ÍSLANDSRÓT

Certificate Policy for Iceland Root (*Íslandsrót*)

Root CA: Islandsrot 2021

Version 1.1

OID: 2 16 352 1 1 1 1

Valid from 05.11.2021

Revision History

Release date	Version	Description	Responsible
27.04.2021	1.0	Primary version.	Ástríður Elín Jónsdóttir
05.11.2021	1.1	Correction – reference to ETSI TS 119 312 for cryptographic algorithms.	Ástríður Elín Jónsdóttir

Table of contents

Rights

Foreword

This policy is written by the Ministry of Finance and Economic Affairs for the issuance of a root certificate (*Íslandsrót*) and intermediate certificates (under the Iceland Root (*Íslandsrót*) infrastructure). This document is written in accordance with requirements in the document "Policy requirements for ISRS certificates in electronic services*"*[1].

Information on Iceland Root (*Íslandsrót*) can be obtained at www.islandsrot.is and information on electronic certificates can be accessed at www.skilriki.is.

Overview

One of the main premise of proliferation of electronic services is that electronic proceedings carry the same level of trust as conventional proceedings. The trust entails that security, confidentiality and integrity in proceedings is independent of the methods used. An important premise of that trust is that parties conducting electronic exchange are certified and that the exchanged information is protected.

An important factor in the proliferation of electronic certificates is that confirming integrity of electronic authentication and signatures is easy and reliable for the users. Confidence in the integrity of information relys on the willingness of a trusted third party to certify to that fact. The Ministry of Finance and Economic Affairs is responsible for generating and managing a "certification root" for Iceland. This root is named "*Íslandsrót*" (Iceland Root).

Iceland Root is a self-signed certificate issued by the Ministry of Finance and Economic Affairs and owned by the Ministry. Iceland Root is used to issue intermediate certificates to trust service providers. The issuance entails the certification of Iceland Root of the subject of the intermediate certificate. Issued intermediate certificates are then used to issue other intermediate certificates or end certificates to be used in electronic exchange. Three types of certificates are relevant in a chain of trust; self-signed root certificate, intermediate certificate and end certificate. Iceland Root is not used to certify end user certificates.

Users of electronic certificates and all who rely on electronic certificates must also trust the certification authority that issues the certificates. The ability of these parties to confirm that the certification authority maintains professional practices and that it ensures the security of the generation, delivery and dissemination of certificates is an important factor in building up trust in the certification authority.

This certificate policy specifies the requirements and policies the relevant certification authority must fulfil in it's operation. It should be accessible for those intending to use or rely on electronic certificates issued by the certification authority, to allow them to assess the robustness of the certificates. The Iceland Root Certification Authority will manage the Iceland Root operation on behalf of the Ministry of Finance and Economic Affairs and publishes this certificate policy.

1 Scope

Iceland Root (*Íslandsrót*) is operated by the Iceland Root Certification Authority (*Vottunarstöð Íslandsrótar*; hereafter called VÍR) on behalf of the Ministry of Finance and Economic Affairs and is the origin of trust in a public key infrastructure. Public key infrastructure is that infrastructure needed to generate keys, certificates and revocation list in addition to activities for dissemination, management and archiving.

The certificate policy specifies the requirements VÍR has to fulfil in issuing electronic certificates. In particular, this policy specifies the requirements necessary for issuing the root; that is the Iceland Root (*Íslandsrót*) and the underlying intermediate certificates. The policy specifies legal and technical requirements VÍR has to fulfil in generating, disseminating, using, storing, revoking and renewing Iceland Root and the certificates it issues. The intention of the requirements is to ensure the security of Iceland Root and assure users and others that rely on the intermediate certificates that they can put their trust in them.

The certificate policy is VÍR's unilateral statement claiming what policies VÍR complies with to ensure the security of the system. Hence, this policy entails that:

- The subscribers of certificates can assess how the security of the system is ensured, how they can use the certificates and what their obligations are.
- Those who rely on the certificates can assess how much trust can be laid on the certificates and the signatures created using them.

The Iceland Root infrastructure takes into account that end certificates fulfilling the requirements for qualified certificates in the legal sense of Act No. 55/2019 on electronic identification and trust services for electronic transactions [2] will be issued by the trust service providers that receive intermediate certificates signed by the Iceland Root.

In this document, the term "Iceland Root" shall be understood to be equalent to the term "Íslandsrót", and reference to the self-signed root CA "Islandsrot 2021".

2 References

The following documents contain conditions and provisions which, through references in this document, constitute its policies.

[1] *Stefnumarkandi kröfur fyrir ISRS skilríki í rafrænni þjónustu: Kröfur til vottunarstöðva sem gefa út dreifilyklaskilríki* (Policy requirements for ISRS certificates in electronic services: Requirements for certification authorities issuing public key certificates). Version 1.0 from May 5th 2008. The Collaboration Group of Ministry of Finance and Economic Affairs and Auðkenni (*Samstarfshópur fjármálaráðuneytisins og Auðkennis*).

[2] Act No. 55/2019 on electronic identification and trust services for electronic transactions (*Lög um rafræna auðkenningu og traustþjónustu fyrir rafræn viðskipti*)., as amended.

[3] eIDAS - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[4] Act No. 90/2018 on the protection of privacy as regards the processing of personal data (*Lög um persónuvernd og vinnslu persónuupplýsinga*), as amended.

[5] ÍST 146:2019 *Innihald almennra rafrænna skilríkja* (Content of federal digital certificates).

[6] *Lýsing á starfsemi skráningarstöðvar: Skráning á kennimarki viðfangs undir landaboga {joint-iso-itu-t(2) country(16) is(352)} fyrir Ísland* (Description of registration authority activities: Registration of Object Identifier under the Iceland country arc {joint-iso-itu-t(2) country(16) is(352)}). The Post and Telecom Administration in Iceland, version 0.3.1 from May 2nd 2007.

[7] FIPS PUB 140-3 (2019): Security Requirements for Cryptographic Modules.

[8] ISO/IEC 15408:2009 (parts 1 to 3): *Information technology – Security techniques – Evaluation criteria for IT security*.

[9] ETSI TS 119 312: Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

[10] ISO/IEC 9594-8:2020|ITU-T Recommendation X.509: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

[11] ÍST EN ISO/IEC 27002:2017 *Upplýsingatækni - Öryggisaðferðir - Starfsvenjur fyrir upplýsingaöryggisstýringar* (Information technology - Security techniques - Code of practice for information security controls).

[12] ÍST EN ISO/IEC 27001:2017 *Upplýsingatækni - Öryggisaðferðir - Stjórnunarkerfi um upplýsingaöryggi - Kröfur* (Information technology - Security techniques - Information security management systems – Requirements).

[13] ISO/IEC 20000:2018 *Information technology: Service management.*

3 Definitions and abbreviations

3.1 Definitions

The following list contains definitions that apply in this Certificate Policy. Homologous terms in Icelandic are in italic typeface within parenthesis.

Activation code (*stofnaðgangsorð*): Password assigned to the subject by the certification authority to create or initiate the certificate and generate a key pair. The subject does not have to use the activation code again.

Agent (*lögbær fulltrúi*): An individual chosen and approved by senior management of an organisation to be an official contact and who has a mandate to represent the organisation to approve and apply for certificates, and/or to manage the organisation‘s certificates.

Attribute (*eigind*): Information bound to an entity that specifies a characteristic of the entity.

CA certificate (*skilríki vottunarstöðvar*): A certificate issued by certification authority for the purpose of issuing end certificates or other CA certificates. The subject can be another certification authority or the same certification authority as the issuer. CA certificate can be a self-signed root certificate.

Certificate (*vottorð; skilríki*): Refers to electronic certificates in the context of public key infrastructure unless other meaning is clear from the context.

Certificate policy (*vottunarstefna*): Named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. The certificate policy reveals the intention regarding the issuance and processing of electronic certificates. The policies regarding the requirements for security and control are also set out in the certificate policy.

Certificate recipient (*móttakandi skilríkja*): The one who receives a certificate in an electronic exchange and has verified the trust he puts on the subject‘s public key.

Certificate revocation (*afturköllun skilríkja*): An irreversible action that entails that the certificate is made invalid before the validation period has expired. Revoked certificates cannot be reinstated.

