Certificate Practice Statement - Faroe Islands RootCA1 v1

Version 1.0 - 01.05.2020

Change Log

Version	Date:	Author:	Change:
0.9	08-03-2020	Jósup Henriksen	Created first version ready for BSI review
0.9.1	20-03-2020	Jósup Henriksen	Adjustments in the risk assessment section 5.1 and added Terms and conditions in section 2.1
1.0	01-05-2020	Jósup Henriksen	CPS approved by Gjaldstovan TSP Management Board

1 Introduction

This Certification Practice Statement (CPS) applies to Faroe Islands RootCA1 v1, and is written according to the structure and requirements of RFC 3647.

The CPS addresses in detail the technical, procedural and organisational practices of the Faroe Islands Root Certification Authority (Root CA) which complies with "Gjaldstovan Certificate Policy - Faroe Islands Root CA" OID:1.2.208.189.1.1.1.

OID for this CPS is: 1.2.208.189.1.1.6

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

Or:

TSP@gjaldstovan.fo

A Certification Practice Statement (CPS) is a Certification Authority's (CA) description of the practices it follows when issuing certificates under one or more Certificate Policies (CP). The purpose of this CPS is to describe the procedures that the CA uses when issuing certificates, and that all Registration Authorities, Certificate Holders and Authorized Relying Parties shall follow in connection with these certificates. This document defines the CPS for the Far oe Islands RootCA1 v1.
This document is divided in to nine sections:

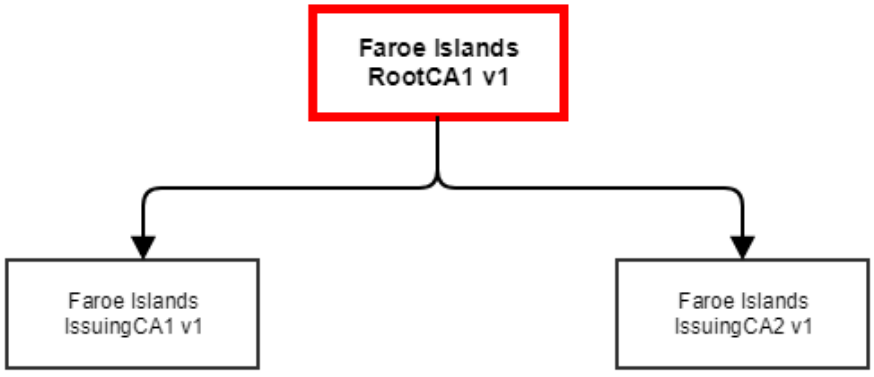
- Section 1 - provides an overview of the policy and set of provisions, as well as the types of entities and the appropriate applications for certificates.
- Section 2 - contains any applicable provisions regarding identification of the entity or entities that operate repositories; responsibility of a PKI participant to publish information regarding its practices, certificates and the current status; frequency of publication; and access control on published information.
- Section 3 - covers the identification and authentication requirements for certificate related activity.
- Section 4 - deals with certificate life cycle management and operational requirements including application for a certificate, revocation, suspension, audit, archival and compromise.
- Section 5 - covers facility, management and operational controls (physical and procedural security requirements).
- Section 6 - provides the technical controls with regard to cryptographic key requirements.
- Section 7 - defines requirements for certificates, Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) formats. This includes information on profiles, versions, and extensions used.
- Section 8 - addresses topics covered and methodology used for assessments/audits; frequency of compliance audits or assessments; identity and /or qualifications of the personnel performing the audit or assessment; actions taken as a result of deficiencies found during the assessment; and who is entitled to see results of an assessment.
- Section 9 - covers general business and legal matters: the business issues of fees, liabilities, obligations, legal requirements, governing laws, processes, and confidentiality.

This CPS generally conforms to the Internet Engineering Task Force (IETF) RFCs:

- RFC 3647 - for Certificate Policy and Certification Practices Framework
- RFC 2119 Key words for use in RFCs to Indicate Requirement Levels

1.1 Overview

This CPS lays out how Faroe Islands RootCA1 v1 conforms to procedures and routines defined in Gjaldst ovan Certificate Policy - "Faroe Islands Root CA" OID:1.2.208.189.1.1.1 when issuing certificates.
The following overview represents the CA structure of the Samleikin PKI.



1.2. Document Name and Identification

This CPS is titled "Faroe Islands RootCA1 v1 Certification Practice Statement" with OID 1.2.208.189.1.1.6 and applies to Faroe Islands RootCA1 v1.

1.3. PKI Participants

This CPS outlines the roles and responsibilities of all parties involved in the generation and use of CA Certificates and the operation of Faroe Islands RootCA1 v1 and its associated registration authority services.

The Root CA holds the root certificate(s) that represents the apex of Samleikin. The Root CA digitally creates, signs and issues CA certificates using its Root CA key(s). CA Certificates are only issued to approved Issuing CAs. An approved Issuing CA utilizes its CA certificate to create, sign and issue certificates to end-users.

Issuing CAs are subordinate services that are:

- Managed and operated by Gjaldstovan; or
- Managed by third party organizations on behalf of Gjaldstovan

Approved Issuing CAs are managed and operated in a manner that meets the contractual, audit and policy requirements dictated by the Gjaldstovan TSP Management Board with regard to operational practices and technical implementation.

This CPS describes all subordinate services that operate under the Root CA, i.e. that are within the “chain of trust”.

Participants within Samleikin include:

- Certification Authorities (CAs);
- Registration Authorities (RAs);
- CA Certificate Holders including applicants for CA Certificates prior to a CA Certificate issuance; and
- Authorized Relying Parties.

The practices described or referred to in this CPS:

- Accommodate the diversity of the community and the scope of applicability within the chain of trust
- Adhere to the purpose of the CPS of describing the uniformity and efficiency of practices throughout Samleikin

In keeping with their primary purpose, the practices described in this CPS:

- Are the minimum practices necessary to ensure that CA Certificate Holders and Authorized Relying Parties have a sufficient level of assurance, and that critical functions are provided at appropriate levels of trust
- Apply to all stakeholders, for the generation, issuance, use and management of all CA Certificates and Key Pairs

CA Certificates comply with Internet Standards (x509 v.3) as set out in RFC 5280 (which supersedes RFC 3280).

CA Certificates may not be used, and no participation is permitted in Samleikin:

- In circumstances that breach Relying Party Agreements or CA Certificate Holder Agreements
- In circumstances that breach, contravene, or infringe the rights of others
- In circumstances that offend, breach, or contravene any applicable law, statute, regulation, order, decree, or judgment of a court of competent jurisdiction or governmental order
- In connection with fraud, pornography, obscenity, hate, defamation, harassment, or other activity that is contrary to public policy.

1.3.1 Certification Authorities

Samleikin contains the following Root Certification Authorities:

- Faroe Islands RootCA1 v1

Issuing CAs are technical components in the Samleikin-PKI, that are operated by Gjaldstovan or an organisation who has been given the responsibility to issue, revoke and otherwise manage certificates to end-users.

Organisations (if it is not Gjaldstovan itself) operating Issuing CAs must be authorized by the Gjaldstovan TSP Management Board to participate within the Samleikin-PKI to issue, revoke and otherwise manage certificates. Generally, Issuing CAs are authorized to issue and manage all types of certificates supported by its applicable CP/CPS.

An Issuing CA is obliged to detail its specific practices and other requirements in a policy and practices statement adopted by it following approval by the Gjaldstovan TSP Management Board.

Within Samleikin all Issuing CAs are responsible for the management of certificates issued by them. Certificate management includes all aspects associated with the application, issue and revocation of certificates, including any required identification and authentication processes included in the certificate application process.

Notwithstanding the foregoing, Issuing CAs are required to conduct regular compliance audits to ensure that they are complying with their obligations bound by its respective combination of CP/CPS. Approved instances of CPS for Root CA and each Issuing CA is available from https://repository.samleiki.fo/legal-repository.

1.3.2 Registration Authorities

Issuing CAs, if authorized to do so by Gjaldstovan, may rely on third party RAs if they meet the requirements stated in the RAP at https://repository.samleiki.fo/legal-repository via a RAPS approved by the Gjaldstovan TSP Management Board. In circumstances where an Issuing CA has relied on a third party RA to perform identification and authentication, the Issuing CA bears all responsibility and liability for the identification and authentication of its Certificate Holders.

Notwithstanding the foregoing, Issuing CAs are required to conduct regular compliance audits of their RAs to ensure that they are complying with their obligations bound by the RAP and its associated RAPS. The RAPSes are kept confidential, but a template RAPS can be requested from the Gjaldstovan TSP Management Board.

1.3.3 Subscribers

CA Certificate Holders (in this CPS that is issuing CAs) are required to act in accordance with this CPS and the CA Certificate Holder Agreement. A CA Certificate Holder represents, warrants and covenants with and to the Root CA, Authorized Relying Parties and the RA processing their application for a CA Certificate that:

- Both as an applicant for a CA Certificate and as a CA Certificate Holder, submit complete and accurate information in connection with an application for a CA Certificate and will promptly update such information and representations from time to time as necessary to maintain such completeness and accuracy.
- Comply fully with any and all information and procedures required in connection with the identification and authentication requirements relevant to the CA Certificate issued.
- Promptly review, verify and accept or reject the CA Certificate that is issued and ensure that all the information set out therein is complete and accurate and to notify the Root CA and/or RA immediately in the event that the CA Certificate contains any inaccuracies
- Secure the Private Key and take all reasonable and necessary precautions to prevent the theft, unauthorized viewing, tampering, compromise, loss, damage, interference, disclosure, modification or unauthorized use of its Private Key (to include password, hardware token or other activation data used to control access to the participant's Private Key)
- Exercise sole and complete control and use of the Private Key that corresponds to the CA Certificate Holder's Public Key
- Immediately notify the Root CA and/or RA in the event that their Private Key is compromised, or if they have reason to believe or suspect or ought reasonably to suspect that their Private Key has been lost, damaged, modified or accessed by another person, or compromised in any other way whatsoever. Following compromise, the use of the CA Certificate Holder's Private Key shall be immediately and permanently discontinued
- Take all reasonable measures to avoid the compromise of the security or integrity of Samleikin.
- Forthwith upon termination, revocation or expiry of the CA Certificate, cease use of the CA Certificate absolutely.
- At all times utilize the CA Certificate in accordance with all applicable laws and regulations
- Discontinue the use of Key Pairs in the event that the Root CA notifies the CA Certificate Holder that Samleikin has been compromised.

CA Certificates include a reference to the relevant CPS, which contains statements detailing limitations of liability and disclaimers of warranty. In accepting a CA Certificate, CA Certificate Holders acknowledge and agree to all such limitations and disclaimers documented in the CPS.

1.3.4 Relying Parties

Authorized Relying Parties are required to act in accordance with this CPS and the Relying Party Agreement found at https://repository.samleiki.fo/legal-repository. An Authorized Relying Party must utilize CA Certificates and their corresponding Public Keys only for authorized and legal purposes and only in support of transactions or communications supported by Samleikin. An Authorized Relying Party shall not place reliance on a CA Certificate unless the circumstances of that intended reliance constitute reasonable reliance and that Authorized Relying Party is otherwise in compliance with the terms and conditions of their Relying Party Agreement. Any such reliance is made solely at the risk of the Authorized Relying Party.

Authorized here means organizations or companies that have signed a Relying Party Agreement regarding participating in the Samleikin PKI.

An Authorized Relying Party shall not place reliance on a CA Certificate unless the circumstances of that intended reliance constitute reasonable reliance (as set out below) and that Authorized Relying Party is otherwise in compliance with the terms and conditions of the Relying Party Agreement and this CPS. For the purposes of this CPS and Relying Party Agreement, the term "reasonable reliance" means:

- That the attributes of the CA Certificate relied upon are appropriate in all respects to the reliance placed upon that CA Certificate by the authorised Authorized Relying Party including, without limitation to the generality of the foregoing, the level of identification and authentication required in connection with the issue of the CA Certificate relied upon
- That the Authorized Relying Party has, at the time of that reliance, used the CA Certificate for purposes appropriate and permitted under this CPS
- That the Authorized Relying Party has, at the time of that reliance, acted in good faith and in a manner appropriate to all the circumstances known, or circumstances that ought reasonably to have been known, to the Authorized Relying Party
- That the CA Certificate intended to be relied upon is valid and has not been revoked, the Authorized Relying Party being obliged to check the status of that CA Certificate utilizing either the Root CAs Certificate Revocation List, or the Root CAs Online Certificate Status Protocol and otherwise in accordance with the provisions of this CPS
- That the Authorized Relying Party has, at the time of that reliance, verified the signature of the CA Certificate

- That the Authorized Relying Party ensures that the data signed has not been altered following signature by utilizing trusted application software
- That the signature is trusted and the results of the signature are displayed correctly by utilizing trusted application software
- That the identity of the CA Certificate Holder is displayed correctly by utilizing trusted application software

CA Certificates include a reference to the relevant CPS, which contains statements detailing limitations of liability and disclaimers of warranty. In accepting a CA Certificate, Authorized Relying Parties acknowledge and agree to all such limitations and disclaimers documented in the CPS.

A Authorized Relying Party shall make no assumptions about information that does not appear in a CA Certificate.

A party cannot rely on a CA Certificate issued by the Root CA if the party has actual notice of the compromise of the CA Certificate or its associated Private Key. Such notice includes but is not limited to the contents of the CA Certificate and information incorporated in the CA Certificate by reference, which includes this CPS and the current set of revoked CA Certificates published by the Root CA. CA Certificates have pointers to URLs where the Root CA publish status information, including Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol responder(s), and Authorized Relying Parties are required to check the most recent CRL or an OCSP responder indicated in the CA Certificate.

1.3.5 Other Participants

Other participants in Samleikin are required to act in accordance with this CPS and/or applicable agreements.

1.4 Certificate Usage

CA Certificates issued by the Root CA may only be used by approved organisations operating Issuing CAs within 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-user certificates shall not be used as CA Certificates.

Issued CA Certificates are not designed, intended, or authorized for use as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of systems, where failure could lead directly to death, personal injury, or severe environmental damage.

1.4.1 Appropriate Certificate Uses

CA Certificates may be used for validating end entity certificates that were generated using the corresponding CA private key.

The use of CA certificates supported by this CPS is restricted to parties authorised by contract to do so. Persons and entities other than those authorised by contract may not use CA Certificates for any purpose. No reliance may be placed on a CA Certificate by any person unless that person is an Authorised Relying Party.
CA Certificates issued by the Root CA does not convey evidence of authority of an individual to act on behalf of any person or to undertake any particular act, and Authorised Relying Parties are solely responsible for exercising due diligence and reasonable judgement before choosing to place any reliance whatsoever on the CA Certificates. The CA Certificates are not a grant, assurance, or confirmation from Gjaldstovan of any authority, rights, or privilege save as expressly set out in this CPS or expressly set out in the CA Certificate.
Any person participating within the Samleikin PKI irrevocably agrees, as a condition to such participation, that the issuance of all products and services contemplated by this CPS shall occur and shall be deemed to occur in the Faroe Islands and that the performance of Gjaldstovan obligations hereunder shall be performed and be deemed to be performed in the Faroe Islands.

