Country Signer Certificate Authority Faroe Islands Certificate Practice Statement

Version 1.0 - 16.11.2021

Change Log

Version	Change date:	Valid from:	Author:	Change:
0.1	14.07.2021		Janus Læarsson	Initial version.
0.2	16.07.2021		Janus Læarsson	Revised after first review.
1.0	16.11.2021	01.01.2022	Janus Læarsson	Finalized.

1 Introduction

This Certification Practice Statement (CPS) applies to Faroe Islands Health Authority CSCA 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 Health Authority Certification Authority (CSCA) which complies with "Country Signer Certificate Authority Faroe Islands Certificate Policy" OID: 1.2.208.189.2.1.1.

OID for this CPS is: 1.2.208.189.2.1.2

Copyright Notices

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

Or:

TSP@gjaldstovan.fo

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

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

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

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

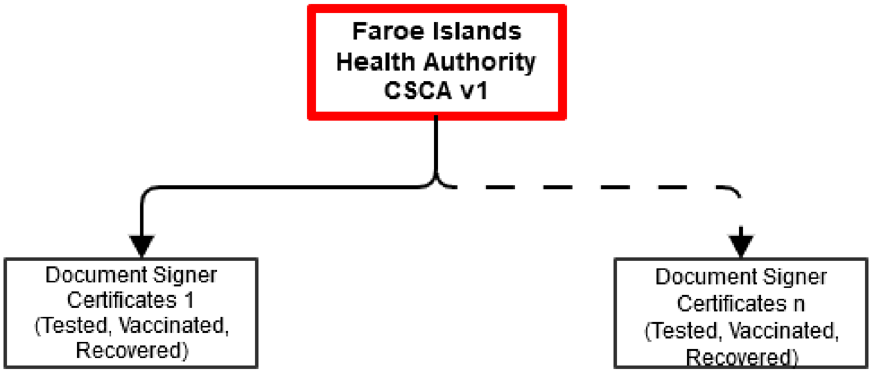
and ICAO on machine readable travel documents:

- ICAO Document 9303 – Machine Readable Travel Documents http://www.icao.int/publications/pages/publication.aspx?docnum=9303

1.1 Overview

This CPS lays out how Faroe Islands Health Authority CSCA v1 conforms to procedures and routines defined in Gjaldstovan Certificate Policy - "Country Signer Certificate Authority Faroe Islands Certificate Policy" OID:1.2.208.189.2.1.1 when issuing certificates.

The following overview represents the CA structure of the Health Authority PKI.


Faroe Islands Health Authority CSCA v1
Document Signer Certificates 1 (Tested, Vaccinated, Recovered)
Document Signer Certificates n (Tested, Vaccinated, Recovered)

1.2. Document Name and Identification

This CPS is titled "Country Signer Certificate Authority Faroe Islands Certificate Practice Statement" with OID 1.2.208.189.2.1.2 and applies to Faroe Islands Health Authority CSCA v1.

1.3. PKI Participants

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

The CSCA holds the root certificate that represents the apex of the Health Authority PKI. The CSCA digitally creates, signs and issues Document Signer Certificates (DSC's) using its CSCA key. DSC's are only issued to approved Holders. An approved DSC Holder utilizes its DSC to create, sign and issue Health Certificates/Machine Readable Documents, such as Digital Green Certificates, to end-users.

DSC's are subordinate services that are:

- Managed and operated by the Faroese Health Authority - Sjúkrahúsverkið, under the Faroese Ministry of Health; or
- Managed by third party organizations

Approved DSC Holders are managed and operated in a manner that meets the contractual, audit and policy requirements dictated by the Gjaldstovan TSP Management Board with regard to operational practices and technical implementation. This CPS describes all subordinate services that operate under the CSCA, i.e. that are within the “chain of trust”.

Participants within the Health Authority PKI include:

- Certification Authorities (CAs);
- Registration Authorities (RAs);
- DSC Holders including applicants for DSC's prior to a DSC issuance; and
- Subscribers, which are the holders of Health Certificates/Machine Readable Documents such as Digital Green Certificates.

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 the Health Authority PKI

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

- Are the minimum practices necessary to ensure that DSC Holders and Subscribers 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 DSC's and Key Pairs

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

DSC's MAY NOT be used, and no participation is permitted in the Health Authority PKI:

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

1.3.1 Certification Authorities

The Health Authority PKI contains the following Root Certification Authorities:

- Faroe Islands Health Authority CSCA v1

DSC's are technical components in the Health Authority PKI, that are operated by an organisation (DSC Holder) who has been given the responsibility to issue, revoke and otherwise manage Health Certificates to end-users.

Organisations operating DSC's MUST be authorized by the Gjaldstovan TSP Management Board to participate within the Health Authority PKI to issue, revoke and otherwise manage certificates. Generally, DSC's are authorized to issue and manage all types of certificates supported by its applicable CP /CPS.

A DSC SHOULD 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 the Health Authority PKI all DSC's 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, DSC Holders are RECOMMENDED to conduct regular compliance audits to ensure that they are complying with their obligations bound by its respective combination of CP/CPS, if such exists. Approved instances of CPS for the Country Signer Certificate Authority are available from https://repository.samleiki.fo/legal-repository/ehealth.

1.3.2 Registration Authorities

The CSCA SHALL act as the RA to manage and approve requests for DSC's. The specific roles of the RA include:

- Process Certificate application requests in accordance with the CPS and applicable RA Agreement, and other policies and procedures with regard to the Certificates issued.
- Maintain and process all supporting documentation related to the Certificate application process,
- Process certificate revocation requests in accordance with this CPS and other relevant operational policies and procedures with respect to the certificates issued. Without limitation to the generality of the foregoing, the RA can request the revocation of any certificate that it has approved for issuance according to the conditions described in this document

For this implementation, the RA accepts certificates dispatched manually. It is the job of the personnel performing the RA role to verify the requests and then process them. An automatic process for certificate request submission MAY be supported. In this case it is secured by SSL and client certificates.