Certificate revocation list (*afturköllunarlisti skilríkja*): List of certificates that are no longer valid because they have been revoked (made invalid) before the validation period expires.

Certificate subscriber (*áskrifandi skilríkja*): An individual or legal entity that is a subscriber at a certification authority on behalf of one or more certification subjects. Subscriber can also be a certification subject.

Certification authority (*vottunarstöð*; *vottunaraðili*): Entity trusted by a stakeholder to create, sign and issue certificates.

Certification authority key (*einkalykill vottunarstöðvar*): Private key belonging to a certification authority and is used for signing the certificates issued by the certification authority.

Certification practice statement (*yfirlýsing um framkvæmd vottunar*): A solemn statement of the certification authority on the procedures and practices employed in issuing and maintaining certificates. The certification practice statement describes processes and policies of the certificate issuer that comply with the requirements in a particular certificate policy.

Certification service provider (*vottunarþjónusta*): An entity that provides universal services related to public key infrastructure components to stakeholders.

Cryptographic module (*dulmálseining*): Hardware module that, among other things, generates and protects keys and applies electronic signature.

Device (*búnaður*): Equipment or system. Device can be either hardware or software. Used in this policy as a synonym with “system”.

Dual control (*tvískipt stjórnun*): A security procedure requiring two people to cooperate in gaining authorized access to a data, files, devices or systems.

Electronic certificate (*rafræn skilríki*): Electronic attestation which links signature-verification data to a person and confirms the identity of that person. Usually refers to public key certificate in the context of public key infrastructure. The certificates contain the subject‘s public key, together with some other information, encrypted with the private key of a certification authority.

Electronic signature (*rafræn undirskrift*): Data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication of that data..

Enabling password (*notkunaraðgangsorð*): Password that protects the subject‘s private key. When enabling password is implemented the subject must enter it to apply the private key. When certificates are protected in a smartcard chip it is common to use a personal identification number (PIN) as an enabling password.

End-entity certificate (*endaskilríki*): Certificate of an end user or an end-entity. The certificate can be tied to a person as a private certificate or an employee certificate. End-entity certificates can also be tied to a non-personal entity, such as a device, an IT system or an organisational unit such as a society or a company branch or department.

End user (*endanotandi*): Subscribers and subjects are called end users since their certificates are at the end of a certification path and are therefore not used to authenticate other certificates.

Iceland Root (*Íslandsrót*): Root which is at the top of a trust hierarchy in public key infrastructure in Iceland. Iceland Root’s private key is used to sign other certificates that rely on that trust.

Interested party (*hagsmunaaðili*): A term used for those that verify certificates or rely on them. See also the terms “relying party” and “verifier”.

Intermediate certificate (*milliskilríki*): CA certificate that lies between a root certificate and end certificates. End certificates, intermediate certificates and root certificates establish a chain of trust in a trust hierarchy.

Key (*lykill*): Usually refers to cryptographic key in the context of public key infrastructure. Bit string of variable length that determines the cryptographic operation.

Legal entity (*lögaðili*): Institution or organisation that is recognised as able to own rights and carry obligations. State, regional government, agencies and organisations are legal entities and hold a unique company registry identification number.

Object identifier - OID (*kennimark viðfangs*): Identifier in the “Certificate Policies” field in certificates that specifies the type of certificate and refers to the certificate policy that applies to the issuance of the certificate and its application.

Personal identification number (*persónulegt kenninúmer*): A short numeric code that an individual uses as a password to an active system, such as mobile phone card, payment card or electronic certificate on a smartcard. Personal identification number functions as an enabling passwords to electronic certificates where the subject enters it to apply the private key. Sometimes called “PIN number“.

Private key (*einkalykill*): Secret key intended for a single user, the owner of the key. In key-pair encryption, as in public key infrastructure, the private key is both used for decryption and to create electronic signature.

Public key (*dreifilykill*): Cryptographic key intended for any entity to apply in encrypted communication with the owner of a corresponding private key. In key-pair encryption the public key is used both for encryption and to verify electronic signature.

Public key certificate (*dreifilyklaskilríki*): Electronic attestation that specifies the subject’s public key and links the public key to the subject in an unambiguous way. See also “certificate”.

Public key infrastructure (*dreifilyklaskipulag*): The infrastructure needed to generate and deliver keys and certificates, maintain certificate status information, make revocation lists accessible and archive relevant information. Public key infrastructure allows the users, among other things, to communicate over public networks such as the Internet in a secure way by applying a pair of cryptographic keys, private key and public key.

Qualified certificate (*fullgild skilríki*): Certificate which contains the information stipulated in Article 7 in the Act No. 28/2001 on electronic signatures [2] and is provided by a certification service provider who fulfils the requirements laid down in Chapter V of the Act.

Qualified electronic signature (*fullgild rafræn undirskrift*): Advanced electronic signature which is based on a qualified certificate and which is created by a secure-signature-creation device.

Registration authority (*skráningarstöð*): Entity responsible for identification and authentication of a certificate subject but does not sign nor issue certificates. Registration authority can take on such tasks on behalf of the certification authority.

Relying party (*treystandi*): Recipient of a certificate that puts his trust on it and/or the electronic signature valdated with it. Sometimes called “interested party” or “certificate user”.

Root (*rót*): The origin of trust in a public key infrastructure. Root is implemented with a certificate called “root certificate”.

Root certificate (*rótarskilríki*): Public key certificate at the top of a trust hierarchy and issued by a certification authority to sign other certificates. Root certificates are signed by the private key of the key pair of the certificate itself. Root certificates are therefore self-signed.

Root key (*rótarlykill*): Certification authority‘s private key that is at the top of a particular trust hierarchy. The root key is used to sign other certificates that rely on that trust.

Secure user device (*öruggur notendabúnaður*): Device which holds the user's private key, protects this key against compromise and performs signing or decryption functions on behalf of the user. Secure user device intended for electronic signing and which meets the requirements laid down in Article 8 of the Act No. 28/2001 on electronic signatures is called “secure signature-creation device”.

Secure signature-creation device (*öruggur undirskriftarbúnaður*): Signature-creation device which meets the requirements laid down in Article 8 of the Act No. 28/2001 on electronic signatures [2]. Secure signature-creation device is a special type of a secure user device which is intended for electronic signatures.

Self-signed certificate (*sjálfundirrituð skilríki*): Certificate (public key) that is signed by its own private key. The certificate‘s public key is therefore a self-signed public key. CA certificates that are used to authenticate issued certificates are self-signed, see also the definition of “root certificate“.

Signature-creation data (*undirskriftargögn*): Unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature.

Signature-creation device (*undirskriftarbúnaður*): Software or hardware used to create an electronic signature using signature-creation data.

Signature verification data (*sannprófunargögn*): Data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature.

Subject (*vottorðshafi*): An individual, a legal entity, an organisational unit or a device identified in a certificate as the holder of the key-pair, private key and public key, given in the certificate. The subject can be a subscribe who receives a key-pair in his own name.

Suspension (*tímabundin ógilding*): Activity that entails the registration by the certification authority of the certificate as invalid for a limited time period. Certification authority can re-instate the certificate by changing their status so that they are no longer invalid.

System (*búnaður*): Used in this policy as a synonym with "device". System can be either hardware or software.

Trust hierarchy (*stigveldi trausts*): Structure of root and CA certificates where trust associated with particular certificates relies on the trust associated with the certificates used to sign them and that are higher in the hierarchy (closer to the root).

Verifier (*sannprófandi*): Recipient of a certificate that verifies it and/or the electronic signature validated with it. Sometimes called "interested party".

3.2 Abbreviations

The following are common abbreviations in English texts on Public Key Infrastructure. Explanations in Icelandic are in italic typeface within parenthesis.

CA **C**ertification **A**uthority (*vottunarstöð*).

CSP **C**ertification **S**ervice **P**rovider (*vottunarþjónusta*).

CRL **C**ertificate **R**evocation **L**ist (*afturköllunarlisti*).

ISRS ***Í**slensk **r**afræn **s**kilríki* – certificates used in electronic services in Iceland that fulfil the uniform requirements laid down in the Collaboration Project of the State, banks and saving banks.

