Gjaldstovan Certificate Policy - NCP+

Version 1.0 - 18.04.2018

Change Log

Version	Date:	Author:	Change:
1.0	18-04-2018	Djóni á Boðanesi	First version on Confluence ready for BSI review document review ETSI 319 411-1 in March 2020
1.0	01-05-2020	Jósup Henriksen	Approved by Gjaldstovan TSP Management Board (No changes to the 1.0 from from 18.04.2018)

Gjaldstovan
Kvíggjartún 1,
FO-160 Argir
Faroe Islands
EAN 5797100000010

Or:

gjaldstovan@gjaldstovan.fo

Table of contents

1 Introduction

1.1 Scope

Faroe Islands Citizen PKI that accommodates citizens and non-citizens within the Faroe Islands.

The possible subscriber entities this CP applies to are:

- Natural persons, aged 15 or above, having a faroese "p-tal".

This document specifies the policy and security requirements for Trust Service Providers (TSP) issuing public key certificates under a Extended Normalized Certificate Policy (NCP+), in compliance with ETSI EN 319411-1. The policy and security requirements are defined in terms of requirements for the issuance, maintenance and life-cycle management of certificates.

This policy applies to issuance of Samleikin issued within the national Faroese eID programme Talgildur Samleiki.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

The following referenced documents are necessary for the application of the document:

- ISO/IEC 15408 (parts 1 to 3): "Information technology – Security techniques – Evaluation criteria for IT security".
- ISO/IEC 19790:2012: "Information technology – Security techniques – Security requirements for cryptographic modules".
- ISO/IEC 9594-8/Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".
- IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".
- IETF RFC 6960: "X.509 Internet Public Key - Infrastructure Online Certificate Status Protocol - OCSP".
- ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers", version 2.2.1.
- ETSI EN 319 411-1: "Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements", version 1.2.2.
- ETSI EN 319 412-2: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons", version 2.1.1.
- ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons", version 1.1.1.
- ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites", version 1.2.1.
- FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules".

3 Definitions, abbreviations and notation

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI EN 319 401 and the following apply:

Auditor: person who assesses conformity to requirements as specified in given requirements documents

Certificate: public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it

Certificate Policy (CP): named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

Certificate Revocation List (CRL): signed list indicating a set of certificates that are no longer considered valid by the certificate issuer

Certification Authority (CA): authority trusted by one or more users to create and assign certificates

Certification Authority Revocation List (CARL): revocation list containing a list of CA-certificates issued to certification authorities that are no longer considered valid by the certificate issuer

Certification Practice Statement (CPS): statement of the practices which a Certification Authority employs in issuing managing, revoking, and renewing or re-keying certificates

Coordinated Universal Time (UTC): As indicated in ETSI EN 319 401.

Cross Certificate: certificate that is used to establish a trust relationship between two certification authorities digital signature: data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

Domain Validation Certificate (DVC): certificate which has no validated organizational identity information for the subject, only identifying the subject by its domain name

EV certificate: See Extended Validation certificate.

Extended Validation Certificate (EVC): As indicated in the EVCG.

High security zone: specific physical location of the security zone (see ETSI EN 319 401, clause 7.8) where the Root CA key is held

Organizational Validation Certificate(OVC): certificate that includes validated organizational identity information for the subject

Publicly-Trusted Certificate (PTC): certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software

Registration Authority (RA): entity that is responsible for identification and authentication of subjects of certificates

Registration officer: person responsible for verifying information that is necessary for certificate issuance and approval of certification requests

Revocation officer: person responsible for operating certificate status changes

Root CA: certification authority which is at the highest level within TSP's domain and which is used to sign subordinate CA(s)

Secure cryptographic device: device which holds the user's private key, protects this key against compromise and performs signing or decryption functions on behalf of the user

Secure zone: area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of the systems used by the TSP

Subject: entity identified in a certificate as the holder of the private key associated with the public key given in the certificate

subordinate CA: certification authority whose Certificate is signed by the Root CA, or another Subordinate CA

Trust anchor: entity that is trusted by a relying party and used for validating certificates in certification paths

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

BRG - Baseline Requirements Guidelines
CA - Certification Authority
CAB - CA/Browser
CAB Forum - CA/Browser Forum
CARL - Certification Authority Revocation List
CP - Certificate Policy
CPS - Certification Practice Statement
CRL - Certificate Revocation List
CSP - Certification Service Provider. The more general term Trust Service Provider is used in preference to CSP in the present document except in relation to external references.
DVC - Domain Validation Certificate
DVCP - Domain Validation Certificate Policy
EAL - Evaluation Assurance Level
EV - Extended Validation
EVC - Extended Validation Certificate
EVCG - Extended Validation Certificate Guidelines
EVCP - Extended Validation Certificate Policy
LCP - Lightweight Certificate Policy
NCP - Normalized Certificate Policy
NCP+ - Extended Normalized Certificate Policy
OCSP - Online Certificate Status Protocol
OID - Object IDentifier
OVC - Organizational Validation Certificate
OVCP - Organizational Validation Certificate Policy
PDS - PKI Disclosure Statement
PIN - Personal Identification Number
PKI - Public Key Infrastructure
PTC - Publicly-Trusted Certificate. Within the context of the present document PTC is used synonymously with EVC, DVC and OVC as per CAB Forum documents.
RA - Registration Authority
TLS - Transport Layer Security
TSP - Trust Service Provider
UTC - Coordinated Universal Time