1.4.2 Prohibited Certificate Uses

CA Certificates may not be used, and no participation is permitted in Samleikin

- In circumstances that breach Relying Party Agreements or CA Certificate Holder Agreements
- In circumstances that breach, contravene, or infringe the rights of others
- In circumstances that offend, breach, or contravene any applicable law, statute, regulation, order, decree, or judgment of a court of competent jurisdiction or governmental order
- In connection with fraud, pornography, obscenity, hate, defamation, harassment, or other activity that is contrary to public policy.

No reliance may be placed on the CA Certificates and the CA Certificates may not be used in circumstances

- where applicable law or regulation prohibits their use;
- in breach of this CPS or the relevant CA Certificate Holder or Relying Party Agreement;
- in any circumstances where the use of the CA Certificate could lead to death, injury, or damage to property; or
- as otherwise may be prohibited by the terms of issue.

1.5 Policy Administration

1.5.1 Organisation adminstering the document

This CPS is regularly reviewed and approved by Gjaldstovan.

1.5.2 Contact person

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

Or:

TSP@gjaldstovan.fo

1.5.3 Person determining CPS suitability for the policy

The Gjaldstovan TSP Management Board

1.5.4 CPS approval procedures

Notice of proposed changes are recorded in the change log at the beginning of this CPS until they are approved, at which time the approved change will be recorded there permanently. Any changes to this CPS must be approved by the Gjaldstovan TSP Management Board.

1.6 Definitions and Acronyms

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

CA - Certification Authority
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.
EAL - Evaluation Assurance Level
OCSP - Online Certificate Status Protocol
OID - Object IDentifier
PDS - PKI Disclosure Statement
PIN - Personal Identification Number
PKI - Public Key Infrastructure
RA - Registration Authority
RAP - Registration Authority Policy
RAPS - Registration Authority Practice Statement
RPA - Relying Party Agreement
TSP - Trust Service Provider
UTC - Coordinated Universal Time

2 Publication and Repository Responsibilities

2.1 Repositories

The Samleikin repository https://repository.samleiki.fo/legal-repository serves as the primary repository. This repository holds CPs,CPSs,RAP:s, and RPA. The related repositories are as follows:

- CPSs - https://repository.samleiki.fo/legal-repository
- RAP:s -https://repository.samleiki.fo/legal-repository
- RPA - https://repository.samleiki.fo/legal-repository
- CA Certificate Holder Agreements - https://repository.samleiki.fo/legal-repository
- Certificate profiles - https://repository.samleiki.fo/profiles
- CA certificates - https://repository.samleiki.fo/legal-repository
- Terms and conditions for end users
- Revoked certificates
    - Root CA1 v1 CRL - http://crl.samleiki.fo/Faroe-Islands-RootCA1-v1.crl
    - Root CA1 v1 OCSP - http://ocsp.samleiki.fo/ocsp
    - Issuing CA1 v1 CRL - http://crl.samleiki.fo/Faroe-Islands-IssuingCA1-v1.crl
    - Issuing CA1 v1 OCSP - http://ocsp.samleiki.fo/ocsp
    - Issuing CA2 v1 CRL - http://crl.samleiki.fo/Faroe-Islands-IssuingCA2-v1.crl
    - Issuing CA2 v1 OCSP - http://ocsp.samleiki.fo/ocsp

2.2 Publication of Certification Information

Public audit reports are published at https://repository.samleiki.fo/legal-repository.

This CPS is published electronically at https://repository.samleiki.fo/legal-repository.

2.3 Time or Frequency of Publication

Newly approved versions of this CPS, CA Certificate Holder or Relying Party Agreements and other relevant documents are published in accordance with the amendment, notification and other relevant provisions contained within those documents. Information about amendments to this CPS may be found in Section 9.12. Certificate information is published promptly following generation and issue and immediately following the completion of the revocation process.

2.4 Access Controls on Repositories

Read-only access to repositories is available to Authorized Relying Parties 24/7, except for reasonable maintenance requirements, where access is deemed necessary. Queries to the repository must specify individual certificate information. The CA is the only entity that has write access to repositories. I nternal documents not published at https://repository.samleiki.fo/legal-repository are available only to participants in Samleikin where deemed necessary.

3 Identification and Authentication

The Root CA implements rigorous authentication requirements to ensure that the identity of the CA Certificate Holder is proven. This includes physical identity verification at the beginning of the CA Certificate request procedure or at some point prior to CA Certificate delivery to the CA Certificate Holder.

3.1 Naming

3.1.1 Types Of Names

All CA Certificate Holders require a distinguished name that is in compliance with the X.500 standard for distinguished names. The Root CA approves naming conventions for the creation of distinguished names for Issuing CAs applicants. Different naming conventions may be used by different Issuing CAs. The subject name of all CA Certificates issued to Individuals shall be the authenticated common name of the CA Certificate Holder. The distinguished name fields are fully disclosed in: https://repository.samleiki.fo/profiles.

.

3.1.2 Need For Names To Be Meaningful

Distinguished names must be meaningful, unambiguous and unique. The Root CA supports the use of CA Certificates as a form of identification within a particular community of interest. The contents of the CA Certificate subject name fields must have a meaningful association with the name of the individual, organization, or device. In the case of organizations, the name shall meaningfully reflect the legal name or registered domain name of the organization or the trading or business name of that organization. In the case of a device, the name shall state the name of the device and the legal name or registered domain name of the organization responsible for that device.

3.1.3 Anonymity or Pseudonymity of Subscribers

Anonymous and pseudonymous CA Certificates are not permitted by this Root CA.

3.1.4 Rules For Interpreting Various Name Forms

Fields contained in CA Certificates are in compliance with this CPS and the certificate profiles are fully disclosed here: https://repository.samleiki.fo/profiles. In general, the rules for interpreting name forms can be found in International Telecommunication (ITU) and Internet Engineering Task Force (IETF) Standards, such as the ITU-T X.500 series of standards and applicable IETF RFCs.

3.1.5 Uniqueness Of Names

The Root CA shall approve distinguished names for applicants, and, as a minimum check that a proposed distinguished name is unique and verify that the name is not already used by a previously issued CA Certificate. The subject name of each issued CA Certificate shall be unique within each class of CA Certificate and shall conform to all applicable X.500 standards for the uniqueness of names.

The Root CA may, if necessary, insert additional numbers or letters to the CA Certificate Holder’s subject common name, or other attribute, in order to distinguish between two CA Certificates that would otherwise have the same subject name.

3.1.6 Recognition, Authentication And Role Of Trademarks

The Root CA is not obligated to seek evidence of trademark usage by any organization.

3.2 Initial Identity Validation

3.2.1 Method To Prove Possession Of Private Key

The Root CA shall establish that each applicant for a CA Certificate is in possession and control of the private key corresponding to the public key contained in the request for a Ca Certificate. From a technical perspective the Root CA shall do so in accordance with PKCS#10. The procedure is as follows for each Issuing CA, performed in a key ceremony approved by the Gjaldstovan TSP Management Board:

1. The Issuing CA Authorized Representative shall have a private/public Key Pair generated along with a PKCS#10 CSR.
2. The Issuing CA Authorized Representative shall store the private key on a Hardware Security Module.
3. The Issuing CA Authorized Representative shall present the PKCS#10 CSR to the Root CA Authorized Representative.
4. The Root CA verifies the signature of the CSR before issuing the CA Certificate.

3.2.2 Authentication of Organisation Identity

The Faroe Islands Root CA will not issue organisational certificates.

3.2.3 Authentication of Individual Identity

For the Root CA the initial identity validation consists of validating the identity and authorization of the authorized representative who represent the individual Issuing CAs. A representative of the Gjaldstovan TSP Management Board shall have the role of identity and authorization verifier of the Issuing C A Authorized Representative and shall perform the verification of the identity and of the authorization of the Issuing CA Authorized Representative to act on behalf of the Issuing CA. The procedure is as follows: the Issuing CA Authorized Representative shall provide physical identification papers, in the form of their passport from the kingdom of Denmark or a Danish or Faroese drivers license as proof of identity. The identity verification is documented in an identity verification form and stored in a safe location at Gjaldstovan.

3.2.4 Non-verified Subscriber Information

Not applicable for the Faroe Islands Root CA.

3.2.5 Validation of Authority

The Gjaldstovan TSP Management Board will decide on authority for applicants of CA Certificates.

3.2.6 Criteria for Interoperation

Gjaldstovan may provide interoperation services to certify a non-Gjaldstovan CA, allowing it to interoperate with the Samleikin PKI. In order for such interoperation services to be provided the following criteria must be met:

- Gjaldstovan will perform due diligence on the CA;
- A formal contract must be entered into with Gjaldstovan, which includes a ‘right to audit’ clause; and
- The CA must operate under a CPS that is approved by the Gjaldstovan TSP Management Board

3.3 Identification and Authentication for Re-key Requests

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

3.3.1 Identification and Authentication for Routine Re-key

Not applicable for the Faroe Islands Root CA.

3.3.2 Identification and Authentication for Re-key after Revocation

Not applicable for the Faroe Islands Root CA.

3.4 Identification and Authentication for Revocation Requests

For the Root CA the identity validation for revocation requests consists of validating the identity of the authorized representative who represents the revocation request. A representative of the Gjaldstovan TSP Management Board shall have the role of identity verifier of the requesting party representative and shall perform the verification of the identity of the requesting party representative. The procedure is as follows: the requesting party repr esentative shall provide physical identification papers, in the form of their passport from the kingdom of Denmark or a Danish or Faroese drivers license as proof of identity. The identity verification is documented in an identity verification form and stored in a safe location at the TSP.

Revocation status information is available as defined in section 4.10 in this CPS.

4 Certificate Life-Cycle Operational Requirements

Certificate applications are subject to various assessment procedures depending upon the type of certificate applied for, as described in this chapter.

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Any registered organisation or legal entity is allowed to apply for a CA certificate. The Gjaldstovan TSP Management Board shall document and approve the application after necessary inspection. As such, the certificate application process will only be initiated once the Gjaldstovan TSP Management Board consider the applicant has met or is in a position to meet all relevant technical, financial, infrastructural, know-how, legal and regulatory requirements. The Gjaldstovan TSP Management Board, in its sole discretion, may refuse to accept an application for a CA Certificate, without incurring any liability for loss or damages arising out of such refusal.

4.1.2 Enrollment Process and Responsibilities

All signed applications shall be securely stored for the lifetime of the issued CA Certificates (or until the Issuing CA is terminated for some reason) in a safe approved by Gjaldstovan TSP Management Board.

An application in a form prescribed by the applicant Issuing CA must be completed by applicants, which includes all registration information as described by this CPS (including, without limitation, that information set out in https://repository.samleiki.fo/profiles) and the CA Certificate Holder Agreement. All applications are subject to review and approval, and acceptance by the Gjaldstovan TSP Management Board at its sole discretion. The CA Certificate application for each Issuing CA is such that the applicant Issuing CA authorized representative shall provide a signed CA Certificate application to the Gjaldstovan TSP Management Board, which includes identifying information to assist the Gjaldstovan TSP Management Board in processing the request and issuing the certificate, along with a PKCS#10 CSR.

The Issuing CA's Key Pair is never generated by the Root CA and the CA Certificate request process shall check that the Issuing CA has possession or control of the private key associated with the public key presented for certification, as described in section 3.2.

The following steps are required in any application for a CA Certificate:

1. Identity of the Holder or Device is to be established in accordance with section 3.2.
2. A Key Pair to a CA Certificate application and its associated certificate is to be generated and stored in a secure fashion on a approved Hardware Security module, certified to FIPS 140-2 level 3 or higher or Common Criteria EAL 4+.
3. The binding of the Key Pair to the certificate shall occur as set forth in this CPS in section 3.2.
4. The Issuing CA shall be in contractual relations - in form of a signed CA Certificate Holder Agreement - with the Gjaldstovan TSP Management Board for the use of that CA Certificate, acting as Issuing CA.

4.2 Certificate Application Processing

4.2.1 Performing Identification And Authentication Functions

The Gjaldstovan TSP Management Board shall have the role of identity and ID document authenticity and validity verifier and shall perform and document the verification of the identity of the applicant Issuing CA authorized representative. The procedure is as follows for each applicant Issuing CA:

1. The applicant Issuing CA authorized representative shall provide physical identification papers, in the form of a passport from the kingdom of Denmark or a Danish or Faroese Drivers License as proof of identity.
2. The identity and ID paper authenticity verifier shall independently approve the correctness of identity and ID document authenticity of the Issuing CA authorized representative. If identification and ID document authenticity succeeds the procedure continues, otherwise the procedure is termina ted and an investigation is initiated to determine the reason and course of action to take.
3. When the applicant Issuing CA authorized presentative's identity is validated successfully, the applicant can move on to next step in the process regarding the CA Certificate issuance, see section below.

4.2.2 Approval Or Rejection Of Certificate Applications

The Gjaldstovan TSP Management Board will at sole discretion approve or reject CA Certificate applications based upon the applicant meeting the requirements of this CPS and the Certificate Profiles used https://repository.samleiki.fo/profiles and being a suitable entity for participation in the Samleikin PKI.

The Gjaldstovan TSP Management Board, in its sole discretion, may refuse to accept an application for a CA Certificate or for the renewal of a CA Certificate, and may refuse to issue a CA Certificate, without incurring any liability for loss or damages arising out of such refusal.

The Gjaldstovan TSP Management Board reserves the right not to disclose reasons for such a refusal.

4.2.3 Time To Process Certificate Applications

The Gjaldstovan TSP Management Board must process the CA Certificate applications within 60 working days. Note that this only applies to the Root CA - sub CAs can define their own time to process certificate applications in their CPSes.

4.3 Certificate Issuance

Issuing a CA Certificate is the Root CAs acceptance of a CA Certificate application from the Gjaldstovan TSP Management Board. The issuance of a CA Certificate means that the Root CA accepts the application and the applicant information that the applicant has declared.

Any key management operation is conducted as part of a key ceremony approved by Gjaldstovan TSP Management Board.

4.3.1 CA Actions During Certificate Issuance

The Root CA only issues CA certificates as specified by approved certificate profiles. These are located here: https://repository.samleiki.fo/profiles and these are:

- Issuing CA1 and OCSP response signing certificate profile:
  - Faroe Islands IssuingCA1 v1
- Issuing CA2 and OCSP response signing certificate profile:
  - Faroe Islands IssuingCA2 v1

The Root CA has the following measures in place to prevent forgery of certificates:

- Physical access to the infrastructure is granted on a four eyes principle. That is at least two trusted persons with authorization need to be present to perform changes on the infrastructure.
- Logical access to cryptographic modules are always secured using both software and hardware token.
- Each custodian of PINs and hardware tokens store these artifacts on site in safes with single access control. The PINs and hardware tokens cannot be stored in the same safe or in different safes where the same person have access.
- The Root CA key never leaves its appointed crypto modules and can't be exported outside its appointed crypto modules.

