Gjaldstovan Certificate Policy - Faroe Islands Root CA

Version 1.1 - 08.03.2020

Change Log

Version	Date:	Author:	Change:
1.1	08-03-2020	Djóni á Boðanesi	First version ready for BSI review document review ETSI 319 411-1 in March 2020
1.1	01-05-2020	Jósup Henriksen	Approved by Gjaldstovan TSP Management Board (No changes to the 1.1 from from 08.03.2020)

Copyright Notices

Requests for any other permission to reproduce this Certificate Policy (as well as requests for copies from Gjaldstovan) must be addressed to:

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

Or:

gjaldstovan@gjaldstovan.fo

Table of contents

1 Introduction

1.1 Scope

This certificate policy, CP, applies to the Root CA of the national Faroese eID programme, named Samleikin PKI.

The possible entities this CP applies to are:

- The Root CA, acting as the trust anchor for the Faroe Islands national eID programme, Samleikin PKI.

This document specifies the policy and security requirements for the Root CA. The policy and security requirements are defined in terms of requirements for the issuance, maintenance and life-cycle management of the Root CA.

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 https://portal.etsi.org/TB-SiteMap/ESI/Trust-Service-Providers

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

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

Root CA: certification authority which is at the highest level within Samleikin PKI 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:

CA - Certification Authority
CARL - Certification Authority Revocation List
CP - Certificate Policy
CPS - Certification Practice Statement
CRL - Certificate Revocation List
EAL - Evaluation Assurance Level
OCSP - Online Certificate Status Protocol
OID - Object IDentifier
PDS - PKI Disclosure Statement
PKI - Public Key Infrastructure
RA - Registration Authority
TLS - Transport Layer Security
TSP - Trust Service Provider
UTC - Coordinated Universal Time

4 General concepts

4.1 General policy requirements concepts

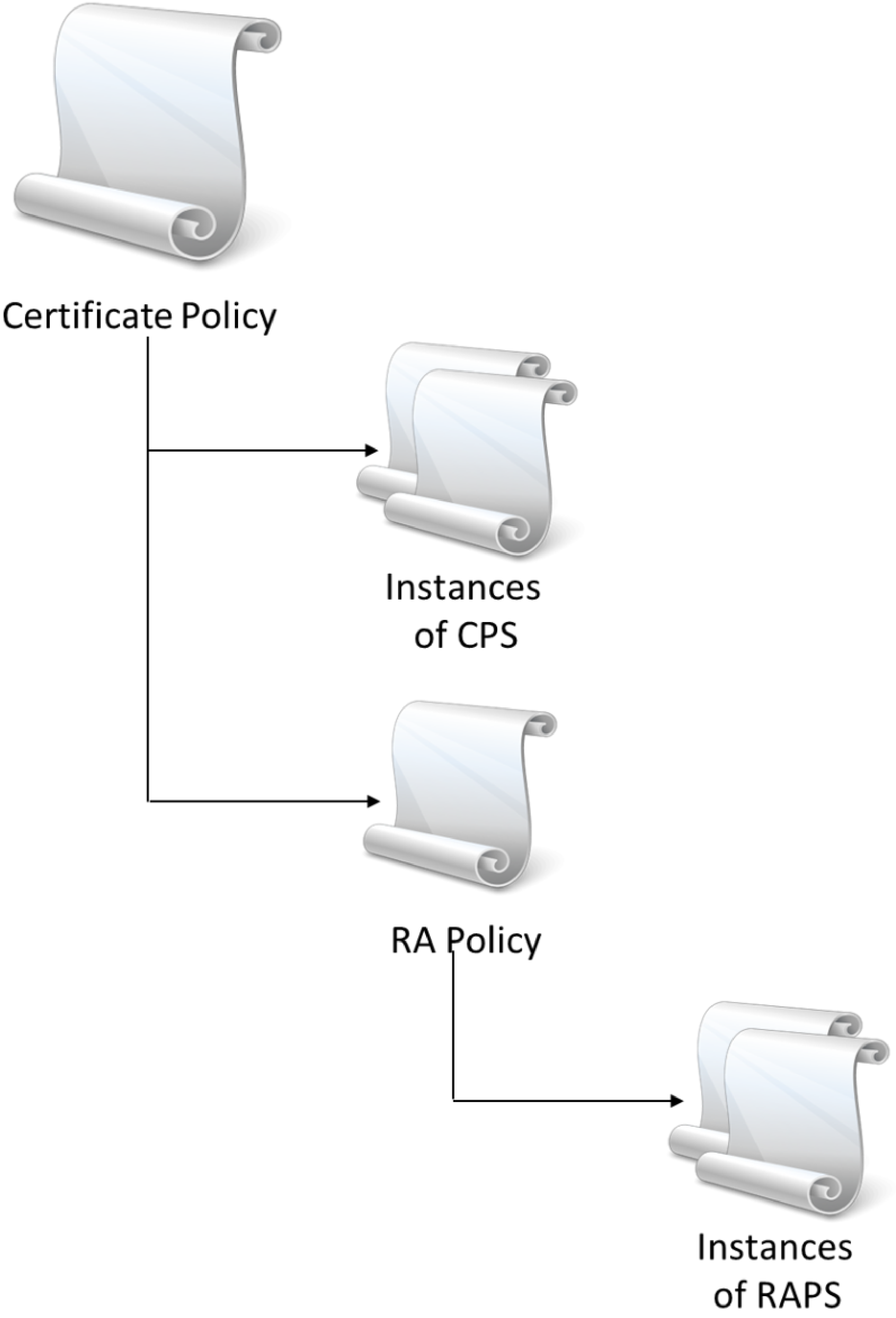
In general, a public-key certificate binds a public key held by an entity to a set of information that identifies the entity associated with use of the corresponding private key. In most cases involving identity certificates, this entity is known as the "subject" or "subscriber" of the certificate.

