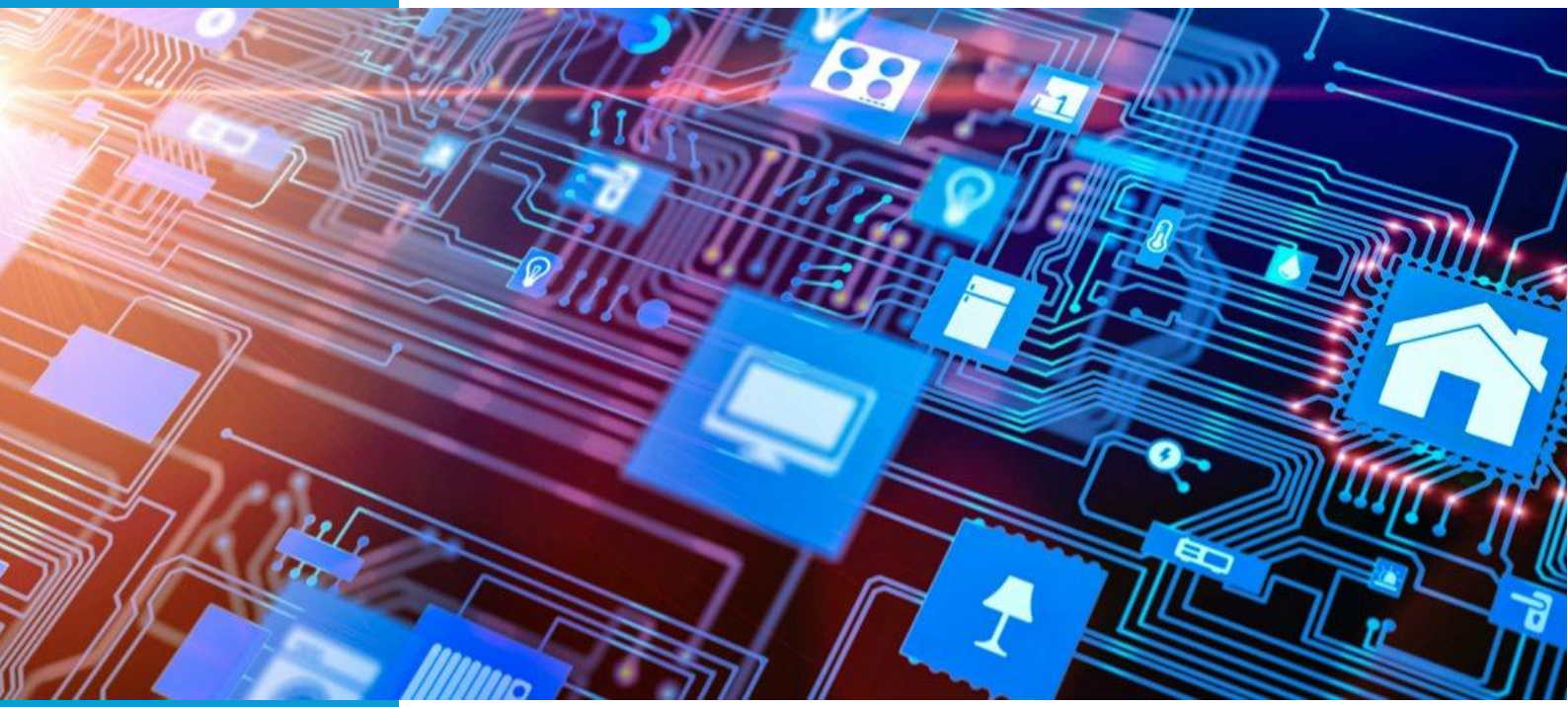
Enabling trusted identities



Nexus GO IoT

Certificate Practice Statement for the Subordinate CAs

Version 1.2 – 2020-01-31

ISO public information

Document identification and ownership

Document issuer:	Technology Nexus Secure Business Solutions AB, Trust Service Provider (TSP) organization
Document name:	Nexus GO IoT – CPS for the Subordinate CAs
Document version:	Version 1.2
Date:	2020-01-31
CPS document OID:	1.3.6.1.4.1.31086.1.2.3.1.0
Relevant CP OID:	1.3.6.1.4.1.31086.1.2.1.1.0
Relevant CP name:	Nexus GO IoT – Certification Policy, version 1.0

Trust Service Provider (TSP) identity

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

Change history

Version	Description	Affected section	Effect date	Responsible
1.0	Initial release		2019-11-15	Nexus TSP, Horvath
1.1	Added information about CA logical separation. Added information about optional publication of Certificate Issuing Lists for customer-named CAs. Removal of a certificate from CRL after expiry applies only to Nexus-named CAs. Added information about CA key backup. Reorganized Subscriber's responsibilities and obligations in Chapter 9.	1.3.1 2.1 2.3 5.1.1.1 5.1.8 9.6.1	2019-11-20	Nexus TSP, Horvath
1.2	Refinements of IPRs: Subscriber owns the revocation information, not the TSP	9.5	2020-01-31	Nexus TSP, Horvath

Contents

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.
Device	'Device' in this CPS is reserved to denote the end entities in the Nexus GO IoT PKI. The Devices can be IoT devices, IoT security gateways, web servers, web clients, network equipment, mobile apps or other technical components, related to the infrastructure.
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.
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.
Subscriber	The Subscriber is the organization (legal entity) who acts in the PKI management processes as subscriber for CA and end entity certificates. The Subscriber is in most cases the Service Customer, but it can also be an appointed contractor of the Service Customer, who acts on behalf of the Service Customer in certain PKI management functions, such as enrolment or provisioning of certificates. An example is the manufacturing site of 'devices', which enrolls certificates for the devices on behalf of the Service Customer for the end entity certificates.
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.

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 IoT - Audit Logging and Archiving Plan"
[Backup Plan]	TSP's specification: "Nexus GO IoT - Backup and Recovery Plan"
[DR Plan]	TSP's specification: "Nexus GO IoT -Disaster Recovery Plan"
[Privacy Plan]	TSP's specification: "Nexus GO IoT - Privacy Plan"
[Termination Plan]	TSP's specification: "Nexus GO IoT -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 IoT applications. The marketing name of the PKI service is 'Nexus GO IoT'. The TSP provides the Nexus GO IoT service (briefly 'the Service') for its contracted Service Customers.

Nexus GO IoT is a multi-tenancy-enabled, shared cloud PKI service, and is one of the 'Nexus GO' cloud services. The central 'TSP Organization' of Nexus operates these services in a cloud 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 the European Union. (Other regions are planned and will be announced in this CPS, when applicable.) The cloud 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 IoT service covers the registration, issuing and lifecycle management (revocation, renewal) of certificates used by IoT devices, IoT security gateways, web servers, web clients, network equipment, mobile apps or other technical infrastructure components (jointly called 'Devices') primarily for communication security (authentication, encryption, integrity validation). Other usages of certificates are possible, e.g. code signing. The TSP operates the necessary PKI infrastructure including Root CA, Subordinate CAs, OCSP responder, CRL Distribution Point, certificate management interfaces (APIs) and web portal.

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 GO IoT service. (The offline Root CA of the Nexus GO IoT service is covered by a separate CPS.) 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. Accordingly, not all requirements of ETSI NCP are applicable for the GO IoT PKI service, which primarily serves to secure communication among IoT devices and technical components in their application infrastructure. In particular, the leaf certificate subjects in the GO IoT PKI are technical components, not natural or legal persons. As there is no industry-standard certificate policy for IoT security application, currently we relate this CPS to the ETSI NCP, which is widely known by the security industry and by auditing organizations.

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

The content and 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

Document name and identification is provided in the preamble on Page 2 of this CPS.