4 General concepts

4.1 General policy requirements concepts

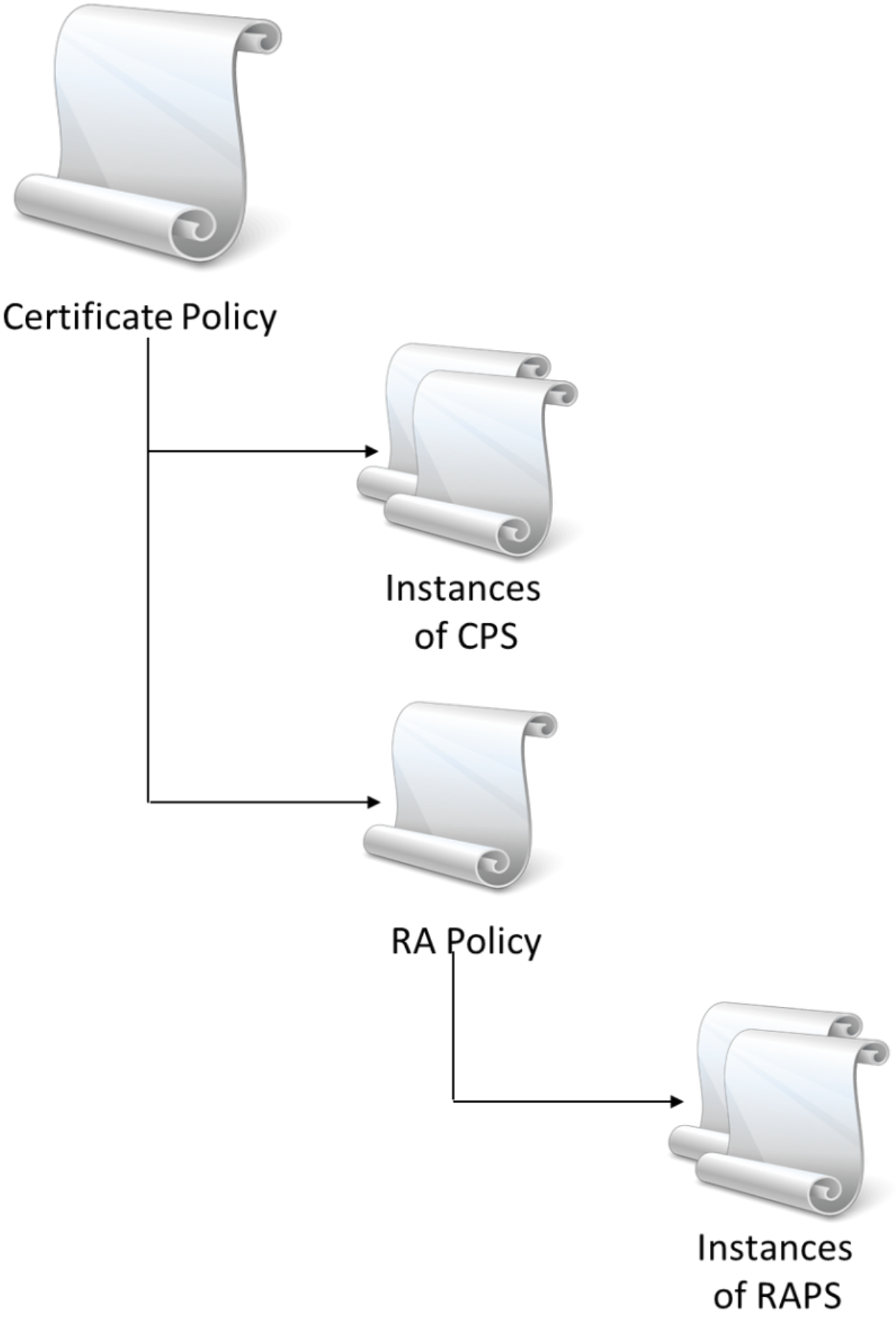
In general, a public-key certificate binds a public key held by an entity to a set of information that identifies the entity associated with use of the corresponding private key. In most cases involving identity certificates, this entity is known as the "subject" or "subscriber" of the certificate.

Two exceptions, however, include devices (in which the subscriber is usually the individual or organization controlling the device) and anonymous certificates (in which the identity of the individual or organization is not available from the certificate itself). Other types of certificates bind public keys to attributes of an entity other than the entity's identity, such as a title. A certificate is used by a "certificate user" or "relying party" that needs to use, and rely upon the accuracy of, the binding between the subject public key distributed via that certificate and the identity and/or other attributes of the subject contained in that certificate.

A relying party is frequently an entity that verifies a digital signature from a certificate subject where the digital signature is associated with an email, web form, electronic document, or other data. Other examples of relying parties can include a sender of encrypted email to the subscriber, a user of a web browser relying on a server certificate during a TLS session and an entity operating a server that controls access to online information using client certificates as an access control mechanism. In summary, a relying party is an entity that uses a public key in a certificate (for signature verification and/or encryption). The degree to which a relying party can trust the binding embodied in a certificate depends on several factors. These factors can include:

- The practices followed by the certification authority (CA) in authenticating the subject
- The CAs operating policy, procedures and security controls
- The scope of the subscriber responsibilities
- The stated responsibilities and liability terms and conditions of the CA

An overview of the policy structure is shown in the diagram below. The Gjaldstovan TSP Management Board owns and maintains this CP.


Certificate Policy
Instances of CPS
RA Policy
Instances of RAPS

4.2 Certificate policy and certification practice statement

When a certification authority issues a certificate, it is providing a statement to a certificate user (i.e., a relying party) that a particular public key is bound to the identity and/or other attributes of a particular entity (the certificate subject, which is usually also the subscriber). The extent to which the relying party should rely on that statement by the CA, however, needs to be assessed by the relying party or entity controlling or coordinating the way relying parties or relying party applications use certificates. Different certificates are issued following different practices and procedures, and may be suitable for different applications and/or purposes.

The X.509 standard defines a CP as "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements". An X.509 Version 3 certificate may identify a specific applicable CP, which may be used by a relying party to decide whether or not to trust a certificate, associated public key, or any digital signatures verified using the public key for a particular purpose.

CPs typically fall into two major categories. First, some CPs "indicate the applicability of a certificate to a particular community". These CPs set forth requirements for certificate usage and requirements on members of a community. For instance, a CP may focus on the needs of a geographical community, such as the ETSI policy requirements for CAs issuing qualified certificates. The second category of typical CPs "indicate the applicability of a certificate to a class of application with common security requirements." These CPs identify a set of applications or uses for certificates and state that these applications or uses require a certain level of security. They then set forth PKI requirements that are appropriate for these applications or uses. A CP within this category often makes sets requirements appropriate for a certain "level of assurance" provided by certificates, relative to certificates issued pursuant to related CPs. These levels of assurance may correspond to "classes" or "types" of certificates.

This CP is an expression of the latter category, specifying requirements for different types of certificates issued under a common CP.

The CP must be represented in a certificate by a unique number called an "Object Identifier" (OID). That OID, or at least an "arc", can be registered. An "arc" is the beginning of the numerical sequence of an OID and is assigned to a particular organization. The registration process follows the procedures specified in ISO/IEC and ITU standards. The party that registers the OID or arc also can publish the text of the CP, for examination by relying parties. Any one certificate will typically declare a single CP. Such declaration appears in the Certificate Policies extension of a X.509 Version 3 certificate. When a CA places multiple CPs within a certificate's Certificate Policies extension, the CA is asserting that the certificate is appropriate for use in accordance with any of the listed CPs.

CPs also constitute a basis for an audit, accreditation, or another assessment of a CA. Each CA can be assessed against one or more certificate policies or CPSs that it is recognized as implementing. When one CA issues a CA-certificate for another CA, the issuing CA must assess the set of certificate policies for which it trusts the subject CA (such assessment may be based upon an assessment with respect to the certificate policies involved). The assessed set of certificate policies is then indicated by the issuing CA in the CA-certificate. The X.509 certification path processing logic employs these CP indications in its well-defined trust model.

The following extension fields in an X.509 certificate are used to support CPs:

- Certificate Policies extension;
- Policy Mappings extension; and
- Policy Constraints extension.

4.2.1 Level of specificity

A CP is a higher level document than a CPS; it can apply to a community to which several CAs belong that abide by the common set of rules specified in that CP. A CPS defines how one specific CA meets the technical, organizational and procedural requirements identified in a CP.

Even lower-level documents can be appropriate for a CA detailing the specific procedures necessary to complete the practices identified in the CPS. This lower-level documentation is generally regarded as internal operational procedure documents, which can define specific tasks and responsibilities within an organization. While this lower-level documentation can be used in the daily operation of the CA and reviewed by those doing a process review, due to its internal nature this level of documentation is considered private and proprietary and therefore beyond the scope of the present document. For example, the policy can require secure management of the private key(s), the practices can describe the dual-control, secure storage practices, while the operational procedures can describe the detailed procedures with locations, access lists and access procedures.