1.3.3 Authorized Relying Parties

Authorized Relying Parties are the DSC Holders that sign objects with DSC's during the personalisation of MRD's.

DSC Holders (Authorized Relying Parties) are required to act in accordance with this CPS and the DSC Holder Agreement. A DSC Holder represents, warrants and covenants with and to the CSCA, Subscribers and the RA processing their application for a DSC that:

- Both as an applicant for a DSC and as a DSC Holder, submit complete and accurate information in connection with an application for a DSC and will promptly update such information and representations from time to time as necessary to maintain such completeness and accuracy.
- Comply fully with any and all information and procedures required in connection with the identification and authentication requirements relevant to the DSC issued.
- Promptly review, verify and accept or reject the DSC that is issued and ensure that all the information set out therein is complete and accurate and to notify the CSCA immediately in the event that the DSC contains any inaccuracies.
- Secure the Private Key and take all reasonable and necessary precautions to prevent the theft, unauthorized viewing, tampering, compromise, loss, damage, interference, disclosure, modification or unauthorized use of its Private Key (to include password, hardware token or other activation data used to control access to the participant’s Private Key).
- Exercise sole and complete control and use of the Private Key that corresponds to the DSC Holder’s Public Key.
- Immediately notify the CSCA 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 DSC Holder’s Private Key SHALL be immediately and permanently discontinued.
- Take all reasonable measures to avoid the compromise of the security or integrity of the Health Authority PKI.
- Forthwith upon termination, revocation or expiry of the DSC, cease use of the DSC absolutely.
- At all times utilize the DSC in accordance with all applicable laws and regulations.
- Discontinue the use of Key Pairs in the event that the CSCA notifies the DSC Holder that the Health Authority PKI has been compromised.

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

1.3.4 Subscribers

Subscribers are, for instance, bearers of Machine Readable Documents such as Digital Green Certificates, or Inspection Systems (for instance QR code scanners). A Subscriber MUST utilize DSC's and their corresponding Public Keys only for authorized and legal purposes and only in support of transactions or communications supported by the Health Authority PKI.

A Subscriber is any entity that places trust on information provided by Certificate Service Providers regarding a specific electronic transaction that the Subscriber uses to accept or reject its participation in the transaction.

The Subscriber is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The Subscriber can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate. A Subscriber MAY use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

A Subscriber SHALL make no assumptions about information that does not appear in a Health Certificates.

1.3.5 Other Participants

Other participants in the Health Authority PKI are required to act in accordance with this CPS and/or applicable agreements.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The CSCA certificate SHALL be the trust point for the Faroe Islands Health Authority.

The CSCA link certificate SHALL be used for verification of a CSCA chain.

The DSC certificate SHALL be used only for signing the data groups as stipulated in the ICAO standards for MRDs.

1.4.2 Prohibited Certificate Uses

Any use not accepted is prohibited.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

This CPS is regularly reviewed and approved by Gjaldstovan.

1.5.2 Contact person

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

Or:

TSP@gjaldstovan.fo

1.5.3 Person Determining CPS Suitability for the Policy

The Gjaldstovan TSP Management Board

1.5.4 CPS Approval Procedures

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

1.6 Definitions and Acronyms

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

CA - Certification Authority

CSCA - Country Signer Certification Authority

CARL - Certification Authority Revocation List

CP - Certificate Policy

CPS - Certification Practice Statement

CRL - Certificate Revocation List

CSP - Certification Service Provider. The more general term Trust Service Provider is used in preference to CSP in the present document except in relation to external references.

CSR - Certicate Signing Request - in the form of a #PKCS10 standard format

DGC - Digital Green Certificate

DSC - Document Signer Certificate

EAL - Evaluation Assurance Level

HSM - Hardware Security Module

MRD - Machine Readable Document

OCSP - Online Certificate Status Protocol

OID - Object IDentifier

PDS - PKI Disclosure Statement

PIN - Personal Identification Number

PKCS - Public Key Cryptography Standards as defined in RFC 2986

PKI - Public Key Infrastructure

RA - Registration Authority

RAP - Registration Authority Policy

RAPS - Registration Authority Practice Statement

RPA - Relying Party Agreement

TLS - Transport Layer Security

TSP - Trust Service Provider

UTC - Coordinated Universal Time

2 Publication and Repository Responsibilities

2.1 Repositories

The Health Authority PKI repository https://repository.samleiki.fo/legal-repository/ehealth serves as the primary repository. This repository holds CP's, CPS's and the RPA. The related repositories are as follows:

- CPSs - https://repository.samleiki.fo/legal-repository/ehealth
- RPA - https://repository.samleiki.fo/legal-repository/ehealth
- Certificate profiles - https://repository.samleiki.fo/profiles
- CA certificates - https://repository.samleiki.fo/legal-repository/ehealth
- CSCA1 v1 CRL - http://crl.samleiki.fo/Faroe-Islands-Health-Authority-CSCA-v1.crl

2.2 Publication of Certification Information

Public audit reports, if such are attained, will be published at https://repository.samleiki.fo/legal-repository/ehealth.

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

2.3 Time or Frequency of Publication

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

2.4 Access Controls on Repositories

Read-only access to repositories is publicly available to 24/7, except for reasonable maintenance requirements, where access is deemed necessary. Queries to the repository MUST specify individual certificate information. The CSCA is the only entity that has write access to repositories. Internal documents not published at https://repository.samleiki.fo/legal-repository/ehealth are available only to participants in the Health Authority PKI where deemed necessary.

3 Identification and Authentication

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

3.1 Naming

3.1.1 Types Of Names

Each CA MUST have a unique and readily identifiable Distinguished Name (DN) according to the X.500 standard. Naming conventions for CAs are approved by the CSCA. Details are found in the certificate profiles: https://repository.samleiki.fo/profiles.