PIN **P**ersonal **I**dentification **N**umber (*persónulegt kenninúmer*).

VÍR *Vottunarstöð **Í**slands**r**ótar* (Iceland Root (*Íslandsrót*) Certification Authority).[1]

[1] Translation note: This definition of the acronym "VÍR" is an addition for clarity in this translated document.

4 General concepts

The main categories of electronic certificates in a public key infrastructure are root certificates, intermediate certificates and end certificates. Root certificates are the origin of trust in an open public key infrastructure, are self-signed and issued by the nominal subscriber. The intermediate certificates are issues to certification authorities and certify that the certification authority is the one indicated in the certificate and that the certificate is tied to it as a legal entity. These certification authorities holding the intermediate certificates then issue either other intermediate certificates or end certificates to the public or legal entities.

This certificate policy discusses requirements and policies for issuing root certificate and other certificates under the root certificate.

Public key infrastructure is used inter alia for information exchange between two parties over open communication network, as the Internet, where a designated third party, called certification authority, is trusted by both parties and is responsible for the verification of their identity. Policy requirements in this document describe the relations between these three parties.

VÍR is a certification authority that generates root and issues certificates complying with the requirements in this policy. The main objective is the secure application of electronic signatures. The trust of subscribers, users of certificates, recipients of electronically signed documents and other interested parties is in part based on this certificate policy.

In public key infrastructure the electronic certificates are signed with certification authority's private key and contain the subject's public key along with other data. In that way, the public key certificates link the verification data to the certified subject, be it individual, device owned be a legal entity or a defined division within an organization, agency or association.

4.1 Certification authority

The authority trusted by the users of the certification services, e.g. subscribers of certificates, certificate subjects, receivers of electronically signed documents as well as other stakeholders, to create and issue certificates is called the certification authority. The certification authority has overall responsibility for the provision of the certification services identified in clause 4.2. The certification authority is identified in the certificate as the issuer and its private key is used to sign qualified certificates. The Iceland Root is a self-signed certificate issued by VÍR. The Iceland Root is at the top of a trust hierarchy and signs intermediate certificates which are lower in the hierarchy. VÍR is therefore a certification authority that issues intermediate certificates.

In this policy the term "certification authority" is used to mean "trust service provider" (as defined in the eIDAS regulation [3]) providing the services identified in clause 4.2. VÍR can authorise other parties to provide parts of the certification service but maintains overall responsibility for all aspects related to the use of certificates and shall ensure that the policies specified in this certificate policy are always met.

4.2 Certification services

Activity of a certification authority is divided into the following components:

Registration service: Verifies the identity and, if applicable, any specific attributes of a subject. The results of this service are passed to the certificate generation service.

Certificate generation service: Creates and signs certificates based on the identity and other attributes verified by the registration service.

Dissemination service: Disseminates certificates to subjects and, if the subject consents, makes them available so that interested parties can access them. This service also makes available the CA's terms, and conditions with any published policy and practice information, to subscribers and interested parties.

Revocation management service: Processes requests and reports relating to revocation to determine the necessary action to be taken. The results of this service are distributed through the revocation status service.

Revocation status service: Provides certificate revocation status information to interested parties. This may be a real time service or based upon revocation information that is updated on a regular basis.

Subject device provision service: Prepares and delivers a signature-creation device or other secure user device to subjects. This service can include generation and delivery of the subject's key pair, preparation of the signature-creation device and activation code and delivery to the subject.

4.3 Certificate policy and certification practice statement

This clause contains a general discussion on the roles of certificate policy and certification practice statement.

4.3.1 Purpose

In public key infrastructure the purpose of the certificate policy is to state the requirements that the certification authority shall meet, while the purpose of a certification practice statement is to state what is

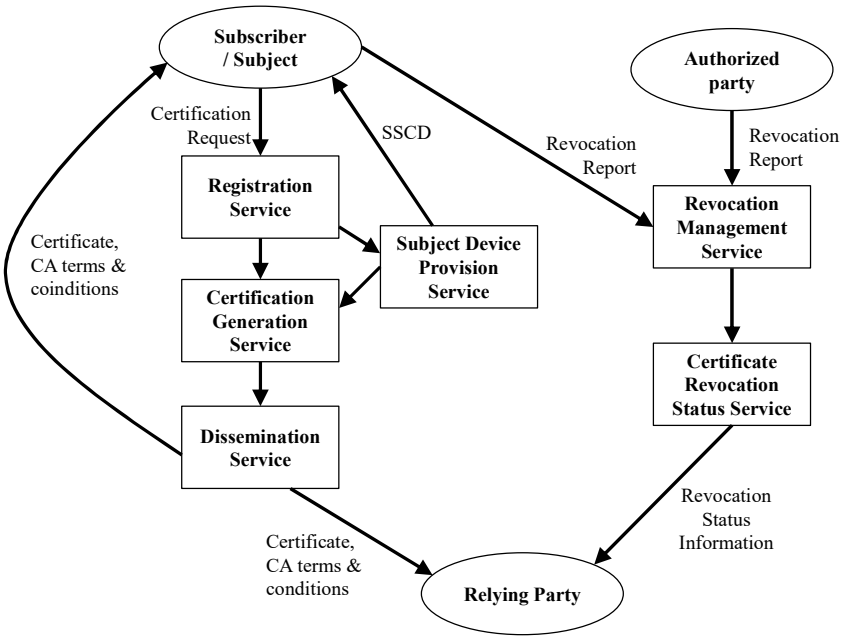

Figure 1: Illustration of subdivision of certification services.

being done at the relevant certification authority to meet the requirements, i.e. the processes used in creating and maintaining the certificate. The certificates contain a reference to the certificate policy, with the policy identifier, to allow the recipient of the electronic certificate to explore the requirements the certification authority must meet, at the minimum.

If any changes are made to a certificate policy which affects the applicability then the policy identifier in the certificates should be changed.

4.3.2 Level of specificity

A certificate policy is a less specific document than a certification practice statement. A certification practice statement is a more detailed description of the practices of a certification authority in issuing and

otherwise managing certificates. A certification practice statement defines how a specific certification authority meets the technical, organizational and procedural requirements identified in a certificate policy.

Even lower-level documents may be appropriate for a CA detailing the specific procedures necessary to complete the practices identified in the certification practice statement. This lower-level documentation is generally regarded as an internal operational procedure document, which define specific tasks and responsibilities within an organization. While this lower-level documentation may be used in the daily operation of the CA and reviewed by those doing a process review it can be beyond the scope of the a certificate policy and a certification practice statement. More detailed descriptions of processes with locations, access lists and access procedures are examples of such documentation.

4.3.3 Approach

The approach of a certificate policy is significantly different from a certification practice statement. A certificate policy is independent of the specific details of the operating environment of a certification authority, whereas a certification practice statement is tailored to the organization, operating procedures, facilities, and computing environment of a certification authority. A certificate policy may be defined by the user of certification services, whereas the certification practice statement is always defined by the provider.

4.3.4 Other CA statements

In addition to the policy and practice statements a CA may issue terms and conditions. Such terms and conditions are usually broad category of terms to cover the broad range of commercial terms regarding certificate issuance and dissemination of information.

A PKI disclosure statement is that part of the CA's terms and conditions which relate to the operation of the PKI and which are considered normal for a CA to disclose to both subscribers of electronic certificates and relying parties.

4.4 Subscriber and subject

In some cases certificates are issued directly to individuals for their own use. However, the party requiring a certificate can be other than the subject to whom the certificate applies. For example, a company may require certificates for its employees to allow them to participate in electronic exchange on behalf of the company. In such situations the entity subscribing to the certification authority is different from the entity which is the subject of the certificate and identified in the certificate as such.

In the present document to clarify the requirements which are applicable to the two different roles that may occur two different terms are used for the subscriber who contracts with the certification authority for the issuance of certificates and the subject the certificate identifies. The subscriber bears responsibility towards the CA for the use of the private key associated with the public key certificate but the subject is the individual or system that uses the private key and is authenticated by the certificate associated with it.

The term subject is used when referring specifically to the entity authenticated by the certificate but the term subscriber is used in all other cases, even when the distinction is not clear from the context.