4.2.2 Approach

The approach of a CP is significantly different from a CPS. A CP is defined independently of the specific details of the specific operating environment of a CA, whereas a CPS is tailored to the organizational structure, operating procedures, facilities, and computing environment of a CA.

4.2.3 Certificate Policy

As described in IETF RFC 3647, clause 3.3, certificates include a CP identifier which can be used by relying parties in determining the certificates suitability and trustworthiness for a particular application.

This CP is the Faroese Extended Normalized Certificate Policy (NCP+), in compliance with ETSI EN 319 411-1 which meets general recognized best practice for TSPs issuing Samleikin certificates.

4.3 Certification services

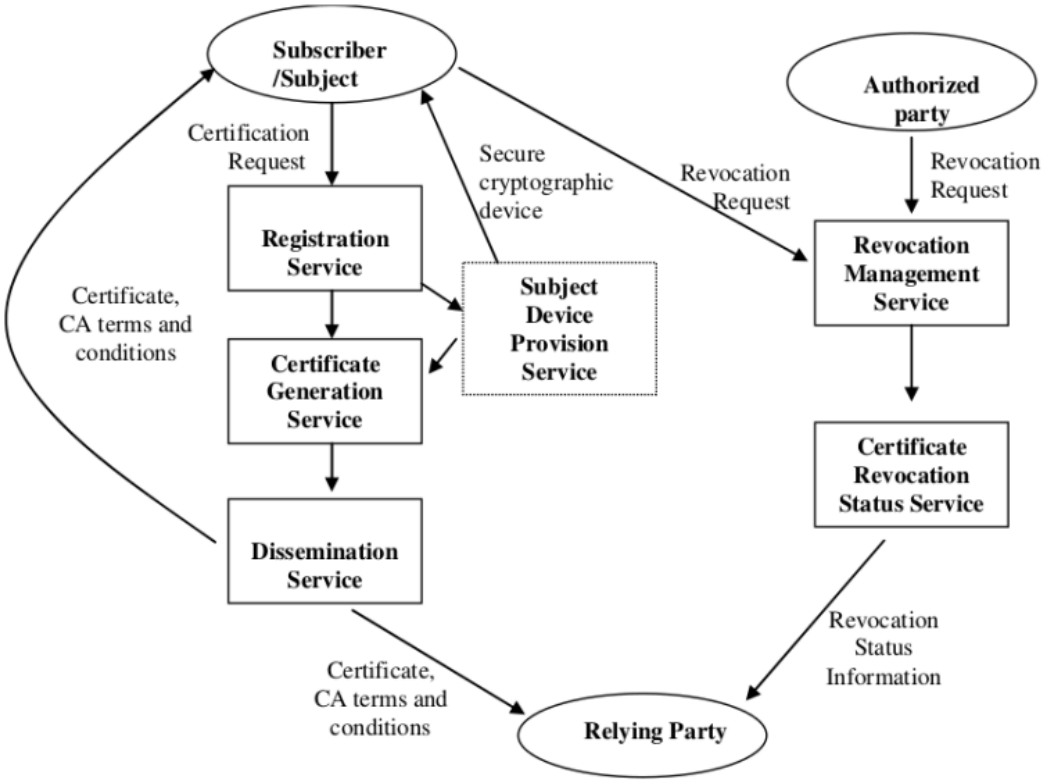
The certification services are broken down in the present document into the following component services for the purposes of classifying requirements:

- Registration service: verifies the identity and if applicable, any specific attributes of a subject. The results of this service are passed to the certificate generation service.
- Certificate generation service: creates and signs certificates based on the identity and other attributes verified by the registration service. This can include key generation.

- Dissemination service: disseminates certificates to subjects, and if the subject consents, makes them available to relying parties. This service also makes available the TSP's terms and conditions, and any published policy and practice information, to subscribers and relying parties.
- Revocation management service: processes requests and reports relating to revocation to determine the necessary action to be taken. The results of this service are distributed through the revocation status service.
- Revocation status service: provides certificate revocation status information to relying parties.
- Subject device provision service (optional): prepares, and provides or makes available secure cryptographic devices, or other secure devices, to subjects.

This subdivision of services is only for the purposes of clarification of policy requirements and places no restrictions on any subdivision of an implementation of the CA services.

The following image declares the relations between certification services:



5 General provisions on Certification Practice Statement and Certificate Policies

5.1 General requirements

This policy is structured broadly in line with IETF RFC 3647. This policy includes the provision of services for registration, certificate generation, dissemination, revocation management and revocation status. Where requirements relate to a specific service area of the TSP then it is listed under one of these subheadings. Where no service area is listed, or "General" is indicated, a requirement is relevant to the general operation of the TSP.

The requirements are indicated in terms of the security objectives followed by more specific requirements for controls to meet those objectives where considered necessary to provide the necessary confidence that those objectives will be met.

5.2 Certification Practice Statement requirements

The general requirements specified in ETSI EN 319 401, clause 6.1 shall apply. In addition the following particular requirements apply:

- The TSP CPS should be structured in accordance with IETF RFC 3647.
- The CPS shall include the complete CA hierarchy, including root and subordinate CA's.
- The CPS shall include the signature algorithms and parameters employed.
- The TSP shall publicly disclose its CPS through an online means that is available on a 24x7 basis.
- The TSPs CPS shall specify the practice regarding the use of CA keys for signing certificates, CRLs and OCSP-services.

5.3 Certificate Policy name and identification

As described in IETF RFC 3647, clause 3.3, certificates include a CP identifier which can be used by relying parties in determining the certificates suitability and trustworthiness for a particular application. The identifier for this certificate policy is:

- NCP+: Normalized Certificate Policy requiring a secure cryptographic device

itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus (2)

5.4 PKI participants

5.4.1 Certification Authority

The authority trusted by the users of the certification services (i.e. subscribers as well as relying parties) to create and assign certificates is called the CA. The CA has overall responsibility for the provision of the certification services identified in clause 4.4. The CA is identified in the certificate as the issuer and its private key is used to sign certificates. The CA may make use of other parties to provide parts of the certification service. However, the CA always maintains overall responsibility and ensures that the policy requirements identified in the present document are met.

A CA is a type of Trust Service Provider (TSP), as defined in the Regulation (EU) No 910/2014, which issues public key certificates.

A TSP may include a hierarchy of CAs. Where a TSP includes a hierarchy of subordinate CAs up to a root CA the TSP is responsible for ensuring the subordinate-CAs comply with the applicable policy requirements. If the TSPs Trust Anchor is signed by a Root CA outside the scope of the TSP policies then the Root CA requirements apply to the TSP's Trust Anchor.

5.4.2 Subscriber and subject

A subject can be:

- natural persons, aged 15 or above, having a faroese "p-tal".

When a subscriber is the subject it will be held directly responsible if its obligations are not correctly fulfilled.