1.3 PKI participants

1.3.1 Certification authorities

The TSP operates following CAs in a 3-tier PKI hierarchy:

- Nexus GO IoT Root CA – covered by a separate CPS
- Nexus Go IoT Immediate CA – covered by this CPS
- Customer-named IoT Issuing CA– may or may not be covered by this CPS

The GO IoT Root CA 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 Subordinate CAs (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 the European Union. (Other regions are planned and will be announced in this CPS, when applicable.) 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 Subordinate CAs are stored in network HSM appliances with secure key backups. In the default setup, the HSMs are shared among the Nexus and the customer-named CAs, and clustered across the data center locations. The HSMs are under the exclusive physical and logical access control of the Nexus TSP organization. The CA keys are backed up properly in both cases.

Subscribers can opt for a customer-named Root CA and/or a customer-named Intermediate CA, which are operated by the TSP in the same manner according to the respective CPS of the TSP.

Furthermore, Subscribers can opt for operating a customer-named CA at any level, which is combined with CAs operated by the TSP. This CPS does not cover such customer-operated CAs and corresponding Registration Authorities.

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-entity certificates is operated by the Subscriber.

The Subscriber can register and request certificates for technical components (referred to as ‘Devices’), which it produces, owns or operates. The Subscriber needs not provide a proof of production, ownership or control of a Device (see 1.3.3), when enrolling for an end-entity leaf certificate.

In relation to the registration of leaf certificate subjects, the Subscriber is responsible for:

- assurance of the uniqueness of Device identities,

- assurance of correctness of the CSR subject attributes,
- assurance of the authorization of CSRs, i.e. no CSRs with unauthorized content can pass authentication.
- the public key sent in the CSR to the certificate service relating to the certificate holder Device indicated in the CSR, and the

As mentioned in 1.3.2, the Subscriber can opt for operating a customer-named CA at any level, which is combined with CAs operated by the TSP. This CPS does not cover such customer-operated CAs and corresponding Registration Authorities.

1.3.3 Subscribers and end-entities

The end-entities (i.e. subjects of leaf certificates) are IoT devices, IoT security gateways, web servers, web clients, network equipment, mobile apps (jointly called 'Devices'), which are owned and/or operated by the Subscriber.

The Subscriber is the organization (legal entity) who acts in the PKI management processes as subscriber for CA and end entity certificates. The Subscriber is in most cases the Service Customer, but it can also be an appointed contractor of the Service Customer, who acts on behalf of the Service Customer in certain PKI management functions, such as enrolment or provisioning of certificates. An example is the manufacturing site of Devices, which enrolls certificates for the Devices on behalf of the Service Customer for the end entity certificates. In such a case, the service agreement handles the responsibilities and authorizations of the appointed contractor.

For the simplicity of this CPS, the appointed contractor of the Service Customer we will also call 'Subscriber'. Please note this slight difference of the terms 'Service Customer' and 'Subscriber'.

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 Subscriber.

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

1.3.5 Other participants

Other participants are not recognized by the TSP and not covered by the present CPS.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The private key belonging to an end-entity certificate can only be used for securing communication among Devices and other technical infrastructure related to the PKI application. This is achieved by means of authentication, decryption and providing proof of origin and integrity. Other usages of the certificates are possible, e.g. code signing (which also a prove of origin and integrity). The key usages have to be agreed with the TSP and are marked in the certificates' key usage fields.

The public key in an end-entity 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-entity, or for validating origin and/or integrity.

The Subordinate CA keys are used according to common practice to sign certificates, CRLs and OCSP responses. Indirect signing of CRLs and OCSP responses is possible within the GO IoT PKI according to agreement with the TSP.

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

Questions regarding this CPS should be addressed to the following address: gopki@nexusgroup.com

1.5.2 Person determining CPS suitability for the policy

A TSP Compliance Officer is responsible for determining the suitability of this CPS and other supplementary documents that are subordinate to this CPS.

1.5.3 CPS approval procedures

Changes in the certificate practices are first drafted in the CPS, then reviewed and approved by the Service Delivery Manager and a Compliance Officers of the TSP organization, who are responsible for service delivery 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 12 of the present document.

2 Publications and repository responsibilities

2.1 Repositories

The CRLs of the Subordinate 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 DP service access is optional for customer-named CAs, i.e. the DP MAY (but need not) be available, based on individual agreement with the Service Customer. The DP is available for Nexus-named CAs. If applicable, the CRL access method (HTTP) and address is asserted in the CRL Distribution Point extension of the respective issued certificate.

In addition to CRLs, the DP MAY publish Certificate Issuing Lists (CILs) for customer-named CAs, if agreed with the Service Customer. The CIL of a CA is signed with either the CA key or an indirect CIL signer key. It contains information – excluding the certificate - about all certificates issued by the respective CA and can thus be used as proof of existence of the certificate. The CIL has a proprietary format. Nexus-named CAs do not publish CILs.

The Subordinate CAs provide OCSP service. The OCSP service access is optional for customer-named CAs, i.e. the OCSP CAN (but need not) be available, based on individual agreement with the Service Customer. OCSP service is available for Nexus-named CAs. If applicable, the OCSP access method and address is asserted in the in the Authority Information Access extension, accessMethod=id-ad-ocsp, accessLocation=URL of the issued certificates.

Subordinate CA certificates are published in the same DP repository as the respective CRLs and are accessible via HTTP protocol. Publication of the Subordinate CA certificates is optional for customer-named CAs. Nexus-named CAs certificates are accessible in the DP. 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.

Accessing information in the DP and the use of the OCSP service is possible without authentication and are free of charge for Relying Parties. The access requires an agreement with the Service Customer.

End entity certificates are NOT published by Nexus-named Issuing CAs. Service Customer can opt for accessing end entity certificate via the REST Interface and/or the Registration Authority portal of the Service. Accessing end entity certificates in either way requires authentication and requires an agreement with the Service Customer.

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.

2.2 Publication of certification information

The Nexus IoT PKI service addresses for certificate information access are the following:

- Distribution Point: http://dp.goiot.nexusgroup.com/
- OCSP: http://ocsp.goiot.nexusgroup.com/
- REST Interface: https://pgw.goiot.nexusgroup.com/<customer serviceID>

- Policies, CA certificates with revocation information for Nexus-named CAs only: https://gopki.nexusgroup.com/

Subscribers can rename the service URLs using a DNS service of their choice.

As mentioned in Section 2.1, Subscribers can opt NOT to open the respective service addresses for their customer-named CAs.

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 GO PKI web page https://gopki.nexusgroup.com/. All earlier CP and CPS versions will be made available.

Any certificate listed in a CRL of a Nexus-named Subordinate 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.

The certificate removal policy is optional for customer-named CAs.

2.4 Access control on repositories

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

The REST interface requires certificate-based TLS authentication for read-accessing end entity certificates.

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 subject name for end entity certificates MAY contain a technical identity of the certificate holder Device, for example a manufacturer ID and a serial number. The subject name form and semantic is defined in the CPS of the respective customer-named Issuing CA. The form is not limited, but the subject name MUST be unique. The Subscriber is responsible for the uniqueness of the end-entity subject names.

3.1.2 Anonymity or pseudonymity of subscribers

Anonymous or pseudonymous subject names MAY be chosen for end-entity certificates, as agreed with the TSP.

3.1.3 Rules for interpreting various name forms

The interpretation of end-entity subject names is not controlled by this CPS. It is in the responsibility of the Subscriber.

3.1.4 Uniqueness of names

Subject names are unique with respect to the certificate holder entity, both for service certificates of the TSP, service certificates related to customer-named CAs and for the end-entities. Several certificates held by the same entity MAY exist with the same subject name.

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. This is in the responsibility of the Subscriber.

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 (Devices), 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 Subscriber, which is named in certificates, is identified by the TSP by means of common commercial method, e.g. a company registry. Ownership of a technical domain (e.g. DNS domain) is verified too, if mentioned in certificates requested by the Subscriber.

Only verified name forms of the Subscriber are inserted in certificates, i.e. a Subscriber cannot request a certificate for a non-verified another legal.