5 Introduction to certificate policies

5.1 Overview

The policy requirements defined in the present document are the requirements that the VÍR will meet for the issuance of certificates in accordance with the scope defined in clause 1. Certificates issued in accordance with the present document include a certificate policy identifier which can be used by interested parties in determining the certificates suitability and trustworthiness for a particular application.

5.2 Identification

This certificate policy is identified with an object identifier (OID) registered at the Post & Telecommunication Administration in Iceland under a recognised country arc for Iceland in accordance with Description of registration authority activities [6] and in accordance with requirements in ISO/IEC 9594-8|ITU-T Recommendation X.509 [10]. This object identifier is: {2 16 352 1 1 1 1}.

{joint-iso-itu-t(2) country(16) is(352) fyrirtæki-samtök-og-stofnanir(1) fjarmalaraduneyti(1) dreifilyklaskipulag-cp(1) íslandsrót(1)}

All certificates issued in conformity with this certificate policy refer to it by including the relevant object identifier field “Certificate Policies” in the certificate. By referring to the certificate policy with the object identifier the VÍR claims conformance of the certificates to the requirements of the certificate policy. VÍR will also specify object identifiers for the terms and conditions published to interested parties to portray claim of conformance to the requirements in this document.

5.3 User community and applicability

In conformity with this certificate policy VÍR issues certificates that meet the following requirements:

a) The certificates meet the requirements for qualified certificates laid down in the eIDAS regulation [3].

b) VÍR as a certification authority meets the requirements for trust service provider laid down in the eIDAS regulation [3].

c) The certificates are issued to certification authorities apart from certificates intended for Iceland Root (*Íslandsrót*) internal operational needs.

5.4 Conformance

5.4.1 Conformance claim

VÍR declares that conditions relevant to the issuance of intermediate certificates that will issue end certificates that can meet requirements for qualified certificates as defined in the Act No. 55/2019 on electronic identification and trust services for electronic transactions [2] are met when issuing, disseminating, publishing and revoking certificates in conformity with this certificate policy.

To provide evidence to support this claim, VÍR will have a competent auditor perform audit confirming that issuance of certificates at VÍR is in conformance with the requirements laid down in this certificate policy. The result of such an audit will be made available to subscribers and interested parties that rely on the certificates. Such an audit will be performed at regular intervals. If such an audit shows VÍR not to be conformant to the requirements laid down in this certificate policy, VÍR will immediately cease issuing certificates until the requirements are met.

5.4.2 Conformance requirements

VÍR meets the requirements in clause 6.1 and has implemented controls which meet the requirements, including the applicable options in clause 7.

6 Obligations and liability

6.1 VÍR obligations

VÍR ensures that all requirements laid down in clause 7 are met and that the implementation of this certificate policy identified in the certificates is in conformance with that requirements (see clause 5.4.2).

VÍR is responsible for conformance with the procedures prescribed in this policy, even if VÍR decides to outsource part of the operation to sub-contractors.

VÍR publishes certification practice statement that complies with this certificate policy. VÍR provides its certification services consistent with its certification practice statement.

6.2 Subscriber obligations

VÍR makes an agreement with the subscriber (see clause 7.3.1) that obliges the subscriber to address the following obligations:

a) submit accurate and complete information to the CA in accordance with the policy, particularly with regards to registration;.

b) protect and use its key pair in accordance with any limitations notified to the subscriber by VÍR (see clause 7.3.4);

c) exercise normal and reasonable measures to avoid unauthorized use of the subject's private key, prevent the loss of the key or its alteration;

d) if the subscriber or subject generates the subject's keys:

   i. generate subject's keys using an algorithm generally recognized as being fit for the purposes of the certified key specified in the VÍR certificate policy;

   ii. use a key length and algorithm which is generally recognized as being fit for the purposes of the certified key during the validity time of the certificate specified in the VÍR certificate policy;

   iii. the subject's private key can be maintained under the subject's sole control.

e) only use the subject's private key for electronic signatures or decryption in a secure user device;

f) if the subject's keys are generated by the subscriber or subject, the subject's key-pair intended for signing or decrypting shall be generated within the SSCD to be used for signing or decrypting;

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

   i. the subject's private key has been lost or stolen;

   ii. the subject no longer has sole control over his private key due to compromise of activation data or other reasons;

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

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

i) in the case of being informed that the CA which issued the certificate has been compromised, ensure that the certificate is not used by the subject.

6.3 Information for interested parties

The terms and conditions made available by VÍR to interested parties (see clause 7.3.4) will include a notice that if it is to reasonably rely upon a certificate, it shall:

a) verify the validity, suspension or revocation of the received certificate using current revocation status information as indicated to the interested party (see clause 7.3.4); and

b) take account of any limitations on the usage of the certificate indicated to the interested parties either in the certificate or the terms and conditions supplied as required in clause 7.3.4; and

c) take any other precautions prescribed in agreements or elsewhere.

6.4 Liability

Liability towards subscribers and interested parties

VÍR is liable for damages to those who rightfully rely on the certificates, as long as the damages result from one of the following:

a) the information contained in the certificate is not correct at the time of issuance;

b) the certificate does not contain all the information required in clause 7.3.3;

c) failure occurs in the revocation of the certificate, see clause 7.3.6;

d) information on revocation status, validity or on limitations on the scope of use or the value of transactions is missing or is wrong, see clauses 7.3.3 and 7.3.6;

e) provisions in clause 7.3.1 are not respected.

The liability clause above only applies if it has been demonstrated that the damage is caused intentionally or is the result of negligence on the part of VÍR employees.

VÍR liability does not apply to any kind of implicit, random or derived damage, including but not limited to any loss of profit, loss of use or loss of penal compensation or sanctions resulting from or related to use, delivery, license, potency or impotency of a certificate or any related practice, activity or service offered or planned.

VÍR can limit its liability to its contracting parties.

7 Requirements on CA practice

VÍR applies controls that meet the requirements in this chapter.

This chapter contains requirements for registration, certificate generation, certificate dissemination, revocation management, revocation status service and delivery of the subject‘s user device (see clause 4.2).

The requirements are indicated in terms of the security objectives followed by more specific requirements for controls to meet those objectives.

7.1 Certification Practice Statement

VÍR issues a statement of the practices and procedures.

In particular, VÍR fulfils the following requirements:

a) Identifies in a certification practice statement how all the requirements identified in this qualified certificate policy are addressed.

b) Identifies in a certification practice statement the obligations of all legal entities supporting the CA activities, including the applicable policies and practices.

c) Makes available to subscribers and relying parties its certification practice statement and other relevant documentation as necessary to assess conformance to the qualified certificate policy. VÍR is not required to make all the details of its practices public.

d) Discloses to all subscribers and potential interested parties the terms and conditions regarding use of the certificate as specified in clause 7.3.4.

e) The VÍR managers are responsible for the certification practice statement and have final authority for approving it.

f) The VÍR senior management is responsible for ensuring that the certification practices established meets at all times the applicable policies specified in the current document.

g) Defines a review process for certification practices including responsibilities for maintaining the certification practice statement.

h) Gives due notice of changes it intends to make in its certification practice statement and, following approval by VÍR senior management as in (e) above, makes the revised Certification Practice Statement immediately available to subscribers and interested parties as required under (c) above.

i) Documents the signature algorithms and parameters employed.

7.2 Public key infrastructure - Key management life cycle

Handling of keys at VÍR is in accordance with ETSI TS 119 312 [9] which contains a list of approved cryptographic algorithms along with requirements for their parameters.

7.2.1 Certification authority private key generation

Certificate generation

VÍR generates its root keys and other private keys used for signing certificates in controlled circumstances. For that purpose, VÍR will in particular fulfil the following requirements:

a) VÍR private keys are generated in a physically secure environment (see clause 7.4.4) by personnel in trusted roles (see clause 7.4.3) under, at least, dual control. The number of personnel authorized to carry out this function is kept to a minimum.

b) VÍR private keys are generated within a device which

   i. meets the requirements identified in FIPS 140-3 [7], level 3 or higher, or

ii. is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [8], or equivalent security criteria. This shall be a part of a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.

c) VÍR private keys are generated using an algorithm recognized as being fit for the purposes of certificate-signing in accordance with ETSI TS 119 312 [9].

d) The key length and algorithm for the VÍR CA-signing key is recognized as being fit for the purposes of certificate-signing in accordance with ETSI TS 119 312 [9].

e) A suitable time before expiration of its CA signing key VÍR generates a new certificate-signing key pair and applies all necessary actions to avoid disruption to the operations of any entity that may rely on the CA key.