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 CA 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 certificates issued under the Root CA.

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 Root CA Certificate Policy.

4.3 Certification services

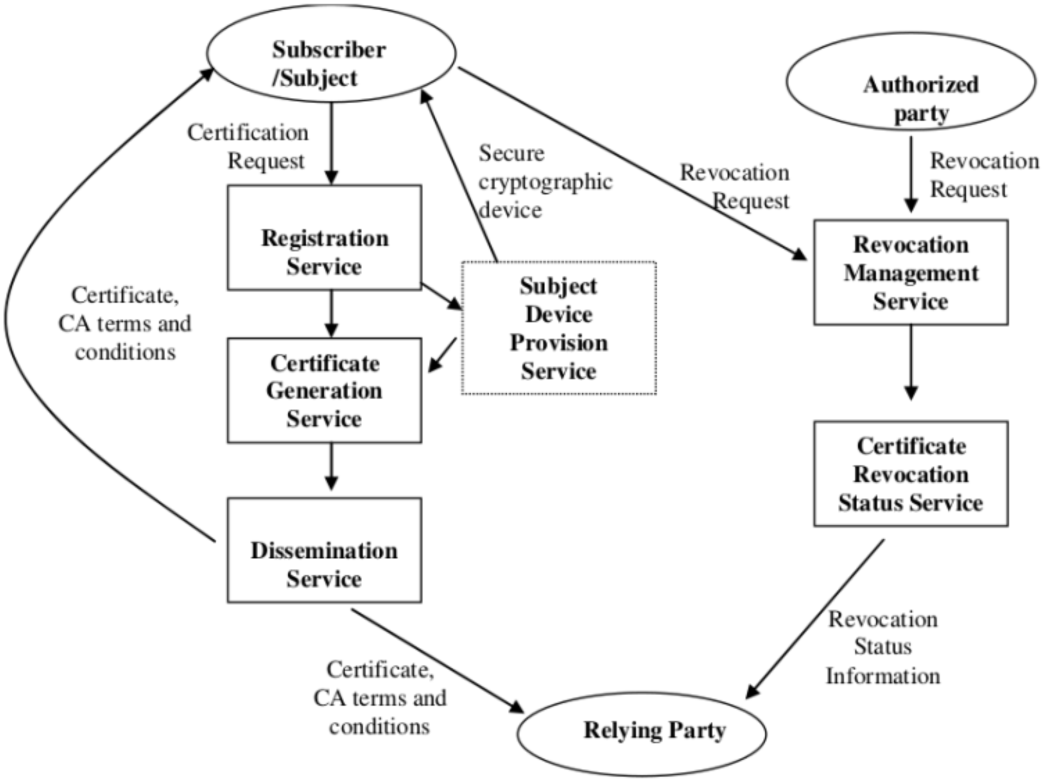
The certification services are broken down in the present document into the following component services for the purposes of classifying requirements:

- 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 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:


Subscriber /Subject
Authorized party
Certification Request
Secure cryptographic device
Revocation Request
Revocation Request
Registration Service
Revocation Management Service
Subject Device Provision Service
Certificate, CA terms and conditions
Certificate Generation Service
Certificate Revocation Status Service
Dissemination Service
Revocation Status Information
Certificate, CA terms and conditions
Relying Party

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 Root CA 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 Root CA.

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

(Based on ETSI EN 319 401, clause 6.1)

The Root CA shall specify the set of policies and practices appropriate for the trust services it is providing. The set of policies and practices shall be approved by management, published and communicated to employees and external parties as relevant.

The Root CA shall have a Root CA CPS for the trust service provided.

In particular:

1. The Root CA shall have a Root CA CPS used to address all the requirements identified in this Root CP.

2. The Root CAs CPS shall identify the obligations of all external organizations supporting the Root CAs services including the applicable policies and practices.
3. The Root CA shall make available to subscribers and relying parties its CPS, and other relevant documentation, as necessary to assess conformance to the service policy.
4. The Root CA shall have a management body with overall responsibility for the Root CA with final authority for approving the Root CAs CPS.
5. The Root CAs management shall implement the CPS.
6. The Root CA shall define a review process for the practices including responsibilities for maintaining the Root CAs CPS.
7. The Root CA shall notify notice of changes it intends to make in the Root CAs CPS.
8. The Root CA shall, following approval as in point 4 above, make the revised Root CAs CPS immediately available as required under point 3 above.
9. The Root CA shall state in its Root CAs CPS the provisions made for termination of service.

In addition the following particular requirements apply:

- The Root CA CPS should be structured in accordance with IETF RFC 3647.
- The Root CA CPS shall include the complete CA hierarchy, including root and subordinate CA's.
- The Root CA CPS shall include the signature algorithms and parameters employed.
- The Root CA shall publicly disclose its CPS through an online means that is available on a 24x7 basis.
- The Root CA 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:

- Root CA Certificate Policy:

  OID: 1.2.208.189.1.1.1

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 4.3. 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.

The Root CA acts as the trust anchor of a hierarchy of issuing CAs.

5.4.2 Subscriber and subject

A subject can be:

- A CA system within Samleikin on the Faroe Islands, operated by or on behalf of Gjaldstovan.

When the subject is acting on behalf of Gjaldstovan, responsibilities of the CA are addressed in clause 6.3.4.

To request a CA Certificate the subject must be an entity approved by the Gjaldstovan TSP Management Board.

5.4.3 Others

No stipulations.

5.5 Certificate usage

Certificates issued under this policy is only intended for use for issuing CAs within Samleikin, including relying parties to Samleikin.

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-entity
certificates shall not be used as CA Certificates.