3.2.3 Authentication of individual entity

Because the end-entities are technical components under control of (i.e. produced, operated or owned by) the Subscriber, individual entities are not verified by the TSP. The existence of the Device and the uniqueness of Device identity are in the responsibility of the Subscriber and MUST be assured during the Subscriber enrolling for end-entity certificates in the Registration Authority role. The TSP does not execute in the Registration Authority role.

The end-entity (Device) can request initial certificates directly via the Service Interface of the TSP. In this case, the end-entity authenticates with an existing key and corresponding valid (non-expired, non-revoked) certificate. The certificate may be a “factory certificate” (or “birth certificate”) created by an “factory CA” under the control of the Subscriber or of a trusted supplier to the Subscriber; or a certificate issued by the TSP itself. The authentication certificate subject MAY be verified by the TSP according to the individual CPS of the customer-named Issuing CA.

3.2.4 Non-verified subscriber information

Service certificates related to the customer-named CA of the Subscriber contains no non-verified information.

End-entity certificate subject names are, in general, not verified by the TSP, as explained in Section 3.2.3. It is the responsibility of the Subscriber to ensure the existence of the end-entity and the uniqueness of its Subject identity, when requesting a certificate for it.

3.2.5 Validation of authority

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

The TSP does not explicitly verify the authorization for a certificate request for end-entity. Successful authentication of the request is considered as evidence of authorization. The Subscriber is responsible for:

- the assurance of the authorization of the request, i.e. no request with unauthorized content can be submitted,
- the public key sent in the CSR to the certificate service to correspond to the certificate holder Device indicated in the requested subject name.

3.2.6 Criteria for interoperation

The Service Interface used to submit initial certificate requests, re-keying requests and revocation requests for end-entities are documented in technical standards (RFCs) or by the TSP (such as the proprietary REST interface). Integration tests are supported by the TSP by means of a test environment and test certificates. The interfaces return error codes in case of any failure in the processing of a certificate or revocation request.

3.3 Identification and authentication for re-keying requests

3.3.1 Identification and authentication for regular re-keying

Authentication and identification for re-keying is handled in similar way as initial certificate issuing:

The end-entity (Device) can request re-keying directly via the Service Interface of the TSP. In this case, the end-entity authenticates with an existing key and corresponding valid (non-expired, non-revoked) certificate. The certificate may be the certificate issued by the TSP itself. The authentication certificate subject MAY be verified by the TSP according to the individual CPS of the customer-named Issuing CA.

3.3.2 Identification and authentication for re-keying after revocation

Authentication and identification for re-keying is handled in the same way as initial certificate issuing with the exception that an end-entity cannot authenticate for re-keying with the help of the revoked certificate.

3.4 Identification and authentication for revocation request

Authentication and identification for revocation is handled in the same way as initial certificate issuing.

4 Certificate life-cycle operational requirements

4.1 Certificate application

The term certificate application refers to the following processes:

a) Initial certificate request

b) Re-keying request

4.1.1 Who can submit a certificate application

Certificate requests (a synonym for certificate application) for end-entities can be submitted via the Service Interface by:

- systems under control of the Subscriber (such as manufacturing equipment, device provisioning service); or
- the end-entity Device itself

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 Subscriber. The Subscriber 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.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

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

As described in Section 3.2.3, the certificate holder entities are Devices produced, operated or owned by the Subscriber, which are not identified or verified by the TSP. The existence of the Device and the uniqueness of Device identity is in the responsibility of the Subscriber and MUST be assured during the Subscriber enrolling for end-entity certificates in the Registration Authority role. The TSP does not execute in the Registration Authority role.

The Service Interface authenticates the certificate request by means of a service client certificate issued for the Subscriber or by means of an existing certificate of the requesting end-entity as described in Section 3.2.3. The Service Interface MAY validate the certificate request according to rules agreed with the Subscriber, such as verification of certain patterns or fixed contents in the requested subject name; or of key algorithm and length. The request validation rules are described in the CPS of the respective customer-named Issuing CA.

4.2.2 Approval or rejection of certificate applications

Certificate requests (applications) are authenticated and certain contents MAY be verified by the Service Interface. The request is refused, and an error message is returned by the Service Interface, if:

- authentication fails,
- the (optional) validation of subject attribute content or public key parameters fails.

4.2.3 Time to process certificate applications

Certificate requests (application) are processed by the Service Interface instantly.

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.

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
- signs the certificate with the help of the private key of the customer-named Issuing CA.

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.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Not applicable to CA or related service certificates.

Not applicable to end-entity certificates. There is no explicit process of certificate acceptance, nor a technical acknowledgement of the reception of the certificate. The Subscriber can send the same certificate request, if the requesting session with the Service Interface happened to be interrupted. The Service Interface will return the same certificate.

4.4.2 Publication of the certificate by the CA

In the default setup, the TSP publishes Subordinate CA certificates in the Repository as described in Section 2.1. The Subscriber can opt not to publish the certificates of its customer-named CAs. The certificates of Nexus-named CAs are also published on the Nexus GO PKI web page.

In the default setup, the TSP does not publish end-entity certificates. The Subscriber can opt to publish the certificates in the Repository as described in Section 2.1.

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 Subscriber private key and certificate usage

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

The end-entities (Devices) 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 Subscriber, who controls the design of the device software/firmware. The end user agreement SHOULD oblige the end user (owner, operator) of the Device to use the Device according to the intended purpose.

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 Subscriber is responsible for handling the agreements with Relying Parties.

4.6 Certificate renewal

Not applicable. Certificate renewal is not practiced in the Service, neither for CA and related service certificates nor for end-entity certificates.

4.7 Certificate re-keying

Certificate re-keying is practicable for CA and related service certificates as well as for end-entity certificates.

Re-keying is implemented using the same security rules and technical processes as initial issuing, but authentication of the re-keying request MAY be different, as described in Section 3.3.1.

4.8 Certificate modification

Not applicable. Certificate modification (synonym for certificate replacement) is not practiced in the Service.

CAs and end-entities 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-entity certificate may be revoked, when:

- it becomes obsolete due to re-keying of the certificate (revocation reason ‘superseded’),
- it becomes obsolete due to termination of use of the Device in the target application (revocation reason ‘cessationOfOperation’),
- the Device 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 Subscriber MAY request revocation of the respective customer-named CA.

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

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

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-entity certificates in automated process. It:

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

In the default service setup, revocations do not immediately appear in the CRL and/or OCSP, but first in the next regular CRL of the issuing CA. OCSP is supplied with revocation information in form of the CRL.

Customers can opt for immediate issuing of a delta CRL upon revocation, which will also effect updating immediately the OCSP responder.

4.9.4 Revocation request grace period

Revocation requests SHOULD be submitted by the Subscriber as promptly as possible after the cause event within an appropriate time reasonable in view of the risks of misuse of a compromised end-entity key. Choosing the grace time is the responsibility of the Subscriber.

4.9.5 Time within which CA must process the revocation request

The Service Interface and the respective CA process the revocation request immediately 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 Subscriber 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 Subscriber 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. The Subscriber MAY chose to publish or NOT publish revocation information via CRLs for a customer-named CA. This is announced in the CPS of the customer-named CA.

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 IoT Root CA	15 months	12 months
Nexus GO IoT Intermediate CA	1 month + 10 days	1 month
Customer-named Issuing CA	10 days	1 day

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

Operation periods and key usage periods of customer-named CAs CAN be individual. They are defined in the individual CPS of the customer-named CA in agreement with the TSP.

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 Superordinate 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

Nexus-named CAs publish revocation information via OCSP. The Subscriber MAY chose to publish or NOT publish revocation information via OCSP for a customer-named CA. This is announced in the CPS of the customer-named CA.

In the default service setup, revocations do not immediately appear in the CRL and/or OCSP, but first in the next regular CRL of the issuing CA. OCSP is supplied with revocation information in form of the CRL.

