Global Informatics Policy

Roche Certificate Policy/Certification Practice Statement

Document ID:	1944210
Version:	1.0
Effective Date:	Date of last approval signature

Document Information

Document Owner	Global Head Information Security & Privacy Governance
Document Location	Electronically: Approved version in Project Library
Geographical Scope	Global
Associated Documents	Roche Information Security Policy (PL ID 1327020) Password Management Standard (PL ID 6305535)

Review

Role	Name	Dept.	Signature Date
Author	Julio Muiños	FGQE	See e-signature page
Head of Global Information Security and Privacy Governance	Dan West	FGQ	See e-signature page
Head of Monitoring and Incident Response	Tim Ehrhart	FGQ	See e-signature page
Head of Secure Access Engineering	Enrique de la Torre	FIRE	See e-signature page
Head of Secure Access Operations	Cédric Heimburger	FIRO	See e-signature page
Enterprise Security Architecture	Carl Koster	FIRA	See e-signature page

Approval

Role	Name	Dept.	Signature Date
Vice President, Global Head, Group Information Security/Privacy, Quality, Process & Risk Management	Vicky Imber	FG	See e-signature page

Note: The electronic signatures for this document can be found on the e-signature page(s). Manual signatures (if any) are scanned and stored in a separate PDF file in the same location as the original document.

Document History

Version	Changes	Effective Date
1.0	New policy content	Date of last approval signature

Table of Contents Page

1. Introduction

This document describes the certificate policy (CP) that defines the set of rules that must be followed by any implementation of a Public Key Infrastructure (PKI) environment at Roche providing global certificate services for Corporate as well as the Pharma and Diagnostics divisions.

The certificate policy details security requirements specifically for the PKI implementation, however, it is subordinate to the existing Roche security policies and standards (see References in section 10), which must be followed as well.

This CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) Certificate Policy and Certification Practices Framework [RFC3647]. The recommendations are intended to support audit programs.

A PKI that uses this CP provides some or all of the following security management services:

- Key generation/storage
- Certificate generation, modification, and distribution
- Certificate Revocation List (CRL) generation and distribution including Online Certificate Status services.
- Repository management of certificate related items
- System management functions (e.g., security audit, configuration management, archive)

CAs that issue certificates under this policy may operate simultaneously under other policies. CAs must not assert this policy in certificates unless they are issued in accordance with all the requirements of this policy.

1.1 Scope

1.1.1 In-scope

The scope of this document includes:

Geographical: Global

Organizational:

Roche Group

- Group functions
- Diagnostics division
- Pharmaceutical division (including Genentech)

Functional:

Roche Group information systems.

Technical:

- Certificates

1.1.2 Out of scope

The scope of this document does not include:

Organizational: Chugai.

Functional: N/A

Technical:

Certificates for external use.

1.2 Definitions and Acronyms

AIA	Authority Information Access
AOR	Authorized Organizational Representative. Person or team member who is authorized according to the PKI assigned roles to make decisions regarding the identification of certificate subjects and other key activities. In some cases, identification can be delegated in automated processes that involves subject identification.
CA	Certification Authority
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Objects Registry
CSR	Certificate Signing Request
CSS	Certificate Status Server
DN	Distinguished Name
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS PUB	(US) Federal Information Processing Standards Publication
FPKI	Federal Public Key Infrastructure
HTTP	Hypertext Transfer Protocol
HR	Human Resources

ICANN	Internet Corporation for Assigned Names and Numbers
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IS	Information System
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
ISO	International Organization for Standardization
ITU-T	International Telecommunications Union – Telecommunications Sector
IoT	Internet of Things
N/A	Not applicable
NIST	National Institute of Standards and Technology
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OZ	Operations Zone
PA	Policy Authority
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PSS	Probabilistic Signature Scheme
PZ	Public Zone
Registrar	Domain registration service provider
RA	Registration Authority
RZ	Restricted Zone
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
RSASSA	RSA Signature Scheme with Appendix
SHA	Secure Hash Algorithm
S/MIME	Secure/Multipurpose Internet Mail Extensions
SAZ	Special Access Zone

SP	Special Publication
SSP-REP	Shared Service Provider Repository Service Requirements
TAM	Trust Anchor Manager
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
U.S.C.	United States Code
UUID	Universal Unique Identifier
VPN	Virtual Private Network
WAP	Wireless Access Point

1.3 Overview

A CA is a collection of hardware, software, personnel, and operating procedures that issue and manage public key certificates, also known as digital certificates. The public key certificate binds a public key to a named subject. This allows relying parties to trust signatures or assertions made by the subject using the private key that corresponds to the public key contained in the certificate.

A fundamental element of modern secure communications is establishing trust in public keys. This begins with a Relying Party obtaining a Subscriber's public key certificate that is issued by a trusted entity certifying that the public key belongs to that Subscriber. Subscriber certificates that are not trusted directly may become trusted through successive validation of a chain of CA certificates from the Subscriber's certificate to a trust anchor (typically a Root-CA public key). Trust anchors are explicitly trusted by Relying Parties. Relying Parties are responsible for securely obtaining trust anchors and for securely managing their trust anchor store. Relying Parties, including the Trust Anchor Managers should configure trust anchors with great caution and should give full consideration to the requirements of this CP and associated compliance annual audit requirements.

1.4 Name and Identification

Title: Roche Certificate Policy/Certification Practice Statement

Version: 1.0

Object Identifier: **2.16.840.1.113995.2.1.1**

By including this policy identifier in a certificate, the CA states conformance to the policy.

1.5 PKI participants

This section identifies roles that are relevant to the administration and operation of CAs under this policy.

1.5.1 PKI Authorities

Policy Authority (PA): This is the entity that decides that a set of requirements for certificate issuance and use are sufficient for a given application. The Policy Authority (PA):

- Establishes and maintains the Certificate Policy (CP).
- Approves the establishment of trust relationships with external PKIs that offer appropriately comparable assurance.

The Policy Authority is represented by Security and Privacy Governance in Roche.

Trust Anchor Managers (TAMs): Authorities who manage a repository of trusted Root CA Certificates. They act on behalf of relying parties, basing their decisions on which CAs to trust on the results of compliance audits. These requirements are based on both security and business needs. The TAM has a duty to enforce compliance with these requirements, for example, requirements around the supply of compliance audit results, on initial acceptance of a root, and on an ongoing basis. TAMs will follow their normal practice of requiring CAs to submit an annual compliance audit report. It is our intention that the requirements in this document will be included in those compliance audit schemes. As specified in Section 5.6, the TAM will require the CA to provide notification of a compromise, and in response, the TAM will take appropriate action.

TAMs is represented by the following roles:

- A representative of Roche IT Security and Privacy Governance, with one or more deputies.
- A representative of Roche Secure Access Operations, with a deputy.
- The Service Owner of the Roche PKI, with a deputy.

1.5.1.1 Certification Authority

The CA is the collection of hardware, software and operating personnel that create, sign, and issue public key certificates to subscribers. This includes centralized, automated systems such as autoenrolled certificates for laptops. The CA is responsible for issuing and managing certificates including:

- Approving the issuance of all certificates, including those issued to subordinate CAs and RAs.
- Publication of certificates
- Revocation of certificates
- Generation and destruction of CA signing keys
- Establishing and maintaining the CA system

Certification Authority (CA) Administrators and Operation Staff: CA components are operated and managed by individuals holding trusted, sensitive roles. Specific responsibilities for these roles, as well as requirements for separation of duties, are described in Section 5.2.

Security Auditor: An individual who is responsible for auditing the security of CAs or Registration Authorities (RAs), including reviewing, maintaining, and archiving audit logs; and performing or overseeing internal audits of CAs or RAs. A single individual may audit both CAs and RAs. Security Auditor is an internal role that is designated as trusted.

1.5.1.2 Online Certificate Status Servers

PKIs may optionally include a service that provides status information about certificates on behalf of a CA through on-line transactions. In particular, PKIs may include Online Certificate Status Protocol (OCSP) responders to provide on-line status information. Such a service is termed a Online Certificate Status Server (OCSS). Where the OCSS is identified in certificates as an authoritative source for revocation information or issued a delegated Responder certificate, the operations of that authority are considered within the scope of this CP.

1.5.2 Registration Authorities (RAs)

The registration authorities (RAs) collect and verify each subscriber’s identity and information that is to be entered into the subscriber’s public key certificate. The RA is responsible for:

- The registration process.
- The identification and authentication process.

Registration Authority Staff: RA Staff are the individuals holding trusted roles that operate and manage RA components.

1.5.3 Trusted Agents

The trusted agent is a person who performs identity proofing as a proxy for the RA. The trusted agent records information from and verifies biometrics (e.g., fingerprints, photographs) on presented credentials for an applicant’s identity on behalf of the RA.

1.5.4 Subscribers

A subscriber is the entity whose name appears as the subject in an end-entity certificate (also known as a subscriber certificate), agrees to use its key and certificate in accordance with the Certificate Policy asserted in the certificate, and does not itself issue certificates. CAs are sometimes technically considered “subscribers” in a PKI. However, the term “subscriber” as used in this document refers only to those who request leaf certificates for uses other than signing and issuing certificates or certificate status information.

Roche may issue certificates for itself and act as subscriber. The same requirements apply to Roche as for all other subscribers.

The targeted PKI subscribers or subjects include, but are not limited to, the following categories of entities:

- Roche employees.
- Roche eligible contractors.
- Roche external business partners.
- Devices (such as client workstations, servers, network equipment, appliances, IoT…): these components must be owned and operated by any of the above person categories (i.e. employees, contractors or business partners), who accept the certificate and are responsible for the correct protection and use of the associated private key.

- Programs/Services.

1.5.5 Relaying Parties

A Relying Party is an entity that relies on the validity of the binding of the Subscriber's name to a public key. The Relying Party uses a Subscriber's certificate to verify or establish the identity and status of the Subscriber. A Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. A Relying Party may use information in the certificate to determine the suitability of the certificate for a particular use.

1.5.6 Other participants

The CAs and RAs operating under the CP may require the services of other security, community, and application authorities.

1.6 Certificate Usage

1.6.1 Appropriate Certificate Uses

The certificates issued by CAs operating under this policy will be used mostly internally for:

- Authentication (e.g. human subscriber, device subscriber)
- Encryption (e.g. email, files/folders)
- Signing (e.g. email, code)

The certificates shall only be used for the applications which are in accordance with the usage specified in the certificate (keyUsage).

Issued certificates will not support legally binding digital signatures/non-repudiation.

Issued certificates have no legal binding to the subscriber/subjects and imply no liability.

The keys of the Root CA are used exclusively for signing CA certificates and revocation lists.

The private keys of Issuing CAs are used to sign the associated leaf certificates and revocation lists.

1.6.2 Prohibited Certificate Usage

Types of use that do not correspond to the use specified in the certificate (keyUsage) are not permitted. Roche shall not be liable for damages resulting from the use of the services beyond these restrictions.

1.7 Policy Administration

1.7.1 Organization Administering the Document

The Policy Authority is responsible for all aspects of this CP.

1.7.2 Contact Person

Contact person for questions related to this policy is the Global Head of Information Security and Privacy Governance or the assigned PKI Service Owner.

2. Publication and Repository Responsibilities

2.1 Repositories

All CAs that issue certificates under this policy are obligated to post all CA certificates issued by or to the CA and CRLs issued by the CA in a repository that is publicly accessible through all Uniform Resource Identifier (URI) references asserted in valid certificates issued by that CA. CAs may optionally post subscriber certificates in this repository. To promote consistent access to certificates and CRLs, the repository shall implement access controls and communication mechanisms to prevent unauthorized modification or deletion of information.