6 Root CA practice

6.1 Publication and repository responsibilities

The Root CA shall make CA Certificates available to issuing CAs within Samleikin, including relying parties to Samleikin. In particular:

Dissemination

a) Upon generation, the complete and accurate certificate shall be available to the requesting CA within Samleikin.

b) Issued CA certificates shall be available for retrieval.

c) The Root CA shall make a formal agreement with the holder of a CA certificate at time of issuance and request, containing 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 CA certificates, as per c) above.

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 Root CA, the Root CA 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 this CP.

6.2.2 Admittance procedure to join the Samleikin PKI

The Root CA 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, the subscriber is identified as the TSP requesting the CA certificate.

In particular:

Registration

a) The Root CA shall collect either direct evidence or an attestation from an appropriate and authorized source, of the identity and authorization to act on behalf of the TSP and if applicable, any specific attributes to whom the certificate is requested. Submitted evidence may be in the form of either paper or electronic documentation (in both cases the Root CA shall validate their authenticity).

b) Evidence of the identity of the authorized representative of the TSP shall be checked directly by physical presence.

c) The Root CA shall record all the information necessary to verify the identity, including any reference number on the documentation used for verification, and any limitations on its validity.

d) Evidence shall be provided that the representative is authorized to act for the TSP as identified.

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

f) The Root CA shall provide evidence of how they meet applicable data protection legislation within their registration process.

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

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 Root CA shall revoke certificates as quickly as practical possible after receiving a validated certificate revocation request.

In particular:

Revocation management

a) The Root CA shall document as part of its CPS (see clause 5.2) the procedures for revocation of 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.

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.

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), the Root CA 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 on every start of the Root CA system, and according to the frequency and manual procedure defined in he Root CA CPS.

b) Requests for revocation and reports of events relating to revocation shall be processed as soon as practically possible. Including compromise of subject's private key.

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 Root CA's practices in its CPS.

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

The application procedure shall be defined in the Root CA CPS.

6.3.3 Certificate issuance

The Root CA shall issue certificates securely to maintain their authenticity.

In particular:

Certificate generation

a) See clause 6.6.1 for certificate profiles.

b) The Root CA shall take measures against forgery of certificates, and in cases where the Root 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 re-key, including the provision of any subject-generated public key.

d) If the Root 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 Root 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 Root CA managing the key on behalf of the subject, the Root CA shall ensure that the subject has sole control over its signing key.

e) Over the life time of the Root 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

g)The Root CA shall have a documented procedure for conducting generation of certificates issued by the Root CA. 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.

h) The Root CA shall produce a report proving that the ceremony was carried out in accordance with the stated procedure and that the integrity and confidentiality the certificates was ensured. This report shall be signed by the trusted role responsible for the security of the Root CA key management ceremony (e.g. security officer) and a trustworthy person independent of the Root CA management (e.g. Notary, auditor) as witness that the report correctly records the key management ceremony as carried out.

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 TSP, the Root CA shall inform the TSP of the terms and conditions regarding use of the CA certificate as given in clause 6.9.4.

b) The TSP shall be informed of the obligations associated with the CA certificate.

c) The Root CA shall communicate the terms and conditions through a durable (i.e. with integrity over time) means of communication, and in a human readable form. The terms and conditions may also be transmitted electronically.

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

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 TSPs obligations (see clause 6.3.4) shall include items a) to l) below.

a) accurate and complete information is submitted to the Root CA 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 TSP;

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

d) if the TSP 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. The Root 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) only use the subject's private key(s) for cryptographic functions within the secure cryptographic device;

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

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

i) the TSPs 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 or other reasons; or

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

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

i) in the case of being informed that the subject's certificate has been revoked, or the Root 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:

j) 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);

k) 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

l) take any other precautions prescribed in agreements or elsewhere

6.3.6 Certificate renewal

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

In particular:

Registration

a)

i) The Root CA 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 terms and conditions has changed, these shall be communicated to the TSP 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 Root 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 security breach.

