Certificate Practice Statement - Faroe Islands IssuingCA1 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 the Faroe Islands IssuingCA1 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 Issuing Certification Authority which complies with "Gjaldstovan Certificate Policy - NCP" OID:1.2.208.189.1.1.2, which in turn is based on the NCP (Normalized Certificate Policy), OID: 0.4.0.2042.1.1 (itu-t (0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncp(1), defined in ETSI EN 319 411-1**.**

OID for this CPS is: 1.2.208.189.1.1.7

- This document is accurately reproduced in full, complete with attribution of the document to Gjaldstovan.

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

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 (RA), Certificate Holders and Relying Parties shall follow in connection with these certificates. This document defines the Certification Practice Statement for the Faroe Islands IssuingCA1 v1
This document is divided in to nine sections:

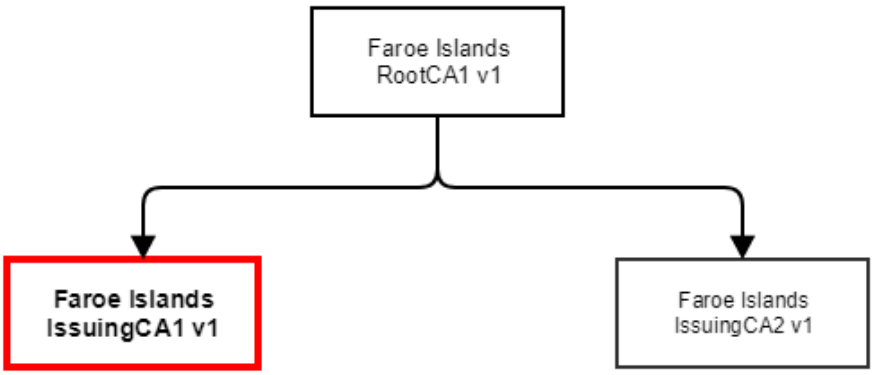
- Section 1 - provides an overview of the policy and set of provisions, as well as the types of entities and the appropriate applications for certificates.
- Section 2 - contains any applicable provisions regarding identification of the entity or entities that operate repositories; responsibility of 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 certificate, 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) RFC:s:

- 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 IssuingCA1 v1 conforms to procedures and routines defined in "Gjaldstovan Certificate Policy - NCP" OID:1.2.208.189.1.1.2 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 IssuingCA1 v1 Certification Practice Statement" with OID 1.2.208.189.1.1.7 and applies to Faroe Islands IssuingCA1 v1.

1.3. PKI Participants

This CPS outlines the roles and responsibilities of all parties involved in the generation and use of certificates under the operation of Faroe Islands IssuingCA1 v1.

The Faroe Islands IssuingCA1 v1 utilizes its Issuing CA Certificate to create, sign and issue certificates. The Faroe Islands IssuingCA1 v1 issuing certificate is signed by the Faroe Islands RootCA1 v1.

The Faroe Islands IssuingCA1 v1 is a subordinate service that is:

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

The Faroe Islands IssuingCA1 v1 is 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 Faroe Islands IssuingCA1 v1.

Participants within Samleikin include:

- Certification Authorities;
- Registration Authorities;
- Certificate Holders including applicants for certificates prior to 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 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 certificates and Key Pairs

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

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

- In circumstances that breach the Relying Party Agreements or the Terms & Conditions (Terms & Conditions = the Certificate Holder Agreement for end-users)
- 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 CA:

Faroe Islands RootCA1 v1

Issuing CAs are authorized by the Gjaldstovan TSP Management Board to participate within Samleikin 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

Samleikin contains the following Issuing Certification Authorities:

- the Faroe Islands IssuingCA1 v1 (subject to this CPS)
- the Faroe Islands IssuingCA2 v1

1.3.2 Registration Authorities

Issuing CAs, if authorized to do so by the Gjaldstovan TSP Management Board, may rely on third party RAs if they meet the requirements stated in the RAP, available 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

Certificate Holders are required to act in accordance with the Terms and Conditions. A Certificate Holder warrants that:

- Both as an applicant for a certificate and as a Certificate Holder, submit complete and accurate information in connection with an application for a certificate and will promptly update such information and representations from time to time as necessary to maintain such completeness and accuracy.
- Promptly review, verify and accept or reject the certificate that is issued and ensure that all the information set out therein is complete and accurate and to notify the CA and/or RA immediately in the event that the 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 the Private Key including the PIN used to control access to the Private Key
- Exercise sole and complete control and use of the Private Key that corresponds to the Certificate Holder's Public Key
- Immediately notify the 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 Certificate Holder's Private Key shall be immediately and permanently discontinued
- Forthwith upon suspension, revocation or expiry of the certificate, cease use of the certificate absolutely.
- At all times utilize the certificate in accordance with all applicable laws and regulations
- Discontinue the use of Key Pairs in the event that the CA notifies the Certificate Holder that Samleikin has been compromised.

1.3.4 Relying Parties

Authorized Relying parties are required to act in accordance with this CPS and the Relying Party Agreement available at https://repository.samleiki.fo/legal-repository. An Authorized Relying Party must utilize 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 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 Authorized 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 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 certificate relied upon are appropriate in all respects to the reliance placed upon that certificate by the 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 certificate relied upon
- That the Authorized Relying Party has, at the time of that reliance, used the 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 Ruthorized Relying Party
- That the 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 certificate utilizing either the CAs Certificate Revocation List, or the CA:s 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 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 Certificate Holder is displayed correctly by utilizing trusted application software

Certificates include a reference to the relevant CPS, which contains statements detailing limitations of liability and disclaimers of warranty. In accepting a 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 certificate.