Customers can opt for immediate issuing of a delta CRL upon revocation, which will also effect updating immediately the OCSP responder.

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

Revocation of Nexus-named CA certificates is published additionally in text form via the Nexus GO PKI web page https://gopki.nexusgroup.com with a latency of at most 31 days.

4.9.12 Special requirements regarding key compromise

The TSP will notify affected Subscribers 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.

4.10 Certificate status service

4.10.1 Operational characteristics

Certificate status services are available for Nexus-named 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.

Certificate status services MAY be available for customer-named CAs via CRLs and/or OCSP, as stated in the individual CPS of the customer-named CA.

4.10.2 Service availability

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

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 is not supported in relation to the Subordinate CAs.

5 Physical, procedural and personnel security controls

5.1 Physical controls

5.1.1 Site location and construction

5.1.1.1 Data center environment

The Service is operated in data centers in the European Union 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) are operated 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 general PKI operational practices are described in [TSP Organization]

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

Not in the data centers are operated 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. The ceremony room and the depot are documented in [TSP organization].

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. The backup plan is detailed in [Backup Plan].

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. 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. Back-up 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 at least two data centers. The back-up copy is stored in the operational data centers, i.e. with physical and procedural controls as the operational environment. The backup plan is detailed in [Backup

plan]. 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. The roles and the authorization process are described in [TSP Roles].

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 (not used in the Service)
- Support Officers (including the general role of Revocation Officers; but revocation not being practiced via Support in the Service)
- Developers

The trusted roles of the TSP organization are described in [TSP Roles].

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 role segregation scheme is described in [TSP Roles]. 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, as described in [TSP Roles] 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 (not used in the Service);
- the acceptance or rejection of revocation requests are tasks of Support Officers (including the role of Revocation Officers, revocation via Support not being used in the Service);
- 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 Subscriber. Identification, authentication and personnel controls are in the responsibility of the Subscriber 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 unfavorable 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

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 [TSP Training Plan] 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 [TSP Training Plan] 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;

5.3.4 Retraining frequency and requirements

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. Any significant change to the operations will be accompanied by updating and executing the [TSP Training Plan]. The execution of the plan is documented in the TSP's logbooks.

5.3.5 Job rotation frequency and sequence

Any rotation of trusted roles or changes in trusted personnel will be considered by a Compliance Officer with respect to the requirements related to segregation of duties in order to make sure that they do not affect the security and privacy of the TSP's trusted services.

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

TSP personnel will be provided with necessary training (see Section 5.3.3) and documentation needed to perform their job responsibilities competently and satisfactorily. Documentation includes at a minimum:

- [C-ITS CP] and this CPS,
- C-ITS related process descriptions and user instructions,

- The TSP Organization's manuals and user instructions, as listed under References in this CPS,
- ISO 27000 related training material and documents,
- Privacy Policy of the provider,
- CA software and 3rd party product documentation as needed.

5.4 Audit logging procedures

Audit logging is handled in detail in the [Audit Log Plan].

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 DevOps development and deployment environment, including changes to infrastructure code for networks, servers, and especially accounts, deployment logs for updates, patching and account management.
- 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 5 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 5 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 containing information that can lead to personal identification are encrypted in such a way that only authorized persons can read them. Personal data is listed, and the protection mechanisms are listed in the [Privacy Plan].

Audit Log data is encrypted when backed up or archived on storage outside the trusted operation environment of the TSP, e.g. on 3rd party cloud storage.

Audit logs are protected to remain readable for the duration of their retention period. This is provided by the respective infrastructure provider.

5.4.5 Audit log backup procedures

Backups are created for all log types by Nexus or by the infrastructure provider, as applicable. Backups are accessible under the same rules as the originals.

Paper-based logs are scanned and backed up/archived on cloud-based storage with proper retention SLA.

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 identity. Regular users of the systems are not notified on a separate channel about their activities. Irregular users, such as Registration Officers of a customer-named CA MAY be notified on a separate channel (e.g. email or SMS) about an action related to their user account.

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 5 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

The availability of archives is supported by backup procedures provided by the storage infrastructure provider, where the archive is stored.

The TSP MAY use independent storage providers to create the backups of the archive. In general, archives and its backups are stored off-site of the operational environment.

5.5.5 Requirements for time-stamping of records

All records in audit logs are time-stamped. No cryptographic timestamp is applied.

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.

5.6 Key changeover

Key changeover (re-keying) for CAs and system certificates (indirect OCSP or CRL signer, TLS server or client certificate) is initiated and applied by the TSP according to the internal schedule, whenever a CA or system certificate is about to expire, and the Service Agreement is still valid and remains valid beyond the expiry. The Subscriber is notified about re-keying such certificates.

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 in order to determine the nature and degree of damage. The personnel responsible for the management of the Service, assess the scope of potential damage in order 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/Subscriber 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 has to 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 Subscriber;

5.7.4 Business continuity capabilities after a disaster

The TSP implements, tests and maintains a disaster recovery plan [DR 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 Subscriber and affected external CAs.

5.8 CA or RA termination

The TSP or the Subscriber 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 Subscriber 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.
- If the Subscriber wants to continue operating the CA, the last CRL is issued with the regular validity time. Otherwise, the last CRL of the CA will be generated with unlimited validity. The CRL is published and archived.
- In case of customer-dedicated HSM hardware, the TSP can hand out the CA private key or the HSM(s). Otherwise, the CA key is destroyed. The CA certificate is not revoked (unless compromised) to avoid issues with leaf certificate validation.
- 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.

- On customer demand, the TSP can also export all certificates and the last CRL, and transfer them to the Subscriber on an agreed data transfer medium.

The Service termination plan is documented in [Termination Plan]. Financial implications are handled in the Service Agreement.

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 Subscriber.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

Private keys of Subordinate CAs, and their indirect OCSP and CRL signers are generated, stored and operated in temper-protected HSMs or – only in case of customer-named issuing CA – temper-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.

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.

End entity private keys of Devices that are exposed to public networks and unsecure physical environments, are generated either in a secure embedded element (chip, on-board “HSM”, TPM) or in a software-protected environment (TEE – trusted execution environment, key chain, encrypted key store or similar).

End-entity private keys of Devices that are not exposed to public networks and unsecure physical environments (such as vehicle-internal network components, Devices within closed networks, IT equipment like servers or network components) MAY be generated, stored and operated in software environment, which is temper-protected at lower security levels (e.g. operating systems’ 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 entity keys CAN be generated outside the end-entity Device by trusted manufacturing equipment or by a secure “factory CA” close to manufacturing of the Devices. The use of an HSM for generating the Device private key is recommended. Customers can opt for server-side generation of end-entity key. In this case, end entity keys are generated by the Service in an HSM and returned to the Subscriber via a TLS-secured protocol. Immediately after returning the private key, it is erased from the HSM and the components forwarding it. Private keys are NOT backed up or archived in the Service.

6.1.2 Private key delivery to subscriber

Customers can opt for server-side generation of end-entity key. In this case, end entity keys are generated by the Service in an HSM and returned to the Subscriber via a TLS-secured protocol. Immediately after returning the private key, it is erased from the HSM and the components forwarding it. Private keys are NOT backed up or archived in the Service.

6.1.3 Public key delivery to certificate issuer

The end entity public key is returned in form of the end entity certificate to the Subscriber 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 default key algorithm and key size at all levels (Root, Intermediate, Issuing) of CAs and PKI system components (indirect OCSP and CRL signer, TLS certificates of the Service) as well as for end entities is ECDSA with the FIPS P-256 curve ([FIPS 186-4], also called secp256r1) and SHA-256 is used for the CA keys. The respective algorithm OID is:

- ECDSA_nistP256_with_SHA256

Alternatively, FIPS P-384 (also called secp384r1) or FIPS P-521 (also called secp521r1) CAN be chosen:

- ECDSA_nistP384_with_SHA384
- ECDSA_nistP521_with_SHA512

Other algorithms MAY be used by customer-named CA and Devices, according to the individual CPS of the customer-named CA, and in agreement with the TSP.