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

In particular:

a) The Root CA, and where applicable the TSP, 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) 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 the Root CA certificate has been revoked.

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

6.3.10 Certificate status services

The Root CA 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 Root CA, the Root CA shall make best endeavors to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the 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 the Root CA 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 status information 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 private keys are forbidden under this CP.

6.4 Facility, management, and operational controls

6.4.1 General

Risk Assessment

The Root CA shall carry out a risk assessment to identify, analyse and evaluate trust service risks taking into account business and technical issues.

The Root CA shall select the appropriate risk treatment measures, taking account of the risk assessment results.

The risk treatment measures shall ensure that the level of security is commensurate to the degree of risk.

The Root CA shall determine all security requirements and operational procedures that are necessary to implement the risk treatment measures chosen, as documented in the information security policy and the practice statement.

The risk assessment shall be regularly reviewed and revised.

The Gjaldstovan TSP management Board shall approve the risk assessment and accept the residual risk identified.

Information security policy

The Root CA shall define an information security policy which is approved by the Gjaldstovan TSP Management Board and which sets out the organization's approach to managing its information security.

Changes to the information security policy shall be communicated to third parties, where applicable. This includes subscribers, relying parties, assessment bodies, supervisory or other regulatory bodies.

In particular:

- The Root CAs information security policy shall be documented, implemented and maintained including the security controls and operating procedures for Root CAs facilities, systems and information assets providing the services.
- The Root CA shall publish and communicate the information security policy to all employees who are impacted by it.
- The Root CA shall retain overall responsibility for conformance with the procedures prescribed in its information security policy, even when the Root CAs functionality is undertaken by outsourcers.
- The Root CA shall define the outsourcers' liability and ensure that outsourcer are bound to implement any controls required by the Root CA.
- The Root CAs information security policy and inventory of assets for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
- Any changes that will impact on the level of security provided shall be approved by the Gjaldstovan TSP Management Board
- The configuration of the Root CAs systems shall be regularly checked for changes which violate the TSPs security policies.
- The maximum interval between two checks shall be documented in the trust service practice statement.

Asset management

The Root CA shall ensure an appropriate level of protection of its assets including information assets.

In particular:

- The Root CA shall maintain an inventory of all information assets and shall assign a classification consistent with the risk assessment.

All media shall be handled securely in accordance with requirements of the information classification scheme. Media containing sensitive data shall be securely disposed of when no longer required.

6.4.2 Physical security controls

The Root CA shall control physical access to components of the Root CAs system whose security is critical to the provision of its trust services and minimize risks related to physical security.

In particular:

- Physical access to components of the Root CAs system whose security is critical to the provision of its trust services shall be limited to authorized individuals.
- Controls shall be implemented to avoid loss, damage or compromise of assets and interruption to business activities.
- Controls shall be implemented to avoid compromise or theft of information and information processing facilities.
- Components that are critical for the secure operation of the trust service shall be located in a protected security perimeter with physical protection against intrusion, controls on access through the security
perimeter and alarms to detect intrusion.

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 Root CA 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 Root CA services being taken off-site without authorization.

f) Other functions relating to Root CA 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

Root CA shall administer user access of operators, administrators and system auditors. This administration shall include user account management and timely modification or removal of access.

Access to information and application system functions shall be restricted in accordance with the access control policy.

The Root CA systems shall provide sufficient computer security controls for the separation of trusted roles identified in the Root CA practice statement, including the separation of security administration and operation functions. Particularly, use of system utility programs shall be restricted and controlled.

The Root CA's personnel shall be identified and authenticated before using critical applications related to the service.

The Root CA's personnel shall be accountable for their activities. This can be achieved by retaining event logs.

With regards to the general requirement "Sensitive data shall be protected", sensitive data includes registration information.

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 Root CA shall ensure that employees and contractors support the trustworthiness of the Root CA's operations.