Over the life time of the CA, its distinguished name which has been used in its certificate will never be re-assigned to another entity. Also when renewing the CA certificate the distinguished name shall reflect that renewal by using a new distinguished name in the new CA certificate.

Faroe Islands RootCA1 v1

The Root CA Certificate has been self-generated and self-signed according in strictly controlled and audited key ceremonies that are approved by Gjaldstov an TSP Management Board and audited by an accredited external auditor.

The Root CA never generates another CAs Key Pair.

The Root CA Key Pairs are generated on behalf of the Root CA.

Samleikin CA Certificates

Upon accepting the terms and conditions of the CA Certificate Holder Agreement by the Issuing CA, successful completion of the Issuing CA application process as prescribed by Gjaldstovan TSP Management Board, the Root CA issues the CA Certificate to the relevant Issuing CA.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The Root CA does in-person notification to applicants when CA Certificates have been issued.

4.4 Certificate Acceptance

When a CA Certificate is accepted, it is published in the Samleikin PKI repository. This CPS sets out what constitutes acceptance of a CA Certificate. An applicant that accepts a CA Certificate warrants to the Root CA, and all Authorised Relying Parties who reasonably rely, that all information supplied in connection with the application process and all information included in the CA Certificate issued to them is true, complete, and not misleading. Without limitation to the generality of the foregoing, the use of a CA Certificate or the reliance upon a CA Certificate signifies acceptance of the terms and conditions of this CPS and CA Certificate Holder Agreement (as the same may, from time to time, be amended or supplemented) by which they irrevocably agree to be bound.

By accepting a CA Certificate, the CA Certificate Holder expressly represents and warrants to the Root CA and all Authorized Relying Parties who reasonably rely on the information contained in the CA Certificate that at the time of acceptance and throughout the operational period of the CA Certificate, until notified otherwise by the CA Certificate Holder, that:

- No unauthorised party has ever had access to the CA Certificate Holder's private key
- All representations made by the CA Certificate Holder regarding the information contained in the CA Certificate are true
- All information contained in the CA Certificate is true to the extent that the CA Certificate Holder had knowledge or notice of such information, and does promptly notify the Root CA of any material inaccuracies in such information
- The CA Certificate is being used exclusively for authorised and legal purposes, consistent with this CPS

Before any CA Certificate is issued, the Gjaldstovan TSP Management Board shall require the CA Certificate Holder of the terms and conditions related to the CA Certificate and require the CA Certificate Holder to enter in a contractual relationship by signing the CA Certificate Holder Agreement https://repository.samleiki.fo/legal-repository. As part of this CA Certificate Holder Agreement the CA Certificate Holder shall be informed of the obligations associated with the CA Certificate.

The Gjaldstovan TSP Management Board shall for the lifetime of the Samleikin PKI record all the signed agreements with the CA Certificate Holders in safe storage.

4.4.1 Conduct Constituting Certificate Acceptance

The CA Certificate Holder is responsible for installing the issued CA Certificate on the CA Certificate Holder’s system environment. A CA Certificate Holder is deemed to have accepted a CA Certificate when:

- The CA Certificate Holder downloads, installs, or otherwise takes delivery of the CA Certificate.
- The CA Certificate Holder fails to notify the Gjaldstovan TSP Management Board that the CA Certificate is not accepted within 10 working days.

4.4.2 Publication of the Certificate by the CA

All CA Certificates are made available here: https://repository.samleiki.fo/legal-repository

4.4.3 Notification of Certificate Issuance by the CA to other Entities

Issuing CAs within Samleikin PKI may choose to notify other entities of CA Certificate issuance.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key And Certificate Usage

Within Samleikin PKI, a CA Certificate Holder may only use the private key and corresponding public key in a CA Certificate for their lawful and intended use. The CA Certificate holder accepts the CA Certificate Holder Agreement and by accepting the CA Certificate unconditionally agrees to use the CA Certificate in a manner consistent with the key-usage field extensions included in the certificate profile of the issued CA Certificate.

All issued CA Certificates must use an algorithm for its associated Key Pair that is specified on the CA Certificate profile of every issued CA Certificate**.** All Key Pairs must be generated by a cryptographic device that meets the requirements dictated by the CA Certificate profile in question. Private keys shall only be stored and used within cryptographic modules that are explicitly approved for the CA Certificate profile in question. These profiles are available at https://repository.samleiki.fo/profiles.

Every CA Certificate Holder shall without any reasonable delay notify The Gjaldstovan TSP Management Board if any of the following occur up to the end of the validity period indicated in the CA Certificate:

- The CA Certificate Holders private key has been lost, stolen, potentially compromised
- Control over the subject's private key has been lost due to compromise of activation data or other reasons
- Inaccuracy or changes to the CA Certificate content

Following a compromise of a CA Certificate Holder private key, the use of that subject's private key is immediately and permanently discontinued by revoking the CA Certificate associated with such a private key.

4.5.2 Relying party Public Key And Certificate Usage

In order to be an Authorised Relying Party, a party seeking to rely on a CA Certificate agrees to and accepts the Relying Party Agreement, https://repository.samleiki.fo/legal-repository, by querying the existence or validity of or by seeking to place or by placing reliance upon a CA Certificate. Authorised Relying Parties are obliged to seek further independent assurances before any act of reliance is deemed reasonable and at a minimum must assess:

- The appropriateness of the use of the CA Certificate for any given purpose and that the use is not prohibited by this CPS
- That the CA Certificate is being used in accordance with its Key-Usage field extensions
- That the CA Certificate is valid at the time of reliance by reference to Online Certificate Status Protocol or certificate revocation list checks.

4.6 Certificate Renewal

Certificate renewal means the issuance of a new certificate without changing the Key-pair. Samleikin does not support certificate renewal for end entity (non-CA) certificates or CA-certificates.

4.6.1 Circumstance for certificate renewal

All forms of certificate renewal is forbidden under this CPS.

4.6.2 Who may request renewal

All forms of certificate renewal is forbidden under this CPS.

4.6.3 Processing certificate renewal requests

All forms of certificate renewal is forbidden under this CPS.

4.6.4 Notification of new certificate issuance to subscriber

All forms of certificate renewal is forbidden under this CPS.

4.6.5 Conduct constituting acceptance of a renewal certificate

All forms of certificate renewal is forbidden under this CPS.

4.6.6 Publication of the renewal certificate by the CA

All forms of certificate renewal is forbidden under this CPS.

4.6.7 Notification of certificate issuance by the CA to other entities

All forms of certificate renewal is forbidden under this CPS.

4.7 Certificate Re-key

Certificate Re-Key is when all the identifying information from a certificate is duplicated in a new certificate, but there is a different public key and a different validity period. All forms of certificate re-keying is forbidden under this CPS.

4.7.1 Circumstance for certificate re-key

All forms of certificate re-key is forbidden under this CPS.

4.7.2 Who may request certification of a new public key

All forms of certificate re-key is forbidden under this CPS.

4.7.3 Processing certificate re-keying requests

All forms of certificate re-key is forbidden under this CPS.

4.7.4 Notification of new certificate issuance to subscriber

All forms of certificate re-key is forbidden under this CPS.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

All forms of certificate re-key is forbidden under this CPS.

4.7.6 Publication of the re-keyed certificate by the CA

All forms of certificate re-key is forbidden under this CPS.

4.7.7 Notification of certificate issuance by the CA to other entities

All forms of certificate re-key is forbidden under this CPS.

4.8 Certificate Modification

Certificate Modification refers to the issuance of a new certificate due to changes in the information in an existing certificate other than its associated public key.

The Root CA may reissue or replace a valid CA certificate when the CA Certificates common name, organization name, device name, or geographic location changes. Modified information must undergo the same identification and authentication procedures as for a new CA Certificate.

CA Certificate modification requests are processed in the same manner as requests for new CA Certificates and in accordance with the provisions of this CPS. As such CA Certificate modification is effectively a new CA Certificate.

4.8.1 Circumstance for certificate modification

CA Certificate modification requests are processed in the same manner as requests for new CA Certificates and in accordance with the provisions of this CPS. As such CA Certificate modification is effectively a new CA Certificate.

4.8.2 Who may request certificate modification

CA Certificate modification requests are processed in the same manner as requests for new CA Certificates and in accordance with the provisions of this CPS. As such CA Certificate modification is effectively a new CA Certificate.

4.8.3 Processing certificate modification requests

CA Certificate modification requests are processed in the same manner as requests for new CA Certificates and in accordance with the provisions of this CPS. As such CA Certificate modification is effectively a new CA Certificate.

4.8.4 Notification of new certificate issuance to subscriber

CA Certificate modification requests are processed in the same manner as requests for new CA Certificates and in accordance with the provisions of this CPS. As such CA Certificate modification is effectively a new CA Certificate.

4.8.5 Conduct constituting acceptance of modified certificate

CA Certificate modification requests are processed in the same manner as requests for new CA Certificates and in accordance with the provisions of this CPS. As such CA Certificate modification is effectively a new CA Certificate.

4.8.6 Publication of the modified certificate by the CA

CA Certificate modification requests are processed in the same manner as requests for new CA Certificates and in accordance with the provisions of this CPS. As such CA Certificate modification is effectively a new CA Certificate.

4.8.7 Notification of certificate issuance by the CA to other entities

CA Certificate modification requests are processed in the same manner as requests for new CA Certificates and in accordance with the provisions of this CPS. As such CA Certificate modification is effectively a new CA Certificate.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

CA Certificates shall be revoked when any of the information on a CA Certificate changes or becomes obsolete or when the private key associated with the CA Certificate is compromised or suspected to be compromised. A CA Certificate will be revoked in the following instances upon notification of:

- CA key compromise
- CA Certificate creation error
- Key compromise including unauthorized access or suspected unauthorized access to private keys, lost or suspected lost keys, stolen or suspected stolen keys, destroyed or suspected destroyed keys or superseded by replacement keys and a new CA Certificate
- The CA Certificate Holder has failed to meet his, her or its obligations under this CPS or any other agreement, regulation, or law that may be in force with respect to a particular certificate
- The CA Certificate was not issued in accordance with the terms and conditions of this CPS or the CA Certificate Holder provided inaccurate, false or misleading information
- The private key corresponding to a CA Certificate has been used to sign, publish or distribute spyware, trojans, viruses, rootkits, browser hijackers, or other content, for phishing, or conduct that is harmful, malicious, hostile or to download malicious content onto a system without consent
- The CA Certificate Holder is operating from a prohibited destination, which is any destination outside of the Faroe Islands (notice that this only applies for CA operations, not e.g. Registration Authorities)
- Where a CA Certificate Holder requests revocation because:
    - A change in the relationship between the CA Certificate Holder and the Root CA
    - The CA Certificate Holder is no longer authorized to act as a CA Certificate Holder
    - The CA Certificate Holder otherwise becomes unsuitable or unauthorized to hold the CA Certificate
- Affiliation change
- Cessation of operation
- Incorrect information contained in a CA Certificate
- CA Certificate Holder bankruptcy
- CA Certificate Holder liquidation
- Breach of CA Certificate Holder Agreement with the Gjaldstovan TSP Management Board
- Any of the information appearing in a CA Certificate is inaccurate or misleading
- The Root CA obtains reasonable evidence that there has been loss, theft, modification, unauthorized disclosure, or other compromise of the private key corresponding to the public key within the certificate, or that the certificate has otherwise been misused
- The Root CA receives notice or otherwise becomes aware that a CA Certificate Holder has breached a material obligation under the CA Certificate Holder Agreement or other contractual obligations
- The Gjaldstovan TSP Management Board receives a lawful and binding order from a government or regulatory body to revoke the CA Certificate
- The Gjaldstovan TSP Management Board determines, in its sole discretion, that the CA Certificate was not issued in accordance with the terms and conditions of this CPS
- The Gjaldstovan TSP Management Board receives notice or otherwise becomes aware that there has been some other modification of the information pertaining to the CA Certificate Holder that is contained within the CA Certificate
- The CA Certificate Holder fails or refuse to comply, or to promptly correct inaccurate, false or misleading information after being made aware of such inaccuracy, misrepresentation or falsity
- Either the CA Certificate Holder's or the Root CA:s obligations under this CPS are delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond reasonable control, and as a result another entity is threatened or compromised
- The technical content or format of the CA Certificate presents an unacceptable risk to Authorized Relying Parties (a deprecated cryptographic /signature algorithm or key size presents an unacceptable risk and that such CA Certificates should be revoked and replaced as soon as reasonably practical upon notification)

The CA Certificate Holder of a revoked CA Certificate, shall be informed of the change of status of the CA Certificate. In the case of the Root CA, Gjaldstovan TSP Management Board shall notify the Issuing CAs representative immediately when the decision is made that the CA Certificate is to be revoked. Furthermore the Gjaldstovan TSP Management Board shall immediately inform the Issuing CAs representative when there is suspicion of the integrity of the CA Certificate.

A revoked CA Certificate is indefinitely revoked and will never be reinstated.

4.9.2 Who Can Request Revocation

The following entities may request revocation of a CA Certificate:

- The Gjaldstovan TSP Management Board, representing the Root CA, may revoke any CA Certificate issued at its sole discretion, and shall publish the list of revoked CA Certificates in a publicly accessible certificate revocation list status service
- A CA Certificate Holder may request revocation of its CA Certificates

4.9.3 Procedure For Revocation Request

The Gjaldstovan TSP Management Board, representing the Root CA, will revoke a CA Certificate upon receipt of a valid request and after approval by the Gjaldstovan TSP Management Board. A revocation request should be promptly and directly communicated to the Gjaldstovan TSP Management Board. The CA Certificate Holder is required to submit the revocation request in person without any reasonable delay.

The Gjaldstovan TSP Management Board maintains a continuous 24/7 ability to respond to any high priority CA Certificate problem report and will take such action as deemed appropriate based on the nature of such a report.

4.9.4 Revocation Request Grace Period

No grace period is permitted once a revocation request has been verified. The Root CA will revoke CA Certificates as soon as reasonably practical following verification of a revocation request.

4.9.5 Time Within Which CA Must Process The Revocation Request

The Gjaldstovan TSP Management Board will begin investigation of a CA Certificate problem report as soon as reasonably practical after its receipt. The Gjaldstovan TSP Management Board shall take reasonable steps to revoke the CA Certificate as soon as reasonably practical after receipt of a valid revocation request.