7.2.2 Certification authority key storage, backup and recovery

Certificate generation

VÍR ensures that its private keys remain confidential and maintain their integrity by inter alia fulfilling the following requirements:

a) VÍR private keys for certificate-signing are held and used within a secure cryptographic device which:

i. meets the requirements identified in FIPS 140-3 [7], level 3 or higher, or

ii. is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [8], or equivalent security criteria. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.

b) If the VÍR private key for certificate-signing is moved between secure cryptographic devices the private key is protected in a way that ensures the same level of protection as provided by the secure cryptographic device, see requirements in a).

c) The VÍR private signing key is stored, backed up and recovered only by personnel in trusted roles using, at least, dual control (see clause 7.4.3) in a physically secure environment (see clause 7.4.4). The number of personnel authorized to carry out this function is kept to a minimum and is consistent with the VÍR's practices.

d) Backup copies of the VÍR private keys are subject to the same or greater level of security controls as private keys currently in use.

e) Where keys are stored in a dedicated key processing hardware module, access controls are in place to ensure that the keys are not accessible outside the hardware module.

7.2.3 VÍR public key distribution

Certificate generation and certificate distribution

VÍR ensures that the integrity and authenticity of the public key used to verify certificate signatures and of any associated parameters are maintained during its distribution to interested parties.

In particular, VÍR will insure that:

a) VÍR public key, that is used to verify certificate signatures, is available to interested parties in a manner that interested parties can confirm the integrity of the public key and authenticate its origin.

7.2.4 Key escrow

a) VÍR does not hold subject private keys.

7.2.5 Certification authority key usage

VÍR ensures that its own private signing keys are not used inappropriately.

Certificate generation

In particular, VÍR will fulfil the following requirements:

a) VÍR ensures that its own private keys used for signing certificates, as defined in clause 7.3.3, or to sign revocation status information, are not used for other purpose.

b) VÍR ensures that certificate signing keys are only used within physically secure premises according to 7.4.4.

7.2.6 End of CA key life cycle

VÍR private keys have a specific validity period. VÍR ensures that a private key used for signing certificates is not used beyond the end of its validity period.

Certificate generation

In particular, VÍR will fulfil the following requirements:

a) The use of the corresponding VÍR's private key shall be limited to that compatible with the hash algorithm, the signature algorithm and signature key length used in the generating certificates, in line with current practice as in clause 7.2.1 d).

b) After the validity period ends VÍR will either destroy the private key or store it in such a way that it can never be used again.

7.2.7 Life cycle management of cryptographic hardware used to sign certificates

VÍR handles and protects cryptographic hardware throughout its lifecycle in accordance with requirements in clause 7.4.

Certificate generation

In particular VÍR will ensure that:

a) certificate and revocation status information signing cryptographic hardware is neither tampered with nor compromised during shipment;

b) certificate and revocation status information signing cryptographic hardware is neither tampered with nor compromised while stored;

c) the handling of VÍR signing keys in cryptographic hardware, including the installation, activation, back-up and recovery after disaster, will be under simultaneous control of at least of two individuals in separate trusted roles at the certification authority;

d) certificate and revocation status information signing cryptographic hardware is always functioning correctly; and

e) signing keys stored on CA cryptographic hardware and intended for signing of certificates and revocation status information are destroyed upon device permanent retirement.

7.2.8 Subject key management services provided by VÍR

VÍR ensures that any subject keys, that it generates, are generated securely and the secrecy of the subject's private key is assured.

Certificate generation

Subject keys generated by VÍR are:

a) generated using an algorithm recognized as being fit for the purposes of the certificate use during the validity time of the certificate as stipulated in this certificate policy, cf. ETSI TS 119 312 [9];

b) of a key length and for use with a public key algorithm which is recognized as being fit for the purposes of certificates during the validity time of the certificate as stipulated in this certificate policy, cf. ETSI TS 119 312 [9];

c) generated and stored securely before delivery to the subject (VÍR destroys any copies of subject private keys once they have been placed in a secure user device);

d) delivered in a manner such that the trust to the key is not compromised and, once delivered to the subject, the private key can be maintained under the subject's sole control;

e) If copy of the subject keys is not stored at VÍR or with other rightful entity after delivery to the subject, cf. 7.2.4, only the subject or the subscriber will have access to the private key. VÍR will destroy all copies of subject keys in such cases.

7.2.9 Preparation of secure user device or secure-signature-creation device

VÍR will ensure secure preparation and delivery of a secure user device when the user device is delivered to the subject.

Subject device provision

a) Secure user device preparation is securely controlled by VÍR.

b) Secure user device is securely stored and distributed.

c) Secure user device deactivation and reactivation is securely controlled.

d) User activation data associated with secure user device are securely prepared and distributed separately from the secure user device.

7.3 Public key infrastructure - Certificate management life cycle

7.3.1 Subject registration

VÍR ensures that data to identify certificate subscribers and subjects, including accuracy of their names and relevant information, is properly examined. VÍR also ensures that certificate requests are correct, contain all information requested and are duly authorized when appropriate.

In particular, VÍR will fulfil the following requirements:

Registration

a) Before entering into a contractual relationship with a certificate subscriber, VÍR will inform the subscriber of the terms and conditions regarding use of the certificate as given in clause 7.3.4.

b) VÍR will communicate information according to a) in a way that permanently secures its integrity. The information is disseminated in a clear and simple language.

c) The certification authority shall collect either direct evidence or a testimony from appropriate and legitimate entity regarding identity (such as name) and, if applicable, any specific attributes of the subject. Submitted evidence may be in the form of either paper or electronic documentation. Assertion of the subject's identity shall be confirmed by appropriate means at the same time as the registration is performed and in accordance with laws.

d) All information necessary to confirm the identity of the subject are documented, and any attributes of the subject if relevant, including reference to documents used for confirmation and any limitations that might apply to their validity.

e) Submitted documents shall provide evidence of the following:

   i. Full name of legal entity (as subject) referencing authorised registration, e.g. the national company register, or other attributes which may be used to distinguish the legal entity from others.

   ii. Full name, identity number (i. kennitala) and status of the certificate subscriber.

   iii. Full name, identity number (i. kennitala) and place of birth of a legal representative of the subject, according to the national population register.

   iv. Association of the legal representative of the subject to the subscriber of the certificate.

v. The legal representative's authorisation to apply for a certificate on behalf of the subject.

f) VÍR records all the information detailed above that are necessary to verify the identities of the subject and the legal representative, including any references to documentation used for verification, and any limitation on its validity.

g) The subscriber shall provide a legal address, e-mail address or other information, which describe how the he may be contacted.

h) VÍR records a signed agreement with the subscriber of the certificates including inter alia:

i. agreement to the subscriber's obligations (see clause 6.2);

ii. agreement with the subscriber regarding use of a secure user device (see clause 7.2.2.a);

iii. subscriber's consent to the keeping of a record by VÍR of information used in registration, subject device provision and revocation (see clause 7.4.11). Also consent to the keeping of a record of identity and other attributes placed in the certificate, and the passing of this information to third parties under the same conditions as required in the case of VÍR terminating its services;

iv. whether, and under what conditions, the subscriber requires and the subject's consents to the publication of the certificate;

v. confirmation that the information held in the certificate is correct.

i) VÍR retains records of the information registered as prescribed in this chapter for as long as necessary for the purpose of providing evidence of certification, inter alia in legal proceedings. VÍR informs the subscribers what information is stored and for how long.

j) If the subject's key pair is not generated by VÍR, VÍR verifies according to procedure for certificate request:

i. that the subject has possession of the private key associated with the public key presented for certification;

ii. that the public key to be certified is from a key pair effectively generated by a secure user device.

k) VÍR sees to it that Act No. 90/2018/2000 on the protection of privacy as regards the processing of personal data [4] is enforced in the registration process, including use of pseudonym if relevant.

l) When verifying identity VÍR will limit the records of identity data to those records necessary for the intended use of the certificates.

