptographic module standards and controls

6.2.1.1 CA Cryptographic module

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+ compliant Hardware Security Modules, or higher.

Devices for protecting the secret elements of end-user:

6.2.1.2 Protection of End-User Private Keys

Private keys associated with end-user certificates shall be generated and remain protected within secure cryptographic devices or environments that ensure non-exportability and resistance to compromise.

Smartcard-based Key Protection

When the private key and certificate are stored on a smartcard, the smartcard must be a Qualified Signature Creation Device (QSCD) that meets the following requirements:

- The device shall be QSCD-certified in accordance with applicable eIDAS and CEN/ETSI standards.

- The device model shall be approved by Digg prior to deployment in the production environment.
- Private keys shall be always generated and remain within the smartcard's secure boundary.
- Key access shall be protected by a user PIN or equivalent strong authentication mechanism.

Only smartcard products that are validated and included in the list of approved QSCD models maintained by the CA Operator may be used.

Mobile ID-based Key Protection

When the private key and certificate are stored and used within a Mobile ID solution, the following controls shall apply:

- Private keys shall be generated and stored in a secure hardware-backed environment (e.g., Secure Element or Trusted Execution Environment) with non-exportable key enforcement.
- Cryptographic keys at rest shall be protected using strong encryption (e.g., AES-based protection) tied to user authentication secrets (e.g., PIN, passcode).
- Biometric authentication (e.g., fingerprint or facial recognition) may be applied as a second factor, where supported by the device and enabled by policy.
- The Mobile ID application shall implement runtime integrity checks, including jailbreak/root detection, to prevent usage on compromised devices.
- Secure communication channels shall be enforced using modern protocols with certificate pinning to mitigate network-based attacks.
- The Mobile ID implementation shall undergo periodic security assessments, vulnerability remediation, and regular updates under a controlled lifecycle management process.

Further technical details regarding the Mobile ID security architecture are documented in the publicly available Mobile ID technical security documentation.

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

Multi-person controls are enforced to protect the administration of the HSMs, which store the private keys of Subordinate CAs, and its indirect OCSP and CRL signers. Any configuration change of any of the CAs also requires multi-person controls.

See also section 5.2.2.

6.2.3 Private key escrow

Key escrow is NOT applied in relation to the Subordinate CAs.

6.2.4 Private key backup

For business continuity reasons, HSM-based private keys of the Service are backed up. The private keys are exchanged in encrypted form among HSMs and backed up in form of an encrypted file according to the multi-factor protection scheme of the HSM manufacturer. The key files do not leave the protected operation environment with one exception: Disaster recovery copy of the key file are created on optical medium and stored in the physically protected off-site secure disaster recovery depots of the TSP.

Private keys of other PKI system components (TLS server and client keys and certificates, log signer keys and certificates) are generated, stored, and operated in the operating systems or the application protected software certificate store. These are backed up in form of the snapshots of the virtual machines and never leave the secure environment of the respective data center.

End-user keys are NOT backed up.

6.2.5 Private key archival

The TSP uses the same process for “backup” and “archival” in relation to private keys of the Service. Refer to Section 6.2.4.

End-user keys are NOT archived.

6.2.6 Private key transfer into or from a cryptographic module

The HSM-based private keys are exchanged in encrypted form among HSMs and backed up in form of an encrypted file according to the multi-factor protection scheme of the HSM manufacturer. The key files do not leave the protected operation environment except for the disaster recovery copy. (See Section 6.2.4)

The HSM-based private keys are not exportable by any other means.

6.2.7 Private Key storage on cryptographic module

Private keys of Subordinate CAs, and their indirect OCSP and CRL signers are generated, stored, and operated in tamper-protected HSMs. Keys are not exportable at all, or are exportable only in encrypted form with proper control of the encryption key. See also 6.2.6.

6.2.8 Method of activating the private key

Private keys of Subordinate CAs, and their indirect OCSP and CRL signers are stored in HSMs and are activated automatically when starting or restarting the Service. The necessary secret factor is stored in an obfuscated (encrypted) configuration file. The encryption uses several secrets, random and system-individual parameters and is linked to the CA software instance. Additionally, the private key must be registered in the CA software by 2 of N Security Officers and linked to a logical CA to use it for certificate, CRL or OCSP signing.