3.1.2 Need For Names To Be Meaningful

Distinguished names MUST be meaningful, unambiguous and unique. The CSCA supports the use of DSC's as a form of identification within a particular community of interest. The contents of the DSC subject name fields MUST have a meaningful association with the name of the individual, organization, or device. In the case of organizations, the name SHALL meaningfully reflect the legal name or registered domain name of the organization or the trading or business name of that organization. In the case of a device, the name SHALL state the name of the device and the legal name or registered domain name of the organization responsible for that device.

3.1.3 Anonymity or Pseudonymity of Subscribers

Anonymous and pseudonymous DSC's are not permitted by this CSCA.

3.1.4 Rules For Interpreting Various Name Forms

Fields contained in CSCA and DSC certificates are in compliance with this CPS and the certificate profiles are fully disclosed here: https://repository.samleiki.fo/profiles. In general, the rules for interpreting name forms can be found in International Telecommunication (ITU) and Internet ring 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 CSCA SHALL approve or assign 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 DSC. The subject name of each issued DSC SHALL be unique within each class of DSC and SHALL conform to all applicable X.500 standards for the uniqueness of names.

The CSCA MAY, if necessary, insert additional numbers or letters to the DSC Holder’s subject common name, or other attribute, in order to distinguish between two DSC's that would otherwise have the same subject name.

3.1.6 Recognition, Authentication And Role Of Trademarks

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

3.2 Initial Identity Validation

3.2.1 Method To Prove Possession Of Private Key

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

1. The DSC Authorized Representative SHALL have a private/public Key Pair generated along with a PKCS#10 CSR.
2. It is strongly RECOMMENDED that the DSC Authorized Representative stores the private key on a Hardware Security Module.
3. The DSC Authorized Representative SHALL present the PKCS#10 CSR to the CSCA.
4. The CSCA verifies the signature of the CSR before issuing the DSC.

3.2.2 Authentication of Organisation Identity

For the CSCA the initial identity validation consists of validating the identity and authorization of the Authorized Representatives who represent the individual DSC's. A representative of the Gjaldstovan TSP Management Board SHALL have the role of identity and authorization verifier of the DSC Holder Authorized Representative and SHALL perform the verification of the identity and of the authorization of the DSC Holder Authorized Representative to act on behalf of the DSC Holder. The procedure is as follows: the DSC Holder Authorized Representative SHALL provide physical identification papers, in the form of their passport or drivers license as proof of identity. The identity verification is documented in an identity verification form and stored in a electronic document archiving system and/or a safe location at Gjaldstovan.

3.2.3 Authentication of Individual Identity

Not applicable for the Faroe Islands Health Authority CSCA.

3.2.4 Non-verified Subscriber Information

Not applicable for the Faroe Islands Health Authority CSCA.

3.2.5 Validation of Authority

The Gjaldstovan TSP Management Board will decide on authority for applicants of DSC's.

3.2.6 Criteria for Interoperation

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

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

3.3 Identification and Authentication for Re-key Requests

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

3.3.1 Identification and Authentication for Routine Re-key

Not applicable for the Faroe Islands Health Authority CSCA.

3.3.2 Identification and Authentication for Re-key after Revocation

Not applicable for the Faroe Islands Health Authority CSCA.

3.4 Identification and Authentication for Revocation Requests

For the CSCA the identity validation for revocation requests consists of validating the identity of the Authorized Representatives who represent the revocation requests. A representative of the Gjaldstovan TSP Management Board SHALL have the role of identity verifier of the requesting party Authorized Representative and SHALL perform the verification of the identity of the requesting party Authorized Representative. The procedure is as follows: the requesting party Authorized Representative SHALL provide physical identification papers, in the form of their passport from the kingdom of Denmark or a Danish or Faroese drivers license as proof of identity. The identity verification is documented in a electronic document archiving system and /or a safe location at Gjaldstovan.

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

4 Certificate Life-Cycle Operational Requirements

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

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

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

4.1.2 Enrollment Process and Responsibilities

All signed applications SHALL be securely stored for the lifetime of the issued DSC's (or until the Issuing CA is terminated for some reason), in an electronic document archiving system and/or in a safe approved by Gjaldstovan.

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

The DSC's Key Pair is never generated by the CSCA and the DSC request process SHALL check that the DSC Holder has possession or control of the private key associated with the public key presented for certification, as described in section 3.2.

The following steps are required in any application for a DSC:

1. Identity of the Holder or Device is to be established in accordance with section 3.2.

2. It is strongly RECOMMENDED that a Key Pair to a DSC application and its associated certificate is to be generated and stored in a secure fashion on an approved Hardware Security Module, certified to FIPS 140-2 level 3 or higher or Common Criteria EAL 4+.
3. The binding of the Key Pair to the certificate SHALL occur as set forth in this CPS in section 3.2.
4. The DSC Holder SHALL be in contractual relations - in form of a signed DSC Holder Agreement - with the Gjaldstovan TSP Management Board for the use of that DSC.

4.2 Certificate Application Processing

4.2.1 Performing Identification And Authentication Functions

The Gjaldstovan TSP Management Board SHALL have the role of identity and ID document authenticity and validity verifier and SHALL perform and document the verification of the identity of the applicant DSC Holder Authorized Representative. The procedure is as follows for each applicant DSC Holder:

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

4.2.2 Approval Or Rejection Of Certificate Applications

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

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

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

4.2.3 Time To Process Certificate Applications

The Gjaldstovan TSP Management Board MUST process the DSC applications within 30 working days.

4.3 Certificate Issuance

Issuing a DSC is the CSCAs acceptance of a DSC application from the Gjaldstovan TSP Management Board. The issuance of a DSC means that the CSCA accepts the application and the applicant information that the applicant has declared.