4.9.6 Revocation Checking Requirement for Relying Parties

Prior to trusting a CA Certificate, it is the Authorized Relying Party's responsibility to check the status of all CA Certificates in the certificate validation chain against the current CRL's or on-line certificate status service (OCSP). A CA Certificate cannot be reasonably relied on if the Authorized Relying Party does not diligently follow the CA Certificate status checking procedures denoted below:

- A Authorized Relying Party shall ensure itself of the authenticity and integrity of the CRLs or on-line certificate status responses by checking the digital signature and the certification path related to it
- The Authorized Relying Party shall also check the validity period of the CRL and OCSP response in order to make sure that the information in the CRL or OCSP response is up-to-date
- CA Certificates may be stored locally by the Authorized Relying Party, but the prevailing revocation status of each of those CA Certificates shall be checked before use
- If valid CA Certificate status information cannot be obtained because of a system or service failure, not a single CA Certificate shall be trusted. The acceptance of a CA Certificate in violation of this condition befalls at the Authorized Relying Party's own risk

4.9.7 CRL Issuance Frequency

The revocation status service is implemented by publishing Certificate Revocation Lists (CRLs), digitally signed by the Root CA, as described section 2.1.

The Root CA must comply to the following:

- A new CRL is published at intervals of not more than 10 months
- The validity time of every CRL is 1 year

There may be several valid CRLs available at the same time. The one of those, which has been published as the latest, contains the most updated information.

4.9.8 Maximum Latency For Certificate Revocation List

The maximum publication latency for the CA Certificate revocation lists is 8 hours.

4.9.9 On-Line Revocation/Status Checking Availability

The Root CA provides Online Certificate Status Protocol (OCSP) checking. The URL for the OCSP responder may be found within the Authority Information Access extension of issued certificates.

OCSP services will, at least, every month update its revocation information by checking the current CRL for the Root CA.

4.9.10 On-Line Revocation Checking Requirements

The validity of a CA Certificate can be checked online using the appropriate certificate revocation list or using the appropriate Online Certificate Status Protocol responder. Failure to do so negates the ability of the Authorized Relying Party to claim that it acted on the CA Certificate with reasonable reliance.

The Root CA supports an OCSP capability using the GET method for certificates. If the OCSP responder receives a request for status of a CA Certificate that has not been issued, then the responder will not respond with a "good" status.

OCSP requests may be unsigned or signed. All responses will be signed by a private key corresponding to a public key certified by the Root CA on which the OCSP request is made.

4.9.11 Other Forms Of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements Re Key Compromise

Should a private key become compromised, the related CA Certificate shall be revoked pending TSP Management Board decision.

4.9.13 Circumstances For Suspension

No suspension of CA Certificates is permissible by the Root CA.

4.9.14 Who Can Request Suspension

No suspension of CA Certificates is permissible by the Root CA.

4.9.15 Procedure For Suspension Request

No suspension of CA Certificates is permissible by the Root CA.

4.9.16 Limits On Suspension Period

No suspension of CA Certificates is permissible by the Root CA.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The status of CA Certificates issued by the Root CA is published in a Certificate Revocation List http://crl.samleiki.fo or is made available via Online Certificate Status Protocol checking http://ocsp.samleiki.fo where available. Revocation entries on a CRL or OCSP response are not removed until after the expiry date of a revoked CA Certificate. The integrity and authenticity of CRL:s is ensured by the Root CA by signing CRL:s with a key in sole possession by the Root CA. The integrity and authenticity of OCSP responses is ensured by the Root CA by signing OCSP responses with a key in sole possession by the OCSP responder.

4.10.2 Service Availability

Certificate status services are available 24 hours a day, 7 days a week, 365 days of the year on http://ocsp.samleiki.fo

4.10.3 Optional Features

Online Certificate Status Protocol is available for all CA Certificates issued by the Root CA. The time used for the provision of revocation services shall be synchronized with UTC on every start of the Root CA system, and every 12 hours, by having an authoritative time source (GPS-bound) with time slaves synching to the firewalls, and then then sync all services with its nearest upstream firewall.

4.11 End of Subscription

A CA Certificate Holder may end a subscription by:

- Allowing a CA Certificate to expire
- Revoking a CA Certificate

4.12 Key Escrow and Recovery

All forms of key escrow and private key recovery of CA Certificate Holders private keys are forbidden for CA Certificates issued by this Root CA.

5 Facility, Management, and Operational Controls

This section describes in general terms how Gjaldstovan meets the requirements set in the CP, regarding non-technical controls (physical, procedural, and personnel), to securely perform the functions related to the root key.

5.1 Physical Controls

Risk Assessment

There are risk assessments for the Root CA environment as a whole and special risk assessments for critical parts.

The risk assessments are reviewed regularly; when significant changes are introduced to the risk picture, and when major changes are made to the Root CA system.

The Gjaldstovan TSP Management Board approves the risk assessments and accepts residual risks identified.

Asset Management

Asset management is in place for all parts of the Root CAs system, and a system, a policy, procedures and controls are in place to ensure the correctness of the content.

Physical and Environmental Security

Physical protection is in place for all critical parts of the Root CAs system.

Root CA private keys

The Root CAs private keys are held physically isolated from normal operations in an offline environment. Backup to the Root CAs regular private keys are held in an offline HSM backup unit which is kept in a safe. The safe is only accessible by authorized individuals. There are multiple control measure in the form of multiple roles with different accesses to different assets, physical and logical keys and PIN:s, which only in combination can grant access to the root keys.

5.1.1 Site Location and Construction

The operation is running from two secure buildings located in Tórshavn, Faroe Islands.

Main data center

The main data center is located in the main building itself, built for the purpose.

The building has appropriate location and construction measures.

Backup data center

The building has appropriate location and construction measures.

Engineering building

The building has appropriate location and construction measures.

5.1.2 Physical Access

During normal office hour there is access to a public area, access to all other areas is restricted. Outside normal office hours, all access to the premises is restricted.

The access to sensitive areas is managed strictly, only authorized individuals have access.

All employees have access to other areas. Visitors to semi-sensitive areas must be signed in and have a visible badge.

Main data center

Before physical accesses are granted to employees, they must have a work-related need, have signed a duty of confidentiality, a background check has been made and a relevant manager has approved the access.

The access is managed with an electronic system. You have to have an access card and use a pin-code to get access to the main data center.

Every access is logged and comings and goings are documented on the video for the data center.

There are only a few secure manual keys to use in emergency.

Furthermore, all equipment and data, which are a part of the TSP solution, are located in special secure racks, equipped with double locks, burglary alarms and video.

There must be two employees in trusted roles present, to get access inside the special secure rack.

Visitors:

- Some regular visitors have a permanent access. They have signed a confidential agreement.
- Some not so regular visitors will be followed to the data center and then left alone. They have signed a confidential agreement.
- Visitors that not have signed at confidential agreement will be accompanied at all times.

Backup data center

Before physical accesses are granted to employees they must have a work-related need, have signed a duty of confidentiality, a background check has been made and a relevant manager have approved the access.

Access is managed with two manual locks on the door to the backup room, which require two different keys, which are held by two different authorized emp loyees.

There is a burglary alarm connected to the room.

Furthermore, all equipment and data, which are a part of Samleikin, are located in special secure racks, equipped with double locks, burglary alarms and video.

There must be two authorized employee present, to get access inside the special secure rack.

Visitors:

- Some regular visitors have a permanent access. They have signed a confidential agreement.
- Some not so regular visitors will be followed to the data center and then left alone. They have signed a confidential agreement.
- Visitors that not have signed at confidential agreement will be accompanied at all times.

Engineering building

Before physical accesses are granted to employees or visitors they must have a work-related need, and a relevant manager has approved the access.

Access is managed with a manual lock on the outer door.

Only a few employees and visitors hold a key.

5.1.3 Power and air conditioning

To protect against unexpected power loss both data centers are equipped with a no-break system and in case of a long time power loss a generator is in place.

The main data center and the engineering building has a cooling system, which blows air through the room.

The cooling of the backup data center is with a standard compressor type system.

There are backup systems for the primary cooling.

5.1.4 Water Exposures

The main data center, the backup data center and the engineering building have concrete wall on the side where a water hazard could occur; furthermore, the buildings are on a hillside, with practically no risk for exposure to water.

The main data center and the engineering building is also equipped with raised floors and drainage.

5.1.5 Fire Prevention and Protection

The main data center and the engineering building are equipped with a fire alarm system with direct connection to the fire station.

The main data center and the engineering building are also equipped with an automatic gas based fire extinguishing system, that will prevent damage to the equipment in case of fire and when the system puts out fires.

There are handheld extinguisher in both data centers and in the engineering building.

The fire station is only a few minutes away.

5.1.6 Media Storage

Media related to CA operations are inside special secure racks and will not be removed except for destruction.

The special secure racks are placed in the data center and have burglar alarms, the secure racks rely on the fire protection of the room they are located in.

The secured rack are certified by the LPCB to LPS 1214 Security Category 2, and CPNI approved.

Some assets are in other secure safes e.g. root HSM:s, the Root CA computer and the activation keys for the HSM;s.

There is a strict procedure in place to get access to media, which involves at least two trusted persons.

5.1.7 Waste Disposal

Media (paper or magnetic) that can contain sensitive information are disposed in a secure manner.

- Magnetic discs are destroyed by crushing them in a die with over 20 tons.
- Magnetic tapes are not used
- Other magnetic media are destroyed by crushing them either by a sledge or by crushing them in a die with over 20 tons
- Printed material are cross-cut shredded in line with DIN-66399 P4

5.1.8 Off-site Backup

All components in the CA environment have their own backup profile assigned. The profile specifies how often backups shall be taken and for how long the backups will be stored.

When a backup has been taken, the data is first placed in backup storage. Within 24 hours the backup data will be copied to another special secure rack located in our backup data center. In that way there are always two copies at two different locations.

The backup system is continuously monitored.

The off-site backup is located in a secure rack in the backup data center.

5.2 Procedural Controls

Administrative processes are described in detail in standard operating procedures and other guidelines approved by the Gjaldstovan TSP Management Board.

All subordinate CAs are required to ensure that administrative procedures related to personnel and procedural requirements, and physical and technological security mechanisms, are maintained in accordance with this CPS and other relevant operational documents.

5.2.1. Trusted Roles

In order to ensure that one person acting alone cannot circumvent security safeguards, responsibilities are shared by multiple roles and individuals. This is accomplished by creating separate roles and accounts on the various components of the CA system, and each role has a limited amount of capability. This method allows a system of "checks and balances" to occur among the various roles. Oversight may be in the form of a person who is not directly involved in issuing certificates (e.g. a system auditor) examining system records or audit logs to ensure that other persons are acting within the realms of their responsibilities and within this CPS.

Gjaldstovan TSP Management Board has limited the system access by appointing only authorized individuals to trusted roles.

The categories of high level trusted roles in use are:

Security Officers: Overall responsibility for administering the implementation of the security practices.

System Administrators: Authorized to install, configure and maintain the CA environment for service management. This includes recovery of the system.

System Operators: Responsible for operating the CA environment on a day-to-day basis. System Operators are also authorized to perform system backup.

System Auditors: Authorized to view archives and audit logs of the CA environment.

HSM specific and other system specific trusted roles are implemented, with requirements set forth by Gjaldstovan TSP Management Board in regards to m of n and segregation of duties.

Only individuals appointed a trusted role by Gjaldstovan TSP Management Board are provisioned with access according to the specific tasks defined to that trusted role.

5.2.2. Number of Persons Required Per Task

The number of individuals required to perform a task is described in the internal documents governed by Gjaldstovan TSP Management Board, describing the different trusted roles.

At least two people are always assigned to each trusted role to ensure adequate support. Some roles are assigned to different people to ensure no conflict of interest occurs and to prevent the possibility of accidental or intentional compromise of any component of the CA infrastructure, most especially the Root CA and Issuing CA Private Keys.

CA Key Pair generation and initialisation of a Root CA or Issuing CA shall require the active participation of at least two trusted individuals in each case. Such sensitive operations also require the active participation and oversight of Gjaldstovan TSP Management Board.

Issuing CAs will utilize the physical, logical and administrative practices stated in this CPS to ensure that one person acting alone cannot circumvent safeguards.

Issuing CAs must ensure that no single individual may gain access to any Private Key (other than the CA Certificate Holders own Private Key). At a minimum, procedural or operational mechanisms must be in place for Issuing CA key recovery in disaster recovery situations. To best ensure the integrity of the CA equipment and operation, Issuing CAs will identify a separate individual for each trusted role.

All personnel authorized to access the system are accountable for their activities as event logs are retained and checked regularly.

Dual control for certificate generation

The implementation ensures that CA Certificate issuance by the Root CA can only be under at least dual control by authorized, trusted personnel such that one person cannot sign subordinate certificates on his/her own.

5.2.3 Identification and Authentication For Each Role

Persons filling trusted roles must undergo an appropriate security screening procedure, according to section 5.3.2 in this CPS.
Each individual performing any of the trusted roles shall use the identification and authentication mechanism specified for the specific trusted role in the internal documents to authenticate themselves.

5.2.4. Roles Requiring Separation of Duties

Operations involving Root Certificate and Issuing CA roles are segregated between M of N employees where M is equal to or greater than 2. (An M-of-N person control means there is a minimum “M” persons present out of a total “N” persons authorised to perform the task.) Creation and maintenance of system audit logs are segregated from those persons who operate such systems.

The internal documents governed by Gjaldstovan TSP Management Board, describe the different trusted roles containing information about segregation of duties for each type of trusted role.

5.3 Personnel Controls

Documented controls are implemented with all personnel that in any way are involved with the CA environment.

5.3.1 Qualifications, experience, and clearance requirements

Staff with roles in the CA environment have the necessary qualifications, expertise and clearances to fulfill their role.

In order to document and keep track of that CA employees maintain their qualifications, all relevant education and training are documented in their staff directory, with result if it is available.

All information gathered from employees is stored on a drive (Personnel Data Drive – PDD) with restricted access. The only people having access to this drive are the CEO and department managers.

An example of data stored on this drive are (not an exhaustive list):

- Signed NDAs
- Employee contracts
- Educational records
- CVs
- Criminal records
- Behavioral history

Every respective department manager is obliged to make sure that all documents related to his/her employees are up to date.

At least yearly Gjaldstovan:

- Controls that documentation is maintained to satisfaction
- Controls that qualifications are maintained to satisfaction
- Verify clearances

Job Descriptions

For each employee in a trusted role, there is a signed document in the staff folder containing at least:

- the name of the trusted employee, with civil registration number when allowed by Faroese law
- title of trusted role
- description of what tasks the role entails
- responsibilities for the employee in the trusted role
- from which date the responsibilities starts
- a signature from the employee with a date for signature
- a signature from the management with a date for signature

If an employee holds multiple trusted roles, there is a separate document for each role.

There is an outline of all employees in trusted roles, which also contain the title of the role.