In particular:

The Root CA shall employ staff and, if applicable, subcontractors, who possess the necessary expertise, reliability, experience, and qualifications and who have received training regarding security and personal data protection rules as appropriate for the offered services and the job function. The personnel should be able to fulfill the requirement of "expert knowledge, experience and qualifications" through formal training and credentials, or actual experience, or a combination of the two. This should include regular (at least every 12 months) updates on new threats and current security practices.

Personnel employed by the Root CA include individual personnel contractually engaged in performing functions in support of the Root CA's services. Personnel who can be involved in monitoring the Root CA's services need not be the Root CA's personnel.

Appropriate disciplinary sanctions shall be applied to personnel violating the Root CA's policies or procedures.

Security roles and responsibilities, as specified by the Root CA's cps, shall be documented in job descriptions or in documents available to all concerned personnel. Trusted roles, on which the security of the Root CA's operation is dependent, shall be clearly identified. Trusted roles shall be named by the management. Trusted roles shall be accepted by the management and the person to fulfil the role.

The CA's personnel (both temporary and permanent) shall have job descriptions defined from the view point of roles fulfilled with segregation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness.

Where appropriate, job descriptions shall differentiate between general functions and the Root CA's specific functions. These should include skills and experience requirements.

Personnel shall exercise administrative and management procedures and processes that are in line with the Root CA's information security management procedures.

Managerial personnel shall possess experience or training with respect to the trust service that is provided, familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.

All the Root CA's personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the Root CA's operations.

Trusted roles shall include roles that involve the following responsibilities:
a) Security Officers: Overall responsibility for administering the implementation of the security practices.
b) System Administrators: Authorized to install, configure and maintain the Root CA's trustworthy systems for service management. This includes recovery of the system.
c) System Operators: Responsible for operating the Root Ca's trustworthy systems on a day-to-day basis. Authorized to perform system backup.
d) System Auditors: Authorized to view archives and audit logs of the Root CA's trustworthy systems.

Additional application specific roles can be required for particular trust services.
The Root CA's personnel shall be formally appointed to trusted roles by senior management responsible for security requiring the principle of "least privilege" when accessing or when configuring access privileges.

Personnel shall not have access to the trusted functions until the necessary checks are completed.

6.4.5 Audit logging procedures

The Root CA shall record and keep accessible for an appropriate period of time, including after the activities of the Root CA have ceased, all relevant information concerning data issued and received by the Root CA, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service.

In particular:

- The confidentiality and integrity of current and archived records concerning operation of services shall be maintained.
- Records concerning the operation of services shall be completely and confidentially archived in accordance with disclosed business practices.
- Records concerning the operation of services shall be made available if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings.
- The precise time of the Root CA's environmental, key management and clock synchronization events shall be recorded.
- The time used to record events as required in the audit log shall be synchronized with UTC at least once a day.
- Records concerning services shall be held for a period of time as appropriate for providing necessary legal evidence and as notified in the Root CA's CPS.
- The events shall be logged in a way that they cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period of time that they are required to be held. This can be achieved, for example, through the use of write-only media, a record of each removable media used and the use of off-site backup or by parallel storage of the information at several (e.g. 2 or 3) independent sites.

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 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 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) identity of entity accepting the application;
v) method used to validate identification documents, if any

Certificate generation

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

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

f) The Root CA 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

g) The Root CA 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 Root CA 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

The Root 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 changeover.

6.4.8 Compromise and disaster recovery

The Root CA shall define and maintain a continuity plan to enact in case of a disaster.

In the event of a disaster, including compromise of a private signing key or compromise of some other credential of the Root CA, operations shall be restored within the delay established in the continuity plan, having addressed any cause for the disaster which may recur (e.g. a security vulnerability) with appropriate remediation measures.

The Root CA shall act in a timely and co-ordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security.

The Root CA shall appoint trusted role personnel to follow up on alerts of potentially critical security events and ensure that relevant incidents are reported in line with the Root CA procedures.