When the subscriber is acting on behalf of one or more distinct subjects to whom it is linked, responsibilities of the subscriber and of the subject are addressed in clause 6.3.4 item e.

The link between the subscriber and the subject is one of the following:

- To request a certificate for a natural person the subscriber is:

i) the natural person itself; or
ii) a natural person mandated to represent the subject

5.4.3 Others

No stipulations.

5.5 Certificate usage

Certificates issued under this policy is only intended for use for authentication of natural persons within the national Faroese eID programme Talgildur Samleiki, including relying parties to Talgildur Samleiki.

Certificates shall be used only to the extent the use is consistent with applicable law. CA Certificates may not be used for any functions except CA functions. In addition, end-user
Subscriber Certificates shall not be used as CA Certificates.

6 Trust Service Providers practice

6.1 Publication and repository responsibilities

The TSP shall make certificates available to subscribers, subjects and relying parties. In particular:

Dissemination

a) Upon generation, the complete and accurate certificate shall be available to the subscriber or subject for whom the certificate is being issued.

b) Certificates shall be available for retrieval in only those cases for which the subject's consent has been obtained. If the subject is a device or system, the consent of the natural or legal person responsible for the operating of the device or system needs to be obtained, instead of the subject.

c) The TSP shall make available to relying parties the terms and conditions regarding the use of the certificate (see clause 6.9.4).

d) The applicable terms and conditions shall be readily identifiable for a given certificate.

e) The information identified in b) and c) above shall be available 24 hours per day, 7 days per week. 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 a maximum period of time as denoted in the CPS.

f) The information identified in c) above should be publicly and internationally available.

6.2 Identification and authentication

6.2.1 Naming

Requirements for naming in certificates are as specified in Recommendation ITU-T X.509 or IETF RFC 5280 and the appropriate part of ETSI EN 319 412. See clause 6.6.1 of the CP.

6.2.2 Initial identity validation

The TSP shall verify the identity of the subscriber and subject and shall check that certificate requests are accurate, authorized and complete according to the collected evidence or attestation of identity.

When registering, a subject is identified as a person with specific attributes.

In particular:

Registration

a) The TSP shall collect either direct evidence or an attestation from an appropriate and authorized source, of the identity (e.g. name) and if applicable, any specific attributes of subjects to whom a certificate is issued. Submitted evidence may be in the form of either paper or electronic documentation (in both cases the RA shall validate their authenticity). Verification of the subject's identity shall be at time of registration by appropriate means.

b) If the subject is a natural person (i.e. physical person as opposed to legal person) evidence of the subject's identity (e.g. name) shall be checked against this natural person either directly by physical presence of the person (the subject shall be witnessed in person unless a duly mandated subscriber represents the subject), or shall have been checked indirectly using means which provides equivalent assurance to physical presence.

c) If the subject is a natural person (i.e. physical personal as opposed to legal person), evidence shall be provided of:

1) full name (including surname and given names consistent with the national identification practices); and

2) date and place of birth, reference to a nationally recognized identity document, or other attributes which can be used to, as far as possible, distinguish the person from others with the same name. The place of birth should be given in accordance to national or other applicable conventions for registering births.

d) If the subject is a natural person who is identified in association with a legal person (e.g. the subscriber), evidence of the identity, in particular the ones listed in e), shall be checked against a natural person either directly by physical presence of the person (the subject shall be witnessed in person unless a duly mandated subscriber represents the subject), or shall have been checked indirectly using means which provides equivalent assurance to physical presence.

e) The TSP shall record all the information necessary to verify the subject's identity and if applicable, any specific attributes of the subject, including any reference number on the documentation used for verification, and any limitations on its validity.

f) If an entity other than the subject is subscribing to the TSP services (i.e. the subscriber and subject are separate entities - see clause 5.4.2) then evidence shall be provided that the subscriber is authorized to act for the subject as identified (e.g. is authorized for all members of the identified organization), in particular:

1) full name (including surname and given names consistent with the national or other applicable identification practices) of the subscriber;

2) when the subscriber represents a natural person (not associated with a legal person) an agreement to this representation; or

3) when the subscriber represents a legal person (either for requesting a certificate for that legal person or to request a certificate for a natural person identified in association with the legal person), an agreement that the subscriber is allowed to represent the legal person and is entitled to request certificates for that legal person or its members are required. In particular, if the subscriber is not a natural person, it shall be represented by a natural person whose authorization to represent the subscriber shall be proved.

g) The subscriber shall provide a physical address, or other attributes, which describe how the subscriber shall be contacted.

h) The TSP shall provide evidence of how they meet applicable data protection legislation within their registration process.

i) The TSP's verification policy shall only require the capture of evidence of identity sufficient to satisfy the requirements of the intended use of the certificate.

j) To avoid any conflicts of interests, the subscriber and TSP organization entity shall be separate entities. The only exception is the organization running all or part of the RA tasks subscribing a certificate for itself or persons identified in association with it (as a subject), and for which the exception is stated in the TSP's policies.

6.2.3 Identification and authentication for Re-key requests

All forms of certificate re-keying is forbidden under this CP.

6.2.4 Identification and authentication for revocation requests

Existing evidences can be re-used to validate the identity depending on applicable legislation and whether the evidence remains valid given the time elapsed. The TSP shall revoke certificates within 12 hours of receiving a validated certificate revocation request.

In particular:

Revocation management

a) The TSP shall document as part of its CPS (see clause 5.2) the procedures for revocation of end user and CA certificates including:

i) Who can submit requests for revocation or reports of events which may indicate the need to revoke a certificate.

ii) How they can be submitted.

iii) Any requirements for subsequent confirmation of requests for revocation or reports of events which may indicate the need to revoke a certificate.

iv) Whether and for what reasons certificates can be suspended or revoked.

v) The mechanism used for distributing revocation status information.

vi) The maximum delay between receipt of a revocation or suspension request and the decision to change its status information being available to all relying parties. This shall be at most 24 hours.

vii) The maximum delay between the confirmation of the revocation of a certificate, or its suspension, to become effective and the actual change of the status information of this certificate being made available to relying parties. This shall be at most 60 minutes. With regard to vii), if the revocation request requires revocation in advance (e.g. subject's planned cessation from his/her duties at a certain date), then the scheduled date may be considered as the confirmation time according to the TSP policies. With regard to vi) and vii), a TSP may give faster process times for certain revocation reasons.

viii) The time used for the provision of revocation services shall be synchronized with UTC at least once every 24 hours.

b) Requests for revocation and reports of events relating to revocation shall be processed on receipt. Including compromise of subject's private key, death of the subject, unexpected termination of a subscriber's or subject's agreement or business functions, violation of contractual obligations.

c) Requests for revocation and reports of events relating to revocation shall be authenticated, checked to be from an authorized source. Such reports and requests will be confirmed as required under the TSP's practices.

6.3 Certificate Life-Cycle operational requirements

6.3.1 Certificate application

In particular:

Registration

a) if the subject's key pair is not generated by the CA, the certificate request process shall check that the subject has possession or control of the private key associated with the public key presented for certification.

6.3.2 Certificate application processing

Application for certificates shall be from a trusted registration service.