When an employee in a trusted role stops being in the trusted role, it will be documented on the original document with:

- a text explaining that the employee no longer is in trusted role
- a date when the employee has stopped in this trusted role
- a signature from the management with a date for signature

Access to the systems and data

All access to the systems and data is granted with the principle of "least privilege" and all forms of data access is also in line with requirements from applicable laws and the outcome of the data classification.

Nobody is granted access before necessary checks are made, they are appointed by senior management and that a signed agreement exist with the person in the trusted role.

Everybody that is granted access to systems or data, have to comply with appropriate procedures in line with the Gjaldstovan TSP Management Board requirements.

5.3.2 Background check procedures

Necessary background checks are made for all personnel who have roles in the CA environment.

Some of the checks for new employee are:

- Relevant education
  The employee has to bring documentation on relevant education, and Gjaldstovan TSP Management Board checks the validity of the most important documents

- Criminal record statement
  The employee has to deliver a criminal record to Gjaldstovan TSP Management Board, which will be checked.
  Before employment, Gjaldstovan TSP Management Board will ask for a criminal record. The record will be sent directly from the relevant authority to a designated email address. A forwarded version from the person himself will not be accepted as valid.
  Criminal records will be required on a yearly basis, and the personnel them self will initiate this process.

- Previous employment
  The employee has to bring documentation on previous employment, which Gjaldstovan TSP Management Board will made relevant checks on

- Professional references
  A new employee has to deliver documentation on professional matters, and Gjaldstovan TSP Management Board will check the most important ones

- Impartiality
  All personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the Samleikin operations.
  Gjaldstovan TSP Management Board will by interview of the employee try to uncover if there is such a conflict of interest

For existing employee Gjaldstovan TSP Management Board will check relevant information and ask for more documentation if needed.

Where the above checks and confirmations cannot be obtained due to a prohibition or limitation of law or other circumstances, other available substitute investigation techniques permitted by law are used that provide similar information, including background checks performed by applicable Government agencies.

5.3.3 Training requirements

Personnel working in the CA environment, have received proper training and have adequate knowledge level.

Personnel in trusted roles meets additional requirements e.g.

- Security Officers
  Have extensive experience in general security, data protection rules and PII protection rules; they attend security courses and security conferences regularly, also will they be trained in the procedures and tools that they will use/be part of.
  Gjaldstovan TSP Management Board is responsible for defining, what security certification is valid and Gjaldstovan TSP Management Board facilit ate necessary education in special Samleikin matters.

- System Administrators
  Systems administrator are well versed in used software, in databases and other equipment related to the Samleikin environment.
  Gjaldstovan TSP Management Board facilitates necessary education in special Samleikin matters.

- System Operators
  Are very skilled at the systems they have to manage/operate, and have received an education and a documented procedure in how to run the system on a daily basis.
  Gjaldstovan TSP Management Board facilitate necessary education in special Samleikin matters.

- Internal Auditors

  Internal auditors that have experience from doing these types of audits, and must at least:

  - have a working knowledge about systems and data in the CA systems
  - have knowledge of the procedures used by the CA
  - know what to look for in archives and audit logs in the CA systems

- know what to look for as suspicious behavior

Gjaldstovan TSP Management Board facilitate necessary education in special Samleikin matters.

5.3.4 Retraining Frequency and Requirements

All personnel in trusted roles must maintain an adequate knowledge level. To ensure adequate knowledge level, there is a training plan for employees in trusted roles and Gjaldstovan TSP Management Board regularly controls that employees in trusted roles participate in necessary training. The Gjaldstovan TSP Management Board will provide and maintain a training program for every type of trusted role. Any training is tailored to every task performed by each respective trusted role, including tools, software and procedures in use by Samleikin.

Regularly and at least yearly, employees in trusted roles must attend a security awareness program, where the risk- and threat landscape and current security practices are among the subjects.

If important threats emerges, relevant employees in trusted roles will be formally informed without unnecessary delay.

5.3.5 Job rotation frequency and sequence

To avoid the issue with key persons, task rotation will be encouraged. For knowledge sharing the personnel holding the same roles, must rotate in performing the relevant tasks to maintain appropriate and required levels of competency across the trusted roles. This will be performed on a ‘best effort’ approach and will therefore not be formalized.

5.3.6 Sanctions for unauthorized actions

Sanctions are in place against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of entity systems.

These sanctions could for example be a warning, notice of discharge, or dismissal.

Every incident will be individually evaluated by appropriate parties to determine possible sanctions.

5.3.7 Independent contractor requirements

Gjaldstovan TSP Management Board does not support the use of independent contractors to fulfill trusted roles. Unless such independent contractors are regulated by a agreement with Gjaldstovan and are subject to the requirements stipulated by this CPS.

5.3.8 Documentation Supplied to Personnel

During initial training and retraining Gjaldstovan TSP Management Board provides personnel with the necessary material to perform their duties.

5.4. Audit Logging Procedures

5.4.1 Types Of Events Recorded

Whenever the Root CA is in use, it will be in a controlled ceremony where a protocol is kept for later audit.

When the Root CA is needed for specific planned events, personnel in trusted roles as key holders follow a strict procedure for accessing the safe containing the Root CA.

The following information will be logged for later audit:

CA key lifecycle management events;

- CA and Certificate lifecycle management events;
- Security events, including successful and unsuccessful PKI system access attempts;
- PKI and security system actions performed;
- Security profile changes;
- System crashes, hardware failures, and other anomalies;
- Entries to and exits from the CA facility.

Event logs include:

- Date and time of the entry
- Serial or sequence number of entry
- Details of the of entry
- Identity of the entity making the journal entry

5.4.2 Frequency Of Processing Log

Audit logs are verified and consolidated at least yearly, but also when starting up the Root CA system.

5.4.3 Retention Period For Audit Log

All Audit logs will be kept for the entire lifetime of Samleikin. For the offline root, the protocol and the log books kept in the safe will be archived for the entire lifetime of Samleikin.

5.4.4 Protection Of Audit Log

Only certain trusted roles have access to the log books and technical logs.

Only certain Trusted Roles and auditors may view audit logs in whole. The Gjaldstovan TSP Management Board decides whether particular audit records need to be viewed by others in specific instances and makes those records available, if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings.

Consolidated logs are protected from modification and destruction by beeing stored at a secure off-site location along with the root. Completed log books will be sealed in af tamper evident bag. The serial number of the TEB will be logged in the new log book.

All audit logs are protected in an encrypted format via a Key and Digital Certificate generated especially for the purpose of protecting the logs, and placed in off-site secure location.

5.4.5 Audit Log Backup Procedures

The protocols from key ceremonies will be kept on electronic media as well as in hard copy.

The Root workstation is connected to the Root CA and the logs are protected in an encrypted format via a Key and Digital Certificate generated especially for the purpose of protecting the logs, and placed in off-site secure location.

5.4.6 Audit Collection System (internal vs. external)

When the Root CA is in use, it will be as a part of a planned event with a manuscript for the procedures.

During the key ceremony a protocol will be kept containing all procedures involving the Root CA. This protocol will be stores securely as an audit log.

For the offline root, a handwritten log book is maintained at the secure location, and all entries are verified by four-eye principle.

The Root CA will collect all entries by people in trusted roles. These technical logs will be copied to electronic media, which will be placed in TEBs and stored at two off-site secure locations. 4 eyes principle is implemented in these procedures.

5.4.7 Notification To Event-Causing Subject

Automatic alerts will not apply for the offline root, since it will be stored in a restricted safe containing a handwritten log book.

All handlings of the Root CA will involve a setup of multiple participants overseeing the procedures.

5.4.8 Vulnerability Assessment

Periodic penetration tests and vulnerability scans are conducted by an external third party. The Gjaldstovan TSP Management Board also performs internal vulnerability assessments on a regular basis.

5.5 Records Archival

5.5.1 Types Of Records Archived

The Root CA archives, and makes available upon authorized request, documentation related to and subject to the Gjaldstovan TSP Management Board do cument access policy.

For each CA Certificate, the records contain information related to creation, issuance, intended use, revocation and expiration. These records will include all relevant evidence in the Root CA's possession including:

- Audit logs;
- Digital Certificate requests and all related actions;
- Contents of issued Digital Certificates;
- Evidence of Digital Certificate acceptance and signed CA Certificate Holder Agreements;
- Revocation requests and all related actions;
- Archive and retrieval requests;
- Digital Certificate Revocation Lists posted;
- Audit reports of the root CA

5.5.2 Retention Period For Archive

For the Root CA audit logs are retained as archive records for the entire lifetime of the Samleikin.

5.5.3 Protection Of Archive

Archives shall be retained and protected against modification or destruction. Only specific Trusted Roles, and auditors may view the archives in whole. The contents of the archives will not be released as a whole, except as required by law. The Gjaldstovan TSP Management Board may decide to release records of individual transactions upon request of any of the entities involved in the transaction or their recognized representatives.

All necessary hardware and software will be retained to protect against obsolescence.

5.5.4 Archive Backup Procedures

The Root CA maintains and implements backup procedures so that in the event of the loss or destruction of the primary archives a complete set of backup copies is readily available.

5.5.5 Requirements For Time-Stamping Of Records

All events that are recorded by the Root CA include the date and time of when the event took place. This date and time are based on the system time on which the CA system is operating. The Root CA uses procedures to review and ensure that all systems operating rely on a trusted time source.

5.5.6 Archive Collection System (internal or external)

The Root CA archive collection system is internal. The Gjaldstovan TSP Management Board provides assistance to operators of the Root CA to preserve their audit trails.

5.5.7 Procedures To Obtain And Verify Archive Information

Only specific Trusted Roles, and auditors may view the archives in whole. The contents of the archives will not be released as a whole, except as required by law. The Gjaldstovan TSP Management Board may decide to release records of individual transactions upon request of any of the entities involved in the transaction or their recognized representatives.

Archives are checked that they have not been altered since it was archived.

5.6 Key Changeover

Key changeover is not automatic, but procedures that enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of the CA Private Key's lifetime, the CA ceases using its expiring CA Private Key to sign Certificates (well in advance of expiration) and uses the old Private Key only to sign CRLs and OCSP responder Certificates associated with that key. A new CA signing Key Pair is commissioned and all subsequently issued Certificates and CRLs are signed with the new private signing key.

Validity period and operational period for certificates are shown in the table below:

CA	Validity Period	Operational period (Stop Issuance Date)
Faroese Root CA v1	20 years	20 years
Faroe Islands IssuingCA1 v1	10 years	7 years
Faroe Islands IssuingCA2 v1	10 years	7 years

At "Stop Issuance Date" CA stops issuing Certificates with the old key and must some time before that initiate generation of a new key pair. CA Key Changeover must be generated in a key-ceremony approved by Gjaldstovan TSP Management Board and witnessed by external auditor regarding the Root CA. For Issuing CAs it can be witnessed by either an external auditor or a Security Officer for the TSP. The new CA Certificate associated with the new public key is published in the Samleikin repository - while the old CA certificates will also be stored in the repository, but in a way that makes it clear that those are old and replaced. Certificate Requests received after the "Stop Issuance Date," will be signed with the new CA Private Key.

When renewing an issuing CA certificate, the Issuance CA will stop to use the old CA certificate and the old Key Pair, but will keep the old CA certificate in order to be able to sign an old CRL with the old Key Pair before it goes into retirement (end of validity period).

If there is need for a key changeover before the "Stop Issuance Date", for example because of key weakness etc., the CA Key Changeover must in the same way as above be generated in a key ceremony approved by Gjaldstovan TSP Management Board and witnessed by external auditor regarding the Root CA. For Issuing CAs it can be witnessed by either an external auditor or a Security Officer for the TSP. The new CA Certificate with the new public key is published in the Samleikin repository - while the old CA certificates will also be stored in the repository, but in a way that makes it clear that those are old and replaced.

Regarding the Root CA a key changeover results in setting up a new root CA, meaning setting up a new Root CA in a new PKI-hierarchy. This way it differs from issuing CAs where it is possible to renew with a new key as long as its parent root CA is active.

5.7 Compromise and Disaster Recovery

The Gjaldstovan TSP Management Board has:

- procedures for incident and compromise handling
- plans and procedures if Computing Resources, Software and/or Data are corrupted
- procedures for handling entity private key compromise
- a plan for Business Continuity Capabilities after a Disaster

The purpose of these procedures and plans are to handle incidents to restore core operations as quickly as practicable when systems and/or operations have been significantly and adversely impacted.

Gjaldstovan TSP Management Board regards these procedures and plans as proprietary, security-sensitive, and confidential. Accordingly, they are not intended to be made generally available.

In the Business Disaster and Continuity Plan there are procedures, that provides for the immediate continuation of certificate revocation services in the event of an unexpected emergency.

5.7.1 Incident and compromise handling procedures

There is constant monitoring of Gjaldstovan's assets e.g.

- Start up and shutdown of the logging function
- Availability and utilization of needed services within the Samleikin network.

There are regular reviews of relevant logs to identify evidence of malicious activity both by an automatic mechanism and with regular audits. If something unusual is found, the system will create an alarm that notifies relevant organizational units that will take appropriate action. Notification are sent to relevant parties if the auditor finds something unusual.

First level support then handles the common events. If this is beyond their capabilities the incident will be forwarded to second level support.

If second level support cannot handle the incident in a normal way, it will be handed to an incident manager.

The incident manager is in charge of the incident until the issue is resolved or forwarded to the Business Disaster and Continuity Team.

All security related incidents would be reported directly to an employee in a trusted role, who without unnecessary delay shall take action, including:

- discover the issue
- limit possible consequences
- notify relevant parties within 24 hours
- 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 natural or legal person will also be notified of the breach of security or loss of integrity without undue delay.

5.7.2 Computing Resources, Software and/or Data are corrupted

If computing resources, software, and/or data are corrupted or suspected to be corrupted, there are procedures as to how the secure environment will be re-established.

The Business Disaster and Continuity Team is responsible.

5.7.3 Entity private key compromise procedures

In the Business Disaster and Continuity Plan there is a procedure with practical steps on what to do in the case that the CA private key has been compromised, lost, or suspected compromised. These steps include that the Gjaldstovan TSP Management Board shall:

- Give information to all relevant entities and Authorized Relying Parties as quick as possible via the PKI repository;
- In the case of compromise
    - Inform all CA Certificate Holders and other entities with which Gjaldstovan has agreements or other form of established relations, among which Authorized Relying Parties and TSPs;
    - Make this information available to other relying parties;
    - Indicate that certificates and revocation status information issued using this CA key may no longer be valid;
- Revoke;
- If possible, steps have to be taken to avoid repetition of this or similar incidents;

In the Business Disaster and Continuity Plan there is a procedure with practical steps regarding what the Gjaldstovan TSP Management Board has to do in case of any of the algorithms, or associated parameters, used by Samleikin or CA Certificate Holders become insufficient for its remaining intended usage. The procedures state e.g. that Gjaldstovan TSP Management Board shall:

1. Inform all CA Certificate Holders and Authorized Relying Parties with whom Gjaldstovan has agreement or other form of established relations. In addition, this information shall be made available to other relying parties;

   and

2. Schedule a revocation of any affected CA Certificate issued by the Root CA.

5.7.4 Business Continuity Capabilities after a Disaster

If a disaster occurs, that makes both primary and secondary sites inactive; there are procedures in place to get them re-established. In addition, there are procedures in place for securing the facilities until the situation is normalized.