2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate Status

The publicly accessible repository system shall be designed and implemented so as to provide 99% availability overall and limit scheduled down-time to 0.5% annually. Where applicable, the certificate status server (CSS) shall be designed and implemented so as to provide 99% availability overall and limit scheduled down-time to 0.5% annually.

2.3 Time or Frequency of Publication

An updated version of the CP will be made publicly available within thirty days of the incorporation of changes. The CRL is published as specified in Section 4.9.7. All information to be published in the repository shall be published promptly after such information becomes available to the CA.

2.4 Access Controls on Repositories

The CA shall protect information not intended for public dissemination or modification. CA certificates and CRLs in the repository shall be publicly available through the Internet. Direct and/or remote access to other information in the CA repositories shall be determined by Policy Authority.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The CA shall assign an X.501 Distinguished Name (DN) to each subscriber. Subscriber certificates may contain any name type appropriate to the application.

3.1.2 Need for Names to be Meaningful

Names used in certificates must represent an unambiguous identifier for the subject. Names shall be meaningful enough for a human to identify the named entity, irrespective of whether the entity is a person, machine, or process. Interpreting the name semantic may require a reference database (e.g., human resources directory or inventory catalog) external to the PKI.

Examples are:

Person Name	*John Smith*
Domain Name	*publicinfo.dept.roche.com*
Machine Name	*"manufacturer=DeviceRoche, model=DC-ABCD, serial=00098765"*
Email Address	*jsmith@roche.com*
IP Address	*192.168.100.75 (shall be a routable, permanent IP address)*

While the issuer name in CA certificates is not generally interpreted by relying parties, this CP still requires use of meaningful names by CAs issuing under this policy. CA certificates that assert this policy shall not include a personal name, but rather shall identify the subject as a CA and include the name-space for which the CA is authoritative. For example:

c= country, o = Issuer Organization Name, cn = *OrganizationX CA-3*

The subject name in CA certificates must match the issuer name in certificates issued by the subject, as required by [RFC5280].

3.1.3 Anonymity or pseudonymity of subscribers

The CA shall not issue anonymous certificates. Pseudonymous certificates, if issued shall be identified as such. CAs issuing pseudonymous certificates shall maintain a mapping of identity to pseudonym.

3.1.4 Rules for interpreting various name forms

Rules for interpreting distinguished name forms are specified in X.501. Rules for interpreting e-mail addresses are specified in [RFC 2822].

3.1.5 Uniqueness of names

Each CA must ensure that each of its subscribers is identifiable by a unique name. Each X.500 name assigned to a subscriber by a CA (i.e., in that CA's namespace) must identify that subscriber uniquely. When other name forms are used, they too must be allocated such that each name identifies only one subscriber of that CA. Name uniqueness is not violated when multiple certificates are issued to the same entity. For certificates that assert names that do not identify individual people, an Authorized Organizational Representative (AOR) shall be identified as having responsibility for the certificate subject.

3.1.6 Recognition, authentication and role of trademarks

CAs operating under this policy shall not issue a certificate knowing that it infringes on the trademark of another. The PA shall resolve disputes involving names and trademarks.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

In all cases where the party named in a certificate generates its own keys, that party shall be required to prove possession of the private key, which corresponds to the public key in the certificate request.

For signature and encryption keys, this may be done by the entity using its private key to create a Certificate Signing Request (CSR), which the CA will then validate. Other mechanisms that are at least as secure as those cited here may be used. The CA shall ensure that any mechanism or procedure used ties the private key to the identity being asserted by the subscriber.

In the case where key generation is performed under the CA or RA’s direct control, proof of possession is not required.

3.2.2 Authentication of organization identity

Requests for CA certificates shall include the CA name, address, and documentation of the existence of the CA. Before issuing CA certificates, an authority for the issuing CA shall verify the information, in addition to the authenticity of the requesting representative and the representative’s authorization to act in the name of the CA.

For subscriber organization certificates, the CA shall verify the existence of the organization by verifying the identity and address of the organization and that the address is the subscriber’s address of existence or operation.

3.2.3 Authentication of individual identity

3.2.3.1 Authentication of human subscribers

The RA shall ensure that the subscriber’s identity information is verified. Identity shall be verified no more than 30 days before initial certificate issuance. RAs may accept authentication of a subscriber’s identity attested to and documented by a trusted agent or notary to support identity proofing of remote subscribers. Authentication by a trusted agent or notary does not relieve the RA of its responsibility to perform steps 1), 2), the verification of identifying information (e.g., by checking official records) in step 3), and the maintenance of records in step 4), below.

At a minimum, authentication procedures for human subscribers must include the following steps:

1. Verify that a request for certificate issuance to the applicant was submitted by the organization.
2. Verify Subscriber’s organizational membership through use of official organization records.
3. Establish subscriber’s identity by in-person proofing before the registration authority, based on the following process:

a) The subscriber presents an official form of identification (e.g., an organization ID badge, a passport, or driver's license) as proof of identity

b) The RA examines the presented credential that can be linked to the subscriber (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and

c) The credential presented above shall be verified by the RA for currency and legitimacy (e.g., the organization ID is verified as valid).

4. Verify information to be included in the certificate (e.g., e-mail address, subject alternative pseudonymous names).
5. Record and maintain records of the applicant by the RA or CA. This information is archived to help establish an audit trail for dispute resolution.

3.2.3.2 Authentication of devices

Some computing and communications devices (e.g. routers, firewalls, etc.) will be named as certificate subjects. In such cases, an Authorized Organizational Representative (AOR), or in certain cases the device itself, must provide identifying information for the device. The AOR/device is responsible for providing registration information which may include:

- Equipment identification (e.g., serial number)
- Equipment certificate signing request CSR
- Equipment authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the AOR when required.

The registration information provided by the AOR/device shall be verified. If the device itself provides this information, the identity of the device shall be authenticated. If the information is provided by an AOR for a single device or batch of devices, the AOR shall be authenticated.

3.2.3.3 Authentication of applications or services

Some software applications or services will be named as certificate subjects. In such cases, an Authorized Organizational Representative (AOR) must provide identifying information for the application or service. The AOR is responsible for providing registration information which may include:

- Unique software application or service name (e.g. DNS name)
- Software application or service certificate signing request CSR
- Software application or service authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the AOR when required.

The registration information provided by the AOR shall be verified. The CA shall validate that the AOR is authorized to request a certificate for the application or service.

3.2.4 Non-verified subscriber information

Information that is not verified shall not be included in certificates. All certificate contents are verified by the CA or RA, either directly or by an attestation from the AOR who is authoritative for the certificate subject.

3.2.5 Validation of Authority

Before issuing CA certificates or signature certificates that assert organizational authority, the CA shall validate the subscriber’s authority to act in the name of the organization. For role certificates that identify subjects by their organizational roles, the CA shall validate that the individual either holds that role or has been delegated the authority to sign on behalf of the role.

3.2.6 Criteria for Interoperation

No interoperability required as there are no other CAs under a different Certificate Policies where interoperability between CAs is required (e.g. direct cross-certification bridge).

3.3 Identification and authentication for revocation request

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's public key, regardless of whether or not the associated private key has been compromised.

4. Certificate life-cycle operational requirements

4.1 Certificate Application

The Certificate application process must provide sufficient information to:

- Establish the subscriber’s authorization (by the employing or sponsoring organization) to obtain a certificate. (per Section 3.2.3)
- Establish and record identity of the applicant. (per Section 3.2.3)
- Obtain the applicant’s public key and verify the applicant’s possession of the private key for each certificate required. (per Section 3.2.1)
- Verify any role or authorization information requested for inclusion in the certificate.

These steps may be performed in any order that is convenient for the CA and applicants that does not compromise security, but all must be completed before certificate issuance.

4.1.1 Who can submit a certificate application

A certificate application shall be submitted to the CA by the Subscriber, AOR, or an RA on behalf of the Subscriber. Multiple certificate requests from one RA or AOR may be submitted as a batch.

4.1.2 Enrollment process and responsibilities

All communications among PKI Authorities supporting the certificate application and issuance process shall be authenticated and protected from modification; any electronic transmission of shared secrets and personally identifiable information shall be protected. Communications may be electronic or out-of-band. Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair shall be used. Out-of-band communications shall protect the confidentiality and integrity of the data.

Subscribers are responsible for providing accurate information on their certificate applications.

4.2 Certificate application processing

Information in certificate applications must be verified as accurate before certificates are issued.

4.2.1 Performing identification and authentication functions

The identification and authentication of the subscriber shall meet the requirements specified for subscriber authentication as specified in Sections 3.2 and 3.3.

4.2.2 Approval or rejection or certificate applications

Any certificate application that is received by a CA under this policy, for which the identity and authorization of the applicant has been validated, will be duly processed. However, the CA shall reject any application for which such validation cannot be completed, or when the CA has cause to lack confidence in the application or certification process.

4.2.3 Time of process certificate applications

Certificate applications must be processed and a certificate issued within 30 days of identity verification.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Upon receiving the request, the CAs/RAs shall:

- Verify the identity of the requester as specified in Section 3.2.
- Verify the authority of the requester and the integrity of the information in the certificate request as specified in Section 4.1.
- Build and sign a certificate if all certificate requirements have been met (in the case of an RA, have the CA sign the certificate).

- Make the certificate available to the subscriber after confirming that the subscriber has formally acknowledged their obligations.

The certificate request may already contain a to-be-signed certificate built by either the RA or the subscriber. This certificate shall not be signed until all verifications and modifications, if any, have been completed to the CA's satisfaction.

All authorization and other attribute information received from a prospective subscriber shall be verified before inclusion in a certificate.

4.3.2 Notification to subscriber by the CA of issuance of certificate

CAs operating under this policy shall inform the subscriber (or other certificate subject) of the creation of a certificate and make the certificate available to the subscriber. For device certificates, the CA shall issue the certificate according to the certificate requesting protocol used by the device (this may be automated) and, if the protocol does not provide inherent notification, also notify the authorized organizational representative of the issuance (this may be in batch).

4.4 Certificate acceptance

Before a subscriber can make effective use of its private key, the CA shall explain to the subscriber its responsibilities and obtain the subscriber's acknowledgement.

4.4.1 Conduct constituting certificate acceptance

Failure to object to the certificate or its contents shall constitute acceptance of the certificate.

4.4.2 Publication of the certificate by the CA

As specified in Section 2.1, all CA certificates shall be published in repositories.
This policy makes no stipulation regarding publication of subscriber certificates.

4.4.3 Notification of certificate issuance by the CA to other entities

PKI Authorities must be notified whenever a CA operating under this policy issues a CA certificate.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The intended scope of usage for a private key shall be specified through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate.

4.5.2 Relaying party public key certificate usage

Certificates may specify restrictions on use through critical certificate extensions, including the basic constraints and key usage extensions. All CAs operating under this policy shall issue CRLs specifying the current status of all unexpired certificates except for OCSP responder certificates. It is recommended that relying parties process and comply with this information whenever using certificates in a transaction.

4.6 Certificate renewal

An old certificate may or may not be revoked, but must not be further re-keyed, or modified.

4.6.1 Circumstance for certificate renewal

Any certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been revoked or compromised, and the Subscriber name and attributes are unchanged. In addition, the validity period of the certificate must not exceed the remaining lifetime of the private key, as specified in Section 5.6. The identity proofing requirements listed in Section 3.3 shall also be met.

CA Certificates and OCSP responder certificates may be renewed as long as the aggregated lifetime of the public key does not exceed the certificate lifetime specified in Section 6.3.2.

The CA may renew previously-issued certificates during recovery from CA key compromise without subject request or approval as long as the CA is confident of the accuracy of information to be included in the certificates.

4.6.2 Who may request renewal

For all CAs and OCSP responders operating under this policy, the corresponding operating authority may request renewal of its own certificate. The Subscriber, RA or AOR may request the renewal of a Subscriber certificate.