A party cannot rely on a certificate issued by the CA if the party has actual notice of the compromise of the certificate or its associated Private Key. Such notice includes but is not limited to the contents of the certificate and information incorporated in the certificate by reference, which includes this CPS and the current set of revoked certificates published by the CA. Certificates have pointers to URLs where the 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 certificate.

1.3.5 Other Participants

Other participants in Samleikin are required to act in accordance with this CPS and/or other applicable agreement's.

1.4 Certificate Usage

All participants using certificates issued by the Faroe Islands IssuingCA1 v1 are required to utilise the certificate in accordance with this CPS and Terms and conditions signed by the Certificate Holder, as well as any Relying Party Agreements.

Issued 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

Certificates issued by the Faroe Islands IssuingCA1 v1 may be used for authentication, non-repudiation and encryption.

1.4.2 Prohibited Certificate Uses

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

- In circumstances that breach the Relying Party Agreements or the Terms and Conditions.
- 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 certificates and the certificates may not be used in circumstances

- where applicable law or regulation prohibits their use;
- in breach of this CPS or the relevant Certificate Holder or Relying Party Agreement;
- in any circumstances where the use of the 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 the Gjaldstovan TSP Management Board.

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

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
CEO - Chief Executive Officer
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.
CSR - Certificate Signing Request
EAL - Evaluation Assurance Level
EAN - European Article Number
ELF - Eventlog Forwarder
ETSI - The European Telecommunications Standards Institute
FIPS -Federal Information Processing Standard
GPS - Global Positioning System
HSM - Hardware Security Module
IETF - Internet Engineering Task Force
ITU - International Telecommunication Union
NCP - Normalized Certificate Policy
NDA - Non-Disclosure Agreement
NTP - Network Time Protocol
OCSP - Online Certificate Status Protocol
OID - Object IDentifier
PDD - Personnel Data Drive
PDS - PKI Disclosure Statement
PII – Personally Identifiable Information
PIN - Personal Identification Number
PKCS - Public Key Cryptography Standards
PKI - Public Key Infrastructure
RA - Registration Authority
RAP - Registration Authority Policy
RAPS - Registration Authority Practice Statement
RFC – Request for comment
RPA - Relying Party Agreement
RSA - Rivest, Shamir, & Adleman (public key encryption technology)
SIEM - Security Incident and Event management
SOC – Security Operation Center
TSP - Trust Service Provider
URL - Uniform Resource Locator
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, 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 every day of the year, 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. Internal 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 CA implements rigorous identification requirements to ensure that the identity of the Certificate Holder is proven. This includes physical identity verification at the beginning of the certificate request procedure or at some point prior to certificate delivery to the Certificate Holder. The registration procedure will depend on the class and type of certificate that is being applied for. The CA may perform the identification and authentication required in connection with the issue of certificates, or it may delegate the responsibility to one or more registration authorities. The level of identification and authentication depends on the class of certificate being issued. For detailed descriptions see: RAP section 5, available at https://repository.samleiki.fo/legal-repository.

3.1 Naming

3.1.1 Types Of Names

All Certificate Holders require a distinguished name that is in compliance with the X.500 standard for distinguished names. The CA approves naming conventions for the creation of distinguished names for Issuing CA applicants. Different naming conventions may be used by different Issuing CAs. The subject name of all certificates issued to individuals shall be the authenticated common name of the Certificate Holder. The distinguished name fields are fully disclosed in the certificate profiles, available at https://repository.samleiki.fo/profiles. The profiles adhere to ETSI EN 319 412 Part 2: Certificate profile for certificates issued to natural persons.

3.1.2 Need For Names To Be Meaningful

Distinguished names must be meaningful, unambiguous and unique. The CA supports the use of certificates as a form of identification within a particular community of interest. The contents of the certificate subject name fields must have a meaningful association with the name of the individual, organization, or device.

3.1.3 Anonymity or Pseudonymity of Subscribers

Anonymous and pseudonymous certificates are not permitted by this CA.

3.1.4 Rules For Interpreting Various Name Forms

Fields contained in 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 Union (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 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 certificate. The subject name of each issued certificate shall be unique within each class of certificate and shall conform to all applicable X.500 standards for the uniqueness of names and associated rules in certificate profiles.

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

3.1.6 Recognition, Authentication And Role Of Trademarks

Not applicable for the Faroe Islands IssuingCA1 v1.

3.2 Initial Identity Validation

3.2.1 Method To Prove Possession Of Private Key

The CA shall establish that each applicant for a certificate is in possession and control of the private key corresponding to the public key contained in the request for a certificate. See the RAP section 5, available at https://repository.samleiki.fo/legal-repository.

3.2.2 Authentication of Organisation Identity

The Faroe Islands IssuingCA1 v1 will not issue organisational certificates.

3.2.3 Authentication of Individual Identity

See the RAP section 5, available at https://repository.samleiki.fo/legal-repository.

3.2.4 Non-verified Subscriber Information

Certificate Holder information relating to official identity information will be verified against their relating registry, i.e. the Faroese Citizen registry, the Faroese Driver's License registry, the Danish Driver's License registry and the Danish/Faroese Passport registry. Phone number and e-mail are not verified against a registry.