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

4.3.1 CA Actions During Certificate Issuance

The CSCA only issues DSC's as specified by approved certificate profiles. These are located here: https://repository.samleiki.fo/profiles and these are:

- Document Signer: DSC Vaccination Profile
- Document Signer: DSC Test Profile
- Document Signer: DSC Recovery Profile
- Document Signer: DSC Profile

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

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

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

Faroe Islands Health Authority CSCA v1

The Health Authority CSCA Certificate has been self-generated and self-signed according to strictly controlled and audited key ceremonies that are approved by Gjaldstovan TSP Management Board and audited by a CSCA Security Officer acting as auditor.

The CSCA never generates another CA's Key Pair.

The CSCA Key Pairs are generated on behalf of the CSCA.

Document Signer Certificates

Upon accepting the terms and conditions of the RPA by the DSC Holder, successful completion of the DSC application process as prescribed by Gjaldstov an TSP Management Board, the CSCA issues the DSC to the relevant DSC Holder.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The CSCA does in-person notification to applicants when DSC's have been issued.

4.4 Certificate Acceptance

This CPS sets out what constitutes acceptance of a DSC. An applicant that accepts a DSC warrants to the CSCA, and all Subscribers who reasonably rely, that all information supplied in connection with the application process and all information included in the DSC issued to them is true, complete, and not misleading. Without limitation to the generality of the foregoing, the use of a DSC or the reliance upon a DSC signifies acceptance of the terms and conditions of this CPS and RPA (as the same MAY, from time to time, be amended or supplemented) by which they irrevocably agree to be bound.

By accepting a DSC, the DSC Holder expressly represents and warrants to the CSCA and all Subscribers who reasonably rely on the information contained in the DSC that at the time of acceptance and throughout the operational period of the DSC, until notified otherwise by the DSC Holder, that:

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

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

The Gjaldstovan TSP Management Board SHALL for the lifetime of the Health Authority PKI record all the signed agreements with the DSC Holders in safe storage.

4.4.1 Conduct Constituting Certificate Acceptance

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

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

4.4.2 Publication of the Certificate by the CA

All DSC's are made available here: https://repository.samleiki.fo/legal-repository/ehealth

4.4.3 Notification of Certificate Issuance by the CA to other Entities

DSC's within Health Authority PKI MAY choose to notify other entities of DSC issuance.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key And Certificate Usage

Within the Health Authority PKI, a DSC Holder MUST only use the private key and corresponding public key in a DSC for their lawful and intended use. The DSC Holder accepts the RPA and by accepting the DSC unconditionally agrees to use the DSC in a manner consistent with the key-usage field extensions included in the certificate profile of the issued DSC.

All issued DSC's MUST use an algorithm for its associated Key Pair that is specified on the DSC profile of every issued DSC. It is RECOMMENDED that all Key Pairs be generated on a hardware security module accredited to FIPS 140-2 level 3 in a configuration that allows non-FIPS algorithms. Furthermore it is RECOMMENDED that private keys only be stored and used within a hardware security module accredited to FIPS 140-2 level 3 in a configuration that allows non-FIPS algorithms.

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

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

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

4.5.2 Subscriber Certificate Usage

Subscribers SHALL use DSC's and associated public keys for the verification of the signed object data (SOD) on a MRD.

The Subscriber is solely responsible for deciding whether or not to rely on the information in a certificate provided to accept or reject their participation in the transaction.

4.6 Certificate Renewal

Certificate renewal means the issuance of a new certificate without changing the Key-pair. The Health Authority PKI does not support certificate renewal for end entity certificates or DSC's.

4.6.1 Circumstance for Certificate Renewal

All forms of certificate renewal is forbidden under this CPS.

4.6.2 Who May Request Renewal

All forms of certificate renewal is forbidden under this CPS.

4.6.3 Processing Certificate Renewal Requests

All forms of certificate renewal is forbidden under this CPS.

4.6.4 Notification of New Certificate Issuance to Subscriber

All forms of certificate renewal is forbidden under this CPS.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

All forms of certificate renewal is forbidden under this CPS.

4.6.6 Publication of the Renewal Certificate by the CA

All forms of certificate renewal is forbidden under this CPS.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

All forms of certificate renewal is forbidden under this CPS.

4.7 Certificate Re-Key

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

4.7.1 Circumstance for Certificate Re-Key

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

4.7.2 Who May Request Certification of a New Public Key

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

4.7.3 Processing Certificate Re-Keying Requests

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

4.7.4 Notification of New Certificate Issuance to Subscriber

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

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

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

4.7.6 Publication of the Re-Keyed Certificate by the CA

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

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

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

4.8 Certificate Modification

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

The CSCA MAY reissue or replace a valid CA certificate when the CA Certificate's common name, organization name, device name, or geographic location changes. Modified information MUST undergo the same identification and authentication procedures as for a new CA Certificate.

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

4.8.1 Circumstance for Certificate Modification

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

4.8.2 Who May Request Certificate Modification

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

4.8.3 Processing Certificate Modification Requests

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

4.8.4 Notification of New Certificate Issuance to Subscriber

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

4.8.5 Conduct Constituting Acceptance of Modified Certificate

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

4.8.6 Publication of the Modified Certificate by the CA

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

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

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

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

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

- Private key compromise
- Certificate creation error
- Key compromise including unauthorized access or suspected unauthorized access to private keys, lost or suspected lost keys, stolen or suspected stolen keys, destroyed or suspected destroyed keys or superseded by replacement keys and a new CSCA Certificate or DSC
- The CSCA or DSC Holder has failed to meet obligations under this CPS or any other agreement, regulation, or law that may be in force with respect to a particular certificate
- The CSCA Certificate or DSC was not issued in accordance with the terms and conditions of this CPS or the CSCA or DSC Holder provided inaccurate, false or misleading information
- The private key corresponding to a CSCA Certificate or DSC has been used to sign, publish or distribute spyware, trojans, viruses, rootkits, browser hijackers, or other content, for phishing, or conduct that is harmful, malicious, hostile or to download malicious content onto a system without consent
- Where a CSCA requests revocation because:

    - A change in the relationship between the DSC Holder and the CSCA
    - The DSC Holder is no longer authorized to act as a DSC Holder
    - The DSC Holder otherwise becomes unsuitable or unauthorized to hold the DSC
- Affiliation change
- Cessation of operation
- Incorrect information contained in a CSCA Certificate or DSC
- DSC Holder bankruptcy
- DSC Holder liquidation
- Breach of RPA with the Gjaldstovan TSP Management Board
- Any of the information appearing in a CSCA Certificate or DSC is inaccurate or misleading
- The CSCA obtains reasonable evidence that there has been loss, theft, modification, unauthorized disclosure, or other compromise of the private key corresponding to the public key within the certificate, or that the certificate has otherwise been misused
- The CSCA receives notice or otherwise becomes aware that a DSC Holder has breached a material obligation under the RPA or other contractual obligations
- The Gjaldstovan TSP Management Board receives a lawful and binding order from a government or regulatory body to revoke the CSCA Certificate or DSC
- The Gjaldstovan TSP Management Board determines, in its sole discretion, that the CSCA Certificate or DSC was not issued in accordance with the terms and conditions of this CPS
- The Gjaldstovan TSP Management Board receives notice or otherwise becomes aware that there has been some other modification of the information pertaining to the DSC Holder that is contained within the DSC
- The DSC Holder fails or refuse to comply, or to promptly correct inaccurate, false or misleading information after being made aware of such inaccuracy, misrepresentation or falsity
- Either the DSC Holder's or the CSCA's obligations under this CPS are delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond reasonable control, and as a result another entity is threatened or compromised
- The technical content or format of the CSCA Certificate or DSC presents an unacceptable risk to Subscribers (a deprecated cryptographic /signature algorithm or key size presents an unacceptable risk and that such CSCA Certificates or DSC's SHOULD be revoked and replaced as soon as reasonably practical upon notification)
- Other reasons as decided by the Gjaldstovan TSP Management Board

The DSC Holder of a revoked DSC, SHALL be informed of the change of status of the DSC. In the case of the CSCA, Gjaldstovan TSP Management Board SHALL notify the DSC Authorised Representative immediately when the decision is made that the CSCA Certificate is to be revoked. Furthermore the Gjaldstovan TSP Management Board SHALL immediately inform the DSC Authorised Representative when there is suspicion of the integrity of the CSCA Certificate or DSC.

A revoked CSCA Certificate or DSC is indefinitely revoked and will never be reinstated.

4.9.2 Who Can Request Revocation

The following entities MAY request revocation of a CSCA Certificate or DSC:

- The Gjaldstovan TSP Management Board, representing the CSCA, MAY revoke any Certificate issued at its sole discretion, and SHALL publish the list of revoked Certificates in a publicly accessible certificate revocation list status service
- A DSC Holder MAY request revocation of its DSC's

4.9.3 Procedure for Revocation Request

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

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

4.9.4 Revocation Request Grace Period

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

4.9.5 Time Within Which CA Must Process the Revocation Request

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

4.9.6 Revocation Checking Requirement for Subscribers

Subscribers SHALL comply with the signature validation requirements defined in this CPS.

4.9.7 CRL Issuance Frequency

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

The CSCA MUST comply to the following:

- A new CRL is published at intervals of not more than 1 day

- The validity time of every CRL is 10 days

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

CRLs SHALL be published immediately in the repositories after certificate revocation. Certificate status information MUST be updated immediately.

4.9.9 On-Line Revocation/Status Checking Availability

No online revocation checking is supported.

4.9.10 On-Line Revocation Checking Requirements

Not applicable.

4.9.11 Other Forms Of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements Re-Key Compromise

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

4.9.13 Circumstances for Suspension

No suspension of Certificates is permissible by the CSCA.

4.9.14 Who Can Request Suspension

No suspension of Certificates is permissible by the CSCA.

4.9.15 Procedure For Suspension Request

No suspension of Certificates is permissible by the CSCA.

4.9.16 Limits On Suspension Period

No suspension of Certificates is permissible by the CSCA.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The status of DSC's issued by the CSCA is published in a Certificate Revocation List http://crl.samleiki.fo/Faroe-Islands-Health-Authority-CSCA-v1.crl. Revocation entries on a CRL are not removed until after the expiry date of a revoked Certificate. The integrity and authenticity of CRL's is ensured by the CSCA by signing CRL's with a key in sole possession by the CSCA.

4.10.2 Service Availability

Certificate status services are available 24 hours a day, 7 days a week, 365 days of the year on http://crl.samleiki.fo/Faroe-Islands-Health-Authority-CSCA-v1.crl.

4.11 End of Subscription

A DSC Holder MAY end a subscription by:

- Allowing a DSC to expire
- Revoking a DSC

4.12 Key Escrow and Recovery

All forms of key escrow and private key recovery of DSC Holders private keys are forbidden for DSC's issued by this CSCA.

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 CSCA 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 CSCA 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 CSCA system, and a system, a policy, procedures and controls are in place to ensure the correctness of the content.

Physical and Environmental Securiy

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

CSCA Private Keys

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

5.1.1 Site Location and Construction

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

Main data center

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

The building has appropriate location and construction measures.

Backup data center

The building has appropriate location and construction measures.

5.1.2 Physical Access

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

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

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

Main data center

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

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

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

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

Furthermore, all equipment and data, which are a part of the Health Authority PKI, 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 they MUST have a work-related need, have signed a duty of confidentiality, a background check has been made and a relevant manager have approved the access.