In particular:

a) when external registration service providers are used registration data shall be exchanged securely and only with recognized registration service providers, whose identity is authenticated.

6.3.3 Certificate issuance

The CA shall issue certificates securely to maintain their authenticity. The requirements for the use of the certificate profiles should be linked to a CP.

In particular:

Certificate generation

a) See clause 6.6.1 for certificate profiles.

b) The CA shall take measures against forgery of certificates, and in cases where the CA generates the subjects' key pair, guarantee confidentiality during the process of generating such data.

c) The procedure of issuing the certificate shall be securely linked to the associated registration, certificate renewal or rekey, including the provision of any subject-generated public key.

d) If the CA generated the subject's key pair:

i) the procedure of issuing the certificate shall be securely linked to the generation of the key pair by the CA; and

ii) the secure cryptographic device containing the subject's private key shall be securely delivered to the registered subject or, in the case of the TSP managing the key on behalf of the subject, the TSP shall ensure that the subject has sole control over its signing key.

e) Over the life time of the CA a distinguished name which has been used in a certificate by it shall never be re-assigned to another entity.

f) Use of the policy identifier:

- The CP identifier shall be as specified in clause 5.3

6.3.4 Certificate acceptance

The terms and conditions shall indicate what is deemed to constitute acceptance of the certificate. See clause 6.9.4.

In particular:

Registration

a) Before entering into a contractual relationship with a subscriber, the TSP shall inform the subscriber of the terms and conditions regarding use of the certificate as given in clause 6.9.4.

b) If the subject is a person and not the same as the subscriber, the subject shall be informed of his/her obligations.

c)

i) The TSP shall communicate the terms and conditions through a durable (i.e. with integrity over time) means of communication, and in a human readable form.

ii) The terms and conditions may be transmitted electronically.

iii) The terms and conditions may use the model PKI disclosure statement given in annex A.

d) The TSP shall record the signed agreement with the subscriber (see clause 6.4.5 c)).

e) Where the subscriber and subject are two separate entities and the subject is a natural person, the signed agreement shall be in 2 parts:

1) The first part shall be signed by the subscriber and shall include:

i) agreement to the subscriber's obligations (see clause 6.9.4) and the general terms and conditions as identified in clause 6.1;

ii) if required by the TSP, agreement by the subscriber to use a secure cryptographic device;

iii) consent to the keeping of a record by the TSP of information used in registration, subject device provision, including whether this is to the subscriber or to the subject where they differ, and any subsequent revocation (see clauses 6.4.5 and 6.4.6), the identity and any specific attributes placedin the certificate, and the passing of this information to third parties under the same conditions as required by this policy in the case of the TSP terminating its services;

iv) whether, and under what conditions, the subscriber requires and the subject consents to the publication of the certificate;

v) confirmation that the information held in the certificate is correct;

vi) obligations applicable to subjects (see clause 6.9.4);

2) The second part shall be signed by the subject and shall include:

i) the agreement by the subject;

ii) obligations applicable to subjects (see clause 6.9.4);

iii) if required by the TSP, agreement by the subject to use a secure cryptographic device;

iv) consent to the keeping of a record by the TSP of information used in registration, subject device provision, including whether this is to the subscriber or to the subject where they differ, and any subsequent revocation (see clauses 6.4.5 and 6.4.6), the identity and any specific attributes placed in the certificate, and the passing of this information to third parties under the same conditions as required by this policy in the case of the TSP terminating its services.

f) Where the subject and subscriber are the same entity the agreement shall be in one or two parts and shall include the part 1 and part 2 items listed abov e.

g) This agreement may be in electronic form.

h) The records identified above shall be retained for the period of time as indicated to the subscriber (see item c) above).

6.3.5 Key pair and certificate usage

The subscriber's obligations (see clause 6.3.4) shall include items a) to j) below.
If the subject and subscriber are separate entities and the subject is a natural person, the subject's obligations shall include at least items b) c) e) f) h) i) and j) (as listed below):

a) accurate and complete information is submitted to the TSP in accordance with the requirements of this policy, particularly with regards to registration;

b) the key pair is only used in accordance with any limitations notified to the subscriber and the subject if the subject is a natural or legal person (see clause 6.9.4);

c) unauthorized use of the subject's private key is avoided;

d) if the subscriber or subject generates the subject's keys:

i) subject keys must be generated using an algorithm as specified in ETSI TS 119 312 for the uses of the certified key as identified in the CP; and

ii) a key length and algorithm should be as specified in ETSI TS 119 312 for the uses of the certified key as identified in the CP during the validity time of the certificate. Each CA issuing certificates under this CP shall in its CPS describe the used algorithms in use for all certificates that are issued, only allowing algorithms within the current version of ETSI TS 119 312.

e) if the subscriber or subject generates the subject's keys and the private key is for creating digital signatures or seals the subject's private key can be maintained under the subject's sole control;

f) only use the subject's private key(s) for cryptographic functions within the secure cryptographic device;

g) if the subject's keys are generated under control of the subscriber or subject, generate the subject's keys within the secure cryptographic device;

h) notify the TSP without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:

i) the subject's private key has been lost, stolen, potentially compromised;

ii) control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons; or

iii) inaccuracy or changes to the certificate content, as notified to the subscriber or to the subject.

i) following compromise, the use of the subject's private key is immediately and permanently discontinued

j) in the case of being informed that the subject's certificate has been revoked, or the issuing CA has been compromised, ensure that the private key is not used by the subject.

The notice to relying parties (see clause 6.9.4) shall recommend the relying party to:

k) verify the validity, suspension or revocation of the certificate using current revocation status information as indicated to the relying party (see clause 6.9.4);

l) take account of any limitations on the usage of the certificate indicated to the relying party either in the certificate or the terms and conditions supplied as required in clause 6.9.4; and

m) take any other precautions prescribed in agreements or elsewhere

6.3.6 Certificate renewal

Requests for certificates issued to a subject who has previously been registered with the same TSP shall be complete, accurate and authorized.

In particular:

Registration

a)

i) The TSP shall check the existence and validity of the certificate to be renewed and that the information used to verify the identity and attributes of the subject are still valid.

b) If any of the TSP terms and conditions has changed, these shall be communicated to the subscriber and agreed to in accordance with clause 6.3.4, items a), b), c) and d).

c) Requirements h) to l) of clause 6.2.2 shall apply.

Certificate generation

d) The CA shall issue a new certificate using the subject's previously certified public key, only if its cryptographic security is still sufficient for the new certificate's validity period and no indications exist that the subject's private key has been compromised nor that the certificate has been revoked due to any other securitybreach.

6.3.7 Certificate Re-key

All forms of certificate re-keying is forbidden under this CP.

6.3.8 Certificate modification

Requests for certificates issued to a subject who has previously been registered with the same TSP shall be complete, accurate and authorized. This includes certificate update due to change to the subject's attributes.

In particular:

Registration

a) If any certified names or attributes have changed, or the previous certificate has been revoked, the registration information shall be verified, recorded, agreed to by the subscriber in accordance with clause 6.2.2.