4.6.3 Processing certificate renewal requests

Subscriber renewal requests may be processed using the same process used for initial certificate issuance.

4.6.4 Notification of renewed certificate issuance to subscriber

The CA shall inform the subscriber of the renewal of his or her certificate and the contents of the certificate.

4.6.5 Conduct constituting acceptance of a renewed certificate

Failure to object to the renewal of the certificate or its contents constitutes acceptance of the certificate.

4.6.6 Publication of the renewed certificate by the CA

As specified in Section 2.1, all CA certificates shall be published in repositories.

Publication of renewed subscriber certificates is subject to the requirements in Section 2 of this policy.

4.6.7 Notification of renewed certificate issuance by the CA to other entities

Not applicable.

4.7 Certificate re-key

Not applicable, as certificates are not re-key at Roche, but re-issued.

4.8 Certificate modification

Modifying a certificate means creating a new certificate that has the same key, a different serial number, and that differs in one or more other fields from the old certificate. Because of the requirement to validate particular field changes, it is often simpler and more secure to require re-certification than to offer certificate modification.

An old certificate may or may not be revoked, but must not be further re-keyed, or modified.

4.8.1 Circumstance for certificate modification

A CA may perform certificate modification for a subscriber whose characteristics have changed (e.g. name change due to marriage). If the subscriber name has changed, the subscriber shall undergo the initial registration process.

4.8.2 Who may request certificate modification

Requests for certificate modification shall be considered as follows:

- Subscribers with a currently valid certificate may request certificate modification.
- CAs and RAs may request certificate modification on behalf of a subscriber.
- For device, application, and role certificates, an AOR may request certificate modification.

4.8.3 Processing certificate modification requests

A certificate modification shall be achieved using the following process:

- Initial registration process as described in Section 3.2

The RA shall complete all required re-verification prior to issuing the modified certificate.

4.8.4 Notification of the new certificate issuance to subscriber

The CA shall inform the subscriber of the modification of his or her certificate and the contents of the certificate.

4.8.5 Conduct constituting acceptance of modified certificate

Failure to object to the certificate or its contents constitutes acceptance of the certificate.

4.8.6 Publication of modified certificate by the CA

All CA certificates must be published as specified in section 2

Publication of renewed subscriber certificates is subject to the requirements in Section 2 of this policy.

4.8.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.9 Certificate revocation and suspension

CAs operating under this policy should issue CRLs, and/or provide OCSP responses covering all unexpired certificates issued under this policy except for OCSP responder. Relying party client software may support on-line status checking and some support only CRLs.

CAs operating under this policy shall make public a description of how to obtain revocation information for the certificates they publish, and an explanation of the consequences of using dated revocation information. This information shall be given to subscribers during certificate request or issuance, and shall be readily available to any potential relying party.

Revocation requests must be authenticated. See Section 3.3 for more details.

4.9.1 Circumstances of revocation

A certificate shall be revoked when the binding between the subject and the subject’s public key defined within the certificate is no longer considered valid. When this occurs the associated certificate shall be revoked and placed on the CRL and/or added to the OCSP responder. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

Examples of circumstances that invalidate the binding are:

- Identifying information or affiliation components of any names in the certificate becomes invalid.
- Any information in the certificate becomes invalid.
- The subscriber can be shown to have violated the stipulations of its subscriber agreement.
- There is reason to believe the private key has been compromised.
- The original certificate request was not authorized.

- The subscriber or other authorized party asks for his/her certificate to be revoked.

The list above is not intended to be an exhaustive list of circumstances for certificate revocation.

4.9.2 Who can request revocation

Within the PKI, a CA may summarily revoke certificates within its domain. A written notice and brief explanation for the revocation should subsequently be provided to the subscriber. The RA can request the revocation of a subscriber's certificate on behalf of any authorized party. A subscriber may request that its own certificate be revoked. The AOR of the organization that owns or controls a device can request the revocation of the device's certificate. Other authorized individuals of the organization may request revocation.

4.9.3 Procedure for revocation request

A request to revoke a certificate shall identify the certificate to be revoked and allow the request to be authenticated (e.g. digitally or manually signed). The CA may request information sufficient to explain the reason for revocation.

4.9.4 Revocation request grace period

There is no grace period for revocation under this policy.

4.9.5 Time within which CA must process the revocation request

CAs will revoke certificates as quickly as practical upon receipt of a proper revocation request and after the requested revocation time. Revocation requests shall be processed within four hours of receipt.

4.9.6 Revocation checking requirements for relaying parties

Use of a revoked certificate could have damaging or catastrophic consequences in certain applications. The matter of how often new revocation data should be obtained is a determination to be made by the relying party.

If it is temporarily infeasible to obtain revocation information, then the relying party must either reject use of the certificate or make an informed decision to accept the risk. Such use may occasionally be necessary to meet an urgent operational requirement.

4.9.7 CRL issuance frequency

CRLs, if issued, shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below.

Certificate status information shall be published no later than the next scheduled update. This will facilitate the local caching of certificate status information for off-line or remote operation.

Online CAs that issue CRLs must issue them at least once every 24 hours, and the *nextUpdate* time in the CRL may be no later than 96 hours after issuance time (i.e., the *thisUpdate* time).

Offline CAs that issue CRLs must issue CRLs at least once every 30 days, and the *nextUpdate* time in the CRL may be no later than 60 days after issuance time (i.e., the *thisUpdate* time).

Circumstances related to emergency CRL issuance are specified in section 4.9.12.

4.9.8 Maximum latency for CRLs

CRLs shall be published within 6 hours of generation. Furthermore, each CRL shall be published no later than the time specified in the *nextUpdate* field of the previously issued CRL for the same scope.

4.9.9 On-line revocation/status checking availability

Where on-line status checking is supported, status information must be updated and available to relying parties within 24 hours of the decision to revoke.

4.9.10 On-line revocation checking requirements

Relying party client software should support on-line status checking. Client software using on-line status checking do not need to obtain or process CRLs.

4.10 End of subscription

Subscription is synonymous with the certificate validity period. The subscription ends when the certificate is revoked or expired.

4.11 Key escrow and recovery

4.11.1 Key escrow and recovery policy and practices

CA private keys shall never be escrowed.

Under no circumstances shall a subscriber signature key be held in trust by a third party. CAs that support private key escrow for key management keys shall document their specific practices and key escrow documentation.

Subscriber key management keys may be escrowed to provide key recovery. Escrowed keys shall be protected at no less than the level of security in which they are generated, delivered, and protected by the subscriber.

5. Facility, management and operational controls

5.1 Physical controls

All CA and RA equipment, including cryptographic modules, shall be protected from theft, loss, and unauthorized access at all times. Unauthorized use of CA and RA equipment is prohibited. CA equipment shall be dedicated to performing CA functions. RA equipment shall be operated to ensure that the equipment meets all physical controls at all times.

The following sections discuss the CA and the RA as if they were physically separate. If they are not, then the most strict of any applicable requirement must apply.

5.1.1 Site location and construction

The location and construction of the facility housing the CA equipment, as well as sites housing remote workstations used to administer the CAs, shall be consistent with facilities used to house high-value, sensitive information, following the Roche Data Center requirements.

5.1.2 Physical access

5.1.2.1 Physical access for CA equipment

Physical access to CA equipment shall be limited to CA Operations Staff and Security Auditors. The security mechanisms shall be commensurate with the level of threat in the equipment environment.

At a minimum, physical access controls for CA equipment and all copies of the CA cryptographic module shall meet the following requirements:

- Ensure that no unauthorized access to the hardware is permitted.
- Be manually or electronically monitored for unauthorized intrusion at all times.
- Ensure an access log is maintained and available for inspection.
- Mandate at least two-person access requirements. Both people must hold trusted roles and at least one individual shall be a member of the CA Operations Staff. Technical or mechanical mechanisms (e.g., dual locks) shall be used to enforce the two-person physical access control.
- Other individuals shall be escorted by two persons. This includes maintenance personnel. All individuals shall be recorded in the access log.
- Upon the permanent departure of trusted personnel, ensure access to sensitive physical areas is denied.

When not in use, removable CA cryptographic modules, removable media, and any activation information necessary to access or enable CA cryptographic modules or CA equipment, or paper containing sensitive plain-text information shall be placed in locked containers sufficient for housing equipment and information commensurate with the sensitivity of the application being protected. Access to the contents of the locked containers shall be restricted to individuals holding CA trusted roles as defined in Section 5.2.1, utilizing two-person access controls, and two-person integrity while the container is unlocked.

CA cryptographic modules held within the work area for intermittent use throughout the day may be kept under one lock, as long as they are stored in an area where there are at least two persons physically present at all times. Knowledge of the combination or access to the key used to secure the lock shall be restricted to authorized individuals only. When in active use, the cryptographic module shall be locked into the system or container (rack, reader, server, etc.) using a physical lock under the control of the CA Operations Staff to prevent unauthorized removal.

Any activation information used to access or enable the cryptographic modules or CA equipment shall be stored separately from the associated modules and equipment. Such information shall either be memorized or recorded and stored in a manner commensurate with the security afforded the associated cryptographic module or equipment.

A security check of the room/rack housing CA equipment shall occur prior to leaving the room/rack unattended by the CA Operations Staff. The check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g. that cryptographic modules are in place when “open”, and secured when “closed”).
- Any security containers are properly secured.
- Physical security systems (e.g., door locks, vent covers) are functioning properly.
- The area is secured against unauthorized access.

The facility shall be protected and continuously attended according to the Roche Data Center requirements.

5.1.2.2 Physical access for RA equipment

RA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. RAs shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module or physical token is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the RA equipment environment.

Any activation information used to access or enable the RA equipment shall be stored separately from the associated modules and equipment. Such information shall either be memorized or recorded and stored in a manner commensurate with the security afforded the associated cryptographic module or equipment.

5.1.2.3 Physical access for CSS equipment

Physical access control requirements for CSS equipment (if implemented), shall meet the CA physical access requirements specified in Section 5.1.2.1.

5.1.3 Power and air conditioning

The CA shall have backup power capability sufficient according to the Roche Data Center requirements.

5.1.4 Water exposures

The CA shall be protected from exposure to water according to the Roche Data Center requirements.

5.1.5 Fire prevention and protection

The CA shall be protected from fire according to the Roche Data Center requirements.

5.1.6 Media storage

Media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic) and unauthorized physical access. Media not required for daily operation or not required by policy to remain with the CA or RA that contains security audit, archive, or backup information shall be stored securely in a location separate from the CA or RA equipment.

Media containing private key material shall be handled, packaged, and stored in a manner compliant with the requirements for the sensitivity level of the information it protects or provides access. Storage protection of CA and RA private key material shall be consistent with stipulations in Section 5.1.2.

5.1.7 Waste disposal

CA and Operations Staff and RA Staff shall remove and destroy normal office waste in accordance with Roche standards. Media used to collect or transmit privacy information shall be destroyed, such that the information is unrecoverable, prior to disposal. Sensitive media and paper shall be destroyed in accordance with the applicable policy for destruction of such material. Destruction of media and documentation containing sensitive information, such as private key material, shall employ methods commensurate with those in Roche Standard for sensitive information disposal.

5.1.8 Off-site backup

A system backup shall be made when a CA system is activated. If the CA system is operational for more than a week, backups shall be made at least once per week. Backups shall be stored offsite. Only the latest backup needs to be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA system. HSMs shall be backed up at least once a year.

The data backup media shall be stored in a facility approved for storage of information of the same value of the information that will be protected by the certificates and associated private keys issued or managed using the equipment with a minimum requirement of transferring, handling, packaging, and storage of the information in a manner compliant with requirements for sensitive material identified in Section 6.2.4.1.