7.3.2 Certificate renewal, rekey and update

VÍR ensures that requests for certificates issued to a subject who has already previously been registered at VÍR are complete, accurate and duly authorized, e.g. based on a valid mandate. This includes certificate renewals, rekey following revocation or prior to expiration, or update due to change to the subject's attributes

In particular, VÍR will fulfil the following requirements:

Registration

a) VÍR checks the existence and validity of the certificate to be renewed and that the information used to verify the identity and attributes of the subject is still valid.

b) If any of VÍR terms and conditions have changed, VÍR will communicate these to the subscriber and enter into an agreement in accordance with clause 7.3.1 a), b) and i)

c) If any certified names or attributes have changed, or the certificate has been revoked, the certification authority will verify, record and enter into an agreement with the subscriber in accordance with clause 7.3.1.

d) VÍR shall issue a new certificate using the subject's previously certified public key, only if its cryptographic security is still sufficient for the new certificate's validity period and no indications exist that the subject's private key has been compromised.

7.3.3 Certificate generation

The certificate issuance at VÍR is performed in a secure manner and their authenticity maintained.

The certificate content is in accordance with criteria in "Electronic certificate profile: Uniform profile for electronic certificates issued in Iceland" [5].

In particular, VÍR will fulfil the following requirements:

Certificate generation

a) The certificates contain the following:
   i. The identification of the certification authority and the State in which it is established.
   ii. The name of the subject or a pseudonym, which shall be identified as such.
   iii. Specific attributes of the subject if the intended purpose of the certificate requires it.
   iv. Public key which correspond to the private key of the subject.
   v. Beginning and end of the period of validity of the certificate.
   vi. The certificate serial number.
   vii. Electronic signature of the certification authority that issues the certificate.
   viii. Limitations on the scope of use of the certificate, if applicable.
b) VÍR takes measures against forgery of certificates, and, in cases where the CA generates the subject's private key, guarantees confidentiality during the process of generating the key.
c) The certificate issuance is securely linked to the associated registration, certificate renewal or rekey, including the provision of any subject generated public key.
d) If VÍR generates the subjects key pair:
   i. VÍR follows procedure of issuing the certificate that is securely linked to the generation of the key pair.
   ii. VÍR securely passes to the subject a qualified electronic signature creation device that contains the subject's private key.
e) VÍR ensures that the distinguished name used in the certificate will never be used to identify another entity.
f) The confidentiality and integrity of registration data shall be protected especially when exchanged with the subscribers and subjects or between distributed CA system components.
g) VÍR verifies that registration data is exchanged with recognized registration service providers, whose identity is authenticated, in the event that external registration service providers are used.

7.3.4 Dissemination of Terms and Conditions

The terms and conditions are made available to subscribers and relying parties.

In particular, VÍR will fulfil the following requirements:

a) VÍR makes available to subscribers and interested parties that rely on the certificates the following terms and conditions regarding the use of the certificate:
   i. This certificate policy.
   ii. Limitations on the certificate use.
   iii. The subscriber's obligations as defined in clause 6.2.
   iv. Information on how to validate the certificate, including how to check the revocation status of the certificate, such that the interested party can rely on the certificate (see clause 6.3).
   v. Limitations of liability including the scope of certificate use or purpose the CA specifies in relation to its liability.
   vi. The retention period of registration information (see clause 7.3.1).

vii. The retention period of CA event logs (see clause 7.4.11).

viii. Procedures for complaints and dispute settlement.

ix. Reference to the applicable legal system.

x. If the CA has been certified to be conformant with the identified certificate policy, and if so through which scheme.

b) VÍR will communicate information according to a) in a way that permanently secures its integrity. The information is disseminated in a clear and simple language.

7.3.5 Certificate dissemination

VÍR makes the certificates available to subscribers, subjects and interested parties that rely on the certificates. For that purpose VÍR provides the following service:

Dissemination

a) Upon certificate generation and following verification of its content it is made available to subscriber or subject for whom the certificate is being issued.

b) With the subject‘s consent the certificates are available for interested parties.

c) The terms and conditions regarding the use of the certificate are available to the relying parties.

d) The applicable terms and conditions shall be readily identifiable for a given a certificate.

e) The information identified in b) and c) above shall be available internationally 24 hours per day, 7 days per week. Upon system or device failure which are not under the control of the CA, the CA shall make best endeavours to ensure that this information is made available within time limit as denoted in the certification practice statement.

7.3.6 Certificate revocation and suspension

VÍR revokes the certificates as soon as possible if the revocation requests is validated and is from source authorised to request revocation. For that purpose, VÍR provides the following service:

Revocation management

a) VÍR documents as part of its certification practice statement the procedures for revocation of certificates. These procedures include inter alia the following:

i. Who is authorised to submit revocation reports and requests.

ii. How revocation reports and requests may be submitted.

iii. The requirements of the CA for subsequent confirmation of revocation reports and requests.

iv. Whether and for what reasons certificates may be suspended.

v. The mechanism used for distributing revocation status information.

vi. The time delay between receipt of a revocation report or request and the change to revocation status information being available to all relying parties.

b) VÍR processes reports and requests relating to revocation immediately on receipt (e.g. due to compromise of subject’s private key, death of the subject, unexpected changes to the relation between subscribers or subjects and because of termination of contractual obligations).

c) VÍR verifies that reports and requests relating to revocation are from an authorized source. Such reports and requests are confirmed as required under VÍR‘s practices.

d) VÍR can suspend certificates whilst the revocation is being confirmed and ensures that a certificate is not kept suspended for longer than is necessary to confirm its status.

e) The subject and the subscriber of a revoked or suspended certificate are informed of the change of status of its certificate.

f) Once a certificate is definitively revoked (i.e. not suspended) it shall not be reinstated.

g) Certificate Revocation Lists (CRL), including any variants (e.g. Delta CRLs), disclosed by VÍR are published at least every 5 years.

h) Only Certificate Revocation Lists (CRL), or variants (e.g. Delta CRLs), are used to disclose revocation status information and the following applies to them:

   i. Every CRL states a time for the next CRL issue.

   ii. A new CRL may be published before the stated time of the next CRL issue.

   iii. The CRL is signed by the certification authority or an entity designated by the CA.

i) VÍR CRLs are in accordance with requirements in ISO/IEC 9594-8|ITU-T X.509 [10].

j) VÍR revocation management services is available 24 hours per day, 7 days per week. Upon disruption of revocation management services for reasons which are not under the control of the CA, the CA will make best endeavours to ensure that this service is made available again within time limit as denoted in the CA's certification practice statement.

Revocation status

k) Revocation status information will be available 24 hours per day, 7 days per week. Upon disruption of revocation status services for reasons which are not under the control of the CA, the CA shall make best endeavours to ensure that information on revocation status is made available again within time limit as denoted in the CA´s certification practice statement.

l) VÍR protects the integrity and authenticity of the status information.

m) Revocation status information include information on the status of certificates at least until the certificate expires.

7.4 CA management and operation

7.4.1 Information security management

VÍR applies administrative and management procedures which are adequate for the operation and correspond to ÍST EN ISO/IEC 27002:2017 [11].

In particular, VÍR will fulfil the following requirements:

CA General

a) VÍR carries out a risk assessment to evaluate business risks and determine the necessary security requirements and operational procedures. The risk analysis is regularly reviewed and revised as necessary.

b) VÍR is responsible for all aspects of the provision of certification services, also those functions that are outsourced to third parties. Responsibilities of third parties is clearly defined by VÍR and appropriate arrangements are made to ensure that third parties are bound to implement any controls required by VÍR. VÍR is responsible for the disclosure of information on the roles of all parties in the certification practice statement.

c) VÍR management provides direction on information security by approving information security policy and through a high level steering forum that is responsible for maintaining the policy and ensuring publication and communication of the policy to all employees and relevant third parties.

d) VÍR has an efficient information security management system in accordance with the model in ÍST EN ISO/IEC 27001:2017 [12]. VÍR Information Security Management System meets the requirements stipulated in ÍST EN ISO/IEC 27001:2017 [12] for all the certification services VÍR provides. Policies for information security management take note of ÍST EN ISO/IEC 27002:2017 [11].

e) VÍR maintains at all times the information security infrastructure necessary to manage the security. Any changes that will impact on the level of security provided shall be approved by the VÍR Security Management Forum.

f) VÍR has documented, implemented and will maintain the security controls and operating procedures for CA facilities, systems and information assets providing the certification services.

g) VÍR maintains that the security of information when the responsibility for CA functions has been outsourced to another organization or entity.