3.2.5 Validation of Authority

Not applicable for the Faroe Islands IssuingCA1 v1.

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:

- the Gjaldstovan TSP Management Board 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 and act under the CP 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 IssuingCA1 v1.

3.3.2 Identification and Authentication for Re-key after Revocation

Not applicable for the Faroe Islands IssuingCA1 v1.

3.4 Identification and Authentication for Revocation Requests

Certificate Holders may request revocation in two ways:

1. Through the identity carrying app
2. By requesting revocation via the RA organization

The identity carrying app includes functionality to revoke the Certificate Holders certificate. In this scenario the Certificate Holders must authenticate using the app in order to access this feature in the app, and is thereby identified as well as authenticated.

In the case where the Certificate Holder does not use the self-service application the subject shall be identified and authenticated by manual means in one of two ways.

1. By contacting the RA office via telephone or online and submitting a revocation request
2. By physically showing up at the RA office and submitting a revocation request

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

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

See section 5.2.2 Who can submit a certificate application in the RAP.

4.1.2 Enrollment Process and Responsibilities

See section 5.2 Application for certificate in the RAP.

4.2 Certificate Application Processing

4.2.1 Performing Identification And Authentication Functions

See section 5.3.1 Performing identification and authentication functions in the RAP.

4.2.2 Approval Or Rejection Of Certificate Applications

See section

- 5.3.2 Approval of certificate applications in the RAP
- 5.3.3 Rejection of certificate applications in the RAP

4.2.3 Time To Process Certificate Applications

See section 5.3.4 Time to process certificate applications in the RAP.

4.3 Certificate Issuance

Issuing a certificate is the CAs acceptance of a certificate application via an approved RA. The issuance of a certificate means that the CA accepts the application and the applicant information that the applicant has declared via an approved RA.

4.3.1 CA Actions During Certificate Issuance

Certificate issuance is governed by and should comply with the practices described in and any requirements imposed by the RAPS of an approved RA.

See also section RA actions during certificate issuance in the RAP.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The first time the Certificate Holder gets a certificate issued a letter will be sent to the home address according to the Faroese Civil Registry via the postal service (snailmail). The Certificate Holder can see a overview of all certificate issuance occasion in the usage log accessible on the self-service portal. The physical letter will only be sent the first time, the Certificate Holder gets a certificate.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

A Certificate Holder is deemed to have accepted a certificate when the Certificate Holder activates the certificate according to section 5.5 Activation data delivery to Certificate Holders in the RAP.

4.4.2 Publication of the certificate by the CA

The certificates are not published.

4.4.3 Notification of certificate issuance by the CA to other entities

Not applicable.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key And Certificate Usage

The Certificate Holder may only use the private Key and corresponding public Key in a certificate for lawful and intended use. The Certificate Holder accepts the Terms and Conditions as part of the application process and if the Terms and Conditions change, the Certificate Holder must accept the changes if he/she still wants to be a Certificate Holder.

4.5.2 Relying party Public Key And Certificate Usage

In order to be an Authorized Relying Party, a party seeking to rely on a certificate agrees to and accepts the Relying Party Agreement, available at https://repository.samleiki.fo/legal-repository, by querying the existence or validity of or by seeking to place or by placing reliance upon a certificate. Authorized 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 certificate for any given purpose and that the use is not prohibited by this CPS
- That the certificate is being used in accordance with its Key-Usage field extensions
- That the 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 according to RFC 3647 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.

The RAP and RAPS however talk about renewal. But it is actually not renewal according to RFC 3647 and ETSI EN 319 411-1 6.3.6, but a new application because it is the issuance of a new certificate with a new Key-pair. To confuse the end-user as little as possible it is however called renewal in the RAP and RAPS, because of the different user experience.

4.6.1 Circumstance for certificate renewal

See section 5.9.2.3 Renewal and replacement in the RAP.

4.6.2 Who may request renewal

See section 5.9.2.3 Renewal and replacement in the RAP.

4.6.3 Processing certificate renewal requests

See section 5.9.2.3 Renewal and replacement in the RAP.

4.6.4 Notification of new certificate issuance to subscriber

The Certificate Holder will receive a push notification on the Samleikin app.

4.6.5 Conduct constituting acceptance of a renewal certificate

See section 5.9.2.3 Renewal and replacement in the RAP.

4.6.6 Publication of the renewal certificate by the CA

The certificates are not published.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable.

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 as such scenarios are treated as new applications.

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.

Certificate modification requests are processed in the same manner as requests for new certificates and in accordance with the provisions of this CPS. As such certificate modification is effectively a new certificate and no publishing of modified certificates is allowed under this CPS.

4.8.1 Circumstance for certificate modification

Certificate modification requests are processed in the same manner as requests for new certificates and in accordance with the provisions of this CPS. As such certificate modification is effectively a new certificate and no publishing of modified certificates is allowed under this CPS.

4.8.2 Who may request certificate modification

Certificate modification requests are processed in the same manner as requests for new certificates and in accordance with the provisions of this CPS. As such certificate modification is effectively a new certificate and no publishing of modified certificates is allowed under this CPS.

4.8.3 Processing certificate modification requests

Certificate modification requests are processed in the same manner as requests for new certificates and in accordance with the provisions of this CPS. As such certificate modification is effectively a new certificate and no publishing of modified certificates is allowed under this CPS.