5.2 Procedural controls

5.2.1 Trusted roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. Trusted role operations include:

- The validation, authentication, and handling of information in Certificate Applications.
- The acceptance, rejection, or other processing of Certificate Applications, revocation requests, renewal requests, or enrollment information.
- The issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository.
- Access to safe combinations and/or keys to security containers that contain materials supporting production services.
- Access to hardware security modules (HSMs), their associated keying material, and the secret share splits of the PINs that protect access to the HSMs.
- Installation, configuration, and maintenance of the CA.
- Access to restricted portions of the certificate repository.
- The ability to grant physical and/or logical access to the CA equipment.

The CA shall maintain lists, including names, organizations, contact information, and organizational affiliation for those who act in CA Administrator, CA Operations Staff, RAs, and Security Auditor trusted roles, and shall make them available during compliance audits. The RA shall maintain lists, including names, organizations, and contact information of those who act in RA Staff, RA Administrators, and RA Security Auditor roles for that RA.

5.2.1.1 CA Administrator

The CA administrator role is responsible for:

- Installation, configuration, and maintenance of the CA and CSS (where applicable).
- Establishing and maintaining CA and CSS system accounts.
- Configuring CA, RA, and CSS audit parameters.
- Configuring CSS response profiles.
- Generating and backing up CA and CSS keys.
- Controlling and managing CA cryptographic modules.
- Performing system backups and recovery.
- Changing recording media.

- Posting Certificates and CRLs.

The CA Administrator shall not issue certificates to subscribers.

5.2.1.2 *CA Operations Staff*

The CA Operations Staff role is responsible for issuing certificates.

The CA Operations role is responsible for:

- Registering new subscribers and requesting the issuance of certificates.
- Verifying the identity of subscribers and accuracy of information included in certificates.
- Approving and executing the issuance of certificates.
- Requesting, approving and executing the revocation of certificates.
- Approving infrastructure certificates issued to support the operations of the CA.
- Approving revocation of certificates issued to CAs or to support the operations of the CA.
- Approving certificates issued to RAs.
- Authorizing RAs.
- Approving revocation of certificates issued to RAs.
- Providing Certificate revocation and suspension status information as part of a CSS (if implemented).
- Generating Certificates and CRLs.
- Configuring certificate profiles or templates.

The CA Operations Staff may act as an RA to register and vet subscribers.

5.2.1.3 *Security Auditor*

Security Auditors are responsible for internal auditing of CAs and RAs. This sensitive role shall not be combined with any other sensitive role, e.g. the Security Auditor shall not also be part of the CA Operations Staff or CA Administrator. Security Auditors shall review, maintain, and archive audit logs, and perform or oversee internal audits (independent of formal compliance audits) to ensure that CAs and RAs are operating in accordance with the associated requirements.

5.2.1.4 *RA Staff*

RA Staff are the individuals holding trusted roles that operate and manage RA components.

The RA Staff role is responsible for:

- Installation, configuration, and maintenance of the RA.
- Establishing and maintaining RA operating system and application accounts.
- Routine operation of the RA equipment such as system backup and recovery or changing recording media.
- Registering new Subscriber and requesting the issuance of certificates.
- Verifying the identity of Subscribers.
- Verifying the accuracy of information included in certificates.
- Approving and executing the issuance of certificates.
- Requesting, approving, and executing the suspension, restoration, and revocation of certificates.

5.2.2 Number of persons required per task

Where multi-party control is required, all participants shall hold a trusted role. Multi-party control shall not be achieved using personnel that serve in a Security Auditor role with the exception of audit functions. The following tasks shall require two or more persons:

- Generation, activation, and backup of CA keys.
- Performance of CA administration or maintenance tasks.
- Archiving or deleting CA audit logs. At least one of the participants shall serve in a Security Auditor role.
- Physical access to CA equipment.
- Access to any copy of the CA cryptographic module.
- Processing of third-party key recovery requests.

5.2.3 Identification and authentication for each role

Individuals holding trusted roles shall identify themselves and be authenticated by the CA and RA before being permitted to perform any actions set forth above for that role or identity. CA Operations Staff and RA Staff shall authenticate using a credential that is distinct from any credential they use to perform non-trusted role functions. This credential shall be generated and stored in a system that is protected following the applicable Roche Security Standard for data protection.

CA and RA equipment shall require, at a minimum, strong authenticated access control for remote access using multi-factor authentication.

CA and RA equipment shall require, at a minimum, authenticated access control (e.g. strong passwords according to the Roche Password Management Standard) for local multi-party access.

Individuals holding trusted roles shall be appointed to the trusted role by an appropriate approving authority. These appointments shall be annually reviewed for continued need, and renewed if appropriate. The approval shall be recorded in a secure and auditable fashion. Individuals holding trusted roles shall accept the responsibilities of the trusted role, and this acceptance shall be recorded in a secure and auditable fashion.

Identity proofing of the RA shall be performed by a member of the CA Operations Staff.

Users shall authenticate themselves to all aspects of the network (servers, operating systems, applications, databases, processes, etc.) before they can access that resource.

5.2.4 Roles requiring segregation of duties

Individuals serving as Security Auditors shall not perform or hold any other trusted role. Only an individual serving in a Security Auditor role may perform internal auditing functions, with the exception of those security audit functions (e.g. configuring, archiving, deleting) that require multi-person control.

An individual that performs any trusted role shall only have one identity when accessing CA equipment.

5.3 Personnel controls

Personnel Security plays a critical role in the CA facility's overall security system. Personnel Security shall be designed to prevent both unauthorized access to the CA facility and CA systems and compromise of sensitive CA operations by CA personnel.

5.3.1 Qualifications, experience and clearance requirements

Personnel seeking to become Trusted Persons shall present proof of the requisite background, qualifications and experience needed to perform their prospective job responsibilities competently and satisfactorily.

Individuals appointed to any trusted role shall meet the following:

- Be Roche employees or Roche contractor and bound by terms of employment or contract.
- Be appointed in writing.
- Have successfully completed an appropriate training program.
- Have demonstrated the ability to perform their duties.
- Have no other duties that would interfere or conflict with their responsibilities as defined in Section 5.2.1.
- Have not been previously relieved of trusted role duties for reasons of negligence or non-performance of duties.

5.3.2 Background check procedures

Persons fulfilling Trusted Roles shall pass a comprehensive background check according to Roche background checks done by the Roche HR local department. The background checks performed by HR local department will be aligned with local policies and regulations.

5.3.3 Training requirements

All personnel performing duties with respect to the operation of the CA, CSS or RA shall receive comprehensive training. Training shall be conducted in the following areas:

- CA/CSS/RA security principles and mechanisms.
- All PKI software versions in use on the CA/CSS/RA system.
- All PKI duties they are expected to perform.
- Disaster recovery and business continuity procedures Stipulations of this policy.

5.3.4 Retraining frequency and requirements

All individuals responsible for PKI Trusted Roles shall be made aware of changes in the CA, CSS, RA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

Documentation shall be maintained identifying all personnel who received training and the level of training completed.

5.3.5 Job rotation frequency and sequence

Not applicable

5.3.6 Sanctions for unauthorized actions

Appropriate administrative and disciplinary actions as documented in organization policy shall be taken against personnel who perform unauthorized actions (i.e. not permitted by this CP or other policies) involving the CA's systems, the certificate status verification systems, and the repository. Disciplinary actions may include measures up to and including termination and shall be commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent contractor requirements

Contractor personnel filling trusted roles shall be subject to all requirements stipulated in this document. Visitors shall be permitted access to the CA's secure facilities only to the extent they are escorted and directly supervised by people holding trusted roles at all times.

5.3.8 Documentation supplied to personnel

Documentation sufficient to define duties and procedures for each role shall be provided to the personnel filling that role.

5.4 Auditing logging procedures

Audit log files shall be generated for all events relating to the security of the CAs, CSS, and RAs. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

5.4.1 Types of events recorded

Security auditing capabilities of CA, CSS, and RA operating system and applications shall be enabled during installation and initial configuration. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event.
- The date and time the event occurred.
- Success or failure where appropriate.
- The identity of the entity and/or operator that caused the event.

Time shall be synchronized with an authoritative time source to within three minutes.

A message from any source requesting an action by the CA, CSS or RA is an auditable event; the corresponding audit record must also include message date and time, source, destination, and contents.

The CA, CSS and RA shall record the events identified in the list below. Where these events cannot be electronically logged, the CA/CSS/RA shall supplement electronic audit logs with physical logs as necessary.

SECURITY AUDIT:

- Any changes to the Audit parameters, e.g. audit frequency, type of event audited.
- Any attempt to delete or modify the Audit logs.
- Obtaining a third-party time-stamp.

IDENTIFICATION AND AUTHENTICATION:

- Successful and unsuccessful attempts to assume a role.
- The value of maximum authentication attempts is changed.
- Maximum unsuccessful authentication attempts occur during user login.
- Attempts to set passwords for local accounts.

- Attempts to modify passwords for local accounts.
- Logon attempts to CA, CSS or RA applications.
- Escalation of privilege.

LOCAL DATA ENTRY:

- All security-relevant data that is entered in the system.

REMOTE DATA ENTRY:

- All security-relevant messages that are received by the system.

DATA EXPORT AND OUTPUT:

- All successful and unsuccessful requests for confidential and security-relevant information.

KEY GENERATION:

- Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys).

PRIVATE KEY LOAD AND STORAGE:

- All access to certificate subject private keys retained within the CA for key recovery purposes.

TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE:

- All changes to the trusted public keys, including additions and deletions.

SECRET KEY STORAGE:

- The manual entry of secret keys used for authentication (e.g. PINs).

PRIVATE AND SECRET KEY EXPORT:

- The export of private and secret keys (keys used for a single session or message are excluded).

CERTIFICATE REGISTRATION:

- All certificate requests.

CERTIFICATE REVOCATION:

- All certificate revocation requests.

CERTIFICATE STATUS CHANGE APPROVAL:

- The approval or rejection of a certificate status change request.

CA/CSS/RA CONFIGURATION:

- Installation of the operating system.
- Installation of the CA, CSS or RA.

- Installing hardware cryptographic modules.
- Removing hardware cryptographic modules.
- Destruction of cryptographic modules.
- System startup.
- Any security-relevant changes to the configuration of the CA, CSS or RA.

ACCOUNT ADMINISTRATION:

- Roles and users are added or deleted.
- The access control privileges of a user account or a role are modified.
- Appointment of an individual to a trusted role.
- Designation of personnel for multi-party control.

CERTIFICATE PROFILE MANAGEMENT:

- All changes to the certificate profile.

REVOCATION PROFILE MANAGEMENT:

- All changes to the revocation profile.

CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT:

- All changes to the certificate revocation list profile.

MISCELLANEOUS:

- Receipt of hardware/software.
- Backing up CA, CSS or RA internal database.
- Restoring CA, CSS or RA internal database.
- File manipulation (e.g., creation, renaming, moving).
- Posting of any material to a repository.
- Access to CA, CSS or RA internal database.
- All certificate compromise notification requests.
- Configuration changes to the CA, CSS or RA server involving:
    - Hardware.
    - Software.
    - Operating system.
    - Patches.

PHYSICAL ACCESS / SITE SECURITY:

- Personnel access to room housing CA, CSS, or RA.
- Access to the CA, CSS, or RA server.
- Known or suspected violations of physical security.
- Any removal or addition of equipment to the CA/CSS/RA enclosure.

ANOMALIES:

- Software error conditions.

- Software check integrity failures.
- Receipt of improper messages.
- Misrouted messages.
- Network attacks (suspected or confirmed).
- Equipment failure.
- Electrical power outages.
- Uninterruptible power supply (UPS) failure.
- Obvious and significant network service or access failures.
- Violations of certificate policy.
- Violations of certification practice statement.
- Resetting operating system clock.