Root CA shall establish procedures to notify the appropriate parties in line with the applicable regulatory rules of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein within 24 hours of the breach being identified.

Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the Root CA shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.

Incident reporting and response procedures shall be employed in such a way that damage from security incidents and malfunctions are minimized.

In addition the following particular requirements apply:

Root CA systems data backup and recovery

a) Root CA systems data necessary to resume CA operations shall be backed up and stored in safe places, preferably also remote, suitable to allow the Root CA 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 Root CA 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 Root CA shall, where practical, take steps to avoid repetition of a disaster.

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

i) inform the following of the compromise: all TSPs and other entities with which the Root CA 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

Algorithm compromise

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

i) inform all TSPs and relying parties with whom the Root CA 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 termination

Potential disruptions to subscribers and relying parties shall be minimized as a result of the cessation of the Root CA's services, and in particular continued maintenance of information required to verify the correctness of trust services shall be provided.
In particular:

1. The Root CA shall have an up-to-date termination plan.

2. Before the Root CA terminates its services at least the following procedures apply:
   a. the Root CA shall inform the following of the termination: all subscribers and other entities with which the Root CA has agreements or other form of established relations, among which relying parties, TSPs and relevant authorities such as supervisory bodies.
   b. the Root CA shall make the information of the termination available to other relying parties.
   c. the Root CA shall terminate authorization of all subcontractors to act on behalf of the Root CA in carrying out any functions relating to the process of issuing trust service tokens.
   d. the Root CA shall transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the Root CA for a reasonable period, unless it can be demonstrated that the Root CA does not hold any such information. 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)
   e. the Root CA's private keys, including backup copies, shall be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved.

3. The Root CA shall have an arrangement to cover the costs to fulfil these minimum requirements in case the Root CA becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy.

4. The Root CA shall state in its practices the provisions made for termination of service. This shall include:
   a. notification of affected entities; and
   b. where applicable, transferring the Root CA's obligations to other parties.

      This shall also include the handling of the revocation status for unexpired certificates that have been issued.

5. The Root CA shall maintain or transfer to a reliable party its obligations to make available its public key or its trust service tokens to relying parties for a reasonable period.

In addition the following particular requirement apply:

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

6.5 Technical security controls

6.5.1 Key pair generation and installation

Appropriate security controls shall be in place for the management of any cryptographic keys and any cryptographic devices throughout their lifecycle.

In addition the following particular requirements apply:

Certificate generation

The Root 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. The Root 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 Root 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 Root CA (TSPs, relying parties) to be aware of this key changeover and to implement the required operations to avoid inconveniences and malfunctions.

f) The Root CA shall have a documented procedure for conducting CA key pair generation. 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 Root CA 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 by the trusted role responsible for the security of the Root CAs key management ceremony (e.g. security officer) and a trustworthy person independent of the Root CA management (e.g. Notary, auditor) as witness that the report correctly records the key management ceremony as carried out.

For subordinate CAs it shall be signed 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.

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.

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

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

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 Root CA 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.

6.5.5 Computer security controls

The following requirements apply:

Certificate generation

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

Dissemination

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

Certificate Revocation status

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

6.5.6 Life cycle security controls

The Root CA shall use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.

In particular:

1. An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project undertaken by the Root CA or on behalf of the Root CA to ensure that security is built into IT systems.
2. Change control procedures shall be applied for releases, modifications and emergency software fixes of any operational software and changes to the configuration which applies the Root CA security policy.
3. The procedures shall include documentation of the changes.
4. The integrity of Root CA systems and information shall be protected against viruses, malicious and unauthorized software.
5. Media used within the Root CA systems shall be securely handled to protect media from damage, theft, unauthorized access and obsolescence.
6. Media management procedures shall protect against obsolescence and deterioration of media within the period of time that records are required to be retained.
7. Procedures shall be established and implemented for all trusted and administrative roles that impact on the provision of services.
8. The Root CA shall specify and apply procedures for ensuring that:
   a) security patches are applied within a reasonable time after they come available;
   b) security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them; and
   c) the reasons for not applying any security patches are documented.