4.8.4 Notification of new certificate issuance to subscriber

Certificate modification requests are processed in the same manner as requests for new certificates and in accordance with the provisions of this CPS. As such certificate modification is effectively a new certificate and no publishing of modified certificates is allowed under this CPS.

4.8.5 Conduct constituting acceptance of modified certificate

Certificate modification requests are processed in the same manner as requests for new certificates and in accordance with the provisions of this CPS. As such certificate modification is effectively a new certificate and no publishing of modified certificates is allowed under this CPS.

4.8.6 Publication of the modified certificate by the CA

Certificate modification requests are processed in the same manner as requests for new certificates and in accordance with the provisions of this CPS. As such certificate modification is effectively a new certificate and no publishing of modified certificates is allowed under this CPS.

4.8.7 Notification of certificate issuance by the CA to other entities

Certificate modification requests are processed in the same manner as requests for new certificates and in accordance with the provisions of this CPS. As such certificate modification is effectively a new certificate and no publishing of modified certificates is allowed under this CPS.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

See section 5.6.1 Circumstances for revocation in the RAP.

4.9.2 Who Can Request Revocation

See section 5.6.2 Who can submit a revocation request in the RAP.

4.9.3 Procedure For Revocation Request

See section 5.6.3 Revocation request handling in the RAP.

4.9.4 Revocation Request Grace Period

See section 5.6.4 Revocation request grace period in the RAP.

4.9.5 Time Within Which CA Must Process The Revocation Request

As soon as possible.

4.9.6 Revocation Checking Requirement for Relying Parties

Prior to trusting a certificate, it is the Authorized Relying Party's responsibility to check the status of all certificates in the certificate validation chain against the current CRL's or on-line certificate status service (OCSP). A certificate cannot be reasonably relied on if the Authorized Relying Party does not diligently follow the 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
- Certificates may be stored locally by the Authorized Relying Party, but the prevailing revocation status of each of those certificates shall be checked before use
- If valid certificate status information cannot be obtained because of a system or service failure, not a single certificate shall be trusted. The acceptance of a 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 CA, as described in section 2.1.

The CA must comply to the following:

- A new CRL is published at intervals of no more than 1 hour
- The validity time of every CRL is 24 hours

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 certificate revocation lists is 10 minutes.

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 hour update its revocation information by checking the CA database.

4.9.10 On-Line Revocation Checking Requirements

The validity of a 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 certificate with reasonable reliance.

The CA supports an OCSP capability using the GET method for certificates. If the OCSP responder receives a request for status of a 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 CA on which the OCSP request is made.

4.9.11 Other Forms Of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements in Relation to Key Compromise

Not applicable.

4.9.13 Circumstances For Suspension

See section 5.7.1 Circumstances for suspension in the RAP.

4.9.14 Who Can Request Suspension

See section 5.7.2 Who can submit a suspension request the RAP.

4.9.15 Procedure For Suspension Request

See section 5.7.3 Suspension request handling in the RAP.

4.9.16 Limits On Suspension Period

When a certificate has been suspended for more than 7 days, the certificate is automatically revoked.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The Status of certificates issued by the Faroe Islands IssuingCA1 v1 is published in a Certificate Revocation List at http://crl.samleiki.fo/Faroe-Islands-IssuingCA1-v1.crl or is made available via Online Certificate Status Protocol checking at http://ocsp.samleiki.fo/ocsp where available. Revocation entries on a CRL or OCSP response are not removed until after the expiry date of a revoked certificate. The integrity and authenticity of CRL:s is ensured by the Faroe Islands IssuingCA1 v1 by signing CRL:s with a key in sole possession by the Faroe Islands IssuingCA1 v1. The integrity and authenticity of OCSP responses is ensured by the Faroe Islands IssuingCA1 v1 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 at http://ocsp.samleiki.fo/ocsp.

4.10.3 Optional Features

Online Certificate Status Protocol is available for all certificates issued by the Faroe Islands IssuingCA1 v1. The CRL:s and OCSP responders have to be consistent and time used for the provision of revocation services shall be synchronized with UTC at least once every 24 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 Certificate Holder may end a subscription by:

- Allowing a certificate to expire
- Revoking a certificate

4.12 Key Escrow and Recovery

All forms of key escrow and private key recovery of Certificate Holders private keys are forbidden for certificates issued by this 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 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 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 CA-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 CA system.

CA private keys
The generation and maintenance of the CA private keys are facilitated through the use of a Hardware Security Module. The Hardware Security Module used by the CA is certified to FIPS 140-2 level 3 security standard in both the generation and the maintenance in all Issuing CA private keys. The HSM has a Common Criteria EAL 4+ validated cryptographic module. 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 CA private 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 backup data center is located in a solid building.

The building has appropriate location and construction measures.

Engineering building

A part of the technical equipment is located in a separate 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 employee 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 have 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 Samleikin 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 confidentiality agreement.
- Some not so regular visitors will be followed to the data center and then left alone. They have signed a confidentiality agreement.
- Visitors that not have signed at confidentiality agreement will be accompanied at all times.

Backup data center

Before physical accesses are granted to employees the 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 loyee.

There is a burglary alarm connected to the room.