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

There is a burglary alarm connected to the room.

Furthermore, all equipment and data, which are a part of the Health Authority PKI, 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.

5.1.3 Power and air conditioning

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

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

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

There are backup systems for the primary cooling.

5.1.4 Water Exposures

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

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

5.1.5 Fire Prevention and Protection

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

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

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

The fire station is only a few minutes away.

5.1.6 Media Storage

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

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

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

Some assets are in other secure safes e.g. offline backup HSM's and the activation keys and PIN's 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 use of a certified disk shredder
- Magnetic tapes are not used
- Other magnetic media are destroyed by use of a certified disk shredder
- 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.

5.2.1. Trusted Roles

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

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

The categories of high level trusted roles in use are:

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

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

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

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

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

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

5.2.2. Number of Persons Required Per Task

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

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

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

DSC's MUST ensure that no single individual may gain access to any Private Key (other than the DSC Holder's own Private Key). At a minimum, procedural or operational mechanisms MUST be in place for DSC key recovery in disaster recovery situations. To best ensure the integrity of the CA equipment and operation, DSC Holders 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 DSC issuance by the CSCA can only be under at least dual control by authorized, trusted personnel such that one person cannot sign subordinate certificates on his/her own.

5.2.3 Identification and Authentication for Each Role

Persons filling trusted roles MUST undergo an appropriate security screening procedure, according to section 5.3.2 in this CPS.

Each individual performing any of the trusted roles SHALL use the identification and authentication mechanism specified for the specific trusted role in the internal documents to authenticate themselves.

5.2.4. Roles Requiring Separation of Duties

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

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

5.3 Personnel Controls

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

5.3.1 Qualifications, Experience, and Clearance Requirements

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

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

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

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

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

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

At least every three years Gjaldstovan TSP Mgmt. Board:

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

Job Descriptions

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

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

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

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

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

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

Access to the Systems and Data

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

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

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

5.3.2 Background Check Procedures

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

Some of the checks for new employee are:

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

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

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

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

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

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

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

5.3.3 Training Requirements

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

Personnel in trusted roles meets additional requirements e.g.

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

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

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

- Internal Auditors

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

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

  Gjaldstovan TSP Management Board facilitate necessary education in special Health Authority PKI matters.

5.3.4 Retraining Frequency and Requirements

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

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

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

5.3.5 Job Rotation Frequency and Sequence

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

5.3.6 Sanctions for Unauthorized Actions

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

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

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

5.3.7 Independent Contractor Requirements

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

5.3.8 Documentation Supplied to Personnel

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

5.4. Audit Logging Procedures

5.4.1 Types of Events Recorded

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

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

The following information will be logged for later audit:

CA key lifecycle management events;

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

Event logs include:

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

5.4.2 Frequency of Processing Log

Audit logs are verified and consolidated at least yearly.

5.4.3 Retention Period for Audit Log

All Audit logs will be kept for the entire lifetime of the Health Authority PKI.

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.’

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

5.6 Key Changeover

Key changeover is not automatic, but procedures that enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of the CA Private Key's lifetime, the CA ceases using its expiring CA Private Key to sign Certificates (well in advance of expiration) and uses the old Private Key only to sign CRL's 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 Health Authority CSCA v1	4 years	2 years

At "Stop Issuance Date" CA stops issuing Certificates with the old key and MUST some time before that initiate generation of a new key pair. CA Key Changeover MUST be generated in a key-ceremony approved by Gjaldstovan TSP Management Board. The new CSCA Certificate associated with the new public key is published in the Health Authority repository - while the old CSCA 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.

If there is need for a key changeover before the "Stop Issuance Date", for example because of key weakness etc., the CA Key Changeover MUST in the same way as above be generated in a key ceremony approved by Gjaldstovan TSP Management Board. The new CSCA Certificate with the new public key is published in the Health Authority 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.

5.7 Compromise and Disaster Recovery

The Gjaldstovan TSP Management Board has:

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

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

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

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

5.7.1 Incident and Compromise Handling Procedures

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

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

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

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

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

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

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

- discover the issue
- limit possible consequences
- notify relevant parties within 24 hours
- where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the natural or legal person will also be notified of the breach of security or loss of integrity without undue delay.

5.7.2 Computing Resources, Software and/or Data are Corrupted

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

The Business Disaster and Continuity Team is responsible.

5.7.3 Entity Private Key Compromise Procedures

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

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

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

1. Inform all CA Certificate Holders and DSC Holders with whom Gjaldstovan has agreement or other form of established relations. In addition, this information SHALL be made available to other Subscribers;

   and

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

5.7.4 Business Continuity Capabilities After a Disaster

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

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

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

CA Systems Data Backup and Recovery

1. To allow the Health Authority PKI to quickly restore operations in case of incident/disasters, 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 CSCA 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 DSC Holders and Subscribers, informing them of the status of the CSCA. In case that the CSCA is publicly used, make public announcement at least three months in advance that operations will cease for the CSCA.
- 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 CSCA 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 CSCA for a reasonable period, unless it can be demonstrated that the CSCA does not hold any such information.

RA Termination

Not applicable.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

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

6.1.1 Key Pair Generation

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

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

- Roles participating in the ceremony (internal and external from the organization)
- Functions to be performed by every role and in which phases
- Responsibilities during and after the ceremony
- Requirements of evidence to be collected of the ceremony

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

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

6.1.2 Private Key Delivery to Subscriber

The CSCA never generate Key Pairs for DSC's and do not have any type of access to private keys associated with issued certificates.

6.1.3 Public Key Delivery to Certificate Issuer

Public Keys are delivered in a secure and trustworthy manner to the CSCA by means of CSRs. Presentation of the PKCS#10 CSR by the DSC Holder Authorized Representative to the CSCA is accomplished in accordance with the formal procedure for certificate application stated in 4.1 of this CPS and in accordance with the identity validation stated in 3.2 of this CPS. For a CSR to be accepted by the CSCA it has to be signed by the requesting subject. Issued DSC's are signed by the CSCA only if it is in compliance with this CPS.