7.4.2 Asset management

VÍR protects its assets and information. VÍR maintains an asset list of all information and specifies level of protection for these assets in accordance with risk assessment.

7.4.3 Human resources security

VÍR resource planning practices are devised to continuously enhance and support the trustworthiness of the operations.

In particular, VÍR will fulfil the following requirements:

CA General

a) VÍR has at its disposal personnel which possess the expert knowledge, experience and qualifications necessary for the offered services and as appropriate to the job function.

b) VÍR applies appropriate disciplinary sanctions to personnel violating CA policies or procedure.

c) Security roles and responsibilities, as specified in VÍR's security policy, are documented in job descriptions. Trusted roles, on which the security of the CA's operation is dependent, are clearly identified.

d) VÍR personnel, both temporary and permanent, have job descriptions defined from the view point of separation of duties and least privilege. The duties and need for access levels to systems and facilities, background screening of individuals, know-how and understanding of relevant roles are evaluated and balanced in the job descriptions. Where appropriate, these are differentiated between general functions and CA specific functions. Job descriptions include skills and experience requirements.

e) Personnel shall exercise administrative and management procedures and processes that are in line with the VÍR's information security management procedures (see clause 7.4.1).

Registration, certificate generation, subject device provision, revocation management

f) VÍR managerial personnel possesses know-how in electronic signature technology, are familiar with security procedures for personnel with security responsibilities and have experience with information security and risk assessment sufficient to carry out management functions.

g) All VÍR personnel in trusted roles are free from conflicting interests that might prejudice the impartiality of the operations.

h) Trusted roles include roles that involve the following responsibilities:

   i. Security Officers: Overall responsibility for administering the implementation of the security practices and approve the generation, revocation and suspension of certificates.

   ii. System Administrators: Authorized to install, configure and maintain the CA trustworthy systems for registration, certificate generation, subject device provision and revocation management.

   iii. System Operators: Responsible for operating the CA trustworthy systems on a day to day basis. Authorized to perform system backup and recovery.

   iv. System Auditors: Authorized to view archives and audit logs of the CA trustworthy systems.

i) VÍR personnel are formally appointed to trusted roles by senior management responsible for security.

j) Individuals who are known to have a conviction for a serious crime or other offence which affects their suitability for the position are not appoint to trusted roles or management. Personnel do not have access to the trusted functions until any necessary checks are completed. VÍR obtains the consent of the employee in question prior to such checks.

7.4.4 Physical security

VÍR ensures that physical access to critical services is controlled and physical risks to its assets minimized.

In particular, VÍR will fulfil the following requirements:

CA General

a) Physical access to facilities concerned with certificate generation, subject device preparation, and revocation management services is limited to properly authorized individuals.

b) VÍR maintains controls to avoid loss, damage or compromise of assets and interruption to business activities.

c) VÍR maintains controls to avoid compromise or theft of information and information processing facilities.

Certificate generation, subject device provision, revocation management

d) The facilities concerned with certificate generation, subject device preparation (see clause 7.2.9) and revocation management is operated in an environment which physically protects the services from compromise through unauthorized access to systems or data.

e) Any persons entering this physically secure area is continuously monitored by an authorized person.

f) Physical protection is achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the secure areas where certificate generation, subject device preparation (see clause 7.2.9) and revocation management services are located. Any parts of the premises shared with other organizations is located outside this perimeter.

g) VÍR maintains security controls to protect the support facilities, the system resources and the facilities for information processing. The VÍR's security policy for systems concerned with certificate generation, subject device preparation (see clause 7.2.9) and revocation management services addresses the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power utilities, power distribution and telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery.

h) VÍR maintains controls to protect against equipment, information, media and software relating to VÍR services being taken off-site without authorization.

7.4.5 Communications and operations management

VÍR ensures that the CA systems are secure and correctly operated according to recognised best practices, with minimal risk of failure or accidents.

In particular, VÍR will fulfil the following requirements:

CA General

a) VÍR protects the integrity of its systems against viruses, malicious and unauthorized software.

b) VÍR minimizes damage from security incidents and malfunctions through the use of incident reporting and response procedures.

c) Data media used within the VÍR are securely handled to protect media from damage, theft and unauthorized access.

d) VÍR media management procedures protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

e) VÍR defines, documents, implements and uses processes and descriptions of fields of responsibility for all trusted and administrative roles that impact on the provision of certification services.

Media handling and security

f) All media is handled securely in accordance with requirements of the information classification scheme (see clause 7.4.2). Media containing sensitive data is securely disposed of when no longer required.

System Planning

g) VÍR monitors capacity demands and has made projections of future capacity requirements to ensure that adequate processing power and storage are always available.

Incident reporting and response

h) VÍR will act in a timely and co-ordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security. All incidents will be reported as soon as possible.

i) Audit processes are invoked at system startup, in line with clause 7.4.11, and cease only at system shutdown.

j) VÍR monitors audit logs and they are reviewed regularly to identify evidence of malicious activity.

Certificate generation, revocation management

Operations procedures and responsibilities

k) VÍR security operations are separated from normal operations in security operations. Security operations' responsibilities include inter alia the following components:

   i. Operational processes and responsibilities.

   ii. Secure systems planning and acceptance.

   iii. Protection from malicious software.

   iv. Daily operation.

   v. Network management.

   vi. active monitoring of audit journals, event analysis and improvements follow-up.

   vii. Media handling and security.

   viii. Handling of data and software.

   These responsibilities are managed by VÍR security operations. Non-specialist operational personnel may perform these security operations under supervision in accordance with appropriate security policy, description of roles and definition of responsibility.

7.4.6 Access control

Access to VÍR's systems is limited to properly authorized individuals

In particular, VÍR will fulfil the following requirements:

CA General

To ensure that access to VÍR's systems is limited to properly authorized individuals VÍR will inter alia implement the following controls:

a) Effective controls (e.g. firewalls) protect the CA's internal network domains from external network domains accessible by third parties.

b) Sensitive data, such as identifiable personal data, is protected against unauthorized access or modification. Sensitive data is protected when exchanged over networks which are not secure.

c) VÍR maintains effective administration of user access, including system operators, administrators and any users given direct access to the system, to maintain system security. That entails inter alia user account management, auditing and timely modification or removal of access.

d) VÍR ensures that access to information and application systems is restricted in accordance with the access control policy and that VÍR systems provide sufficient computer security controls for the separation of trusted roles identified in CA's practices, including the separation of security administrator and operation functions. Use of system utility programs is restricted and tightly controlled. Access is restricted only allowing access to resources as necessary for carrying out the role allocated to a user.

e) Personnel are identified and authenticated before using critical applications related to certificate management.

f) VÍR personnel are accountable for their activities and shall retain event logs (see clause 7.4.11).

g) Sensitive data, such as registration information, is protected against being revealed through re-used data storage devices (e.g. deleted files) being accessible to unauthorized users.

Certificate generation

h) VÍR ensures that local network components (e.g. routers and switches) are kept in a physically secure environment and their implementation and configurations periodically audited for compliance with security requirements.

i) Measures with continuous monitoring and alarm facilities are provided to make it possible to detect, register and react in a timely manner upon any unauthorized or irregular attempts to access VÍR facilities and assets.

Dissemination

j) Dissemination application enforces access control to prevent attempts to add or delete certificates and modify other associated information.

Revocation management

k) VÍR has continuous monitoring and alarm facilities to make it possible to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.

Revocation status

l) Revocation status application shall enforce access control to prevent attempts to modify revocation status information.