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 entity certificates are verified to be in line with this CPS before their inclusion in a certificate.

6.1.7 Key usage purposes

Public key usage settings for certificates of CAs and PKI system component are pre-configured in the CA software according to [RFC 5280].

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

6.2 Private Key protection and cryptographic module controls

6.2.1 Cryptographic module standards and controls

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.

Customer-named, customer-operated Issuing CAs may take an exception and use another temper-resistant secure cryptographic module (such as “USB HSMs”) and mention them in the individual CPS of the CA.

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.

Customer-named, customer-operated Issuing CAs may take an exception and use simpler cryptographic devices.

In general, end entity keys are used automatically, i.e. without administration or activation by a person.

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 cloud 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 cloud environment of the respective data center.

End entity 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 entity 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 cloud 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 temper-protected HSMs or – only in case of customer-named issuing CA – temper-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.

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 has to 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 entity private keys need, in general, no activation. Activation mechanism may be enforced by the Subscriber, if usage of PKI functionality is bound to conditions in the agreement with the Device owner

or operator. The conditions and method of activation is described in the individual CPS of the customer-named CA.

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 entity private keys are, in general, not deactivated. Deactivation mechanism may be enforced by the Subscriber, if usage of PKI functionality is bound to conditions in the agreement with the Device owner or operator. The conditions and method of deactivation is described in the individual CPS of the customer-named CA.

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 and according to the vendor's 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.

End entity private keys are destroyed, in general, when the Device is destroyed and "hard reset". Other conditions may be enforced by the individual CPS of the customer-named CA.

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+ 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 TSP 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.

As default policy, the TSP does not archive the end entity public keys or certificates. Individual CPS of customer-named CA may enforce archival in agreement with the TSP.

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.

IMPORTANT!

The TSP cannot guarantee with 100% certainty the security of the cryptographic algorithm over the validity period of the respective certificates. However, some applications require that the validity period of certificates possibly covers the lifetime of end entity products. In order to enable long validities of certificates, Subscribers are strongly encouraged to implement secure mechanisms in the application

infrastructure to roll out new authority certificate to Devices, related services and relying parties. This is a relevant recommendation of this CPS, but it is in the responsibility of the Subscriber.

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 IoT Root CA	5 years	30 years
Nexus GO IoT Intermediate CA	5 years	30 years
Customer-named Issuing CA	5 years	5-30 years as agreed
End entity (Device)	the same as validity	0-30 years as agreed

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

These default validity and operation periods are applied to Nexus-named CAs. They are designed to cover the product lifetime of Devices up to 30 years.

Operation periods and key usage periods of customer-named CAs CAN be individual. They are defined in the individual CPS of the customer-named CA in agreement with the TSP.

6.4 Activation data

6.4.1 Activation data generation and installation

The Subordinate CA, 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.

The method of activation data generation for end entity private keys is – if applicable - described in the individual CPS of the customer-named CA.

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.

Protection mechanisms for activation data for end entity private keys are – if applicable - described in the individual CPS of the customer-named CA.

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
- Roles are assigned to users and every user only has permissions appropriate for his or her roles
- 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

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

The TSP itself operates a SIEM within its organization and IT according to 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 cloud environment (infrastructure as a code). Both the product and infrastructure code are developed by highly professional, background-checked, trained employees of the TSP. The development 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 development environment is in the secure office facilities of the TSP with multi-zone access control. Developer's computers apply disk encryption. The code repository is accessed via VPN. User accounts and privileges are controlled by IT and/or the TSP organization.

The TSP's technical and personnel controls cover the whole life-cycle of the CA software and of the infrastructure code:

The TSP also 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 “code”.

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 (Developers), reviewed, tested in the staging environments and finally deployed in the productive environment by trusted System Administrators.

Vulnerability scan and penetration tests are performed regularly.

The TSP operates a SIEM system according to ISO 27001.

6.6.3 Life-cycle security controls

Any change to the keys, certificate and policy settings of Subordinate CAs is performed in controlled ceremonies under multiple persons’ 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 temper-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 virtual 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.

The Service is deployed with redundancy in each of the two data centers for the sake of high availability.

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.

7 Certificate, CRL and OCSP profiles

This section describes formats of certificates, CRLs and OCSP.

7.1 Certificate profile

The certificate profiles described in this section apply as default profiles. The default profiles follow the recommendations of [RFC 5280] and aim at enabling a Relying Party without prior knowledge of service addresses and subordinate CA certificates to build the CA certificate path and verify revocation status of any end-entity certificates in an open ecosystem of Devices, services and trust providers.

Other PKIs MAY have different conditions (e.g. closed ecosystem with central trust services) and MAY therefore require other profiles. Individual profiles CAN be used by customer-named CAs at any level of the CA hierarchy in agreement with the TSP.

7.1.1 Version numbers

All certificates used and issued by the Service – include the CA, end-entity and other related system certificates are "v3" certificates according to the X.509 specification.

7.1.2 Certificate extensions

The TSP uses the certificate extensions defined in the X.509v3 specifications and indicates the necessity of their interpretation by Relying Parties in their 'critical' fields.

The TSP uses the following Certificate extensions:

Extension	Subfield	Criti-cal	Content in Intermediate and Issuing CA certificate	Content in OCSP signer certificate	Content in end-entity certificate
tbsCert.extensions. AuthorityKeyIdentifier	keyIdentifier	-	the same value as SKI of the issuing CA cert	the same value as SKI of the issuing CA cert	the same value as SKI of the issuing CA cert
tbsCert.extensions. SubjectKeyIdentifier	-	-	according to RFC5280, 4.2.1.2. method (2)	according to RFC5280, 4.2.1.2. method (2)	according to RFC5280, 4.2.1.2. method (2)
tbsCert.extensions. KeyUsage		+	keyCertSign, crlSign	contentCommitment	digitalSignature, keyEncipherment, dataEncypherment, key Agreement
tbsCert.extensions. CertificatePolicies		-	1.3.6.1.4.1.31086.1.2.1.1.0	1.3.6.1.4.1.31086.1.2.1.1.0	1.3.6.1.4.1.31086.1.2.1.1.0
tbsCert.extensions. SubjectAltNames		-	-	-	-
tbsCert.extensions. IssuerAltNames		-	HTTP address of signer CA certificate: http://dp.gopki.nexusgroup.com/<cert-file-name>	HTTP address of signer CA certificate: http://dp.gopki.nexusgroup.com//<cert-file-name>	HTTP address of signer CA certificate: http://dp.gopki.nexusgroup.com//<cert-file-name>

Extension	Subfield	Criti-cal	Content in Intermediate and Issuing CA certificate	Content in OCSP signer certificate	Content in end-entity certificate
tbsCert.extensions. BasicConstraints		+	+	+	+
	ca		TRUE	FALSE	FALSE
	pathLengthConstraint		0	n.a.	n.a.
tbsCert.extensions. ExtendedKeyUsage		+	-	id-kp-OCSPSigning	-
tbsCert.extensions. CRLDistributionPoints		-	Access to CRL: http://dp.gopki.nexusgroup.com/<crl_file_name>	-	Access to CRL: http://dp.gopki.nexusgroup.com/<crl_file_name>
tbsCert.extensions. FreshestCRL		-	-	-	-
tbsCert.extensions. AuthorityInfoAccess	accessMethod	-	id-ad-ocsp	id-ad-ocsp	id-ad-ocsp
	accessLocation. dNSName		http://ocsp.goiot.nexusgroup.com	http://ocsp.goiot.nexusgroup.com	http://ocsp.goiot.nexusgroup.com