Furthermore, all equipment and data, which are a part of the Samleikin solution, 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 confidentiality agreement.
- Some not so regular visitors will be followed to the data center and then left alone. They have signed a confidentiality agreement.
- Visitors that not have signed at confidentiality agreement will be accompanied at all times.

Engineering building

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 building.

Every access is logged.

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

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 rooms.

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 CA:s 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 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 in regards to m of n and segregation of duties.

Only individuals appointed a trusted role by the 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, 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 Certification Authority and Issuing CA Private Keys.

CA Key Pair generation and initialisation of a Root CA or Issuing CA shall require the active participation of a substantial number of trusted individuals in each case. Such sensitive operations require the active participation and oversight of senior management.

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 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 certificate issuance by the Faroe Islands IssuingCA1 v1 can only be under at least dual control by authorized, trusted personnel such that one person cannot perform all steps of the process resulting in signing an end-user certificate on his/her own.

See also section RA actions during certificate issuance in the RAP.

5.2.3 Identification and Authentication For Each Role

Persons filling trusted roles must undergo an appropriate security screening procedure, according to 5.3.2 of 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, describing the different trusted roles contain information about segregation of duties for each type of trusted role.

5.3 Personnel Controls

Documented controls are implemented with all personnel in any way 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 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 the Gjaldstovan TSP Management Board checks the validity of the most important documents

- Criminal record statement
  The employee has to deliver a criminal record to the Gjaldstovan TSP Management Board, which will be checked.
  Before employment, the 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 the Gjaldstovan TSP Management Board will made relevant checks on

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

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

For existing employee the Gjaldstovan TSP Management Board will check relevant information and ask for more 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.
  The Gjaldstovan TSP Management Board is responsible for defining, what security certification is valid and the Gjaldstovan TSP Management Board facilitate 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.
  The 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.
  The Gjaldstovan TSP Management Board facilitate necessary education in special Samleikin matters.

- System Auditors

  Are internal auditors and they 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

  The 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 the 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, a kind of 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 do not support the use of independent contractors to fulfill trusted roles. Unless such independent contractors are regulated by written agreements 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 provides personnel with the necessary material to perform their duties.

5.4. Audit Logging Procedures

5.4.1 Types Of Events Recorded

The CA records details of the actions taken to process a certificate request and to issue a certificate, including all information generated and documentation received in connection with the certificate request.

The CA logs the following events:

- CA key life-cycle management events
- CA certificate life-cycle events
- All events relating to the life cycle of keys managed by the CA, including any subject keys generated by the CA
- All requests and reports relating to revocation, as well as the resulting action
- CA and Certificate Holder certificate life-cycle management events, including
    - All events related to registration including requests for certificate re-key or renewal is logged by the RA.
    - All registration information including the following shall be recorded:
        - i) type of document(s) presented by the applicant to support registration;
        - ii) record of unique identification data, numbers, or a combination thereof of identification documents, if applicable;
        - iii) storage location of copies of applications and identification documents
        - iv) identity of entity accepting the application;
        - v) method used to validate identification documents, if any; and

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;
- Firewall and router activities; and
- Entries to and exits from the CA facility.

Event logs include at a minimum:

- Date and time of the entry
- Serial or sequence number of entry (for automatic journal entries)
- Details of the entry (name, type etc)
- Source of entry (for example, terminal, port, location, IP address)
- Destination address (if relevant)
- Identity of the entity making the journal entry (e.g. User ID)

The time used to record events as required in the audit log is synchronized with UTC at least once a day. See 6.8 Timestamping, as date and time are described within that scope.

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

Audit logs are retained for the entire lifetime of Samleikin or at least ten (10) years. Audit logs relating to the certificate lifecycle are retained as archive records for the entire lifetime of Samleikin or at least ten (10) years for any certificates issued by the root CA.

5.4.4 Protection Of Audit Log

The relevant audit data collected is regularly analysed for any attempts to violate the integrity of any element of the CA.
Only certain Trusted Roles and auditors may view audit logs in whole. Gjaldstovan 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 being stored at a secure off-site location.

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 at a secure off-site location.

5.4.5 Audit Log Backup Procedures

The CA performs a daily onsite backup of the audit logs. The backup process includes replication to two sites.

5.4.6 Audit Collection System (internal vs. external)

Log collection is handled using ELF (Eventlog Forwarder) on all servers – this setup is described in the Operations manual, chapter ‘Logging -> Log collection.’

For the offline root, a handwritten journal is maintained, and all entries are verified by four-eye principle.

5.4.7 Notification To Event-Causing Subject

In the case of security incidents, alerts are automatically sent from the SIEM (Security Incident and Event management) solutions to the Security Operation Center. Every incident is handled by 1. Level SOC that registers the incident and delegates 2. Level SOC to further investigate the incident. If required the incident is escalated for further expert investigation and processing.

5.4.8 Vulnerability Assessment

The CA undergoes periodic penetration tests 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 CA archives, and makes available upon authorized request, documentation related to and subject to the the Gjaldstovan TSP Management Board document access policy. For each certificate, the records contain information related to creation, issuance, intended use, revocation and expiration. These records will include all relevant evidence in the CA's possession including:

- Audit logs
- Certificate requests and all related actions
- Contents of issued certificates
- Evidence of certificate acceptance and signed (electronically or otherwise) Terms and Conditions
- Revocation requests and all related actions
- Archive and retrieval requests
- Certificate Revocation Lists posted
- Lifecycle events of CA keys
- Audit opinions as discussed in this CPS

5.5.2 Retention Period For Archive
Audit logs relating to the certificate life-cycle are retained as archive records for a period no less than ten (10) years after a certificate ceases to be valid.