End-user private keys are activated by two-factor (PIN, and access to device).

6.2.9 Method of deactivating the private key

Private keys of CAs, indirect OCSP and CRL signers can be deactivated in the CA software. This is not practiced only in the inactive periods of Intermediate CAs. These keys are also deactivated under irregular circumstances, like power outage or other failure of the HSM.

End-users are responsible for deactivating their private keys when not in use.

6.2.10 Method of destroying private key

When terminating the service of a CA, indirect OCSP or CRL signer due to obsoletion, expiry of key usage period or compromise, the respective private key is destroyed (i.e. erased) with the help of HSM vendor’s native software or hardware, and according to the vendors description. Special care is taken

to erase the private key in all HSM instances of the HSM cluster (by synchronizing them) and to remove all instances of backups of the key file used for synchronization. Finally, the archived key file on the optical medium in the secure depots is replaced with an update and then destroyed by Security Officers in a ceremony.

The Customer or the User is responsible for the destruction of User private keys when the corresponding certificate is revoked or expired, or if the private key is no longer needed.

6.2.11 Cryptographic module rating

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.

6.3 Other aspects of key pair management

6.3.1 Public key archival

The Service archives public keys (in form of the certificates) of the Subordinate CAs, and their indirect OCSP and CRL signers are archived as described in Section 5.5.1.

The Service stores all CA certificates, and end-user public keys or certificates for at least 10 years.

6.3.2 Certificate operational periods and key pair usage periods

The validity period of the TSP's certificates and the private keys belonging to them are chosen so that their cryptographic algorithms can be anticipated to remain secure for the validity time of the respective certificates.

The TSP makes sure that the Subordinate CA certificates' validity neither extends the operation period of the key pair, nor it extends the validity of the issuer CA certificate. The end-entity certificates' validity never extends the expiration date of the issuer CA.

The default validity and the operation period for the CAs and end-entities is defined below:

Entity	Operation period	Validity period
Nexus GO eID Root CA G1	20 years	30 years
Nexus GO eID Intermediate CA G1	15 years	30 years
Nexus GO eID Nexus Issuing CA G1	10 years	15 years
Customer-named Issuing CA G1	10 years	15 years
End-user certificate (Device)	the same as validity	0-5 years

The expiry date of any Subordinate CA certificate or of end-user certificate never exceeds the expiry date of the CA that issued the Subordinate CA certificate.

These validity and operation periods are applied to all Nexus-named and customer-named CAs.

Nexus may retire its CA private keys before the operational period ends for the respective CA for other reasons than that the operational period ends.

6.4 Activation data

6.4.1 Activation data generation and installation

The Subordinate CAs, and its indirect OCSP and CRL signer private keys are protected, generated, and installed in accordance with the procedures, requirements defined in the used Hardware Security Module user guide and the certification documents. For the sake of automated start and restart of the Service, the CA software application automatically authenticates at the so-called logical key provider (so called “PKCS#11 slot”) of the private key inside HSM by means of a one-factor passphrase (the so-called “PKCS#11 PIN”). The initial value of this complex passphrase is generated randomly and entered by a Security Officer in the CA application during the deployment of the CA software. The CA software stores this passphrase in an obfuscated configuration file, which is encrypted with several secret, random and system-individual factors.

See also section 6.2.2.

6.4.2 Activation data protection

Activation data (“PKCS#11) for TSP private keys, as described in Section 6.4.1. is stored securely in an obfuscated configuration file, which is encrypted with several secret, random and system-individual factors. The passphrase is not stored electronic form anywhere else. Only two paper-based copies are created at the time of generation and saved for disaster recovery purpose in seal security envelops in off-site secure depots. Only trusted personal (Depot Officers) can access the Depots.

Users are required to protect their activation data by protecting their device and access to the application with a user-selected PIN that is at least six digits long. The user is encouraged to always keep the PIN secret. Activation data is added after the user has selected a PIN to either a security hardware token, smartcard, TPM, or Nexus SmartID mobile app.

6.4.3 Other aspects of activation data

Not applicable.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The hosting data centers’ computer security controls are designed in accordance with the high security level by adhering to the requirements of ISO/IEC 27002.