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.

6.5.7 Network security controls

The Root CA system shall be located and operated in a high security zone that is offline and separated by air gapping mechanisms.

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 Gjaldstovan. These profiles are available at https://repository.samleiki.fo/legal-repository

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 services offered by the Root CA.

6.8.2 Financial responsibility

No stipulations.

6.8.3 Confidentiality of business information

No stipulations.

6.8.4 Privacy of personal information

Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

In addition the following particular requirements apply:

a) The confidentiality and integrity of registration data shall be protected.

6.8.5 Intellectual property rights

TSPs shall not use names in their certificate applications that infringe upon the intellectual property rights of others. The Root CA shall 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. The Root CA 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 Root CA shall retain overall responsibility for conformance with the procedures prescribed in its information security policy, even when the Root CA functionality is undertaken by outsourcers. The Root CA shall define the outsourcers' liability and ensure that outsourcer are bound to implement any controls required by the Root CA. Clause 6.4 of the present document shall apply.

In addition the following particular requirements apply:

a) The Root CA 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 CA Certificate Holder Agreement shall at least specify for each trust service policy supported by the Root CA procedures for complaints and dispute settlement.

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.

The Root CA 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 Root CA shall provide evidence on how it meets the applicable legal requirements.

6.8.16 Miscellaneous provisions

No stipulations.

6.9 Other provisions

6.9.1 Organizational

Organization reliability

The Root CA organization shall be reliable.

In particular:

- Trust service practices under which the Root CA operates shall be non-discriminatory.
- The Root CA should make its services accessible to all applicants whose activities fall within its declared field of operation and that agree to abide by their obligations as specified in the CA Certificate Holder Agreement
- The Root CA shall maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with applicable law, to cover liabilities arising from its operations and/or activities.
- The Root CA shall have the financial stability and resources required to operate in conformity with this policy.
- The Root CA shall have policies and procedures for the resolution of complaints and disputes received from customers or other relying parties about the provisioning of the services or any other related matters.
- The Root CA shall have a documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements.

Segregation of duties
Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the Root CAs assets.

In addition the following particular requirements apply:

Certificate generation and revocation management

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

6.9.2 Additional testing

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

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

6.9.3 Disabilities

No stipulations.

6.9.4 Terms and conditions

The Root CA shall make the terms and conditions in the CA Certificate Holder Agreement regarding its services available to all subscribers and relying parties.

The terms and conditions in the CA Certificate Holder Agreement shall at least specify for each trust service policy supported by the Root CA the following:

a) the trust service policy being applied;
b) any limitations on the use of the service provided including the limitation for damages arising from the use of services exceeding such limitations;
c) the subscriber's obligations, if any;
d) information for parties relying on the trust service;
e) the period of time during which the Root CA event logs are retained;
f) limitations of liability;
g) the applicable legal system;
h) procedures for complaints and dispute settlement;
i) whether the Root CA trust service has been assessed to be conformant with the trust service policy, and if so
through which conformity assessment scheme;
j) the Root CA contact information; and
k) any undertaking regarding availability.

CA Certificate Holders shall be informed of precise terms and conditions in the CA Certificate Holder Agreement, including the items listed above, before entering into a contractual relationship.

Terms and conditions in the CA Certificate Holder Agreement shall be made available through a durable means of communication.
Terms and conditions in the CA Certificate Holder Agreement shall be available in a readily understandable language.
Terms and conditions in the CA Certificate Holder Agreement may be transmitted electronically.

In addition the following particular requirements apply:

a) The CA Certificate Holder Agreement shall include a notice as specified in clause 6.3.4.