5.4.2 Frequency processing log

The audit log shall be reviewed at least once every 30 days and before being archived. All significant events shall be explained in an audit log summary. Actions taken as a result of these reviews shall be documented.

Such reviews involve verifying that the log has not been tampered with and performing a thorough examination of any alerts or irregularities in the logs. A statistically significant portion of the security audit data generated by the CA, CSS and RA since the last review shall be examined.

Real-time automated analysis tools should be used. All alerts generated by such systems shall be analyzed.

5.4.3 Retention period for audit log

Audit logs shall be retained on-site for at least 60 days in addition to being archived as described in section 5.5. The individual who removes audit logs from the CA system shall be an official different from the individuals who, in combination, command the CA signature key. For the CSS and RA, a CA Administrator other than the CSS operator or RA shall be responsible for managing the audit log.

5.4.4 Protection of audit log

The security audit data shall not be open for reading or modification by any human, or by any automated process, other than those that perform security audit processing.

Electronic logs shall be protected to prevent alteration and detect tampering. Examples include digitally signing audit records or the use of a data diode to transfer logs to a separate system to prevent modification after the log is written to media.

Physical logbooks shall implement controls to allow for the detection of the removal of pages or deletion of entries.

Security audit data shall be moved to a safe, secure storage location separate from the location where the data was generated.

CA/CSS/RA system configuration and procedures must be implemented together to ensure that only authorized people archive or delete security audit data. Procedures must be implemented to protect archived data from deletion or destruction before the end of the security audit data retention period (note that deletion requires modification access).

5.4.5 Audit log backup procedures

Audit logs and audit summaries shall be backed up at least every 30 days. A copy of the audit log shall be sent off-site every 30 days.

5.4.6 Audit collection system (Internal vs. External)

The audit log collection system may or may not be external to the CA/CSS/RA system. Automated audit processes shall be invoked at system or application startup, and cease only at system or application shutdown. Audit collection systems shall be configured such that security audit data is protected against loss (e.g. overwriting or overflow of automated log files). Should it become apparent that an automated audit system has failed; CA/CSS/RA operations shall be suspended until the security audit capability can be restored.

5.4.7 Notifications to event-causing subject

None

5.4.8 Vulnerability assessments

See Section 6.7.7 for requirements on regular penetration testing.

5.5 Records archival

5.5.1 Types of events archived

CA/CSS/RA archive records shall be sufficiently detailed to determine the proper operation of the CA/CSS/RA and the validity of any certificate (including those revoked or expired) issued by the CA. At a minimum, the following data shall be recorded for archive:

- Certificate policy.
- Certification practice statement.
- Contractual obligations.
- Other agreements concerning operations of the CA/CSS/RA.
- System and equipment configuration.
- Subscriber identity authentication data as per section 3.2.3.
- Documentation of receipt and acceptance of certificates (if applicable).
- Subscriber agreements.
- All CRLs issued and/or published.
- All Certificates issued.

- All Audit logs.
- Other data or applications to verify archive contents.
- Compliance Auditor reports.
- Any changes to the Audit parameters, e.g. audit frequency, type of event audited.
- Any attempt to delete or modify the Audit logs.
- All access to certificate subject private keys retained within the CA for key recovery purposes.
- All changes to the trusted public keys, including additions and deletions.
- Remedial action taken as a result of violations of physical security.
- Violations of Certificate Policy.
- Violations of Certification Practice Statement.

5.5.2 Retention period for archive

Archive records must be kept for a minimum of 3 years without any loss of data, but longer retention periods may be applicable according to Roche Coremap principles.

5.5.3 Protection of archive

No unauthorized user shall be permitted to write to, modify, or delete the archive. For the CA and CSS, the authorized individuals are Security Auditors. For the RA, authorized individuals are designated by the CA administrator and must be someone other than the RA.

For the CA/CSS/RA, archived records may be moved to another medium. The contents of the archive shall not be released. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents.

Archive media shall be stored in a safe, secure storage facility separate from the CA/CSS/RA with physical and procedural security controls equivalent to or better than those of the CA/CSS/RA. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site.

5.5.4 Archive backup procedures

Archive records shall be backed up according to the Roche backup standards and Roche COREMAP principles.

5.5.5 Requirements for time-stamping of records

CA/CSS/RA archive records shall be automatically time-stamped as they are created. The system clocks used for time-stamping shall be configure according to Roche standards.

5.5.6 Archive collection system (internal or external)

Archive data shall be collected in an expedient manner.

5.5.7 Procedures to obtain and verify archive information

Procedures, detailing how to create, verify, package, transmit, and store the CA archive information, shall be in accordance with Roche archive standards.

5.6 Compromise and disaster recovery

5.6.1 Incident and compromise handling procedures

CA organizations shall have an Incident Response Plan and a Disaster Recovery Plan.

If compromise of a CA is suspected, certificate issuance by that CA shall be stopped immediately. An independent, third-party investigation shall be performed in order to determine the nature and the degree of damage. The scope of potential damage shall be assessed in order to determine appropriate remediation procedures. If a CA private signing key is suspected of compromise, the procedures outlined in Section 5.6.3 shall be followed.

In case of a CSS key compromise, all certificates issued to the CSS shall be revoked and the revocation information shall be published immediately in the most expeditious manner. Subsequently, the CSS shall be re-issued.

The CA shall notify the trust anchor managers in the case of a Root CA or notify the superior CA in the case of a issuing CA if any of the following occur:

- Suspected or detected compromise of any CA system or subsystem.
- Physical or electronic penetration of any CA system or subsystem.
- Successful denial of service attacks on any CA system or subsystem.
- Any incident preventing a CA from issuing and publishing a CRL or OCSP response prior to the time indicated in the *nextUpdate* field in the currently published CRL or OCSP response.
- Suspected or detected compromise of a certificate status server (CSS) if
  - The CSS certificate has a lifetime of more than 72 hours; and
  - the CSS certificate cannot be revoked (e.g., an OCSP responder certificate with the *id-pkix-ocsp-nocheck* extension)

5.6.2 Computing resources, software, and/or data are corrupted

When computing resources, software, and/or data are corrupted, CAs operating under this policy shall respond as follows:

- Notify trust anchor managers or the superior CA as soon as possible.
- Ensure that the system’s integrity has been restored prior to returning to operation and determine the extent of loss of data since the last point of backup.

- Reestablish CA operations, giving priority to the ability to generate certificate status information within the CRL issuance schedule.
- If the CA signing keys are destroyed, reestablish CA operations as quickly as possible, giving priority to the generation of a new CA signing key pair.
- If the integrity of the system cannot be restored, or if the risk is deemed substantial, reestablish system integrity before returning to operation.

5.6.3 Entity (CA) private key compromise procedures

5.6.3.1 Root CA compromise procedures

In the case of the Root CA compromise, the CA shall notify the trust anchor managers and relying parties via public announcement, and any cross-certified PKIs, of the Root CA compromise so that they can revoke any cross certificates issued to the Root CA or any Subordinate CAs and notify all Subscribers and Relying Parties to remove the trusted self-signed certificate from their trust stores. Notification shall be made in an authenticated and trusted manner. Initiation of notification to the trust anchor managers and any cross-certified PKIs shall be made at the earliest feasible time and shall not exceed 24 hours beyond determination of compromise or loss unless otherwise required by law enforcement. Initiation of notification to relying parties and subscribers may be made after mediations are in place to ensure continued operation of applications and services. If the cause of the compromise can be adequately addressed, and it is determined that the PKI can be securely re-established, the CA shall then generate a new Root CA certificate, solicit requests and issue new Subordinate CA certificates, securely distribute the new Root CA certificate, and re-establish any cross certificates.

5.6.3.2 Intermediate or subordinate CA compromise procedures

In the event of an Intermediate or Subordinate CA key compromise, the CA shall notify the trust anchor managers and Superior CA. The superior CA shall revoke that CA’s certificate, and the revocation information shall be published immediately in the most expedient, authenticated, and trusted manner but within 18 hours after the notification. The Compromised CA shall also investigate and report to the trust anchor managers and Superior CA what caused the compromise or loss, and what measures have been taken to preclude recurrence. If the cause of the compromise can be adequately addressed and it is determined that the CA can be securely re-established, then, the CA shall be re-established. Upon re-establishment of the CA, new Subscriber certificates shall be requested and issued.

For Subordinate CAs, when a Subscriber certificate is revoked because of compromise, suspected compromise, or loss of the private key, a revocation notice as specified in Section 4.9, shall be published at the earliest feasible time by the supporting CA, but in no case more than 6 hours after notification.

5.6.3.3 CSS compromise procedures

In case of a CSS key compromise, the CA that issued the CSS a certificate shall revoke that certificate, and the revocation information shall be published immediately in the most expedient, authenticated, and trusted manner. The CSS shall subsequently be re-issued. If the CSS is self-signed and the CSS certificate expiration is more than 7 days away, the CA shall immediately notify the trust anchor managers, relying parties, and any cross-certified PKIs of the CSS compromise so that they can notify all Subscribers and Relying Parties to remove trust in the CSS certificate from each Relying Party application, and install the re-issued certificate.

It is recommended that the CSS have certificates with shorter lifetimes. A shorter lifetime minimizes the time that a compromised certificate is available.

5.6.3.4 RA compromise procedures

In case of an RA compromise, the CA shall disable the RA. In the case that an RA's key is compromised, the CA that issued the RA certificate shall revoke it, and the revocation information shall be published within 24 hours in the most expedient, authenticated, and trusted manner. The compromise shall be investigated by the CA in order to determine the actual or potential date and scope of the RA compromise. All certificates approved by that RA since the date of actual or potential RA compromise shall be revoked. In the event that the scope is indeterminate, then the CA compromise procedures in Section 5.6.3.2 shall be followed.

5.6.4 Business continuity capabilities after a disaster

CAs shall be required to maintain a Disaster Recovery Plan. The CA Disaster Recovery Plan shall be coordinated with any overarching Disaster Recovery Plan that the broader organization may have. The Disaster Recovery Plan shall identify what procedures are in place to mitigate risks to environmental controls, procedures for annual testing of processes to restore service, individuals on call for this type of activity, and the order of restoral of equipment and services.

In the case of a disaster in which the CA equipment is damaged and inoperative, the CA operations shall be re-established as quickly as possible, giving priority to the ability to revoke subscriber's certificates. If the CA cannot re-establish revocation capabilities prior to date and time specified in the *nextUpdate* field in the currently published CRL issued by the CA, then the inoperative status of the CA shall be reported to the trust anchor managers and Superior CA. The trust anchor managers and Superior CA shall decide whether to declare the CA private signing key as compromised and re-establish the CA keys and certificates, or allow additional time for reestablishment of the CA's revocation capability.

In the case of a disaster whereby a CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, the CA shall request that its certificates be revoked. The CA installation shall then be completely rebuilt by re-establishing the CA equipment, generating new private and public keys, being re-certified, and re-issuing all cross certificates. Finally, all Subscriber certificates will be re-issued. In such events, any Relying Parties who continue to use certificates signed with the destroyed private key do so at their own risk, and the risk of others to whom the data is forwarded, as no revocation information will be available (if the CRL signing key was destroyed).

5.7 CA or RA termination

When a CA operating under this policy terminates operations before all certificates have expired, entities shall be given as much advance notice as circumstances permit.

Prior to CA termination, notice shall be provided to all cross-certified CAs requesting revocation of all certificates issued to it. In addition:

- The CA shall issue a CRL revoking all unexpired certificates prior to termination. This CRL shall be available until all certificates issued by the CA expire.
- The CA, CSS, and RA shall archive all audit logs and other records prior to termination
- The CA, CSS, and RA shall destroy all private keys and their backups upon termination
- The CA, CSS, and RA archive records shall be transferred to an appropriate authority.
- If a Root CA is terminated, the Root CA shall use secure means to notify the subscribers to delete all trust anchors representing the terminated CA.