7.1.3 Algorithm object identifiers

The default key algorithm and key size of the Intermediate and Issuing CAs and PKI system components (indirect OCSP and CRL signer, TLS certificates of the Service) as well as for end entities is ECDSA with the FIPS P-256 curve ([FIPS 186-4], also called secp256r1) and SHA-256 is used for CA the keys. The respective algorithm OID is:

- ECDSA_nistP256_with_SHA256

Alternatively, FIPS P-384 (also called secp384r1) or FIPS P-521 (also called secp521r1) CAN be chosen:

- ECDSA_nistP384_with_SHA384
- ECDSA_nistP521_with_SHA512

7.1.4 Name forms

The following default name forms are applied:

Name field	Subfield	Content in Intermediate and Issuing CA certificate	Content in OCSP signer certificate	Content in end-entity certificate
tbsCert.subject	commonName	”Nexus GO IoT Intermediate CA Gx” or Customer entity name	”Nexus GO IoT Intermediate OCSP Gx” or ”<Customer short name>” CA Gx” or as agreed	as agreed
	organizationName	"Technology Nexus SBS AB“ or Customer entity name	"Technology Nexus SBS AB“ or Customer entity name	as agreed
	country	SE	SE or Customer’s country	as agreed
	other attributes	-	-	as agreed
extensions.subjectAltNames		-	-	-

Other name forms CAN be used by customer-named CA and Devices, according to the individual CPS of the customer-named CA, and in agreement with the TSP.

7.1.5 Name constraints

Name constraint are NOT used in the default certificate profiles and are NOT recommended to be used by customer-named CAs.

7.1.6 Certificate policy object identifier

The policy OID used in all the default certificate profiles is 1.3.6.1.4.1.31086.1.2.1.1.0, the OID of the Certificate Policy of the Nexus GO IoT service.

Other policy OID will be used by customer-named CA and Device certificates, according to the individual CPS of the customer-named CA, and in agreement with the TSP.

7.1.7 Usage of Policy Constraints extension

Name constraint are NOT used in the default certificate profiles and are NOT recommended to be used by customer-named CAs.

7.1.8 Policy qualifiers syntax and semantics

The extension PolicyQualifierInfo is NOT used in the default certificate profiles and are NOT recommended to be used by customer-named CAs.

7.1.9 Processing semantics for the critical Certificate Policies extension

The extension CertificatePolicies is NOT critical in the default certificate profiles and is NOT recommended to be critical in certificates issued by customer-named CAs.

7.2 CRL profile

The default CRL profile used by Subordinate CA follows the recommendations of [RFC 5280] and aims at enabling a Relying Party without prior knowledge of service addresses and subordinate CA certificates to build the CA certificate path and verify the CRL in an open ecosystem of Devices, services and trust providers.

Other PKIs MAY have different conditions (e.g. closed ecosystem with central trust services) and MAY therefore require another profile. An individual CRL profile CAN be used by customer-named CAs at any level of the CA hierarchy in agreement with the TSP.

The CRLs include the serial numbers of all revoked certificates that were issued by this CA. The default CRL format includes the following data:

- Version
- Signature algorithm
- Issuer
- Issuing date
- Validity period
- List of all revoked serial numbers
- Serial number
- Timestamp of revocation
- Signature of CRL

In the default setup:

- the Subordinate CA issues only base CRLs, no delta CRLs.
- The Subordinate CA key is used to sign the CRL.

In agreement with the TSP, customer-named CAs MAY choose NOT to issue CRLs at all.

In agreement with the TSP, customer-named CAs MAY choose to issue delta CRLs.

In agreement with the TSP, customer-named CAs MAY choose to let a delegated CRL signer signing the CRLs.

7.3 OCSP profile

The OCSP requests and responses are compliant to [RFC 6960]. In the default setup, the OCSP Responses are signed by a delegate OCSP Signer Authority. The certificate of the OCSP Signer certificate is signed by the same CA key and certificate, which are used to sign the certificates, for which certificates the OCSP Signer is supposed to sign revocation information. The OCSP Signer applies the same cryptographic algorithm as the corresponding CA.

8 Compliance audit and other assessments

8.1 Frequency or circumstances of assessment

The TSP performs an audit of the Service annually on the initiative and at the costs of the TSP.

The audit assesses compliance of the Service practices with respect to the present CPS or later versions of it.

8.2 Identity/qualifications of assessor

Proper knowledge of PKI practices, experience with PKI audits and knowledge of the current version of this CPS are pre-conditions for the auditor.

8.3 Assessor's relationship to assessed entity

The audit is performed by a Security Auditor outside the TSP Organization designing, implementing and operating the Service. The auditor may be an internal auditor in the CSO office or a contracted, independent auditor.

8.4 Topics covered by assessment

Not applicable.

8.5 Actions taken as a result of deficiency

The TSP defines measure to counteract of deficiencies determined by an audit within reasonable time in relation to the respective business risks.

8.6 Communication of results

The audit report is presented under NDA to the Service Customer.

9 Other business and legal matters

9.1 Fees

The fees and terms of payment are defined, in general, in the Service Agreement between the TSP and the Service Customer who use the Service defined in this CPS.

9.1.1. Certificate issuance or renewal fees

The general condition applies, see the beginning of Section 9.1.

9.1.2. Certificate access fees

In the default setup, Relying Parties can access certificate information in the Repository free of payment to the TSP. The Relying Parties' transaction volume is estimated in the Service Agreement and appropriately covered with the service fees. Relying Parties may need an agreement with the Service Customer to be able to use the Repository.

9.1.3. Revocation or status information access fees

The general condition applies, see the beginning of Section 9.1.

9.1.4. Fees for other services

The general condition applies, see the beginning of Section 9.1.

9.1.5. Refund policy

The general condition applies, see the beginning of Section 9.1.

9.2 Financial responsibility

TSP complies with the financial and liability requirements below.

9.2.1. Insurance coverage

The TSP has liability insurance that sufficiently covers damages according to Section 9.8.

9.2.2. Other assets

The TSP has sufficient financial resources to maintain long-term operations, to perform the duties, and to bear the risk of liability towards subscribers and relying parties.

9.2.3. Insurance or warranty coverage for end-entities

The TSP is liable for the damages caused to third parties that it does not have a contractual relationship with in accordance with the general rules of the Civil Code.

9.3 Confidentiality of business information

The TSP manages Service Customers' data according to legal regulations. The TSP has a Data Protection Policy enforced in the entire business organization, and a [Privacy Plan] in relation to the Service, which address the processing of personal data in particular (see also Section 9.4).

When the obligation of storage expires, the TSP irrevocably deletes the confidential information from its systems.

In the Services Agreement, the Service Customers give their consent to the TSP for retaining and processing their personal data, if such personal data is processed by the Service. The Service processes personal data in the Service only in relation to providing certificates for authorized operators of the Subscriber, so that they can perform operational tasks in the Service. Such certificates are not published. End-entity certificates contain no personal data, unless the Service Agreement defines some certificate data to be private.

The TSP uses Service Customers' data solely in connection with the provision of its Service. The TSP stores personal data in a secured manner, for the purpose of providing evidence about the person's identity and the represented organization's organizational identity.

In the course of retaining data, the TSP provides for the integrity, confidentiality, and secure storage of information.

9.3.1. Scope of confidential information

The TSP treats following data confidentially:

- all Service Customer data, with the exception of specified in section 9.3.2
- private keys
- Service Agreements
- transaction related data and log data
- non-public regulations
- all data that if disclosure would have an adverse effect on the security of the service
- all data that if disclosed could lead to third parties learning of the above data

9.3.2. Information not within the scope of confidential information

The TSP does not consider the following information as confidential:

- the data that is indicated in the end-entity certificate (Device certificate), unless the Service Agreement made a statement otherwise,
- the end-entity certificate data required to provide revocation validation services (OCSP, CRL)

The TSP considers all data public that can be obtained from a public source, or to the disclosure of which the Subscriber gave its consent in writing beforehand.

9.3.3. Responsibility to protect confidential information

The TSP takes all measures, including the method defined in the Data Protection Policy, for the secure handling of the confidential information.