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 Boardmay decide to release records of individual transactions upon request of any of the entities involved in the transaction or their recognized representatives.

Archives are stored in multiple copies, in secured on-site and off-site locations.

Archives are stored on redundant media at each site, and all archive data is migrated to new set of media regularly.

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

5.5.4 Archive Backup Procedures
The 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
The CA supports time stamping of its records. All events that are recorded by the 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 CA uses procedures to review and ensure that all systems operating rely on a trusted time source.

All systems synchronize with a time source local to their security zone. The local time sources synchronize with a central hardware based stratum 1 time source.

5.5.6 Archive Collection System (internal or external)
The CA archive collection system is internal. The Gjaldstovan TSP Management Board provides assistance to operators of the 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 regularly checked for consistency. Archives are checked that they have not been altered since it was archived. Archives are also compared across sites.

5.6 Key Changeover

Key changeover is not automatic, but procedures 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 the 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 the 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 CA:s 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
- plan to test backup/restore/continuity arrangements regularly.
- 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.

The 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
  and
- Availability and utilization of needed services with the TSP's network.

There is regular review 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.

In situations where the breach of security or loss of integrity is likely to adversely affect a natural person to whom the trusted service has been provided, the appropriate supervisory body will be contacted 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 Certificate Holders and other entities with which Gjaldstovan has agreements or other form of established relations, among which Authorized Relying Parties and TSP's;
  - 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 Gjaldstovan has to do in case of any of the algorithms, or associated parameters, used by Gjaldstovan or its Certificate Holders become insufficient for its remaining intended usage. The procedures state e.g. that the Gjaldstovan TSP Management Board shall:

1. Inform all 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 certificate issued by the Issuing 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.

Samleikin systems data backup and recovery

1. To allow Samleikin to quickly restore operations in case of incident/disasters, Samleikin's 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 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 Certificate Holders and Authorized Relying Parties, informing them of the status of the CA. In case that the CA is publicly used, make public announcement at least three months in advance that operations will cease for the 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 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 CA for a reasonable period, unless it can be demonstrated that the CA does not hold any such information.

RA termination

See section 8 RA termination in the RAP.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

Each key pair is generated and installed by the Certificate Holders themselves on their smartphone in a self-service activity. The generalized process for eID app installation and certificate generation is described in the RAPS. The key pair is generated on the basis of a sufficiently pseudo random number input which is determined long enough for a validity period of two years. The public key algorithm is RSA with a modulus length of 2048 bit.

6.1.1 Key Pair Generation

Key Pair generation takes place on each Certificate Holder's smartphone during the Certificate Holder enrollment. Proprietary app vendor software ensures that the quality of the key material is sufficient. The private key of the Certificate Holders never leaves the device it was generated on.

Certificate Holder certificates are signed using algorithm as specified in the certificate profiles, available at https://repository.samleiki.fo/profiles, for the certificate signing purposes.

6.1.2 Private Key Delivery To Subscriber

Key Pairs are generated on-device by means of self-service. As such private keys are generated by the Certificate Holder and on the Certificate Holder's smartphone, and they never leave the smartphone.

6.1.3 Public Key Delivery To Certificate Issuer

Public Keys are delivered in a secure and trustworthy manner to the issuing CA by means of CSR:s. Presentation of the PKCS#10 CSR by the Certificate Holder to the Issuing CA is accomplished via encrypted communication between the Certificate Holder smartphone and the PKI system.

For a CSR to be accepted by the CA it has to be signed by the requesting subject. Issued certificates are signed by the 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 certificates within Samleikin are determined by the Gjaldstovan TSP Management Board and defined in the certificate profiles of each type of certificate that can be issued as specified in the certificate profiles, available at https://repository.samleiki.fo/profiles.

6.1.6 Public Key Parameters Generation and Quality Checking

For Certificate Holders, the quality of parameters used to create Public Keys are determined by the relevant Registration Authority application or by the Certificate Holder’s client application.

For Samleikin PKI, its Issuing CAs and RAs, all hardware and associated software platforms meet the requirements of FIPS 140-2, 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)

Keys may be used for the purposes and in the manner described in the certificate profiles, available at https://repository.samleiki.fo/profiles.

This 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 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 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 CA private keys are facilitated through the use of a Hardware Security Module. The Hardware Security Module used by the CA is certified to FIPS 140-2 level 3 security standard in both the generation and the maintenance in all Issuing CA private keys. The HSM has a Common Criteria EAL 4+ validated cryptographic module.

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

All Issuing 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. CA private signing keys stored on the CA's 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

Issuing 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.

Certificate Holder private keys are not backed up.

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.

Certificate Holder private keys are never transferred from their originating device.

6.2.7 Private Key Storage on Cryptographic Module

CA private keys are generated and stored in a physically secure environment within cryptographic modules that are validated to FIPS 140-2 Level-3 and Common Criteria EAL 4+.

The private key of Certificate Holders is stored on a dedicated area on the Certificate Holder's smartphone's disk, inaccessible by other apps and the operating system in an app container, protected by encryption

6.2.8 Method Of Activating Private Key

The private key is activated in an authentication activity by entering a PIN code in the app, known only to the Certificate Holder. 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 CA termination, the 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 video recorded event according to a script approved by the TSP Management Board.