6.3.9 Certificate revocation and suspension

The TSP shall revoke certificates in a timely manner based on authorized and validated certificate revocation requests.

In particular:

a) The subject, and where applicable the subscriber, of a revoked or suspended certificate, shall be informed of the change of status of the certificate.

b) Once a certificate is definitively revoked (i.e. not suspended) it shall not be reinstated.

c) Where Certificate Revocation Lists (CRLs) concerning end users certificates including any variants (e.g. Delta CRLs) are used, these shall be published at least every 24 hours; and

i) every CRL shall state a time for next scheduled CRL issue;
ii) a new CRL may be published before the stated time of the next CRL issue;
iii) the CRL shall be signed by the CA or an entity designated by the TSP

d) Where CARL is used a new CARL shall be generated at least once a year with a nextUpdate of at most 1 year after the issuing date. In any case, a new CARL shall be generated once a CA certificate has been revoked.

e) In the case of any cross-certificates issued by the CA, the CARL should be issued at least every 31 days.

6.3.10 Certificate status services

The TSP shall provide services for checking the status of the certificates.

In particular:

Revocation status

a) Revocation status information shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under the control of the TSP, the TSP shall make best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted inthe CPS.

b) The integrity and authenticity of the status information shall be protected.

c) Revocation status information shall include information on the status of certificates at least until the certificate expires.

d) OCSP shall be supported.

e) CRL should be supported.

f) If a TSP supports multiple methods (CRL and on-line certificate status service) to provide revocation status, any updates to revocation status shall be available for all methods, and the information provided by all services shall be consistent over time taking into account different delays in updating the statusinformation for all the methods.

g) The revocation status information shall be publicly and internationally available.

6.3.11 End of subscription

No stipulations.

6.3.12 Key escrow and recovery

All forms of key escrow and private key recovery of subscriber private keys are forbidden under this CP.

6.4 Facility, management, and operational controls

6.4.1 General

The requirements identified in ETSI EN 319 401, clauses 5, 6.3 and 7.3, shall apply.

6.4.2 Physical security controls

The requirements identified in ETSI EN 319 401, clause 7.6, shall apply. In addition the following particular requirements apply:

Certificate generation and revocation management

a) The facilities concerned with certificate generation and revocation management shall be operated in an environment which physically protects the services from compromise through unauthorized access to systems or data.

b) Every entry to the physically secure area shall be subject to independent oversight and non-authorized person shall be accompanied by an authorized person whilst in the secure area. Every entry and exit shall be logged.

c) Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the certificate generation and revocation management services. Any parts of the premises shared with other organizations shall be outside this perimeter.

d) Physical and environmental security controls shall be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. The TSP's physical and environmental security policy for systems concerned with certificate generation and revocation management services shall address the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery.

e) Controls shall be implemented to protect against equipment, information, media and software relating to the TSP services being taken off-site without authorization.

f) Other functions relating to TSP operations may be supported within the same secured area provided that the access is limited to authorized personnel.

g) Root CA private keys shall be held and used physically isolated from normal operations such that only designated trusted personnel have access to the keys for use in signing subordinate CA certificates.

6.4.3 Procedural controls

The requirements identified in ETSI EN 319 401, clause 7.4, items REQ-7.4-04, REQ-7.4-05, REQ-7.4-07, REQ-7.4-08, and REQ-7.4-09 shall apply.

In addition the following particular requirements apply:

Certificate generation

a) Certificate issuance by the root CA shall be under at least dual control by authorized, trusted personnel such that one person cannot sign subordinate certificates on his/her own.

6.4.4 Personnel controls

The requirements identified in ETSI EN 319 401, clause 7.2 shall apply:

a) In addition to the trusted roles identified in ETSI EN 319 401, 7.2 item REQ-7.2-15, the trusted roles, of the registration and revocation officers responsibilities as defined in CEN TS 419 261 shall be supported.

6.4.5 Audit logging procedures

The requirements identified in ETSI EN 319 401, clause 7.10, shall apply. In addition the following particular requirements apply:

a) All security events shall be logged, including changes relating to the security policy, system start-up and shutdown, system crashes and hardware failures, firewall and router activities and PKI system access attempts.

Registration

b) All events related to registration including requests for certificate re-key or renewal shall be logged.

c) All registration information including the following shall be recorded:

i) type of document(s) presented by the applicant to support registration;
ii) record of unique identification data, numbers, or a combination thereof (e.g. applicant's identity card or passport) of identification documents, if applicable;
iii) storage location of copies of applications and identification documents, including the signed subscriber agreement (see clause 6.3.4, item d);
iv) any specific choices in the subscriber agreement (e.g. consent to publication of certificate) see clause 6.3.4, item d);
v) identity of entity accepting the application;
vi) method used to validate identification documents, if any; and
vii) name of receiving TSP and/or submitting Registration Authority, if applicable.

d) The TSP shall maintain the privacy of subject information.

Certificate generation

e) The TSP shall log all events relating to the life-cycle of CA keys.

f) The TSP shall log all events relating to the life-cycle of certificates.

g) The TSP shall log all events relating to the life cycle of keys managed by the CA, including any subject keys generated by the CA

Revocation management

h) The TSP shall log all requests and reports relating to revocation, as well as the resulting action.

6.4.6 Records archival

The following particular requirements apply:

a) The TSP shall retain the following for at least seven years after any certificate based on these records ceases to be valid:

i) log of all events relating to the life cycle of keys managed by the CA, including any subject key pairs generated by the CA (see clause 6.4.5, item g);

ii) documentation as identified in clause 6.3.4.

6.4.7 Key changeover

A CA cannot generate a certificate whose end date comes after the expiry date of the corresponding CA certificate. The validity period of the CA certificate must therefore extend beyond that of the certificates that it signs. A corresponding CPS details the applicable procedures in the event of a CA key changeo ver.

6.4.8 Compromise and disaster recovery

The requirements identified in ETSI EN 319 401, clauses 7.9 and 7.11, shall apply. In addition the following particular requirements apply:

TSP systems data backup and recovery

a) TSP systems data necessary to resume CA operations shall be backed up and stored in safe places, preferably also remote, suitable to allow the TSP to timely go back to operations in case of incident/disasters.

b) In line with ISO/IEC 27002, clause 12.3: Back-up copies of essential information and software should be taken regularly. Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure. Back-up arrangements should be regularly tested to ensure that they meet the requirements of business continuity plans.

c) Backup and restore functions shall be performed by the relevant trusted roles specified in clause 6.4.4.

d) If risk analysis identifies information requiring dual control for management, for example keys, then dual control should be applied to recovery.

CA key compromise

e) The TSP's business continuity plan (or disaster recovery plan) shall address the compromise, loss or suspected compromise of a CA's private key as a disaster and the planned processes shall be in place.

f) Following a disaster, the TSP shall, where practical, take steps to avoid repetition of a disaster.

g) In the case of compromise the TSP shall as a minimum:

i) inform the following of the compromise: all subscribers and other entities with which the TSP has agreements or other form of established relations, among which relying parties and TSPs. In addition, this information shall be made available to other relying parties;

ii) indicate that certificates and revocation status information issued using this CA key may no longer be valid; and

iii) revoke any CA certificate that has been issued for the compromised TSP when a TSP is informed of the compromise of another CA.