6.1.4 CA Public Key Delivery to Authorized Relying Parties

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

6.1.5 Key Sizes

The following key sizes SHALL be supported:

- CSCA: 256 bits
- DSC: 256 bits

6.1.6 Public Key Parameters Generation and Quality Checking

The following parameters and algorithms SHALL be supported:

- CSCA: ECDSA, prime256v1 named curve, SHA-256
- DSC: ECDSA, prime256v1 named curve, SHA-256

6.1.7 Key Usage Purposes (as per. x.509 v3 Key Usage Field)

Private Keys corresponding to Faroe Islands Health Authority CSCA v1 Certificates are not used to sign Certificates except in the following cases:

(i) Self-signed Certificates to represent the Faroe Islands Health Authority CSCA itself;

(ii) CRL signing

(iii) DSC signing

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

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

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

All CSCA 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 CSCA 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. CSCA private signing keys stored on the CSCA'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

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

6.2.5 Private Key Archival

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

6.2.6 Private Key Transfer Into or From a Cryptographic Module

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

6.2.7 Private Key Storage on Cryptographic Module

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

6.2.8 Method of Activating Private Key

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

6.2.9 Method of Deactivating Private Key

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

6.2.10 Method Of Destroying Private Key

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

6.2.11 Cryptographic Module Rating

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

6.3 Other Aspects of Key Pair Management

CSCA signing key(s) used for signing issued DSC's and/or issuing revocation status information, are not used for any other purpose.

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

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

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

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

6.4.2 Activation Data Protection

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

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

6.4.3 Other Aspects of Activation Data

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

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Certificate generation and revocation management is a manual procedure. All PKI operations require multiple roles and duties separation and are logged.

The CSCA 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.

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

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

6.5.2 Computer Security Rating

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

6.6 Life Cycle Security Controls

All hardware and software procured for operating the CSCA is purchased in a manner that will mitigate the risk that any particular component was tampered with. Equipment developed for use within the Health Authority PKI 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 CSCA MUST be maintained by causing it to be shipped or delivered via controlled methods. CSCA equipment SHALL NOT have installed applications or component software that is not part of the CSCA configuration. All subsequent updates to CSCA 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 CSCA follows the Certificate Issuing and Management Components (CIMC) Family of Protections Profiles 1.5 that defines the requirements for components that issue, revoke and manage Public Key Certificates, such as X.509 Certificates. The CIMC is based on the common Criteria/ISO IS15408 standards.

6.6.3 Life Cycle Security Controls

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:

- Availability, access control and secure defaults
- Network segmentation

6.7.1 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.

6.7.2 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 the Health Authority PKI components are regulary synchronized with a reliable and accurate time service using Network Time Protocol (NTP).

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

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

7.1.1 Version Numbers

Certificate profile version is 1.

7.1.2 Certificate Extensions

The extensions defined for X.509 v3 certificates provide methods for associating additional attributes with public keys and for managing relationships between CAs. The certificate profile of each type of issued DSC describes every certificate extension used for each type of issued DSC. 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:1.2.208.189.2.1.1. OID assigned for this CPS is: 1.2.208.189.2.1.2.

7.1.7 Usage of Policy Constraints Extension

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

7.1.8 Policy Qualifiers Syntax and Semantics

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

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

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

7.2 CRL Profile

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

CRL basic fields are listed in the table below:

Field name	Field description and contents	Critical
CRL Version	This field states which of the CRL versions defined in the X.509 standard the CRL conforms to. The CRLs conform to the version 2.	2

Signature Algorithm	The CRLs are signed by using the same algorithm as is used for signing of the certificates. The algorithm used is ecdsa-with-SHA512.	ecdsa-with-SHA256

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 Health Authority CSCA v1

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 the Health Authority PKI the ecdsa-with-SHA256 hash algorithm is used to calculate the identifier.	ee3c81a6e61eb6517444e0d0f43033e2ea6abea1
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.	N/A

7.2.1 Version Number

The CSCA issues X.509 version 2 Certificate Revocation Lists.

7.2.2 CRL and CRL Entry Extensions

See table in 7.2.

7.3 OCSP Profile

Online Certificate Status Protocol is not enabled within the Health Authority PKI.

7.3.1 Version Numbers

Not applicable.

7.3.2 OCSP Extensions

Not applicable.

8 Compliance Audit and Other Assessment

The TSP Management Board MAY require ad-hoc compliance audits of CSCA to validate that it is operating in accordance with the respective CP, CPS, and other supporting operational policies and procedures.

8.1 Frequency or Circumstances of Assessment

No stipulations.

8.2 Identity/Qualifications of Assessor

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

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 CSCA may include but may not be limited to:
- Security Policy and Planning;
- Physical Security;
- Technology Evaluation;
- Services Administration;
- Personnel Vetting;
- Contracts; and
- Privacy Considerations.

8.5 Actions Taken as a Result of Deficiency

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

8.6 Communication Of Results

Any audit results - for instance a conformity certificate - will be posted at https://repository.samleiki.fo/legal-repository/ehealth.

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

Gjaldstovan is required to demonstrate that they have the financial resources necessary to discharge their obligations under its CP/CPS and any other relevant and associated documentation or agreements.

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

Gjaldstovan is a governmental institution. Gjaldstovan is, as a governmental institution, part of the faroese yearly Finance Act. Funds for Samleikin is additionally authorized by law of the Løgting about Talgildu Føroyar (Løgtingslóg nr. 77 frá 29. mai 2017 um Talgildu Føroyar).

The state's insurance policies are laid down in government circular "Rundskriv nr. 9000 frá 21. november 2003 um tryggingarviðurskifti landsins".