6.2.11 Cryptographic Module Rating

The generation and maintenance of the private keys are facilitated through the use of a Hardware Security Module. The Hardware Security Module used by the CA is certified to FIPS 140-2 level 3 security standard in both the generation and the maintenance in all Issuing CA private keys. The HSM has a Common Criteria EAL 4+ validated cryptographic module.

6.3 Other Aspects of Key Pair Management

CA signing key(s) used for signing issued certificates and/or issuing revocation status information, are not used for any other purpose. The 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, available at https://repository.samleiki.fo/legal-repository.

Public keys associated with Certificate Holders will be recorded in Certificate Holder certificates. The Issuing CA keeps a record of all issued certificates throughout their lifecycle.

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 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 is used to protect access to a private key. One of these factors is the smartphone of the Certificate Holder on which the eID app is installed and the other factor is a PIN-code associated with each certificates private key. The PIN code is generated during the eID enrollment phase. An eID app shall only contain one active certificate.

6.4.2 Activation Data Protection

Activation data is strictly personal and must never be shared with anyone.

Activation data consists of a 6-digit PIN code. See also section RA actions during certificate issuance in the RAP.

6.4.3 Other Aspects Of Activation Data

The user is required to enter the 6-digit PIN code before they are able to use the keys on every use.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The Issuing CA is safeguarded according to best practices and security standards. Rules and requirements 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.
- Principles of least privilege and need-to-know.
- Archive of CA history and audit data.

The Issuing CA is connected to a protected segment of the network with high availability and redundancy measures in place to ensure availability of critical services. Information on this functionality is provided in the respective sections of this CPS.

All security events and PKI operations are logged.

6.5.2 Computer Security Rating

Hardened security modules and software used is certified to FIPS 140-2 level 3 or higher or Common Criteria EAL 4+

6.6 Life Cycle Security Controls

All hardware and software procured for operating the 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 CA must be maintained by causing it to be shipped or delivered via controlled methods. CA equipment shall not have installed applications or component software that is not part of the CA configuration. All subsequent updates to 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 CA follows the Certificate Issuing and Management Components (CIMC) Family of Protections Profiles Version 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

Change control procedures are applied for releases, modifications and emergency software fixes of any operational software and changes to the configuration in the CA systems, including documentation of the changes.

The change control procedures contain a patch management procedure stating that:
a) security patches are applied within a reasonable time after they come available;
b) security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them; and
c) the reasons for not applying any security patches are documented.

The integrity of the CA systems and information is protected against viruses, malicious and unauthorized software. Media used within the CA systems is securely handled to protect media from damage, theft, unauthorized access and obsolescence, within the period of time that records are required to be retained.

The CA employs a configuration management methodology for the installation and ongoing maintenance of the CA 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

For security reason, the details of the network security architecture cannot be disclosed in a public document and are part of the internal documents that are confidential.

Security controls are in line with rules and requirements and include but are not limited to:

- Restricted offline zone
- Availability, Access control and secure defaults
- Network Segmentation

6.7.1 Restricted offline zone

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

6.7.2 Availability, Access control and secure defaults

High availability and redundancy measures are in place to ensure availability of critical services. Firewall access control policies deny any access that is not explicitly permitted (implicit deny) and All security related events are logged. Accounts, applications, services, protocols and ports that are not required or used in the CA's operations are removed or disabled.

6.7.3 Network Segmentation

The network is segmentet into functional, logical or physical segments that are separated and protected by next-generation firewalls using access control policies, Intrusion Protection Systems and Advanced Threat Protection. Operational and administrative networks are separate.

Local network components are kept in a physically and logically secure environment. Local network component configurations are periodically checked for compliance with the requirements specified by the Gjaldstovan TSP Management Board.

6.8 Time-stamping

All Samleikin components are regulary synchronized with a reliable and accurate time service using Network Time Protocol (NTP).

Samleikin uses ntp.elektron.fo as source to establish the correct time for:

- Date and time in audit events
- PKI Operations (CA, VA, RA)
- Timestamping Authority (TSA)

Automatic or manual procedures may be used to maintain system time. Clock adjustmenst are auditable events.

7 Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

All certificates and certificate revocation list profiles conform to RFC 5280 and utilize the ITU-T X.509 version 3 standard.

All 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, using X.509 version 3.

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 certificate describes every certificate extension used for each type of issued 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:1.2.208.189.1.1.2**.** OID assigned for this CPS is: 1.2.208.189.1.1.7.

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. CRLs 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 IssuingCA1 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 hour

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 CA issue 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 performs quarterly internal audits to verify compliance in between external audits.

The Issuing 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 in accordance with ETSI EN 319403 by independent, recognized, credible, and established audit firms accredited as a certifying body for the mentioned ETSI-standards 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.

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 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.

Where the CA fails to take appropriate action in response to an irregularity, the Gjaldstovan TSP Management Board may:

- Indicate the irregularities, but allow the CA to continue operations for a limited period of time
- Allow the CA to continue operations for a maximum of thirty (30) days pending correction of any problems

Any decision regarding which of these actions to take will be based on the severity of the irregularities. Any remedy may include permanent or temporary cessation of the CA's services, but all relevant factors must be considered prior to making a decision. A special audit may be required to confirm the implementation and effectiveness of any remedy.

