Samleikin PKI disclosure statement

Version 1.1 - 09.06.2021

Change Log

Version	Change date:	Valid from	Author:	Change:
0.9	08-03-2020		Jósup Henriksen	Created first version with version control
1.0	01-05-2020		Jósup Henriksen	PDS approved by Gjaldstovan TSP Management Board
1.1	16-03-2021	09-06-2021	Jósup Henriksen	PDS approved by Gjaldstovan TSP Management Board 7th of May 2021. Link to RAP corrected Reference to old faroese data protection law (persónsupplýsingarlógin) corrected to the new law (dátuverndarlógin) BSI certified added (before this was in process)

Introduction

The purpose of this document is to summarise the key points of the Samleikin Certificate Policies, CP, and Certificate Practice Statments, CPS, for the benefit of Certificate Holders and Relying Parties

This document (PKI Disclosure Statement) does not substitute or replace any CP's or CPS's under which digital certificates issued by Samleikin CAs are issued.

You must read the CP's and CPS's at https://repository.samleiki.fo/legal-repository before you apply for or rely on a certificate issued by Samleikin CAs

CA contact information

Queries regarding this Samleikin PKI Disclosure Statement shall be directed to:

Gjaldstovan
Kvíggjartún 1
160 - Argir
Faroe Islands

Tel: +298 35 24 00
E-mail: gjaldstovan@gjaldstovan.fo
homepage: www.gjaldstovan.fo

Certificate types, validation procedures and usage

Certificate types

Within the Samleikin eID PKI, there is the Samleikin Root CA plus two types of issuing CAs that have been approved to issue digital certificates. The Issuing CAs can only issue digital certificates with approved
certificate profiles (link to certficate profiles) for that certificate type. The issuing CAs are named:

- Faroe Islands IssuingCA1 v1
- Faroe Islands IssuingCA2 v1

Issuing CAs are subordinate CA services that are managed and operated by Gjaldstovan or managed by third party organizations on behalf of Gjaldstovan.

The Samleikin Root CA holds the Root Certificate(s) that represents the apex of Samleikin. The Root CA digitally creates, signs and issues Issuing CA certificates using its Root CA key(s). Issuing CA Certificates are only issued to approved Issuing CAs. An approved Issuing CA utilizes its Issuing CA certificate to create, sign and issue certificates to Certificate Holders, e.g. citizens of the Faroe Islands.

Faroe Islands IssuingCA1 v1

This issuing CA can issue certificates for physical persons using the Samleikin mobile app.

Faroe Islands IssuingCA2 v1

This issuing CA certificates for physical persons using the Samleikin hardware token.

Validation procedures

Applications for a certificate issued by "Faroe Islands IssuingCA1 v1" must be either:

- in person by visiting a Samleikin Registration Authority (RA) office or
- via online registration to the RA on the Samleikin app

The applicant's identity is verified according to procedures described in the Registration Autority Policy (see RAP here: https://repository.samleiki.fo/legal-repository/).

If the identity verification is succesful the RA sets out a request to the Issuing CA for a certificate to the applicant. If the requirements for the certificate issuance request have been fulfilled the Issuing CA issues the certificate to the applicant and and the applicant can activate it via a activation code.

Applications for a "IssuingCA2 v1 certificate" go through the same procedure, however the online registration is not possible for this kind of certificates.

Use of certificates

The Issuing CA Certificates mentioned above must only be used for personal authentication towards Relying Parties that are approved within the Samleikin eID PKI.

Reliance limits

Certificates issued under the Samleikin PKI are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage. Gjaldstovan and its CAs and RAs are not responsible for assessing the appropriateness of the use of a Certificate. Relying Parties must make sure that certificates will not be used or relied upon beyond the limitations set forth in the Reliying Holder Agreement with Gjaldstovan or in applicable law.

Obligations for Certificate Holders

A Certificate Holder is the applicant for a certificate to whom the certificate was issued to and whom entered into Certificate Holder Agreement with Gjaldstovan. The basic obligations for the Certificate Holder include:

- to provide truthful and complete information when registering for the certificate;
- to immediately inform the RA of changes in data contained in the issued certificate,
- to familiarize himself/herself with the Terms and Conditions and Certificate Holder Agreement;
- to check whether the information given in the application for the certificate are correct and to use the devices (app or USB) and the private key corresponding to the public key in the issued certificate in such a way so as to prevent its unauthorized use;
- to immediately request revocation or suspension of the certificate and terminate the use of the relevant private key, especially in the case of private key compromise or suspicion that the private key has been abused.

Certificate status checking obligations of relying parties

The basic obligations for the relying parties are:

- Be sufficiently informed about the use of digital certificates and PKI;
- Receive notice and adhere to the conditions in the relevant CPS and associated conditions for Relying Parties;
- Validate a certificate by using the CRL or OCSP certificate validation service;
- Trust a certificate within its validity period only if it has not been suspended or revoked;
- Rely on a certificate, as may be reasonable under the circumstances.

Limitations of liability

Gjaldstovans liability for breach of its obligations for Issuing CA certificates shall, absent fraud or wilful misconduct on the part of Gjaldstovan, be subject to a monetary limit of 10.000 DKK.

Applicable agreements, certification practice statement and certificate policy

- A Samleikin CA Certificate Holder Agreement can be found at: link
- A Samleikin Terms and Conditions/Certificate Holder Agreement can be found at: link
- A Samleikin Relying Party Agreement can be found at: link
- This document (PKI Disclosure Statement) can be found at: link
- The Samleikin Certificate Policies (CP) can be found at: link
- The Samleikin Certification Practice Statements (CPS) can be found at: link

Privacy policy

The protection of personal data is resolved in compliance with applicable legislation concerning personal data, that is:

- Dátuverndarlógin (the faroese data protection law)

Refund policy

No refunds will be made.

Applicable law and dispute resolution

All services concerning certificates are governed exclusively by Faroese law.

CA and repository licenses, trustmarks and audit

Gjaldstovan TSP is approved as a trust service provider, TSP, that meets the requirements set out in ETSI policy:

- ETSI EN 319 411-1, policies NCP and NCP+

The certification is carried out by the accredited company:

BSI Group The Netherlands B.V., a company incorporated in The Netherlands with registration number 33264284 with address at John M. Keynesplein 9, 1066 EP Amsterdam, The Netherlands.