A regularly tested Business Disaster and Continuity Plan, has been implemented.

The plan is covering a large number of different scenarios; some of these are especially related to the CA-environment.

CA systems data backup and recovery

1. To allow Samleikin to quickly restore operations in case of incident/disasters, Samleikin systems data that is necessary to resume CA operations is backed up regularly and stored safely in two locations,
2. To ensure that all essential information and software can be recovered following a disaster or media failure facilities are in place. To ensure that back-up procedures and arrangements meets the requirements of the Business Disaster and Continuity Plan, these are regularly tested.
3. Relevant personnel in trusted roles are in charge of backup and restore functions.
4. To minimize the risk of an incorrect restore, at least two personnel in trusted roles have to activate the restore before it takes place.

5.8 CA or RA Termination

CA termination

In the event that it is necessary for the Root CA to cease operation, the Gjaldstovan TSP Management Board will analyze the impact of the termination and minimize the impact as much as possible in light of the prevailing circumstances. The Gjaldstovan TSP Management Board has procedure in place that will invoke in such cases where analysis is conducted and then a detailed termination plan is set in motion, in relation to the severeness of the situation.

The termination plan must at least address the following measures (if applicable):

- Inform parties affected by the termination, such as CA Certificate Holders and Authorized Relying Parties, informing them of the status of the Root CA. In case that the Root CA is publicly used, make public announcement at least three months in advance that operations will cease for the Root CA.
- Inform certifying bodies.
- Ensure that all private keys, including backup copies, is destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved.
- To revoke all active non-revoked certificates at the end of a notice period.
- Terminate all rights for subcontractors to act in the name of the Root CA which will cease to operate.
- Ensure that all archives and logs are stored for the stated storage time and in accordance with this CPS.
- Transfer obligations to the Gjaldstovan TSP Management Board 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.

RA termination

Not applicable.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

The CA private Keys are protected within a hardware security module accredited to FIPS 140-2 level 3 in a configuration that allows non-FIPS algorithms. Access to the modules are restricted by the use of hardware tokens, with associated PIN-codes, and passphrases. These hardware tokens and passphrases are allocated among the multiple members of Samleikin management and operational teams. For access to the modules and the keys within, at least 2 of 6 persons with the specific role that has access to the partitions need to participate, in accordance with the role matrix of the hardware security module, to ensure that no one member of the team holds total control over any component of the system. The hardware security modules are always stored in a physically secure environment and are subject to security controls throughout their life cycle as stated in chapter 5 of this CPS.

6.1.1 Key Pair Generation

Root CA Key Pair generation is witnessed by a qualified Auditor and follows a formal key generation script. Proof of the ceremony has been conducted in accordance with the script is a printed and signed copy of the protocol along with a video recording of the entire ceremony. The protocol and video recording will be stored in tamper evident bags in a physically secured environment. In all instances, CA private keys are generated in a physically secure environment within cryptographic modules. CA Certificate signing keys are only used within this secure environment. Access to the modules within the operating environment, including the private keys, is restricted by the use of hardware tokens, with associated PIN-codes, and associated passphrases.

The key ceremonies shall have a documented procedure for conducting CA Key Pair generation. This procedure shall indicate, at least, the following:

- Roles participating in the ceremony (internal and external from the organization)
- Functions to be performed by every role and in which phases

- Responsibilities during and after the ceremony
- Requirements of evidence to be collected of the ceremony

The auditor of key ceremonies shall produce an audit 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 key management ceremony (e.g. security officer) and a trustworthy person independent of the CA management (e.g. Notary, auditor) as witness that the report correctly records the key management ceremony as carried out.

CA certificates are signed using algorithm as specified in https://repository.samleiki.fo/profiles for the CA's signing purposes.

Before expiration of the currently active CA certificate, used for signing issued certificates, the CA generates a new certificate for signing issued certificates and applies actions to avoid disruption to the operations of any entity that may rely on the CA certificate. The new CA certificate shall also be distributed in accordance with the section "Publication of Certificate Information" in chapter 2 of this CPS. These operations should be performed within two years prior to expiration of the currently active CA certificate to allow all parties that have functional relationships with the CA and to be aware of this key changeover and to implement the required operations to avoid inconveniences and malfunctions. This does not apply in case the CA will cease its operations before its own certificate-signing certificate expiration date.

6.1.2 Private Key Delivery To Subscriber

The Root CA never generate Key Pairs for issuing CAs and do not have any type of access to private keys associated with issued certificates.

6.1.3 Public Key Delivery To Certificate Issuer

Public Keys are delivered in a secure and trustworthy manner to the Root CA by means of CSRs. Presentation of the PKCS#10 CSR by the Issuing CA authorized representative to the Root CA is accomplished in accordance with the formal procedure for certificate application stated in 4.1 of this CPS and in accordance with the identity validation stated in 3.2 of this CPS. For a CSR to be accepted by the Root CA it has to be signed by the requesting subject. Issued CA certificates are signed by the Root CA only if it is in compliance with this CPS.

6.1.4 CA Public Key Delivery to Relying Parties

CA public keys are delivered to Authorized Relying Parties via the Samleikin PKI respository as defined in section 2.1.

6.1.5 Key Sizes

Key lengths of issued CA Certificates within Samleikin are determined by the Gjaldstovan TSP Management Board and defined in the certificate profiles of each type of CA Certificate that can be issued as specified in https://repository.samleiki.fo/profiles

6.1.6 Public Key Parameters Generation and Quality Checking

For CA Certificate Holders, the quality of parameters used to create Public Keys are determined by the relevant RA application or by the CA Certificate Holder’s client application.
For Samleikin PKI, its Issuing CAs and RAs, all hardware and associated software platforms meet the requirements of FIPS 186-2, which ensures the proper parameters and their quality (e.g. random-generation and primality).
Samleikin PKI programmatically checks key size, public exponent range and modulus of incoming public key parameters against regulatory requirements and industry best practices.

6.1.7 Key usage purposes (as per. x.509 v3 key usage field)

Private Keys corresponding to Faroe Islands Root CA1 v1 Certificates are not used to sign Certificates except in the following cases:
(i) Self-signed Certificates to represent the Faroe Islands Root CA itself;
(ii) Certificates for Subordinate CAs and Cross Certificates; and
(iii) Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates).

Keys may be used for the purposes and in the manner described in the certificate profiles as specified in as specified in https://repository.samleiki.fo/profiles.
An Issuing CA’s Private Keys may be used for certificate signing and CRL and OCSP response signing. Keys may also be used to authenticate the Issuing CA to a Repository.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The Root CA is required to take all appropriate and adequate steps to protect private keys in accordance with the requirements of this CPS. Without limitation to the generality of the foregoing the Root CA must:

- Secure its private keys and take all reasonable and necessary precautions to prevent the loss, damage, disclosure, modification, or unauthorized use of private keys (including passwords, tokens or other activation data used to control access to private keys)
- Exercise sole and complete control and use of private keys

6.2.1 Cryptographic Module Standards and Controls

The generation and maintenance of the Root CA private keys are facilitated through the use of a Hardware Security Module. The Hardware Security Module used by the Root CA is certified to FIPS 140-2 level 3 security standard in both the generation and the maintenance in all Root CA private keys.

6.2.2 Private Key (N out Of M) Multi-Person Control

All Root CA Private Keys are accessed / activated through m-of-n multi-person control (e.g. a minimum threshold of splits of a Private Key decryption key must be used to decrypt or access a private CA signing key). A role matrix is maintained by the Gjaldstovan TSP Management Board.

All HSM:s and their cryptographic modules are validated before use to ensure they have not been tampered with. Root CA private signing keys stored on the Root CAs secure cryptographic device are to be destroyed upon device retirement, using the same method as destruction of private keys as stated below in this section.

6.2.3 Private Key Escrow

Private Key escrow is not allowed.

6.2.4 Private Key Backup

Root CA private keys that are kept for backup purposes are protected in dedicated backup cryptographic modules that meet the same level of protection as the cryptographic modules where keys are created and used. Such backup units are certified to FIPS 140-2 level 3 security standard and enforce M Of N Multi-Person Control as described in the role matrix.

6.2.5 Private Key Archival

Private Keys are not to be allowed outside its cryptographic module.

6.2.6 Private Key Transfer Into Or From A Cryptographic Module

Private keys are generated in its designated crypto module(s) and remain there in encrypted form, and be decrypted only at the time at which it is being used. Private keys will never exist in plain-text form outside the cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key is encrypted during transport.

6.2.7 Private Key Storage on Cryptographic Module

CA private keys that are kept for backup purposes are protected in dedicated backup cryptographic modules that meet the same level of protection as the cryptographic modules where keys are created and used. Such backup units are certified to FIPS 140-2 level 3 security standard and enforce M Of N Multi-Person Control as described in the role matrix.The HSM has a Common Criteria EAL 4+ validated cryptographic module.

6.2.8 Method Of Activating Private Key

The appropriate role must be authenticated to the cryptographic module before the activation of a private key. This authentication is in a combination of a hardware tokens, with associated PIN-codes, and a password. When deactivated, private keys kept in encrypted form only.

6.2.9 Method Of Deactivating Private Key

Cryptographic Modules that have been activated must not be left unattended or otherwise open to unauthorised access. After use, they must be deactivated, using, for example, a manual logout procedure or a passive timeout. When not in use, hardware Cryptographic Modules should be removed and stored safely in its designated offline storage.

6.2.10 Method Of Destroying Private Key

Private Keys are destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. Private Keys are to be destroyed within the cryptomodule(s) they reside as well as backup unit crypto modules. Upon expiration of a Key Pair’s allowed lifetime, or upon Root CA termination, the Root CA private key is destroyed by deleting and overwriting the data (e.g., via re-initialization or zeroization) or physical destruction (e.g., with a metal shredder or hammer). Such destructions are conducted, in a documented and videorecorded event according to a script approved by the Gjaldstovan TSP Management Board.

6.2.11 Cryptographic Module Rating

The generation and maintenance of the Root CA private keys are facilitated through the use of a Hardware Security Module. The Hardware Security Module used by the Root CA is certified to FIPS 140-2 level 3 security standard in both the generation and the maintenance in all Root CA private keys.

6.3 Other Aspects of Key Pair Management

Root CA signing key(s) used for signing issued CA Certificates and/or issuing revocation status information, are not used for any other purpose. The CA Certificate signing keys are only used within its designated cryptographic modules as dictated by this CPS.

6.3.1 Public Key Archival

Public Keys associated with CA certificates in the Samleikin PKI will be recorded in certificates that in turn will be archived in the repository https://repository.samleiki.fo/profiles. No separate archive of public keys will be maintained.

6.3.2 Certificate Operational Periods And Key Pair Usage Periods

Usage periods for public and private keys shall be in accordance with each type of certificate being issued by the Root CA as stated in the table in section 5.6 of this CPS**.**

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Two-factor authentication are used to protect access to a private key. One of these factors is a hardware token assigned to the appropriate role holder, and the other factor is a PIN-code associated with each hardware token. For the Root CA to use activated keys a dedicated password is also required. This is conducted in key generation ceremonies that are audited by external auditors.

6.4.2 Activation Data Protection

Activation data is never shared with any other role holder than the one using specific activation data. The activation data is kept in safes other than the hardware tokens, and separate trusted role holders have access to the safes, maintaining the m of n principle, so no single person can get to both hardware tokens and activation data, without the required set of trusted role holders present, as the procedure approved by TSP Management Board sets forth.

Activation data must consist of a set of characters to activate a set of hardware tokens.

6.4.3 Other Aspects Of Activation Data

Where a PIN code is used, the user is required to enter the PIN code before they are able to access keys using a dedicated PIN-entry device associated with the cryptomodule.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

Certificate generation and revocation management is a manual procedure requiring physical access to the high security offline zone. All PKI operations require multiple roles and duties separation and are logged.

The Root CA is not connected to any network and is securely stored in a restricted high security offline zone. Computer security controls are in line with rules and requirements and include but are not limited to:

- Strict identification of trusted personnel, roles, and responsibility
- Enforced separation of duties.
- Physical safeguards, logical access controls and multi-factor authentication.
- Hardened security modules and software certified to FIPS 140-2 level 3 or higher or Common Criteria EAL 4+
- Archive of Root CA history and audit data.

6.5.2 Computer security rating

The core Root CA software used has obtained the globally recognized EAL 4+ certification.

6.6 Life Cycle Security Controls

All hardware and software procured for operating the Root CA is purchased in a manner that will mitigate the risk that any particular component was tampered with. Equipment developed for use within Samleikin shall be developed in a controlled environment under strict change control procedures. A continuous chain of accountability, from the location where all hardware and software that has been identified as supporting the Root CA must be maintained by causing it to be shipped or delivered via controlled methods. Root CA equipment shall not have installed applications or component software that is not part of the Root CA configuration. All subsequent updates to Root CA equipment must be purchased or developed in the same manner as the original equipment and be installed by trusted and trained personnel in a defined manner.

6.6.1 System Development Controls

Formal procedures are followed for the development and implementation of new systems. An analysis of security requirements is carried out at the design and requirements specification stage. Outsourced software development projects are closely monitored and controlled.

6.6.2 Security Management Controls

The Root CA follows the Certificate Issuing and Management Components (CIMC) Family of Protections Profiles 1.5 that defines the requirements for components that issue, revoke and manage Public Key Certificates, such as X.509 Certificates. The CIMC is based on the common Criteria/ISO IS15408 standards.

6.6.3 Life Cycle Security Controls

The Root CA employs a configuration management methodology for the installation and ongoing maintenance of the Certificate Authority system components. The Hardware Security Modules, cryptographic modules and the certificate authority software, when first loaded provide a method to verify that:

- It originated from the vendor
- Has not been modified prior to installation or use
- Is the version intended for use

The Security Officer periodically verifies the integrity of the Hardware security modules, the cryptographic modules and the certificate authority software and monitors the configuration of the certificate authority system components.

6.7 Network Security Controls

The Root CA is not connected to any network and is securely stored in a restricted high security offline zone. Tasks that require transferring digital data between the Root CA and the network is a manual process using approved procedures and portable media. The portable media is required to undergo removable media protection using offline data sanitization security appliances, also known as Content Disarm and Reconstruction.

6.8 Time-stamping

The Root CA is not connected to any network and is securely stored in a restricted high security offline zone. Local system clock is used as time source for:

- Audit events
- PKI Operations

Manual procedures are used to maintain system time. Clock adjustments are auditable events.