9.2.2 Other Assets

The CA and RAs SHALL maintain sufficient assets and financial resources to perform their duties within the Health Authority PKI and be reasonably able to bear liability to DSC Holders and Subscribers.

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 DSC Holders and Subscribers on questions relating to the different types of insurance available. DSC 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.

Subscribers are entitled to apply to commercial insurance providers for protection against financial loss.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

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

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

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

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

9.3.2 Information Not Within the Scope of Confidential Information

The following information is not deemed to be confidential:

- This CPS and each CPS referring to this CPS
- Information in issued CA Certificates including public keys
- 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 CSCA 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

- Dátuverndarlógin (Løgtingslóg nr. 80 frá 7. juni 2020 um vernd av persónupplýsingum) and any amending and/or implementing legislation enacted from time to time.

9.4.2 Information Treated as Private

All information about DCS 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 a DSC due to:

- The compromise of the DSC's Private Key, in which case a disclosure may be made that the Private Key has been compromised
- The termination of an DSC within the Health Authority PKI, 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 CSCA is public information and deemed not private
- Certificate Revocation Lists are not considered to be confidential information
- This CPS and any associated CPs, is a public document and is not confidential information and is not treated as private

9.4.4 Responsibility to Protect Private Information

Information supplied to the CSCA as a result of the practices described in this CPS may be covered by national government or other privacy legislation or guidelines. The CSCA will not divulge any private DSC 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 CSCA, and used as explained in the registration process. They have also been given an opportunity to decline from having their personal data used for particular purposes. They have also agreed to let certain personal data appear in publicly accessible directories and be communicated to others.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

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

Release as Part of Civil Discovery

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

9.4.7 Other Information Disclosure Circumstances

The Gjaldstovan TSP Management Board and the CSCA 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 Health Authority PKI system components.

Confidentiality and integrity of data

By complying to international standards, regulation, the Health Authority policies and other relevant demands, the Health Authority PKI 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 CSCA 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 CSCA represents and warrants that, during the period when the certificate is valid, the CSCA has complied with this CPS in issuing and managing the certificate to the parties listed below:

- The party to the relevant RPA
- All Subscribers who reasonably rely on a valid CA Certificate

The CSCA discharges its obligations by:

- Providing the operational infrastructure and certification services, including the Repository 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 CSCA

The CSCA warrants:

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

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

9.6.2 RA Representations and Warranties

No stipulations

9.6.3 Subscriber Representations and Warranties

As part of the RPA agreed to by all DSC Holders, the following commitments and warranties are made for the express benefit of the CSCA, DSC Holders and all Subscribers:

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

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

Upon accepting a DSC the DSC Holder represents to the CSCA and to Subscribers that at the time of acceptance and until further notice:

- The DSC Holder retains control of the DSC 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 DSC Holder’s private key
- All representations made by the DSC Holder to the CSCA regarding the information contained in the DSC are accurate and true to the best of the DSC Holder’s knowledge or to the extent that the DSC Holder receives notice of such information, the DSC Holder SHALL act promptly to notify the CSCA of any material inaccuracies contained in the DSC
- The DSC is used exclusively for authorized and legal purposes, consistent with this CPS
- The DSC Holder agrees with the terms and conditions of this CPS and other agreements and policy statements of the Gjaldstovan TSP Management Board.

9.6.4 Subscriber Representations and Warranties

Subscribers represent and warrant that:

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

9.6.5 Representations and Warranties of Other Participants

Participants within the Health Authority PKI 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 and the RPA and any other contractual documentation applicable within the Health Authority PKI 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 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.

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 the Health Authority PKI, any person that participates within the Health Authority PKI 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 the Health Authority PKI.

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

Mitigation of Gjaldstovans Liability

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

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

These measures include but are not limited to:

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

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

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

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

9.9 Indemnities

If an invalid claim for damages will be presented against the Gjaldstovan, the DSC 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 DSC Holder or Subscriber from the Health Authority PKI with respect to all actions based upon the use of or reliance upon a certificate or other participation within the Health Authority PKI. Any such termination or withdrawal SHALL NOT act so as to prejudice or affect any right of action or remedy that may have accrued to any person up to and including the date of withdrawal or termination.

9.11 Individual notices and communications with participants

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

9.12 Amendments

9.12.1 Procedure For Amendment

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

There are two possible types of policy change:

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

If an existing CPS requires re-issue, the change process employed is the same as for initial publication, as described above. If a policy change is determined to have a material impact on a significant number of DSC Holders and Subscribers, 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 the Health Authority PKI.

DSC Holders are notified of changes to the CPS as and when they are approved.

9.12.2 Notification Mechanism and Period

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

9.12.3 Circumstances Under Which OID Must Be Changed

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

9.13 Dispute Resolution Provisions

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

E-mail adress is: gjaldstovan@gjaldstovan.fo

Postal mail:

Gjaldstovan
Kvíggjartún 1,
FO-160 Argir
Faroe Islands

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

Any controversy or claim between two or more participants in the Health Authority PKI 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 CSCA 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 CSCA, comply with applicable national, local and foreign laws, rules, regulations, ordinances, decrees and orders.

9.16 Miscellaneous Provisions

9.16.1 Entire agreement

No stipulations.

9.16.2 Assignment

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

9.16.3 Severability

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

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

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

9.16.5 Force Majeure

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

9.17 Other Provisions

The parts of the Health Authority PKI concerned with certificate generation and revocation management SHALL be independent of other organizations for its decisions relating to the establishing, provisioning and maintaining and suspending of services in conformance with the applicable certificate policies. In particular its senior executive, senior staff and staff in trusted roles, SHALL be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides. The parts of the Health Authority PKI concerned with certificate generation and revocation management SHALL have a documented structure which safeguards impartiality of operations.

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