Algorithm compromise

h) Should any of the algorithms, or associated parameters, used by the TSP or its subscribers become insufficient for its remaining intended usage then the TSP shall:

i) inform all subscribers and relying parties with whom the TSP has agreement or other form of established relations. In addition, this information shall be made available to other relying parties; and

ii) schedule a revocation of any affected certificate.

6.4.9 Certification Authority or Registration Authority termination

The requirements identified in ETSI EN 319 401, clause 7.12, shall apply. In addition the following particular requirements apply:

a) Regarding the requirement REQ-7.12-06 of clause 7.12 of ETSI EN 319 401, this shall apply to registration information (see clauses 6.2.2, 6.3.1 and 6.3.4), revocation status information (see clause 6.3.10) and event log archives (see clauses 6.4.5 and 6.4.6) for their respective period of time as indicated to the subscriber and relying party (see clause 6.8.10).

b) Regarding the requirement REQ-7.12-10 of clause 7.12 of ETSI EN 319 401, this shall also include the handling of the revocation status for unexpired certificates that have been issued.

c) When another cross certified TSP stops all operations, including handling revocation (see clause 6.4.9 b), all cross certificates to that TSP shall be revoked.

6.5 Technical security controls

6.5.1 Key pair generation and installation

The requirements identified in ETSI EN 319 401, clause 7.5, shall apply.

In addition the following particular requirements apply:

Certificate generation

The CA shall generate its keys securely and the private key shall be secret throughout its defined lifetime.

a) CA key pair generation and the subsequent certification of the public key, shall be undertaken in a physically secured environment (see clause 6.4.2) by personnel in trusted roles (see clause 6.4.4) under, at least, dual control. The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the CA's practices.

b) CA key pair generation should be performed using an algorithm as specified in ETSI TS 119 312 for the CA's signing purposes.

c) The selected key length and algorithm for CA signing key should be one which is specified in ETSI TS 119 312 for the CA's signing purposes. Each CA shall in its CPS describe the used algorithms in use for its CA-keys, only allowing algorithms within the current version of ETSI TS 119 312.

d) Before expiration of its CA certificate which is used for signing subject keys (for example as indicated by expiration of CA certificate), the CA shall generate a new certificate for signing subject key pairs and shall apply all necessary actions to avoid disruption to the operations of any entity that may rely on the CA certificate. The new CA certificate shall also be generated and distributed in accordance with this policy.

e) These operations should be performed with a suitable interval between certificate expiry date and the last certificate signed to allow all parties that have relationships with the TSP (subjects, subscribers, relying parties, CAs higher in the CA hierarchy, etc.) to be aware of this key changeover and to implement the required operations to avoid inconveniences and malfunctions. This does not apply to a TSP which will cease its operations before its own certificate-signing certificate expiration date.

f) The TSP shall have a documented procedure for conducting CA key pair generation for all CAs, whether root CAs or subordinate CAs, including CAs that issue certificates to end users. This procedure shall indicate, at least, the following:

i) roles participating in the ceremony (internal and external from the organization);

ii) functions to be performed by every role and in which phases;

iii) responsibilities during and after the ceremony; and

iv) requirements of evidence to be collected of the ceremony.

g) The TSP shall produce a report proving that the ceremony was carried out in accordance with the stated procedure and that the integrity and confidentiality of the key pair was ensured. This report shall be signed:

i) For root CA: by the trusted role responsible for the security of the TSP's key management ceremony (e.g. security officer) and a trustworthy person independent of the TSP management (e.g. Notary, auditor) as witness that the report correctly records the key management ceremony as carried out.
ii) For subordinate CAs: by the trusted role responsible for the security of the TSP's key management ceremony (e.g. security officer) as witness that the report correctly records the key management ceremony as carried out.

Certificate generation and dissemination

h) CA signature verification (public) keys shall be available to relying parties in a manner that assures the integrity of the CA public key and authenticates its origin.

Certificate generation

If the CA generates the subject's keys:

i) CA-generated subject keys shall be generated using an algorithm defined in the CP during the validity time of the certificate.

j) CA-generated subject keys should be of a key length and for use with a public key algorithm as specified in the CP during the validity time of the certificate.

k) CA-generated subject keys shall be generated and stored securely whilst held by the TSP and must not be stored by the TSP after issuance to a subscriber.

Subject device provision

l) The subject's private key shall be delivered to the subject's device or to the TSP managing the subject's private key, in a manner such that the secrecy and integrity of the key is not compromised. If the TSP or any of its designated RAs become aware that a subject's private key has been communicated to an unauthorized person or an organization not affiliated with the subject, then the TSP shall revoke all certificates that include the public key corresponding to the communicated private key.

m) The CA shall delete all copies of a subject private key after delivery of the private key to the subject, except for conditions as described in clause 6.3.12.

n) The TSP shall secure the issuance of a secure cryptographic device to the subject. In particular:

i) Secure cryptographic device preparation shall be done securely.

ii) Secure cryptographic device shall be securely stored and distributed.

6.5.2 Private key protection and cryptographic module engineering controls

Certificate generation

In addition to requirements in clause 6.5.1 the following particular requirements apply:

a) CA key pair generation shall be carried out within a secure cryptographic device which:

i) is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO/IEC 15408, or equivalent national or internationally recognized evaluation criteria for IT security. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures; or

ii) meets the requirements identified in ISO/IEC 19790 or FIPS PUB 140-2 level 3.

The secure cryptographic device should be as per i).

b) The CA private signing key shall be held and used within a secure cryptographic device as indicated in a) above.

c) If outside the secure cryptographic device (see item b) above) the CA private key shall be protected in a way that ensures the same level of protection as provided by the secure cryptographic device.

d) The CA private signing key shall be backed up, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment (see clause 6.4.2). The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the CA's practices.

e) Copies of the CA private signing keys shall be subject to the same or greater level of security controls as keys currently in use.

f) Where the CA private signing keys and any copies are stored in a dedicated secure cryptographic device, access controls shall be in place to ensure that the keys are not accessible outside this device.

g) The secure cryptographic device shall not be tampered with during shipment, this must be validated by the TSP.

h) The secure cryptographic device shall not be tampered with while stored, this must be validated by the TSP.

i) The secure cryptographic device shall be functioning correctly, this must be validated by the TSP.

j) The CA private signing keys stored on the CA's secure cryptographic device shall be destroyed upon device retirement.

6.5.3 Other aspects of key pair management

The TSP shall use appropriately the CA private signing keys and shall not use them beyond the end of their life cycle.

In particular:

Certificate generation

a) CA signing key(s) used for generating certificates as defined in clause 6.3.3, and/or issuing revocation status information, shall not be used for any other purpose.

b) The certificate signing keys shall only be used within physically secure premises.

c) The use of the CA's private key shall be compatible with the hash algorithm, the signature algorithm and signature key length used for generating certificates, in line with current practice as in clause 6.5.1, item c).

d) All copies of the CA private signing keys shall be destroyed at the end of their life cycle.