6. Technical Security Controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 CA key pair generation

Cryptographic keying material used by CAs to sign certificates, CRLs or status information shall be generated in cryptographic modules validated to [FIPS 140] Level 3, or some other equivalent standard. Multi-party control is required for CA key pair generation, as specified in section 6.2.2.

CA key pair generation must create a verifiable audit trail demonstrating that the security requirements for procedures were followed. The documentation of the procedure must be detailed enough to show that appropriate role separation was used. An independent third party shall validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

6.1.1.2 RA key pair generation

Cryptographic keying material used by RAs to sign request and authenticate to the CA shall be generated in hardware cryptographic modules validated to [FIPS 140] Level 2, or some other equivalent standard.

6.1.1.3 Subscriber key pair generation

Subscriber key pair generation shall be performed by either the subscriber, CA, or RA. If the CA or RA generates subscriber key pairs, the requirements for key pair delivery specified in section 6.1.2 must also be met.

Software or hardware cryptographic modules validated to [FIPS 140], or some other equivalent standard, should be used to generate all subscriber key pairs, as well as pseudo-random numbers and parameters used in key pair generation.

6.1.1.4 CSS key pair generation

Cryptographic keying material used by CSSes to sign status information shall be generated in [FIPS 140] Level 3, or equivalent, validated cryptographic modules.

6.1.2 Private key delivery to subscriber

If subscribers generate their own key pairs, then there is no need to deliver private keys, and this section does not apply.

When CAs or RAs generate keys on behalf of the subscriber, then the private key must be delivered securely to the subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements must be met:

- Anyone who generates a private signing key for a subscriber shall not retain any copy of the signing key after delivery of the private signing key to the subscriber.
- The private key(s) must be protected from activation, compromise, or modification during the delivery process.
- The subscriber shall acknowledge receipt of the private key(s).
- Delivery shall be accomplished in a way that ensures that the correct keys and activation data are provided to the correct subscribers.
    - For hardware modules, accountability for the location and state of the module must be maintained until the subscriber accepts possession of it.
    - For electronic delivery of private keys, the key material shall be encrypted using a FIPS-approved cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure channel.

The CA must maintain a record of the subscriber acknowledgment of receipt of the key.

6.1.3 Public key delivery to certificate issuer

Where key pairs are generated by the subscriber or RA, the public key and the subscriber’s identity must be delivered securely (e.g. using TLS with approved algorithms and key lengths) to the CA for certificate issuance. The delivery mechanism shall bind the subscriber’s verified identity to the public key.

6.1.4 CA public key delivery to relaying parties

The public key of a Root CA shall be provided to the subscribers acting as relying parties in a secure manner so that it is not vulnerable to modification or substitution.

6.1.5 Key sizes

This CP requires use of RSA PKCS #1, RSASSA-PSS, DSA, or ECDSA signatures; additional restrictions on key sizes and hash algorithms are detailed below. Certificates issued under this policy shall contain RSA public keys.

All certificates that expire on or before December 31st, 2030 shall contain subject public keys of at least 2048 bits for RSA/DSA, and be signed with the corresponding private key.

All certificates that expire after December 31st, 2030 shall contain subject public keys of at least 3072 bits for RSA/DSA, and be signed with the corresponding private key.

RSA signatures on CRLs that only provide status information for certificates that were generated using SHA-1 may continue to be generated using SHA-1.

Where implemented, CSSs shall sign responses using the same signature algorithm, key size, and hash algorithm used by the CA to sign CRLs.

6.1.6 Public key parameters generation and quality checking

Public key parameters shall always be generated and validated in accordance with [FIPS 186-4].

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

The use of a specific key is constrained by the key usage extension in the X.509 certificate. All certificates shall include a critical key usage extension.

Human subscriber certificates that contain signature keys shall assert the *digitalSignature* bit. Human subscriber certificates that contain RSA public keys that are to be used for key transport shall assert the *keyEncipherment* bit.

Public keys that are bound into CA certificates shall be used only for signing certificates and status information (e.g. CRLs). CA certificates whose subject public key is to be used to verify other certificates shall assert the *keyCertSign* bit. CA certificates whose subject public key is to be used to verify CRLs shall assert the *cRLSign* bit. CA certificates whose subject public key is to be used to verify Online Certificate Status Protocol (OCSP) responses shall assert the *digitalSignature* bit.

Public keys that are bound into device, applications, and service certificates may be used for digital signature (including authentication), key management, or both. Device certificates to be used for digital signatures shall assert the *digitalSignature* bit. Device certificates that contain RSA public keys that are to be used for key transport shall assert the *keyEncipherment* bit. Device certificates to be used for both digital signatures and key management shall assert the *digitalSignature* bit and either the *keyEncipherment* (for RSA).

The *dataEncipherment*, *encipherOnly*, and *decipherOnly* bits shall not be asserted in certificates issued under this policy. In addition, *anyExtendedKeyUsage* shall not be asserted in extended key usage extensions.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

CAs shall use a hardware cryptographic module validated to [FIPS 140] Level 3 (or higher), or some other equivalent standard for signing operations. RAs shall use a hardware cryptographic module validated to [FIPS 140] Level 2 (or higher), or some other equivalent standard for signing operations.

CSSes that provide status information shall use a cryptographic module validated to [FIPS 140] Level 3 (or higher), or some other equivalent standard for signing operations.

Subscribers should use a cryptographic module validated to [FIPS 140], or some other equivalent standard, for all cryptographic operations.

6.2.2 Private key (N of M) multi-person control

A single person shall not be permitted to activate or access any cryptographic module that contains the complete CA signing key. CA signing keys shall be backed up only under multi-party control. Access to CA signing keys backed up for disaster recovery shall be under multi-party control. The names of the parties used for multi-party control shall be maintained on a list that shall be made available for inspection during compliance audits.

6.2.3 Private key escrow

CA private keys shall never be escrowed.

Subscriber key management keys may be escrowed to provide key recovery as described in section 4.11. If a device has a separate key management key certificate, the key management private key may be escrowed. The private key associated with a certificate that asserts a *digitalSignature* key usage shall not be escrowed.

6.2.4 Private key backup

6.2.4.1 Backup of CA private signature key

The CA private signature keys shall be backed up under the same multiparty control as the original signature key. At least one copy of the private signature key shall be stored off-site. All copies of the CA private signature key shall be accounted for and protected in the same manner as the original. Backup procedures shall be included in the CA’s Operational documentation.

6.2.4.2 Backup of human subscriber and role private keys

Backed up human subscriber and role private keys shall not be stored in plaintext form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the subscriber’s cryptographic module and shall be under the control of the subscriber.

6.2.4.3 Backup of CSS private key

CSS private keys may be backed up. If backed up, all copies shall be accounted for and protected in the same manner as the original.

6.2.4.4 Backup of device, application private keys

Device and application private keys may be backed up or copied, but must be held under the control of the AOR. Backed up private keys shall not be stored in plaintext form outside the cryptographic module. Backup copies shall be controlled at the same security level as the original cryptographic module.

6.2.5 Private key archival

CA private signature keys and subscriber private signature keys shall not be archived. CAs that retain subscriber private encryption keys for business continuity purposes shall archive such subscriber private keys in accordance with Section 4.11.

6.2.6 Private key transfer into or from a cryptographic module

CA private keys may be exported from the cryptographic module only to perform CA key backup procedures as described in Section 6.2.4.1. At no time shall the CA private key exist in plaintext outside the cryptographic module.

All other keys shall be generated by a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport; private keys must never exist in plaintext form outside the cryptographic module boundary.

Transport keys used to encrypt private keys shall be handled in the same way as the private key.

For CA private keys, this means key transport keys must be protected under multi-person control.

6.2.7 Private key storage on cryptographic module

No stipulation beyond that specified in FIPS 140.

6.2.8 Method of activating private key

The subscriber must be authenticated to the cryptographic token before the activation of the associated private key(s). Acceptable means of authentication include but are not limited to passphrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

A device or application may be configured to activate its private key without requiring activation data, provided that appropriate physical and logical access controls are implemented for the device and its cryptographic token. The AOR shall be responsible for ensuring that the system has security controls commensurate with the level of threat in the device's environment. These controls shall protect the device's hardware, software, and the cryptographic token and its activation data from compromise.

6.2.9 Method of deactivating private key

Cryptographic modules that have been activated shall not be available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure or automatically after a period of inactivity. CA cryptographic modules shall be removed and stored in a secure container when not in use.

6.2.10 Method of destroying private key

Individuals in trusted roles shall destroy CA, RA, and CSS (e.g., OCSP server) private signature keys when they are no longer needed. Subscribers shall either surrender their cryptographic module to CA/RA personnel for destruction or destroy their private signature keys, when they are no longer needed or when the certificates to which they correspond expire or are revoked. Physical destruction of hardware is not required.

6.2.11 Cryptographic module rating

See section 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Certificate operational periods and key usage periods

The usage period for the Root CA key pair is a maximum of 20 years.

For all other CAs operating under this policy, the usage period for a CA key pair is a maximum of 20 years. All certificates signed by a specific CA key pair must expire before the end of that key pair's usage period.

Subscriber signature private keys have the same usage period as their corresponding public key. The usage period for subscriber key management private keys is not restricted.

6.4 Activation data

6.4.1 Activation data generation and installation

CA activation data may be user-selected (by each of the multiple parties holding that activation data). If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

RA and subscriber activation data may be user-selected. The strength of the activation data shall meet or exceed the requirements for authentication mechanisms stipulated for Level 2 in [FIPS 140], or some other equivalent standard. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

6.4.2 Activation data protection

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data shall be either:

- memorized
- biometric in nature; or
- recorded and secured at the level of assurance associated with the activation of the cryptographic module, and shall not be stored with the cryptographic module.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

6.5.1.1 Access control

Access to information such as sensitive details about customer accounts, passwords, and ultimately, CA-related private keys should be carefully guarded, along with the machines housing such information.

6.5.1.1.1 Access controls policy and procedures

The CA shall create and document roles and responsibilities for each trusted role employee job function in the Operational documentation. The CA shall create and maintain a mapping of these trusted roles and their associated responsibilities to specific employees and their accounts on CA and/or RA systems.

6.5.1.1.2 Account management

Information system account management features shall ensure that users access only that functionality permitted by their role or function. All account types with access to information systems shall be documented along with the conditions and procedures to follow in creating new accounts. Groups and roles shall have a documented relationship to the business or mission roles involved in operating the CA.

Section 5.2.1 of this document defines roles and job functions for personnel that the CA will use when defining access control mechanisms. The CA shall employ the principle of least privilege when creating users and assigning them to groups and roles; membership to a group or role shall be justified based upon business need. The CA shall take appropriate action when a user no longer requires an account, their business role changes, or the user is terminated or transferred. The CA shall annually review all active accounts to match active authorized users with accounts, and disable or remove any accounts no longer associated with an active authorized user.

Automated systems shall be employed to maintain access for only those users who are still authorized to use the information system. After an inactivity period defined in the IAM processes, an account shall be automatically disabled and attempts to access any deactivated account shall be logged.

All account administration activities shall be logged and made available for inspection by appropriate security personnel. Account administration activities that shall be audited include account creation, modification, enabling, disabling, group or role changes, and removal actions. See Section 5.4 for detailed requirements for these logs.

Guest/anonymous accounts for logon to information systems shall be prohibited. Accounts shall be assigned to a single user and shall not be shared.