7 Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

All CA Certificates and CRL profiles conform to RFC 5280 and utilize the ITU-T X.509 version 3 standard.

All CA Certificates issued under this policy must adhere to the certificate profiles dictated by the Gjaldstovan TSP Management Board. These profiles are available at https://repository.samleiki.fo/profiles.

7.1.1 Version Numbers

Certificate profile version is 1.

7.1.2 Certificate Extensions

The extensions defined for X.509 v3 certificates provide methods for associating additional attributes with public keys and for managing relationships between CAs. The certificate profile of each type of issued CA Certificate describes every certificate extension used for each type of issued CA Certificate. These profiles are available at https://repository.samleiki.fo/profiles.

7.1.3 Algorithm Object Identifiers

As defined by each certificate profile. These profiles are available at https://repository.samleiki.fo/profiles.

7.1.4 Name Forms

As defined by each certificate profile. These profiles are available at https://repository.samleiki.fo/profiles.

7.1.5 Name Constraints

As defined by each certificate profile. These profiles are available at https://repository.samleiki.fo/profiles.

7.1.6 Certificate Policy Object Identifier

OID assigned to the CP is OID:1.2.208.189.1.1.1. OID assigned for this CPS is: 1.2.208.189.1.1.6.

7.1.7 Usage Of Policy Constraints Extension

As defined by each certificate profile. These profiles are available at https://repository.samleiki.fo/profiles.

7.1.8 Policy Qualifiers Syntax And Semantics

As defined by each certificate profile. These profiles are available at https://repository.samleiki.fo/profiles.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

As defined by each certificate profile. These profiles are available at https://repository.samleiki.fo/profiles.

7.2 CRL Profile

CRLs conform to RFC 5280. The information contained in a Certificate Revocation List is described below. CRL:s are used to state which of the certificates, whose validity period has not yet expired, have been revoked.

CRL basic fields are listed in the table below:

Field name	Field description and contents	Critical
CRL Version	This field states which of the CRL versions defined in the X.509 standard the CRL conforms to. The CRLs conform to the version 2.	2
Signature Algorithm	The CRLs are signed by using the same algorithm as is used for signing of the certificates. The algorithm used is ecdsa-with-SHA512.	ecdsa-with-SHA512
Issuer	This field states the name of the Issuer of the CRL. The CRL issuer name is always the same as the Issuer name (the CA's name) in the certificates listed on the CRL.	C=FO O=Gjaldstovan CN=Faroe Islands RootCA1 v1
This update	Date and time of the CRL issuance.	
Next update	Date and time by which the next CRL shall be issued. The next CRL may be issued at any time after the issuance of the previous CRL, however, it shall be issued before the time stated in the "Next update" field. The time difference between "This update" and "Next update" is defined in section 4.9.	1 year
Revoked certificates	This field states the serial numbers of revoked certificates, and for each revoked certificate the date and time of revocation and the reason for revocation.	N/A
Authority key identifier	The identifier of the public key of the CRL Issuer is given in this field. The identifier can be used to identify the public key that corresponds to the private key used for the signing of the CRL. Within Samleikin the ecdsa-with-SHA512 hash algorithm is used to calculate the identifier.	**?**
CRL number	The CRL number is a number that indicates the position of the CRL in the sequence of issued CRLs. The numbering starts with 1, and it increase monotonically by one for each issued CRL. Based on the CRL number it can be determined if a certain CRL replace another CRL.	1

7.2.1 Version Number

The Root CA issues X.509 version 2 Certificate Revocation Lists.

7.2.2 CRL and CRL Entry Extensions

See table in 7.2.

7.3 OCSP Profile

Online Certificate Status Protocol is enabled for all certificates within Samleikin

7.3.1 Version Numbers

Online Certificate Status Protocol, as defined by RFC6960, is supported within Samleikin.

7.3.2 OCSP Extensions

No stipulations.

8 Compliance Audit and Other Assessment

The results of audits in the form of such publicly available audit reports as provided by external auditors that comply with ETSI EN 319 403 is appointed by the Gjaldstovan TSP Management Board for conducting these audits. These audit reports will be published at https://repository.samleiki.fo/legal-repository. Compliance audits as carried out under these provisions may substitute for audits noted in this CPS where this is explicitly stated as allowed.

8.1 Frequency or circumstances of assessment

An independent, qualified third party will perform an compliance audit every second year. Gjaldstovan TSP Management Board performs quarterly internal audits to verify compliance in between external audits.

The Root CA is audited in accordance with

- **ETSI EN 319 401 (General Requirements for Trust Service Providers)**
- **ETSI EN 319 411-1**

These audits shall include the review of all relevant documents maintained by the CA regarding operations within Samleikin and under this CPS, and other related materials referenced from this CPS.

8.2 Identity/Qualifications Of Assessor

The audit services are performed by independent, recognized, credible, and established audit firms or information technology consulting firms; provided they are qualified to perform and are experienced in performing the required audits, specifically having significant experience with PKI and cryptographic technologies.

The audits are performed in accordance with ETSI EN 319 403 (conformity assessment requirements).

8.3 Assessor’s Relationship To Assessed Entity

The auditor and the CA under audit, must not have any other relationship that would impair the auditor’s independence and objectivity under Generally Accepted Auditing Standards. These relationships include financial, legal, social or other relationships that could result in a conflict of interest.

8.4 Topics Covered By Assessment

The topics covered by an audit of the Root CA will include but may not be limited to:
• Security Policy and Planning;
• Physical Security;
• Technology Evaluation;
• Services Administration;
• Personnel Vetting;
• Contracts; and
• Privacy Considerations.

8.5 Actions Taken As A Result Of Deficiency

Actions taken as the result of deficiency will be determined by the nature and extent of the deficiency identified. Any determination will be made by the Gjaldstovan TSP Management Board with input from the auditors. The course of action and time frame for rectification of any deficiency as set by the independent auditor must be followed.

8.6 Communication Of Results

The results of the most recent audit - the conformity certificate - will be posted at https://repository.samleiki.fo/legal-repository.

9 Other Business and Legal Matters

9.1 Fees

No stipulations

9.1.1 Certificate issuance or renewal fees

No stipulations

9.1.2 Certificate access fees

No stipulations

9.1.3 Revocation or status information access fees

No stipulations

9.1.4 Fees for other services

No stipulations

9.1.5 Refund policy

No stipulations

9.2 Financial Responsibility

Gjaldstovan is a governmental institution under the jurisdiction of the Ministry of Finance in the Faroe Islands.

Gjaldstovan is responsible for maintaining its financial books and records in accordance with faroese legislation (Løgtingslóg um landsins almenna roknskaparhald v.m., sum broytt við løgtingslóg nr. 33 frá 30. apríl 2015 and related orders/decrees and executive orders) and shall engage the services the state-authorized public accountant to provide financial services, according to Løgtingslóg um grannskoðan av landsroknskapinum v.m., sum broytt við løgtingslóg nr. 33 frá 30. apríl 2015.

9.2.1 Insurance Coverage

Within Samleikin the Root CA and all Issuing CAs and RAs are required to demonstrate that they have the financial resources necessary to discharge their obligations under its CP/CPS/RAP/RAPS and any other relevant and associated documentation or agreements.

Gjaldstovan and each CA and/or RA shall maintain appropriate insurances necessary to provide for their respective liabilities as participants within Samleikin. Failure to establish and maintain insurances may be the basis for the revocation of their respective certificates.

Gjaldstovan is a governmental institution. Gjaldstovan is, as a governmental institution, part of the faroese yearly Finance Act. Funds for Samleikin is additionally authorized by law of the Løgting about Talgildu Føroyar (Løgtingslóg nr. 77 frá 29. mai 2017 um Talgildu Føroyar). The state's insurance policies are laid down in government circular "Rundskriv nr. 9000 frá 21. november 2003 um tryggingarviðurskifti landsins".

9.2.2 Other Assets

The CA and RAs shall maintain sufficient assets and financial resources to perform their duties within Samleikin and be reasonably able to bear liability to CA Certificate Holders and Authorized Relying Parties.

9.2.3 Insurance Or Warranty Coverage For End-Entities

Gjaldstovan will - to the best of Gjaldstovan knowledge and without any admission of liability - give advice to and support CA Certificate Holders and Autorized Relying Parties on questions relating to the different types of insurance available. CA Certificate Holders are entitled to apply to commercial insurance providers for financial protection against accidental occurrences such as theft, corruption, loss or unintentional disclosure of the private key that corresponds to the public key in their certificate.

Authorized Relying Parties are entitled to apply to commercial insurance providers for protection against financial loss.

9.3 Confidentiality of Business Information

9.3.1 Scope of confidential information

Information which is not explicitly defined as non-confidential, is treated as confidential by the Gjaldstovan TSP Management Board and will not be disclosed without the consent of a participant.

The Gjaldstovan TSP Management Board will disclose confidential information where this is required by law or by a decision in a court of law or Faroese government authority.

The Gjaldstovan TSP Management Board is responsible for classification of each asset and for involving relevant persons in the risk assessment and risk management, to document them and keep them up to date.

The Gjaldstovan TSP Management Board sets forth the procedures for handling all data in accordance with the sensitivity of any information collected or analyzed, and must ensure that all employees that can come in contact with the information are educated in the classification procedures in use by the Gjaldstovan TSP management board.

9.3.2 Information not within the scope of confidential information

The following information is not deemed to be confidential:

- This CPS and each CPS referring to this CPS
- Information in issued CA Certificates including public keys
- Revocation lists and OCSP responses
- General key holder terms and conditions
- All other information stored in the repository defined in section 2 in this CPS

9.3.3 Responsibility to protect confidential information

PKI participants are responsible for protecting confidential information in their possession, custody or control.

All confidential information will be physically and/or logically protected by Root CA from unauthorized viewing, modification or deletion, see chapter 5.

9.4 Privacy of Personal Information

9.4 1 Privacy Plan

PKI participants using or accessing any personal data in connection with matters dealt with this CPS shall comply with

- Persónsupplýsingarlógin (The faroese Act on processing of personal data - Løgtingslóg nr. 73 frá 8. mai 2001 um viðgerð av persónsupplýsingum, sum broytt við løgtingslóg nr. 24 frá 17. mai 2004) and any amending and/or implementing legislation enacted from time to time.

9.4.2 Information Treated As Private

All information about CA Certificate Holders that is not publicly available through the content of issued certificates, certificate directories or online repositories is treated as private.

Registration Records

All registration records are considered confidential information and treated as private.

Certificate Revocation

Except for reason codes contained in a Certificate Revocation List, the detailed reason for a certificate being revoked, (if applicable), is considered to be confidential information, with the sole exception of the revocation of an Issuing CA's Issuing Certificate due to:

- The compromise of the Issuing CA's Private Key, in which case a disclosure may be made that the Private Key has been compromised
- The termination of an Issuing CA within Samleikin, in which case prior disclosure of the termination may be given

9.4.3 Information Deemed Not Private

The following information is not considered as private:

- Certificate Contents, the content of certificates issued by the Root CA is public information and deemed not private
- Certificate Revocation Lists/OCSP responses, are not considered to be confidential information
- This CPS and any associated CPs, is a public document and is not confidential information and is not treated as private

9.4.4 Responsibility To Protect Private Information

Information supplied to the Root CA as a result of the practices described in this CPS may be covered by national government or other privacy legislation or guidelines. The Root CA will not divulge any private CA Certificate Holder information to any third party for any reason, unless compelled to do so by law or regulatory authority.

9.4.5 Notice And Consent To Use Private Information

In the course of accepting a certificate, all certificate holders have agreed to allow their personal data submitted in the course of registration to be processed by and on behalf of the Root CA, and used as explained in the registration process. They have also been given an opportunity to decline from having their personal data used for particular purposes. They have also agreed to let certain personal data appear in publicly accessible directories and be communicated to others.

9.4.6. Disclosure pursuant to judicial or administrative process

As a general principle, no document or record belonging to the Gjaldstovan TSP Management Board is released to law enforcement agencies or officials except where a properly constituted instrument, warrant, order, judgment, or demand is produced requiring production of the information, having been

issued by a court of jurisdiction, and not known to Gjaldstovan TSP Management Board to be under appeal when served on the Gjaldstovan TSP Management Board, and which has been determined by a court of jurisdiction to be valid, subsisting, issued in accordance with general principles of law and otherwise enforceable under the laws of the jurisdiction of the Root CA and enforceable in that jurisdiction or enforceable under the laws otherwise governing the operations of the Root CA.

Release As Part Of Civil Discovery

As a general principle, no document or record belonging to Gjaldstovan is released to any person except where a properly constituted instrument, warrant, order, judgment, or demand is produced requiring production of the information, having been issued by a court of jurisdiction, and not known to the Gjaldstovan TSP Management Board to be under appeal when served on the Gjaldstovan TSP Management Board, and which has been determined by a court of jurisdiction to be valid, subsisting, issued in accordance with general principles of law and otherwise enforceable under the laws of the jurisdiction of the Root CA and enforceable in that jurisdiction or enforceable under the laws otherwise governing the operations of the Root CA.

9.4.7 Other Information Disclosure Circumstances

The Gjaldstovan TSP Management Board and the Root CA are under no obligation to disclose information other than is provided for by a legitimate and lawful judicial order that complies with requirements of this CPS.

The confidentiality and integrity of registration data shall be protected, especially when exchanged with the Certificate Holder or between distributed Samleikin system components.

Confidentiality and integrity of data

By complying to international standards, regulation, the Samleikin policies and other relevant demands, The Samleikin core systems will ensure that confidential and/or private information is protected from
compromise and shall not use confidential and/or private information beyond what is required. The core systems will be audit yearly by external auditors.

9.5 Intellectual Property Rights

All intellectual property rights including all copyright in all certificates and all Gjaldstovan documents (electronic or otherwise) belong to and will remain the property of Gjaldstovan. Private keys and public keys are the property of the applicable rightful private key holder. Certificates issued and all intellectual property rights including all copyright in all certificates and all Gjaldstovan documents (electronic or otherwise) belong to and will remain the property of Gjaldstovan.

This CPS and the proprietary marks are the intellectual property of Gjaldstovan. Gjaldstovan retains exclusive title to and copyright of this CPS.

Certificate applicants are not allowed to use names in their certificate applications that infringe upon the intellectual property rights of others. The CA will 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 is entitled, without liability to any certificate applicant, to reject or suspend any certificate application because of such disputes.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

By issuing a certificate, the Root CA represents and warrants that, during the period when the certificate is valid, the Root CA has complied with this CPS in issuing and managing the certificate to the parties listed below:

- The party to the relevant CA Certificate Holder Agreement
- All Authorized Relying Parties who reasonably rely on a valid CA Certificate

The Root CA discharges its obligations by:

- Providing the operational infrastructure and certification services, including the Repository, OCSP responders and CRLs
- Making reasonable efforts to ensure it conducts and efficient and trustworthy operation
- Maintaining this CPS and enforcing the practices described within it and in all relevant collateral documentation
- Investigating any suspected compromise which may threaten the integrity of the Root CA

The Root CA warrants:

- It has taken reasonable steps to verify that the information contained in any CA Certificate is accurate at the time of issuance
- CA Certificates shall be revoked if the Root CA believes or is notified that the contents of the CA Certificate are no longer accurate, or that the key associated with a CA Certificate has been compromised in any way

The Root CA makes no other warranties, and all warranties, express or implied, statutory or otherwise, are excluded to the greatest extent permissible by applicable law.