7.4.7 Information systems acquisistion, development and maintenance

VÍR uses trustworthy systems and products that are protected against modification. Systems and devices shall {confirm to suitable protection profiles defined[2]} in accordance with ISO/IEC 15408 [8] or similar. For that purpose, VÍR will:

a) ensure that analysis of security requirements are carried out at the design and requirements specification stage of any systems development project undertaken by VÍR or on behalf of VÍR, to ensure that security is built into IT systems;

b) maintain documented management system for releases, modifications and emergency software fixes for any operational software, e.g. in accordance with the international standard ISO/IEC 20000 *Information technology: Service management* [13].

7.4.8 Business continuity management and information security incident management

VÍR ensure that in the event of a disaster, including compromise of the CA's private signing key, operations are restored as soon as possible

In particular, VÍR will fulfil the following requirements:

CA General

a) VÍR defines and maintain a business continuity plan to enact in case of a disaster.

[2] Translation note: In the authoritative text in Icelandic, the control objective is incomplete in that it refers to the international standard ISO/IEC 15408 for requirements on protection of VÍR's trustworthy systems and devices. The standard defines evaluation criteria for IT security; it does not define system protection requirements. The control objective must therefore refer to the conformity of protection profiles, not system protection. See ETSI TS 101 456 v 1.4.3; NOTE 1 in clause 7.4.7.

CA systems data backup and recovery

b) VÍR backs up the systems data necessary to resume operations and stores them in safe places suitable to allow VÍR to timely go back to operations for CA services in case of incident or disasters.

c) Back-up and restore functions are performed by the relevant trusted roles specified in clause 7.4.3.

CA key compromise

d) VÍR's business continuity plan (or disaster recovery plan) defines security breach or suspected security breach of a CA's private signing key as a disaster and the planned processes are in place.

e) Following a disaster VÍR will, where practical, take steps to avoid repetition of a disaster.

Revocation status

f) In the case of compromise VÍR will inter alia provide the following undertakings:

   i. Inform the following of the compromise: all subscribers and other entities with which VÍR has agreements or other form of established relations, among which parties relying on security in the CA's operation, and other CAs. In addition, this information shall be made available to other parties relying on security in the CA's operation.

   ii. Indicate that certificates and revocation status information issued using the CA private key may no longer be valid.

Algorithm compromise

g) Should any of the algorithms, or associated parameters, used by VÍR or its subscribers become insufficient for its remaining intended usage then VÍR will:

   i. inform all subscribers and those entities relying on security in the VÍR's operation with which the CA has agreement or other form of established relations. In addition, this information shall be made available to other relying parties relying on security in the CA's operation;

   ii. revoke any certificate affected by the algorithms or associated parameters.

7.4.9 Service termination

VÍR ensures that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the CA's services and operation, and ensures continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings.

In particular, VÍR will fulfil the following requirements:

CA General

a) Before VÍR terminates its services the following procedures will be executed:

   i. Inform the following of the compromise: all subscribers and other entities with which VÍR has agreements or other form of established relations, among which parties relying on security in the CA's operation, and other CAs. In addition, this information shall be made available to other parties relying on security in the CA's operation.

   ii. Terminate all authorization of subcontractors to act on behalf of VÍR in the performance of functions related to the process of issuing certificates.

   iii. Perform necessary undertakings to transfer obligations for maintaining registration information (see clause 7.3.1), and event log archives (see clause 7.4.11) for their respective period of time as indicated to the subscriber and relying party (see clause 7.3.4).

   iv. Destroy, or withdraw from use, those CA systems important to cease using after termination, e.g. the CA's private keys if certificate issuance is terminated, as defined in clause 7.2.6.

b) VÍR has the capability to meet these minimum requirements above.

c) VÍR states in its certification practice statement the provisions made for termination of service. This shall include inter alia:

i. The notification of entities affected by the termination.

ii. The transfer of its obligations to other parties.

iii. The handling of the component services necessary to retain after termination, possibly by third party. This can include handling of revocation status for certificates that have been issued.

7.4.10 Compliance

VÍR complies with legal requirements

In particular, VÍR will fulfil the following requirements:

CA General

a) VÍR meets all applicable statutory requirements for protecting records from loss, destruction and falsification. Some records may need to be securely retained to meet statutory requirements, as well as to support essential business activities (see clause 7.4.11).

b) In processing of personal data VÍR meets the requirements of Act No. 90/2018 on the protection of privacy as regards the processing of personal data [4]

c) VÍR takes appropriate technical and organizational measures against unauthorized or unlawful processing of personal data and against loss, destruction of, or damage to, personal data.

d) The information that users contribute to VÍR are completely protected from disclosure without the user's agreement, a court order or other legal authorization.

7.4.11 Recording of information

VÍR ensures that all relevant information concerning a certification services (including registration information and information concerning significant environmental, key management and certificate management events) is recorded for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings

In particular, VÍR will fulfil the following requirements:

General

VÍR ensures the following in recording information:

a) the confidentiality and integrity of both current and archived records concerning certificates;

b) records concerning certificates are completely and confidentially archived in accordance with disclosed business practices;

c) records concerning certificates are made available if required for the purposes of providing evidence of certification for the purpose of legal proceedings. The subject, and within the constraints of data protection requirements (see clause 7.4.10) the subscriber, have access to registration and other information relating to the subject;

d) the precise time of significant CA environmental, key management and certificate management events is recorded;

e) documents concerning certificates are protected for an appropriate period of time as indicated in the terms and conditions (see clause 7.4.10) for the purpose of providing evidence to support electronic signatures in accordance with applicable legislation;

f) the events are logged in a way that they cannot be easily deleted or destroyed within the period of time that they are required to be held;

g) specification of what events shall be logged and how.

Registration

h) VÍR ensures that all events relating to registration including requests for certificate re-key or renewal, are logged.

i) VÍR ensures that all registration information including the following is recorded:

   i. type of documents presented by the applicant to support registration;

   ii. record of unique identification data, numbers, or a combination thereof (e.g. applicant's drivers license number) of identification documents, if applicable;

   iii. storage location of copies of applications and identification documents, including the signed subscriber agreement (see clause 7.3.1);

   iv. any specific choices in the subscriber agreement (e.g. consent to publication of certificate and other information, see clause 7.3.1);

   v. identity of entity accepting application;

   vi. method used to validate identification documents, if any;

   vii. name of receiving CA or submitting Registration Authority, if applicable.

j) VÍR logs all events relating to the life-cycle of its own private keys[3].

Certificate generation

k) VÍR logs all events relating to the life-cycle of its own private keys.

l) VÍR logs all events relating to the life-cycle of certificates.

Subject device provision

m) VÍR logs all events relating to the life cycle of keys managed by the CA, including any subject keys generated by the CA.

n) If applicable, VÍR logs all events relating to the preparation of secure user devices.

Revocation management

o) VÍR logs all requests and reports relating to revocation, as well as the resulting action.

7.5 Organization

VÍR ensures that the CA operation is reliable

In particular, VÍR will fulfil the following requirements:

CA general

VÍR fulfils the following conditions inter alia so that the CA operation is reliable.

a) Operates under non-discriminatory policies and procedures.

b) Offers its services to all applicants whose activities fall within its declared field of operation.

c) Is a registered legal entity.

d) Has adequate insurance to cover liabilities arising from its operations and/or activities.

e) Has the strength and financial stability required to operate in conformity with this policy.

f) Ensures that there are policies and procedures for the resolution of complaints and disputes received from customers or other parties about the provisioning of certification services or any other related matters.

[3] Translation note: In the authoritative text in Icelandic, control 7.4.11 j) is an exact copy of control 7.4.11 k). This is most likely an error. In the underlying technical specification ETSI TS 101 456 v1.4.3, control 7.4.11 j) is “the CA shall ensure that privacy of subject information is maintained“.

g) Properly documents agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements.

Certificate generation, revocation management

h) The parts of VÍR concerned with certificate generation and revocation management is independent of other organizations for its decisions relating to the establishing, provisioning and maintaining and suspending of services in conformity with this policy. Senior executives, senior staff and staff in trusted roles are free from any commercial, financial or other interests which might adversely influence trust in the services it provides

i) The parts of VÍR concerned with certificate generation and revocation management has a documented structure which safeguards impartiality of operations.