6.5.1.1.3 Least privilege

In granting rights to accounts and groups, the CA shall employ the principle of least privilege, allowing only authorized access for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. The CA shall explicitly authorize access to accounts and groups for controlling security functions and security-relevant information. The CA shall authorize access to privileged commands and features of information systems only for specific, organization-defined compelling operational needs and documents the rationale for such access. The CA shall require that users of information systems with access to administrative privileges to utilize non-privileged accounts or roles when accessing non-privileged functions (such as reading email).

6.5.1.1.4 Access control best practices

The next best practices shall be implemented in the CA systems:

- Automatic session locks shall be implemented after periods of inactivity of maximum 15 minutes.
- Internet browsing to publicly available websites is not allowed from the CA systems.
- 2 factor authentication (2FA) shall be implemented to access the CA systems.

6.5.1.1.5 Authentication: passwords and accounts

When the authentication mechanism uses operator selectable passwords, strong passwords shall be employed, as defined in Roche Password Management Standard. Passwords for CA authentication shall be different from non-CA systems.

The CA shall have the minimum number of user accounts that are necessary to its operation. Account access shall be locked after 5 unsuccessful login attempts. Restoration of access shall be performed by a different person who holds a trusted role, or restore access after a timeout period.

6.5.1.1.6 Permitted actions without identification or authentication

The CA shall document in the Operational documentation a specific list of actions that can be performed on specifically enumerated information systems without identification or authentication, such as retrieving or verifying a published CRL from an Internet-accessible server or accessing a publicly available website. Furthermore, the organization shall document and provide supporting rationale in its security policy and procedures an enumerated list of user actions and systems not requiring identification or authentication (i.e., anonymous access).

6.5.1.2 System integrity

6.5.1.2.1 System isolation and partitioning

CA systems shall be configured, operated, and maintained so as to ensure the continuous logical separation of processes and their assigned resources. This separation shall be enforced by:

- Physical and/or logical isolation mechanisms, such as dedicated systems or virtualization.
- Protecting an active process and any assigned resources from access by or interference from another process.
- Protecting an inactive process and any assigned resources from access by or interference from an active process.
- Ensuring that any exception condition raised by one process will have no lasting detrimental effect on the operation or assigned resources of another process.

All trusted components should be logically separated from each other, and shall be logically separated from any untrusted components of the CA system. The Roche Solution Architecture documentation shall document how this logical isolation of components is accomplished.

Security critical processes shall be isolated from processes that have external interfaces. For example, the CA signing processes shall be isolated from registration processes. The Operational documents shall outline how security critical processes are protected from interference by externally facing processes.

If there are system resources shared amongst trusted and/or untrusted processes, the underlying system(s) shall prevent any unauthorized and unintended information transfer between processes via those shared system resources.

The CA shall develop and document controlled procedures for transferring software updates, configuration files, certificate requests, and other data files between trusted components.

6.5.1.2.2 Malicious code protection

The CA system shall employ malicious code protection mechanisms to mitigate the risk of malicious code on CA system components. Malicious code on trusted CA components could allow an attacker to issue fraudulent certificates, create a rogue intermediate or signing CA server, or compromise the availability of the system.

CA system components running standard operating systems that are not air-gapped from the Internet shall employ host-based anti-malware tools to detect and prevent the execution of known malicious code. These tools shall be configured to automatically scan removable media when it is inserted, as well as files received over the network. Introduction of removable media shall not cause automatic execution of any software residing on the media.

Anti-malware tools employed by a CA shall be properly maintained and updated by the CA. Anti-malware tools on networked systems shall be updated automatically as updates become available, or CA Administrators shall push updates to system components on a weekly basis. Anti-malware tools may be employed on air-gapped systems. If anti-malware tools are employed on air-gapped systems, the CA shall document in the Operational documents how these tools will be updated, including mitigations intended to reduce the risks of spreading malware and exfiltration of data off of compromised CA systems. Anti-malware tools shall alert CA Administrators of any malware detected by the tools.

On system components that do not implement host-based anti-malware tools, the CA shall identify and employ other malicious code protection mechanisms to prevent the execution of malicious code, detect infected files or executables, and remediate infected systems. These mechanisms could include, but are not limited to, compensating physical protection on hosts, network-based malware detection tools at boundary points, application whitelisting, and manually scanning removable media by trusted CA personnel. The CA shall document all malware protection mechanisms in the Operational documents.

6.5.1.2.3 Software and firmware integrity

The CA shall employ technical and procedural controls to prevent and detect unauthorized changes to firmware and software on CA systems. Access control mechanisms and configuration management processes (see Section 6.5.1.1 and 6.6.2) shall ensure that only authorized CA Administrators are capable of installing or modifying firmware and software on CA systems.

Root and subordinate CA servers shall implement automated technical controls to prevent and detect unauthorized changes to firmware and software. Example technical controls include signature verification prior to firmware/software installation or execution (such as firmware protections that comply with [SP800-147] or [SP800-147B]), or hash-based white-listing of executables. Unauthorized software or firmware detected by these mechanisms should be blocked from executing. Any instances of unauthorized firmware or software detected by the system shall be logged, and CA Administrators shall be notified of these events.

6.5.1.2.4 Information protection

The CA shall protect the confidentiality and integrity of sensitive information stored or processed on CA systems that could lead to abuse or fraud. For example, the CA shall protect customer data that could allow an attacker to impersonate a customer. The CA shall employ technical mechanisms to prevent unauthorized changes or accesses to this information, such as access control mechanisms that limit which users are authorized to view or modify files. Sensitive information stored on devices that are not physically protected from potential attackers shall be stored in an encrypted format.

6.6 Life cycle of technical controls

6.6.1 System development controls

The system development controls address various aspects related to the development and change of the CA system through aspects of its life-cycle.

The CA system shall be implemented and tested in a non-production environment prior to implementation in a production environment. No change shall be made to the production environment unless the change has gone through the change control process as defined for the system baseline.

In order to prevent incorrect or improper changes to the CA system, the CA system shall require multi- party control for access to the CA system when changes are made.

For any software developed by the CA, evidence shall be produced relating to the use of a defined software development methodology setting out the various phases of development, as well as implementation techniques intended to avoid common errors to reduce the number of vulnerabilities. Automated software assurance (i.e. static code analysis) tools shall be used to catch common error conditions within developed code. For compiled code, all compiler warnings shall be enabled and addressed or acknowledged to be acceptable. Input validation shall be performed for all inputs into the system.

Hardware and software procured to operate the CA shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g. by ensuring the vendor cannot identify the PKI component that will be installed on a particular device). The hardware and software shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use. Hardware and software updates shall be purchased or developed in the same manner as original equipment, and shall be installed by trusted and trained personnel in a defined manner.

All data input to CA system components from users or other system components shall be validated prior to consumption by the receiving entity. Validating the syntax and semantics of system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match the expected definitions for format and content.

6.6.2 Security management controls

A list of acceptable products and their versions for each individual CA system component shall be maintained and kept up-to-date within a configuration management system. Mechanisms and/or procedures shall be in operation designed to prevent the installation and execution of unauthorized software. A signed whitelist of the acceptable software for the system should be one of the ways to control the allowed software. A CA system shall have automated mechanisms to inventory on at least a daily basis software installed on a system and alert operators if invalid software is found.

To reduce the available attack surface of a CA system, only those ports, protocols, and services that are necessary to the CA system architecture are permitted to be installed or operating. The CA system shall maintain a list of ports, protocols, and services that are necessary for the correct function of each component within the CA system. There shall be automated mechanisms to monitor the running processes and open ports against the permitted list.

To validate the integrity of the CA system, automated tools that validate all static files on a component shall be in operation to notify operators when a protected file has changed.

The CA system shall establish and document mandatory configuration settings for all information technology components which comprise the CA system. All configuration settings capable of automated assessment shall be validated to be set according to the guidance contained within a documented security configuration checklist on at least daily basis for powered on systems or next power-on for systems which are not left powered-on.

6.6.3 Life cycle security controls

For flaw remediation, the CA shall scan all online CA systems for vulnerabilities using at least one vulnerability scanner every two weeks. The use of multiple scanners on the most sensitive systems is strongly encouraged.

Each vulnerability found shall be entered into a vulnerability tracking database, along with the date and time of location, and shall be remediated within one week. Remediation shall be entered into the vulnerability database as well (including date and time).

The CA shall monitor relevant notification channels on a daily basis for updates to packages installed on CA systems (including networking hardware). CAs shall have a plan for receiving notification of software and firmware updates, for obtaining and testing those updates, for deciding when to install them, and finally for installing them without undue disruption. For critical vulnerabilities, the CA shall evaluate and install the update within 72 hours. For less critical vulnerabilities, the CA shall evaluate each package to determine whether an update is required, and if so, that update shall be applied to all affected CA systems within one week. A log shall be kept of the notifications, the decision to apply/not apply including reason, and the application of relevant updates/patches.

From time to time, the CA may discover errors in configuration files, either because of human error, source data error, or changes in the environment which have made an entry erroneous. The CA shall correct such errors within 72 hours of discovery, and shall document the reason for the error, and the associated correction.

Remediation activities should not cause unavailability of revocation information.

6.7 Network security controls

Many components of a CA are connected to each other and their customers via various forms of networks. While it is necessary for connections to customers and administrative systems, care needs to be taken to ensure those connections do not adversely impact the security of those components. Guidelines for effective CA networking security are discussed in the following sections.

6.7.1 Isolation of networked systems

Communication channels between the network-connected CA components and the trusted CA processing components shall be protected against attack. Furthermore, information flowing into these CA components from the network-connected CA components shall not lead to any compromise or disruption of these components.

The components of a CA requiring direct network connections shall be minimized. Those networked components shall be protected from attacks through the use of firewalls to filter unwanted protocols (utilizing access rules, whitelists, blacklists, protocol checkers, etc., as necessary). Data loss prevention tools shall be employed to detect inappropriate leakage of sensitive information.

6.7.2 Boundary protection

The following sections will describe boundary protections in the context of four zone types. The zones are not assumed to be nested. They may be interconnected, but are independent. Zone boundaries are defined by limits of authority over the security of the data processed within the boundary. Interconnection of two zones, even at the same protection level, must be done in a way that respects the different authorities of the two zones.

The zones are:

- Special Access Zone (SAZ) - highly controlled network area for processing and storage of especially high value data. It should be assumed that a network in this zone is not interconnected to any other network.
- Restricted Zone (RZ) - controlled network area for sensitive data processing and storage.
- Operations Zone (OZ) - network area containing systems for routine business operations.

- Public Zone (PZ) - any network area that is not behind a protective boundary controlled by the organization. Includes the public Internet and the public telephone network. Since there is no presumed control over the Public Zone, there are no requirements for boundary protection.

6.7.2.1 PKI network zones overview

- A Root CA is expected to reside in a Special Access Zone with no network connection to any other network at all.
- Subordinate CAs are expected to reside in one or more Restricted Zones, with connections allowed from the Public Zone for RA Agent access and from the Operations Zone for business function access.
- The RA Server is expected to reside in a Restricted Zone distinct from the Restricted Zone occupied by the CA Signing Servers.
- The RA Agent may reside in a Restricted, Operations, or Public Zone. While the RA Agent may use special hardware and software to accomplish their tasks, the organization will have no control over the RA Agent’s workstation’s network connection if it operates in the Public Zone. The data must be self- protecting or session protected as it leaves the RA Agent’s workstation.

6.7.2.2 Special access zone boundary

A SAZ has no physical nor logical interconnection to any other network.