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 Registration Authorities 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 Registration Authority 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 Registration Authorities shall maintain sufficient assets and financial resources to perform their duties within Samleikin and be reasonably able to bear liability to 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 Certificate Holders and Authorized Relying Parties on questions relating to the different types of insurance available. 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 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 RAP referring to this CPS
- Information in issued 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 the Faroe Islands IssuingCA1 v1 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 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 Faroe Islands IssuingCA1 v1 is public information and deemed not private
- Certificate Revocation Lists/OCSP responses, are not considered to be confidential information
- This CPS and associated RAP, 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 Faroe Islands IssuingCA1 v1 as a result of the practices described in this CPS may be covered by national government or other privacy legislation or guidelines. The Faroe Islands IssuingCA1 v1 will not divulge any private 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 Faroe Islands IssuingCA1 v1, 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 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 Faroe Islands IssuingCA1 v1 and enforceable in that jurisdiction or enforceable under the laws otherwise governing the operations of the Faroe Islands IssuingCA1 v1.

Release As Part Of Civil Discovery

As a general principle, no document or record belonging to the Gjaldstovan TSP Management Board 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 Faroe Islands IssuingCA1 v1 and enforceable in that jurisdiction or enforceable under the laws otherwise governing the operations of the Faroe Islands IssuingCA1 v1.

9.4.7 Other Information Disclosure Circumstances

The Gjaldstovan TSP Management Board and the Faroe Islands IssuingCA1 v1 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 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 CA represents and warrants that, during the period when the certificate is valid, the CA has complied with this CPS in issuing and managing the certificate to the parties listed below:

- The Certificate Holder
- All Authorized Relying Parties who reasonably rely on a valid certificate

The 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 CA

The CA warrants:

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

The 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

RAs will perform their functions and will operate their certification services in accordance with:

- Any applicable RA Agreement
- The RAP and associated RAPS
- All certificate policies under which they issue certificates
- Documented operational procedures
- Applicable law and regulation.

Authorized RA operating within Samleikin hereby warrant that:

- They take reasonable steps to verify that the information contained in any certificate is accurate at the time of issue
- They will request that certificates be revoked by the CA if they believe or are notified that the contents of the certificate are no longer accurate, or that the private key associated with a certificate has been compromised in any way.

9.6.3 Subscriber Representations And Warranties

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

- Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of certificate(s)
- Protection of private key: An obligation and warranty by the 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 certificate(s) and any associated access information or device such as a password or token
- Acceptance of certificate: An obligation and warranty that it will not install and use the certificate(s) until it has reviewed and verified the accuracy of the data in each certificate
- Use of Certificate: An obligation and warranty to use the certificate solely in compliance with all applicable laws, and solely in accordance with the Terms and Conditions 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 certificate, in the event that any information in the certificate is or becomes incorrect or inaccurate or there is any actual or suspected misuse or compromise of the Certificate Holder's private key associated with the public key listed in the certificate
- Termination of use of certificate: An obligation and warranty to promptly cease all use of the private key corresponding to the public key listed in a certificate upon expiration or revocation of that certificate

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

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

- The Certificate Holder retains control of the 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 Certificate Holder's private key
- All representations made by the Certificate Holder to the CA regarding the information contained in the certificate are accurate and true to the best of the Certificate Holder's knowledge or to the extent that the Certificate Holder receives notice of such information, the Certificate Holder shall act promptly to notify the CA of any material inaccuracies contained in the certificate
- The certificate is used exclusively for authorized and legal purposes, consistent with this CPS
- The Certificate Holder agrees with the Terms and Conditions of Samleikin.

9.6.4 Relying Party Representations And Warranties

Authorized Relying Parties represent and warrant that:

- They will collect enough information about a certificate and its corresponding holder to make an informed decision as to the extent to which they can rely on the certificate
- That they are solely responsible for making the decision to rely on a certificate
- That they shall bear the legal consequences of any failure to perform 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 Terms and Conditions, the Relying Party Agreement, the registration authority 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 Certificate Holders or Authorized 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 1.000.000 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, Terms and Conditions, 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 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 certificate or any password or activation data used to control access thereto
- If the 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 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 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 Terms and conditions or any applicable law or regulation
- If the private key associated with the certificate held by the claiming party or otherwise the subject of any claim has been compromised
- If the 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

Certificate Loss Limits

Without prejudice to any other provision of this section, Gjaldstovans liability for breach of its obligations pursuant to this CPS shall, absent fraud or wilful misconduct on the part of Gjaldstovan, be subject to a monetary limit determined by the type of certificate held by the claiming party and shall be limited absolutely to the monetary amounts set out below.

Certificate type	Loss limit
Faroe Islands IssuingCA1 v1	10.000 DKK

In no event shall Gjaldstovans liability exceed the loss limits set out in the table above. The loss limits apply to the life cycle of a particular certificate to the intent that the loss limits reflect Gjaldstovans total potential cumulative liability per certificate per year (irrespective of the number of claims per certificate). The foregoing limitation applies regardless of the number of transactions or causes of action relating to a particular certificate in any one year of that certificate's life cycle.

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 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 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 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 Certificate Holders and Authorized 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.

9.12.2 Notification Mechanism And Period

New or amended CPS: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

Gjaldstovan 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 Gjaldstovan 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 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 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 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

No stipulation.