The TSP is obligated its employees, subcontractors, affiliated partners to protects all confidential data by signing declaration of confidentiality or by contract.

The Service Provider stores in an electronic format any data that it was provided in an electronic format; any information provided to it in hard copy format can be stored and managed in both hard copy form and/or electronic format.

The TSP processes confidential information according to the provisions of the Swedish Law and the regulations of the European Union.

9.4 Privacy of personal information

The Service processes personal data in the Service only in relation to providing certificates for authorized operators of the Subscriber, so that they can perform operational tasks in the Service. Such certificates are not published. End-entity certificates contain no personal data, unless the Service Agreement defines some certificates data to be private.

The TSP takes care of the protection of personal data and manages it in accordance with the Swedish Law and the regulations of the European Union.

The TSP preserves and deletes data in accordance with the legal requirements and the provision of the CPS, Certificate Policy and other related regulations.

9.4.1. Privacy plan

The TSP has a Data Protection Policy enforced in the entire business organization, and a [Privacy Plan] in relation to the Service, for data processing that contain detailed requirements for the personal data management.

9.4.2. Information treated as private

The Service processes personal data in the Service only in relation to providing certificates for authorized operators of the Subscriber, so that they can perform operational tasks in the Service. Such certificates are not published.

9.4.3. Information not deemed as private

End-entity certificate subject information is not deemed private, unless the Service Agreement defines some contents as private.

9.4.4. Responsibility to protect private information

The TSP protects the personal data security, and prevents data loss, damages, and the incorrect or unauthorized use in the manner laid out in Section 5.5 and by taking into account the IT security requirements of Section 6.5.

Only authorized persons have access to personal information and only to the extent that necessary for their work.

9.4.5. Notice and consent to use private information

The TSP hands over personal data to third parties solely in cases where this is stipulated by a legal regulation or if the person has granted its consent to this in writing.

9.4.6. Disclosure pursuant to judicial or administrative process

In cases defined in legal regulations, the TSP may disclose the stored personal data about a person without notifying the person.

9.4.7. Other information disclosure circumstances

In the interest of uncovering and preventing crimes with the use of the trust services that it provides, as well as for reasons of national security, the TSP shall forward data free of charge to investigating authorities and national security services if the conditions for data requests set forth in separate legislation are met. The fact of provisioning the data is recorded by the TSP; however, the TSP does not inform the Relying Parties of provisioning the data.

9.5 Intellectual property rights

During its business operation, the TSP takes care not to harm any intellectual property rights of a third person.

The Subscriber is the owner of the public and private keys, and the certificates issued by the TSP for the customer-named CA and for the end-users (Devices) affiliated to the Subscriber. The Device named in the subject field of the end-user certificate is the “user” of the end-user certificate and the public key included therein.

The TSP manages the issued certificates, with public key contained in the certificates, and may optionally publish them according to Section 2.1, if agreed so with the Subscriber.

The Subscriber is also the owner of certificate revocation status information related to the customer-named CA and end-user certificates issued by it. The revocation information may be published by the TSP as defined in Section 2.1, as agreed with the Subscriber.

The named Device and the Subscriber are entitled to the use of the identification in the end-user certificate (which identifies the certificate subject, the Device).

The service configuration, operational and audit logs, regulations, contractual conditions, other documents and information prepared by it are owned by the TSP. The Subscriber and other Relying Parties are only entitled to use the documents according to the requirements specified in them; any other use for commercial or other purposes are strictly prohibited.

9.6 Representations and warranties

9.6.1. CA representations and warranties

The TSP’s responsibility

The responsibility of the TSP is defined in the current version of this CPS, the related Certificate Policy, and the Service Agreement with the Service Customer and its attachments.

The TSP assumes responsibility for

- compliance with the procedures described in Certificate Policy it supports;
- the damages caused during the provision of the Service by its subcontractors;
- breach of contract according to the Civil Code of Sweden in relation to the Service Customer which are in contractual relationship with it;
- causing non-contractual damages to third parties according to the Civil Code of Sweden.

The TSP will pay compensation for damages with the limitations specified in its regulations, and the Service Agreements concluded with Service Customers for proven damages that occur in the scope of its responsibility.

The TSP has liability insurance which appropriate for the provision of services.

The TSP is not responsible for:

- the Device' usage of the private key;
- the certificate verification and usage activities of the Relying Parties.

The TSP's obligation

The obligations of the TSP are specified in the current version of this CPS, the related Certificate Policy, and the Service Agreement with the Service Customer and its attachments and other regulations.

The main obligations of the TSP are the followings:

- to establish the legal, regulatory, material, contractual, etc. framework appropriate for the service;
- to provide high standard and secure services in accordance with the applicable regulations;
- to continuously operate and audit organisations associated with the Service;
- to abide by the procedures prescribed in the regulations, and to avoid or eliminate any potentially occurring incorrect operation;
- to ensure the Service to every Service Customer who accepts the terms and conditions specified in the regulations.

TSP Organisation's obligation

The TSP Organization is responsible to operate the Service.

The internal regulations of the TSP regulate how the TSP Organization shall be operated.

The TSP Organization's task is to manage the regulation in which the TSP Organization is assumed responsibility for

- the specification, approval, and maintenance of certificate types that are used;
- preparing the public regulations of the Service and internal (not public) stipulations, their reconciliation with legal regulations and internal (not public) regulations, furthermore carrying out any updates;
- the recording of observations associated with regulations applicable to the services, and to evaluate recommendations.

The TSP Organization is responsible:

- for the authenticity and accuracy of the certificates it issued;
- for the regulations it has issued, and for their conformity and compliance with statutory regulations;
- for the compliance of the key pairs it generated, and for the relationship between the private-public key and the Certificate;
- in general, for the compliance with its obligations.

9.6.2. RA representations and warranties

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

The Registration Authority for the end-entity certificates is operated by the Subscriber. In relation to the registration of end-entity certificate subjects, the Subscriber is responsible for:

- assurance of the uniqueness of Device identities,
- assurance of correctness of the CSR subject attributes,
- assurance of the authorization of CSRs, i.e. no CSRs with unauthorized content can pass authentication.
- the public key sent in the CSR to the certificate service relating to the certificate holder Device indicated in the CSR, and the

9.6.3. Subscriber representations and warranties

The Subscriber's responsibilities

The Subscriber's responsibilities are defined in the Service Agreement and its attachments (including terms and conditions).

The responsibility of the Subscriber is to act – in relation to the Service - in accordance with the contractual terms and regulations of the TSP. The Subscriber is responsible - among others - for:

- the authentication, accuracy and validity of the data provided during registration;
- the verification of the data indicated in the certificates;
- using the private key and Certificate according the regulations;
- the secure management of any secret codes and authentication information;
- the correct and secure usage of the service;
- for the immediate notification and for full information of the TSP in cases of dispute;
- to generally comply with its obligations.

The Subscriber's rights

The rights of the Subscriber are specified in the current version of this CPS, the related Certificate Policy, and the Service Agreement and its attachments and other regulations.

The Subscribers have right to use the provision of services as they are specified in the above-mentioned documents.

Subscribers are entitled to specify which Subjects should be allowed to receive certificates.

The Subscriber has the right to apply for Certificates in accordance with the CPS.

The Subscribers' obligations

The Subscriber's obligations are the followings:

- read carefully this CPS before using the Service;
- completely provide the data required by the TSP necessary for using the Service, and to provide truthful data;
- use the service solely for the purposes allowed or not proscribed by legal regulations, according to the cited regulations and documents;
- ensure that no unauthorized individuals have access to data and tools (passwords, secret codes) necessary for using the Service;

- notify the TSP in writing and without delay in case a legal dispute starts in connection with any of the Certificates associated with the service;
- cooperate with the TSP;
- acknowledge that the TSP issues Certificates in the manner specified in the CPS.