The TSP ensures the security technical requirements in the design and implementation of operating system and application level security:

- Users are authenticated with 2-factor authentication before granting access to the system or application (see section 5.2)

- Roles are assigned to users and every user only has permissions appropriate for his or her roles (see section 5.2.3)
- A log entry is created for every transaction at any level of the infrastructure, and the log entries are archived
- Proper procedures are implemented to ensure service recovery after system failure or interruption

6.5.2 Computer security rating

To keep the high security of the computer infrastructure, the hosting data center operates a quality management system according to ISO 9001 and ISO 27001.

6.6 Life cycle technical controls

6.6.1 System development controls

The TSP uses trustworthy services and products that are protected against modification and ensure the technical security and reliability of the processes supported by them. The manufacturers of the equipment are organizations with numerous references and a reliable background.

The TSP develops on itself the CA software and the code, which deploys and configures firewall rules, virtual machines, operating systems, databases, the CA software in the environment. Both the product and infrastructure are deployed and developed by highly professional, background-checked, trained employees of the TSP. The development and deployment process follows quality and security processes (including code reviews, staging, automated testing etc.) and is supported by a secure repository with version control and audit log. The version control indicates any kind of unauthorized changes, data entry that affects the software or infrastructure code.

The environment is in the secure office facilities of the TSP with multi-zone access control.

The TSP ensures that the operating system, applications, and the CA software to be deployed is the proper version and free from any unauthorized modification. Only authorized persons can make changes to the any code or configuration in the environment.

6.6.2 Security management controls

The TSP implements processes for documenting, operating, verifying, monitoring, and maintaining the systems used in the Service.

Changes in the Service are initiated by the Service Delivery Manager, are implemented in the infrastructure code by trusted persons, reviewed, tested in the staging environments, and finally deployed in the productive environment by trusted System Administrators.

Vulnerability scans and penetration tests are performed regularly.

6.6.3 Life-cycle security controls

Any change to the keys, certificate, and policy settings of the Root CA, and the Subordinate CAs, is performed in controlled ceremonies under multiple person control.

The TSP ensures the protection of the used HSMs during their whole life cycle which means, among others, the following:

- Each Hardware Security Module applied by the TSP has been verified on origin, integrity, and is tested.
- The HSM is verified to have the right certification, firmware version and tamper-protection status.
- The HSMs (including spare HSMs) are always stored in a secure location.
- The operation of the Hardware Security Module continuously complies with the requirements specified in its certification report and user guide
- The TSP irrevocably deletes the provider keys from the Hardware Security Modules permanently or temporarily withdrawn from use.

6.7 Network security controls

The networks of the hosting data centers as well as the networks of the TSP are hardened against attacks in line with the requirements and implementation guidance of ISO/IEC 27001 and ISO/IEC 27002. Entry firewall, virtual networks with virtual firewall-protected dedicated connections and hardened OS are applied. DDoS protection is provided by an 3rd party infrastructure provider.

Suspicious network activity is monitored, and alerts are sent to a monitoring system.

6.8 Time stamping

Certificates, CRLs, and audit log entries contain time and date information. Such time information is based on the data centers trusted network time (NTP) signal. The time stamps are not cryptography-based.

The offline systems are set to the correct time when used.

7 Certificate, CRL and OCSP profiles

This section describes the formats and contents of issued certificates, Certificate Revocation Lists (CRLs), and OCSP responses. Detailed technical specifications, including extensions, syntax, and conformance requirements, are defined in the Certificate Profile documentation referenced by the Certificate Policy (CP). The CA Operator shall ensure that all certificate and revocation information conform to the applicable profiles and supported standards.

8 Compliance audit and other assessments

The CA Operator shall ensure that periodic compliance audits and security assessments are performed to verify conformance with the Certificate Policy (CP), this Certification Practice Statement (CPS), and applicable regulatory and industry requirements. The scope, frequency, audit criteria, and auditor qualifications are defined in the CP. The CA Operator shall provide all necessary documentation, evidence, and access required to support these audits and assessments.

9 Other business and legal matters

Business, legal, and contractual provisions applicable to the CA services, including liability, dispute resolution, confidentiality, privacy, and intellectual property rights, are defined in the Certificate Policy (CP). This CPS adheres to those provisions and describes the operational practices implemented by the CA Operator to support compliance with such requirements.