9.6.2 RA Representations and Warranties

No stipulations

9.6.3 Subscriber Representations And Warranties

As part of the CA Certificate Holder Agreement agreed to by all CA Certificate Holders, the following commitments and warranties are made for the express benefit of the Root CA and all Authorized Relying Parties:

- Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to the Root CA, both in the certificate request and as otherwise requested by the Root CA in connection with the issuance of certificate(s)
- Protection of private key: An obligation and warranty by the CA Certificate Holder or a subcontractor (e.g. hosting provider) to take all reasonable measures necessary to maintain sole control of, keep confidential, and properly protect at all times the private key that corresponds to the public key to be included in the requested CA Certificate(s) and any associated access information or device such as a password or token
- Acceptance of CA Certificate: An obligation and warranty that it will not install and use the CA Certificate(s) until it has reviewed and verified the accuracy of the data in each CA Certificate
- Use of CA Certificates: An obligation and warranty to use the CA Certificate solely in compliance with all applicable laws, and solely in accordance with the CA Certificate Holder Agreement and for its intended purpose
- Reporting and revocation upon compromise: An obligation and warranty to promptly cease using a certificate and its associated private key, and promptly request that the CA revoke the CA Certificate, in the event that any information in the CA Certificate is or becomes incorrect or inaccurate or there is any actual or suspected misuse or compromise of the CA Certificate Holder's private key associated with the public key listed in the CA Certificate
- Termination of use of the CA Certificate: An obligation and warranty to promptly cease all use of the private key corresponding to the public key listed in a CA Certificate upon expiration or revocation of that CA Certificate

Without limiting other CA Certificate Holder obligations stated in this CPS, CA Certificate Holders are solely liable for any misrepresentations they make in CA Certificates to third parties that reasonably rely on the representations contained therein.

Upon accepting a CA Certificate the CA Certificate Holder represents to the Root CA and to Authorized Relying Parties that at the time of acceptance and until further notice:

- The CA Certificate Holder retains control of the CA Certificate Holder's Private key, uses a trustworthy system, and takes reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use and that no unauthorized entity has ever had access to the CA Certificate Holder' s private key
- All representations made by the CA Certificate Holder to the Root CA regarding the information contained in the CA Certificate are accurate and true to the best of the CA Certificate Holder's knowledge or to the extent that the CA Certificate Holder receives notice of such information, the CA Certificate Holder shall act promptly to notify the Root CA of any material inaccuracies contained in the CA Certificate
- The CA Certificate is used exclusively for authorized and legal purposes, consistent with this CPS
- The CA Certificate Holder agrees with the terms and conditions of this CPS and other agreements and policy statements of the Gjaldstovan TSP Management Board.

9.6.4 Relying Party Representations And Warranties

Authorized Relying Parties represent and warrant that:

- They will collect enough information about a CA Certificate and its corresponding holder to make an informed decision as to the extent to which they can rely on the CA Certificate
- That they are solely responsible for making the decision to rely on a CA Certificate
- That they shall bear the legal consequences of any failure to perform their Authorized Relying Party obligations under the terms of this CPS and the Relying Party Agreement

9.6.5 Representations And Warranties Of Other Participants

Participants within Samleikin represent and warrant that they accept and will perform any and all duties and obligations as specified by this CPS.

9.7 Disclaimers of Warranties

To the extent permitted by applicable law, this CPS, the CA Certificate Holder Agreement, the Relying Party Agreement and any other contractual documentation applicable within Samleikin shall disclaim Gjaldstovans possible warranties. To the extent permitted by applicable law, Gjaldstovan makes no express or implied representations or warranties pursuant to this CPS. Gjaldstovan expressly disclaims any and all express or implied warranties of any type to any person.

9.8 Limitations of Liability

Gjaldstovan shall be liable to CA Certificate Holders or Autorized Relying Parties only for direct loss arising from any breach of this CPS or for any other liability it may incur in contract, tort or otherwise, including liability for negligence up to an aggregated maximum limit of 2.000.000 DKK for any one event or series of related events.

Gjaldstovan shall not in any event be liable for any loss of profits, loss of sales or turnover, loss or damage to reputation, loss of contracts, loss of customers, loss of the use of any software or data, loss or use of any computer or other equipment (save as may arise directly from breach of this CPS), wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage, and for the purpose of this paragraph, the term "loss" means a partial loss or reduction in value as well as a complete or total loss.

Gjaldstovans liability to any person for damages arising under, out of or related in any way to this CPS, CA Certificate Holder Agreement, the applicable contract or any related agreement, whether in contract, warranty, tort or any other legal theory, shall, subject as hereinafter set out, be limited to actual damages suffered by that person. Gjaldstovan shall not be liable for indirect, consequential, incidental, special, exemplary, or punitive damages with respect to any person, even if Gjaldstovan has been advised of the possibility of such damages, regardless of how such damages or liability may arise, whether in tort, negligence, equity, contract, statute, common law, or otherwise. As a condition to participation within Samleikin, any person that

participates within Samleikin irrevocably agrees that they shall not apply for or otherwise seek either exemplary, consequential, special, incidental, or punitive damages and irrevocably confirms to Gjaldstovan their acceptance of the foregoing and the fact that Gjaldstovan has relied upon the foregoing as a condition and inducement to permit that person to participate within Samleikin.

Excluded Liability

Gjaldstovan shall bear absolutely no liability for any loss whatsoever involving or arising from any one (or more) of the following circumstances or causes:

- If the CA Certificate held by the claiming party or otherwise the subject of any claim has been compromised by the unauthorized disclosure or unauthorized use of the CA Certificate or any password or activation data used to control access thereto
- If the CA Certificate held by the claiming party or otherwise the subject of any claim was issued as a result of any misrepresentation, error of fact, or omission of any person, entity, or organization
- If the CA Certificate held by the claiming party or otherwise the subject of any claim had expired or been revoked prior to the date of the circumstances giving rise to any claim
- If the CA Certificate held by the claiming party or otherwise the subject of any claim has been modified or altered in any way or been used otherwise than as permitted by the terms of this CPS and/or the relevant CA Certificate Holder Agreement or any applicable law or regulation
- If the private key associated with the CA Certificate held by the claiming party or otherwise the subject of any claim has been compromised
- If the CA Certificate held by the claiming party was issued in a manner that constituted a breach of any applicable law or regulation
- Computer hardware or software, or mathematical algorithms, are developed that tend to make public key cryptography or asymmetric cryptosystems insecure, provided that Gjaldstovan uses commercially reasonable practices to protect against breaches in security resulting from such hardware, software, or algorithms
- Power failure, power interruption, or other disturbances to electrical power, provided Gjaldstovan uses commercially reasonable methods to protect against such disturbances
- Failure of one or more computer systems, communications infrastructure, processing, or storage media or mechanisms, or any sub components of the preceding, not under the exclusive control of Gjaldstovan and/or its subcontractors or service providers
- One or more of the following events: a natural disaster (including without limitation flood, earthquake, or other natural or weather related cause), a labor disturbance, war, insurrection, or overt military hostilities, adverse legislation or governmental action, prohibition, embargo, or boycott, riots or civil disturbances, catastrophic epidemic, any lack of telecommunications availability or integrity, legal compulsion including any judgments of a court of jurisdiction to which Gjaldstovan is, or may be, subject and any event or occurrence or circumstance or set of circumstances that is beyond the control of Gjaldstovan

Mitigation Of Gjaldstovans Liability

The Gjaldstovan TSP Management Board has introduced a number of measures to reduce or limit its liabilities in the event that the safeguards in place to protect its resources fail to:

- Inhibit misuse of those resources by authorized personnel
- Prohibit access to those resources by unauthorized individuals

These measures include but are not limited to:

- Identifying contingency events and appropriate recovery actions in a contingency & disaster recovery plan
- Performing regular system data backups
- Performing a backup of the current operating software and certain software configuration files
- Storing all backups in secure local and offsite storage
- Maintaining secure offsite storage of other material needed for disaster recovery
- Periodically testing local and offsite backups to ensure that the information is retrievable in the event of a failure
- periodically reviewing its contingency & disaster recovery plan, including the identification, analysis, evaluation and prioritization of risks
- Periodically testing uninterrupted power supplies

The Gjaldstovan TSP Management Board is regularly checking for new and emerging vulnerabilities. A vulnerability not previously addressed will be dealt with within a period of 4 weeks after its discovery, by an employee in a trusted role.

For any vulnerability, given the potential impact, the trusted role will

- create and implement a plan to mitigate the vulnerability
  or
- document the factual basis for the determination that the vulnerability does not require remediation

Claims Against Gjaldstovans Liability

Gjaldstovan shall have no obligation pursuant to any claim for breach of its obligations hereunder unless the claiming party gives notice to Gjaldstovan within ninety (90) days after the claiming party knew or ought reasonably to have known of a claim, and in no event more than three (3) years after the expiration of the certificate held by the claiming party.

As a precondition to Gjaldstovans payment of any claim under the terms of this CPS, a claiming party shall do and perform, or cause to be done and performed, all such further acts and things, and shall execute and deliver all such further agreements, instruments, and documents as Gjaldstovan may reasonably request in order to investigate a claim of loss made by a claiming party.

9.9 Indemnities

If an invalid claim for damages will be presented against the Gjaldstovan, the CA Certificate Holder shall be bound to compensate Gjaldstovan for any damages and costs due to the claim and the necessary statement of defense, including any legal expenses.

9.10 Term and Termination

9.10.1 Term

This CPS becomes effective upon publication in the repository. Amendments to this CPS become effective upon publication in the repository.

9.10.2 Termination

This CPS shall remain in force until it is amended or replaced by a new version.

9.10.3 Effect of termination and survival

The provisions of this CPS shall survive the termination or withdrawal of a CA Certificate Holder or Authorized Relying Party from Samleikin with respect to all actions based upon the use of or reliance upon a certificate or other participation within Samleikin. Any such termination or withdrawal shall not act so as to prejudice or affect any right of action or remedy that may have accrued to any person up to and including the date of withdrawal or termination.

9.11 Individual notices and communications with participants

Electronic mail, postal mail and web pages will all be valid means for Gjaldstovan to provide any of the notices required by this CPS, unless specifically provided otherwise. Electronic mail and postal mail will be valid means of providing any notice required pursuant to this CPS to Gjaldstovan unless specifically provided otherwise.

9.12 Amendments

9.12.1 Procedure For Amendment

Amendments to this CPS are made and approved by the Gjaldstovan TSP Management Board. Amendments shall be in the form of an amended CPS or a replacement CPS. Updated versions of this CPS supersede and designated or conflicting provisions of the referenced version of the CPS.

There are two possible types of policy change:

- The issue of a new CPS
- A change to or alteration of an existing CPS

If an existing CPS requires re-issue, the change process employed is the same as for initial publication, as described above. If a policy change is determined to have a material impact on a significant number of CA Certificate Holders and Autorized Relying Parties, then the Gjaldstovan TSP Management Board may, at its sole discretion, assign a new object identifier for certificates issued pursuant to the modified CPS.

The only changes that may be made to this CPS without notification are editorial or typographical corrections or minor changes that do not, in the opinion of the Gjaldstovan TSP Management Board, materially impact any participants within Samleikin.

Issuing CAs are notified of changes to the CPS as and when they are approved.

9.12.2 Notification Mechanism And Period

New or amended CP:es are published on the web site at https://repository.samleiki.fo/legal-repository. Any change that increases the level of trust that can be placed in certificates issued under this CPS or under policies that make reference to this CPS requires thirty (30) days prior notice. Any change that decreases the level of trust that can be placed in certificates issued under this CPS or under policies that make reference to this CPS requires forty-five (45) days prior notice. The CPS applicable to any certificate supported by this CPS shall be the CPS currently in effect.

9.12.3 Circumstances Under Which OID Must Be Changed

The Gjaldstovan TSP Management Board reserves the right to amend this CPS without notification for amendments that are not material, including corrections of typographical errors, changes to URLs and changes to contact details. The decision to designate amendments as material or non-material to this CPS is at the sole discretion of the Gjaldstovan TSP Management Board. Unless the Gjaldstovan TSP Management Board determines otherwise, the Object Identifier to this CPS shall not change.

9.13 Dispute Resolution Provisions

Complaints can be communicated to Gjaldstovan via electronic or postal mail.

E-mail adress is: gjaldstovan@gjaldstovan.fo

Postal mail:

Gjaldstovan
Kvíggjartún 1,
FO-160 Argir
Faroe Islands

Complaints will be considered by the Gjaldstovan TSP Management Board and then the appropriate steps will be taken.

Any controversy or claim between two or more participants in Samleikin arising out of or relating to this CPS shall be shall be referred to Føroya Rætt, Tórshavn.

9.14 Governing Law

This CPS 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 CPS.

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.

9.15 Compliance with Applicable Law

Gjaldstovan will, in relation to the Root CA, comply with applicable national, local and foreign laws, rules, regulations, ordinances, decrees and orders.

9.16 Miscellaneous Provisions

9.16.1 Entire agreement

No stipulations.

9.16.2 Assignment

Parties to this CPS may not assign any of their rights or obligations under this CPS or applicable agreements without the written consent of the Gjaldstovan TSP management Board, and any such attempted assignment shall be void.

9.16.3 Severability

Any provision of this CPS that is determined to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this CPS or affecting the validity or enforceability of such remaining provisions.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Except where an express time frame is set forth in this CPS, no delay or omission by Gjaldstovan to exercise any right, remedy, or power it has under this CPS shall impair or be construed as a waiver of such right, remedy, or power. A waiver by Gjaldstovan of any breach or covenant in this CPS shall not be construed to be a waiver of any other or succeeding breach or covenant. No waiver shall be effective unless it is in writing. Bilateral agreements between Gjaldstovan and the parties to this CPS may contain additional provisions governing enforcement.

9.16.5 Force Majeure

Gjaldstovan accepts no liability for any breach of warranty, delay or failure in performance that results from events beyond its control such as acts of war, acts of terrorism, epidemics, power or telecommunication services failure and natural disasters. See also Section 9.8.

9.17 Other Provisions

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

The Gjaldstovan TSP Management Board shall provide the capability to allow third parties to check and test all the CA certificate types that the Root CA issues. Any test certificates should clearly indicate that they are for testing purposes (e.g. by the subject name).