9.6.4. Relying party representations and warranties

The Relying Parties decide based on their discretion and/or their policies about the way of accepting and using the certificates. During the verification of the validity for keeping the security level guaranteed by the TSP, it is necessary for the Relying Party to act with caution, so it is particularly recommended to:

- comply with the requirements, regulations defined in the Certificate Policy and the corresponding CPS;
- use reliable IT environment and applications;
- take into consideration every restriction in relation to the certificate usage which is included in the Certificate, in the Certificate Policy and the CPS;
- take any other precautions prescribed in the agreement or elsewhere.

9.6.5. Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

The TSP excludes its liability if:

- the Devices do not follow the requirements related to the private key;
- the damage comes from a vulnerability or error of the accepted cryptographic algorithms;
- it is unable to provide information or fulfil communication obligations due to the problems of the Internet, or part of it
- the Relying Party did not proceed in accordance with the current version of this CPS, related standards and recommendations, or other relevant legislation.
- the regulations issued by the Relying Parties or others do not meet the requirements of the present the CPS.

9.8 Limitations of liability

The TSP is not responsible for damages that arise from the Relying Party failing to proceed as recommended according to effective legal regulations and the TSP's regulations in the course of validating and using certificates.

The TSP will reject claims for warranty, guarantee, or compensation against the TSP for its services if the event on which it is based can be traced back to the Service Customer's omission, failure to meet an obligation or responsibility, or an external, unforeseeable event.

The TSP is only liable for contractual and non-contractual damages connected to its services in relation to third parties that occur solely on account of the chargeable violation of its obligations.

The TSP is not liable for damages that result from the operational malfunction of the internet or one of its components because of an external incident beyond its control.

The TSP assumes liability solely for providing the services in accordance with the provisions of this CPS, as well as the documents to which reference is cited herein (Certification Policies, standards, recommendations), moreover with its proprietary internal regulations.

The TSP logs its activities, protects the intactness and authenticity of log entries, moreover retains (archives) log data over the long term in the interest of allowing for the establishing, documenting, and evidencing of financial accountability, its proprietary liability related to damage it causes, as well as that of damage compensation due to it for damage it suffers.

The Service Provider does not assume liability for using test certificates for other purposes than testing.

Financial liability

The TSP has liability insurance in order to ensure reliability. The TSP limits its liability insurance related to its services.

If the valid claim of several entitled parties related to an insurance event exceeds the amount defined for an insurance event in the liability insurance for the damages, then the compensation of the claims takes place in a relative ratio to the amount determined in the liability contract.

9.9 Indemnities

9.9.1. Indemnification by the Trust Service Provider

The TSP has liability insurance to cover its indemnification obligations. The rules of the indemnities of the TSP are specified in this regulation and the Service Agreement concluded with the Service Customer.

The Service Agreement is obligated to indemnify the TSP for any proven losses or damages that are incurred by the TSP as a result of the Service Agreement to meet obligations or adhere to recommendations either intentionally or through negligence.

9.9.2. Indemnification by subscriber

The Subscriber is liable for damages to the TSP for the loss or damage caused by non-compliance with their obligations and the relevant recommendations.

9.9.3. Indemnification by relying parties

See Section 9.8.

9.10 Term and termination

9.10.1. Term

The term of this CPS starts on the day this version becomes effective as indicated on the cover (effective date).

The personal scope of this CPS extends to the TSP’s trusted employees and other contracted personnel, the TSP’s partners, to Service Customers, and to all Relying Parties.

The scope of this CPS includes the provision and usage of services as defined in Section 1.1 of this document.

9.10.2. Termination

The CPS remains valid without a specified time limit until the service is terminated, the CPS is revoked, or until a new version enters effect.

9.10.3. Effect of termination and survival

In case of withdrawal, the TSP publishes on its website the detailed rules for revocation and the rights and obligations that remain in effect thereafter. The TSP undertakes to guarantee that the regulations pertaining to the protection of confidential information as defined by relevant legislation remains in effect even if the CPS is revoked.

9.11 Individual notices and communications with participants

The contact information of the Service Support can be found in Section 1.1. The Customer Service primarily communicates with the Service Customer via the Support Portal.

Service Customers may make their legal declarations to the TSP solely in writing and in executed form.

9.12 Amendments

The TSP reserves the right to change the CPS in a controlled way in case of the change of normative rules, security requirements, market conditions or other circumstances.

9.12.1. Procedure for amendment

The TSP only discloses those of its procedures in its public domain regulations whose knowledge does not jeopardize the security of the services. The TSP has internal security and other regulations, as well as operation-level stipulations which it treats in confidence.

A team responsible for maintaining regulations and documentation operates within the TSP Organization. This team collects change requests, carries out modifications, and meets any internal and external information provision related obligations.

All documents go under internal review before being published. The TSP only issues new regulation at the least frequent intervals as possible.

The TSP reviews the CPS annually or in case of exceptional request for change with priority and performs the necessary changes.

The TSP will notify Service Customers about a change 14 days prior to the planned effect date and accept remarks connected to new regulations at the email address specified in sec. 1.1.

The TSP will close and publish the version of the regulation as amended with remarks on the 7th day prior to its becoming effective unless it is not feasible due to extreme circumstances.

9.12.2. Notification mechanism and period

The TSP notifies the Relying Parties of new document version issuances as described in Section 9.12.1.

9.12.3. Circumstances under which OID must be changed

The TSP issues a new version number in case of even the smallest change to the CPS. Any change to the document will result in an OID change, namely two documents – entered into force – with different content cannot have the same OID.

9.13 Dispute resolution procedures

The TSP aims for the peaceful and negotiated settlement of the disputes arising from its operation.

The TSP and the Service Customer mutually agree that in the case of any disputed issue or complaint arising whatsoever, they will attempt amicable consultation through negotiation before taking the dispute to legal channels. The initiating party will be obligated to notify every other affected party promptly and to inform them fully concerning all of the case's implications.

If any disputes or complaints occur, Service Customers are obligated and Relying Parties and other third parties are recommended to notify the Service Provider immediately before taking legal steps and to inform the Service Provider of all aspects of the case.

The TSP will examine complaints within 30 calendar days of their receipt and will inform the complainant by email of the results of the inspection unless agreed on otherwise by the parties.

After examining the complaint, the TSP will fix (if applicable) or take any corrective actions on the error or act within a reasonable time and will inform the reporting party about this activity in writing.

If the reporting Service Customer does not accept the response, it can initiate negotiations with the Service Provider.

If the dispute cannot be settled within 30 business day calculated as of the compliant being submitted or the refusal of the response, the Parties may take the case to court. In this case, the Parties subject themselves to the sole jurisdiction of Swedish courts.

9.14 Governing law

The TSP at all times operates in accordance with the Swedish legislation in force. The Swedish law is the governing law of the TSP contracts, regulations and their execution, and they are construed by the Swedish law.

9.15 Compliance with applicable law

The TSP conducts its activity in line with applicable law and standards.

9.16 Miscellaneous provisions

9.16.1. Entire agreement

No stipulation.

9.16.2. Assignment

The providers included in the provision of services may only assign their rights and delegate their obligations to third parties if granted the TSP's preliminary written consent.

9.16.3. Severability

If any of the provisions of the current version of this CPS become invalid for any reason, the remaining provisions will remain in effect unchanged

9.16.4. Enforcement (attorneys' fees and waiver of rights)

The TSP is entitled to claim payment for damages and attorney fees for reimbursement of the damages, losses, expenses caused by its partners. If in a particular case the TSP does not exercise its claim for damages that does not mean that in similar cases in the future or in case of violation of other provisions of the current version of this CPS, it would relinquish the enforcement of claims for damages.

9.16.5. Force Majeure

The TSP is not responsible for the defective or delayed performance of the requirements set out in the Certificate Policy and the CPS if the reason for failure or delay was a condition that is outside the control of the TSP.

9.17 Other provisions

No stipulation.