6.5.4 Activation data

The following particular requirements apply:

Certificate generation

a) The installation and recovery of the CA's key pairs in a secure cryptographic device shall require simultaneous control of at least two trusted employees.

Subject device provision

In particular, if the TSP issues a secure cryptographic device:

b) Secure cryptographic device (e.g. smartcard) deactivation and reactivation shall be done securely.

c) Where the secure cryptographic device (e.g. smartcard) has associated user activation data (e.g. PIN code), the activation data shall be securely prepared and distributed separately from the secure cryptographic device.

6.5.5 Computer security controls

The requirements identified in ETSI EN 319 401, clause 7.4, items REQ-7.4-02, REQ-7.4-03 and REQ-7.4-10, shall apply.

In addition the following particular requirements apply:

Certificate generation

a) Local network components (e.g. routers) shall be kept in a physically and logically secure environment and their configurations shall be periodically checked for compliance with the requirements specified by the TSP.

b) The TSP shall enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

Dissemination

c) Dissemination application shall enforce access control on attempts to add or delete certificates and modify other associated information.

Certificate Revocation status

d) Revocation status application shall enforce access control on attempts to modify revocation status information.

Certificate generation and revocation management

e) Continuous monitoring and alarm facilities shall be provided to enable the TSP to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.

6.5.6 Life cycle security controls

The requirements identified in ETSI EN 319 401, clause 7.7 shall apply for all service components.

In addition the following particular requirements apply:

System planning

a) capacity demands shall be monitored and projections of future capacity requirements shall be made to ensure that adequate processing power and storage are available.

Certificate generation and revocation management

c) See clause 6.5.5, item e).

6.5.7 Network security controls

The requirements identified in ETSI EN 319 401, clause 7.8 shall apply.

In addition the following particular requirements apply:

a) The TSP shall maintain and protect all CA systems in at least a secure zone and shall implement and configure a security procedure that protects systems and communications between systems inside secure zones and high security zones.

b) The TSP shall configure all CA systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's operations.

c) The TSP shall grant access to secure zones and high security zones to only trusted roles.

d) The Root CA system shall be in a high security zone.

6.5.8 Timestamping

No stipulations.

6.6 Certificate, CRL, and OCSP profiles

6.6.1 Certificate profile

The certificates shall meet the requirements, specified in Recommendation ITU-T X.509 or IETF RFC 5280.

All certificates issued under this policy must adhere to the certificate profiles dictated by the Gjaldstovan TSP Management Board. These profiles are available at http://www.talgildu.fo/talgildur-samleiki/certificate-profiles

The certificate shall be issued according to the relevant certificate profile as identified below:

i) for issuance of certificates to natural persons: ETSI EN 319 412-2

6.6.2 CRL profile

The CRL shall be as defined in ISO/IEC 9594-8/Recommendation ITU-T X.509 or IETF RFC 5280

6.6.3 OCSP profile

The OCSP shall be as defined in IETF RFC 6960.

6.7 Compliance audit and other assessment

Compliance audits and other assessments shall be conducted in accordance with the requirements stipulated by the current version of ETSI EN 319 403.

6.8 Other business and legal matters

6.8.1 Fees

These policy requirements are not meant to imply any restrictions on charging for TSP services.

6.8.2 Financial responsibility

The requirements identified in ETSI EN 319 401, clause 7.1.1, item REQ-7.1.1-04 shall apply.

6.8.3 Confidentiality of business information

No stipulations.

6.8.4 Privacy of personal information

The requirements identified in ETSI EN 319 401, clause 7.13, item REQ-7.13-05 shall apply.

In addition the following particular requirements apply:

a) The confidentiality and integrity of registration data shall be protected, especially when exchanged with the subscriber/subject or between distributed TSP system components.

b) Some records may need to be securely retained to meet statutory requirements, as well as to support essential business activities (see clauses 6.4.5 and 6.4.6).

6.8.5 Intellectual property rights

Certificate applicants shall not use names in their certificate applications that infringe upon the intellectual property rights of others. Gjaldstovan shall not be required to determine whether a certificate applicant has intellectual property rights to the name appearing in a certificate application or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name or trademark. Gjaldstovan shall be entitled, without liability to any certificate applicant, to reject or suspend any certificate application because of such disputes.

6.8.6 Representations and warranties

The requirements identified in ETSI EN 319 401 clause 6.3, items REQ-6.3-05 and REQ-6.3-06 and clause 6.4 of the present document shall apply. TSP has the responsibility for conformance with the procedures prescribed in this policy, even when the TSP functionality is undertaken by outsourcers.

In addition the following particular requirements apply:

a) The TSP shall provide all its certification services consistent with its CPS.

6.8.7 Disclaimers of warranties

See clause 6.8.6.

6.8.8 Limitations of liability

Limitations on liability are covered in the terms and conditions as per clause 6.9.4.

6.8.9 Indemnities

No stipulations.

6.8.10 Term and termination

No stipulations.

6.8.11 Individual notices and communications with participants

No stipulations.

6.8.12 Amendments

No stipulations.

6.8.13 Dispute resolution procedures

The requirements identified in ETSI EN 319 401, clauses 6.2, item REQ-6.2-02 (i) and 7.1.1, item REQ-7.1.1-06 shall apply.

6.8.14 Governing law

This CP shall be governed in accordance with Faroese legislation

Subject to any limits appearing in applicable law, the laws of the Faroe Islands shall govern the enforcement, construction, interpretation and validity of this CP.

CAs must provide information in accordance with Faroese applicable laws.

If a dispute cannot be settled by conciliation, either of the parties may choose to bring the dispute before the ordinary courts. The venue is Føroya Rættur, Tórshavn. The applicable law is Faroese law.

6.8.15 Compliance with applicable law

The requirements identified in ETSI EN 319 401, clause 7.13, item REQ-7.13-02 shall apply.

6.8.16 Miscellaneous provisions

No stipulations.

6.9 Other provisions

6.9.1 Organizational

The requirements identified in ETSI EN 319 401, clause 7.1 shall apply.

In addition the following particular requirements apply:

Certificate generation and revocation management

a) The parts of the TSP concerned with certificate generation and revocation management shall be independent of other organizations for its decisions relating to the establishing, provisioning and maintaining and suspending of services in conformance with the applicable certificate policies; in particular its senior executive, senior staff and staff in trusted roles, shall be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides.

b) The parts of the TSP concerned with certificate generation and revocation management shall have a documented structure which safeguards impartiality of operations.

6.9.2 Additional testing

a) The TSP shall provide the capability to allow third parties to check and test all the certificate types that the TSP issues.

b) Any test certificates should clearly indicate that they are for testing purposes (e.g. by the subject name).

6.9.3 Disabilities

The requirements identified in ETSI EN 319 401, clause 7.13, items REQ-7.13-03 and REQ-7.13-04 shall apply.

6.9.4 Terms and conditions

The requirements identified in ETSI EN 319 401, clause 6.2 shall apply.

In addition the following particular requirements apply:

a) The terms and conditions shall include a notice as specified in clause 6.3.4.