- Physical boundary protection measures shall include checks for network elements (cables, routers, wireless equipment) that indicate interconnection.
- Physical boundary protection devices shall fail securely in the event of an operational failure. Incoming communication is limited to certificate signing requests, revocation requests, and system maintenance data.
- Outgoing communication is limited to signed certificates, CRLs, and any data related to monitoring and audit.
- Communication shall be accomplished by means of write-once media or media that is sanitized on first use and between uses. Media shall be scanned after writing. The sanitization and scanning shall take place on a device isolated and designated solely for this purpose.
- Auditing functions shall be enabled on systems in the SAZ, according to the requirements in Section 5.4.
- Systems shall be physically isolated to separate platform instances and uniquely identified on each subnet within SAZ boundary with managed interfaces.

6.7.2.3 Restricted zone boundary

An RZ has physical interconnections to other RZs, OZs, and potentially the PZ.

- Physical interconnections must be documented as to where they exist, for what purpose, and what protections are provided.
- All physical systems shall identify and limit all systems to managed interfaces.
- All interconnections must be filtered based on origin, destination, and type.
- Physical boundary protection measures shall include checks for network elements (cables, routers, wireless equipment) that indicate unauthorized interconnection.
- Physical boundary protection devices shall fail securely in the event of an operational failure.
- Connections with other RZs may be firewalled interconnections that maintain the security posture of each RZ.
- Connections with OZs must be limited to specific protocols, and connections digitally authenticated. If there is a Wireless Access Point in the OZ, a VPN Gateway shall be used to connect to the Restricted Zone.
- Confidentiality shall be provided depending on the sensitivity of the information transferred and the route of the connection.
- Connection with the PZ must be made through a jump station that is hardened for exposure to a hostile network environment. Such jump stations must be minimized in number and documented as to location, purpose, and system and service configuration.
- Firewalls shall allow only those protocols necessary to perform a function and only from recognized network origins by denying network traffic by default and allowing network traffic only by exception (i.e. deny all, permit by exception).
- All communications shall be source authenticated and should be encrypted.
- Incoming communications shall be limited to certificate signing requests, CRL requests, key recovery requests, key escrow messages, revocation requests, responses from support systems (e.g. from a directory), and system maintenance data.
- Outgoing communications shall be limited to signed certificates, CRLs, key recovery data, revocation request responses, requests for subscriber authentication and authorization data, and any data related to monitoring and audit.
- Monitoring and auditing functions shall be enabled on the systems in the RZ, including network components where appropriate, according to the requirements in Sections 5.4 and 6.7.5.
- Indications that boundary protections have failed must be dealt with urgently (see Section 5.6).
- Wireless access points (WAP) shall NOT be allowed in the Restricted Zone at any time.

6.7.2.4 Operation zone boundary

An OZ has physical interconnections to other OZs, RZs, and the PZ.

- Physical interconnections must be documented as to where they exist, for what purpose, and what protections are provided.

- All interconnections must be filtered based on origin, destination, and type.
- Physical boundary protection measures shall include checks for network elements (cables, routers, wireless equipment) that indicate unauthorized interconnection.
- Physical boundary protection devices shall fail securely in the event of an operational failure.
- Connections with RZs shall be driven by the RZ boundary protection requirements.
- Connections with other OZs may be firewalled router interconnections that maintain the security posture of each OZ.
- Connections with the PZ must be limited to specific protocols, and connections digitally authenticated.
- Confidentiality of any interconnection shall be provided depending on the sensitivity of the information transferred and the route of the connection.
- Firewalls shall allow only those protocols necessary to perform a function and only from recognized network origins by denying network traffic by default and allowing network traffic by exception (i.e., deny all, permit by exception).
- All communications shall be source authenticated and should be encrypted.
- Incoming and outgoing communications shall be limited to data related to the business of the organization, system maintenance data, and any data related to monitoring and audit.
- Monitoring and auditing functions shall be enabled on the systems in the OZ, including network components where appropriate, according to the requirements in Sections 5.4 and 6.7.5.
- Indications that boundary protections have failed must be dealt with promptly (see Section 5.6).
- Wireless Access Points (WAP) should NOT be allowed in the OZ unless the radio frequency can be physically contained with high assurance to systems isolated in the OZ of the building structure.

6.7.3 Availability

CA systems shall be configured, operated, and maintained to maximize uptime and availability. Scheduled downtime shall be announced to Subscribers.

Services supporting revocation requests shall be configured and deployed in such a manner and capacity that overall availability shall be maintained at a minimum of 99.9%, with no single outage lasting longer than 10 minutes. Additionally, such services shall be homed in a minimum of two geographically independent locations with no single-points of failure (SPOFs – e.g., same backbone provider), which could affect availability.

6.7.3.1 Denial of service protection

CAs shall state acceptable methods to request revocation in their Operational documents. At least one of those methods shall be out of band (i.e. network connectivity is not required).

CAs shall take reasonable measures to protect certificate request and issuing services from known DoS attacks. The CA request and issuing availability required by a Subscriber application shall be stated in its Operational documents.

6.7.3.2 Public Access Protection

Personal Identity Information used in the identity proofing process shall be protected at all times in accordance with local law and shall not be available to public access.
Revocation information and CA certificate information shall be made available in accordance with Section 2 of this CP. However, individual subscriber certificates need not be made available for public access.
CAs shall employ firewalls or air-gap procedures to protect privacy-sensitive information from public access.

6.7.4 Communication security

This section covers three forms of CA communication: Intra-CA communications, CA to RA communications, and RA to Subscriber communications. While communications security is necessary across all three forms of communication, the threats, vulnerabilities, and technological capabilities change depending on the environment.

6.7.4.1 Transmission integrity

Source authentication and integrity mechanisms shall be employed to all certificate request, manufacture, and issuance communications, including all related services irrespective of whether those services are hosted on the same or different platform than the CA workstation. Communications between CAs and RAs shall be mutually authenticated to detect changes to information during transmission.

Source authentication for RA to Subscriber communications may employ either online (cryptographic) or offline methods. Offline RA to Subscriber communications shall be protected by traditional means that are legally sufficient (e.g., ink signatures on paper). Initial Subscriber data that has been collected in an unauthenticated or mutable manner shall be verified by the RA before the certificate request is created.

6.7.4.2 Transmission confidentiality

Intra-CA communications that cross the physical protection barrier of the certificate-signing portion of the CA system shall be confidentiality-protected. Services used by the CA system that are not administered by the CA administrative staff shall provide protection commensurate with the CP.

Confidentiality of Subscriber data shall be maintained. CA to RA communications shall employ encryption to prevent unauthorized disclosure of information during transmission.

The level of protection for RA to Subscriber communications shall be determined by the Subscriber (or the Subscriber's organization); in any case, the RA shall be prepared to employ typical techniques for Internet confidentiality (e.g. single-side authenticated TLS).

6.7.4.3 Network disconnects

Network connection lifetimes between co-located services are driven by the traffic between them. Connections should be terminated after a period of inactivity that is defined in the CA's Operational documents.

Network connections between CAs, RAs, and Subscribers shall be terminated at the end of the session or after a period of inactivity. The length of the period of inactivity is defined in the CA's Operational documents. Keep-alive and quick-reconnect mechanisms should not be employed, so that message replay and session hijacking are avoided.

6.7.4.4 Cryptographic key establishment and management

Cryptographic key management for network connections between CAs, RAs and Subscribers includes all aspects of cryptographic key life cycle: key generation, distribution, storage, access and destruction for both symmetric and asymmetric keys.

Key generation and management shall be performed in cryptographic modules that are validated to [FIPS- 140] Level 1 or higher. Keys that are backed up for business continuity shall have protection comparable to the operational key. All cryptographic key management processes shall be described in the CA's Operational documents.

RAs shall employ key protection mechanisms implemented in a hardware cryptographic module validated to [FIPS 140], or some other equivalent standard (e.g., smart token).

Keys that protect the integrity and confidentiality of an enrollment session shall be generated and managed using cryptographic mechanisms implemented in a cryptographic module validated to [FIPS 140], or some other equivalent standard.

6.7.4.5 Cryptographic key protection

Cryptographic mechanisms implemented in a cryptographic module validated to [FIPS 140], or some other equivalent standard, shall be employed to detect changes to information during transmission of Intra-CA communications.

Communications between the CA and RA systems shall use cryptographic mechanisms that are implemented in a cryptographic module validated to [FIPS 140], or some other equivalent standard.

Cryptographic processes for RA to Subscriber communications shall be implemented in a cryptographic module validated to [FIPS 140], or some other equivalent standard.

6.7.4.6 Application session authenticity

For stateless connections between CAs, RAs and Subscribers, a unique, random session identifier for each session shall be generated. The session identifiers shall be validated for each request. Session identifiers shall be invalidated at logout to preserve session authenticity. A logout capability shall be provided with an explicit logout message that indicates the reliable termination of authenticated communications sessions. Session identifiers shall be invalidated after 30 minutes of inactivity.

6.7.5 Networking monitoring

The CA shall be monitored to detect attacks and indicators of potential attacks. This includes intrusion detection tools.

6.7.5.1 Events and transactions to be monitored

The CA shall identify a list of essential information, transaction types and thresholds that indicate potential attacks. These events should include:

- Bandwidth thresholds
- Inbound and outbound communication events and thresholds
- Unauthorized network services
- CPU usage thresholds
- Certificate request thresholds from a single RA
- Access Control thresholds

6.7.5.2 Monitoring devices

A CA shall deploy intrusion detection tools and other monitoring devices with the CA to collect intrusion information and at ad hoc locations within the system to track specific types of transactions of interest to the organization, according to the Roche monitoring standards. These monitoring devices shall be configurable to react to specific indications of increased risk or to comply with law enforcement requests. The devices shall alert security personnel when suspected unauthorized activity is occurring. These devices shall be network-based and should be also host-based. Only persons holding trusted roles shall manage the operating state of monitoring devices. The CA, or the Monitoring and Incident Response team at Roche, should utilize automated tools to support near real-time analysis of events and these tools should be integrated into access control and flow control mechanisms for rapid response to attacks.

6.7.5.3 Monitoring of security alerts, advisories and directives

A CA shall monitor information system security alerts, advisories, and directives on an ongoing basis. The CA shall generate and disseminate internal security alerts, advisories, and directives as deemed necessary. The CA should employ automated mechanisms to make security alert and advisory information available throughout the organization as needed. The CA shall implement security directives in accordance with established time frames, or notifies the compliance auditor of the degree of noncompliance.

6.7.6 Remote Access/External Information systems

6.7.6.1 Remote Access

Remote Access to the CA is permitted for the PKI Operational team using the standard Roche Remote Access solution.

6.7.6.2 Jump Station

All access to CA signing systems and RA servers shall be mediated by a jump station (i.e. a machine that presents a limited interface for interaction with the other elements of the CA). No direct access is permitted. The jump station shall be patched regularly, maintained, and shall only run applications required to perform its duties.

6.7.6.3 Documentation

The CA shall document allowed methods of remote access to CA systems, including usage restrictions and implementation guidance for each allowed remote access method.

6.7.6.4 Logging

Logging shall be performed on the jump station for each remote access session with the CA, consistent with Section 5.4. In particular, logs shall include date and time of the connection, the authenticated identity of the requestor, the IP address of the remote system and should also include the commands sent to the jump station. Logs shall be maintained on a corporate audit server (e.g. Splunk).

6.7.6.5 Automated monitoring

Automated monitoring shall be performed on all remote sessions with the jump station, and on all interactions between the jump station and other CA systems. Upon detection of unauthorized access, the CA shall terminate the connection and log the event.

6.7.6.6 Security of remote management system

Machines used for remote access to the CA system shall be either corporately managed (including patching) or shall be a machine dedicated to that purpose. In particular, it shall not be used as a personal machine for the remote user. The machine shall be maintained at the same level as the machines that it accesses (i.e. all policies on patching, virus scanning, etc. that are levied on the target systems shall apply to this machine as well). The CA should make use of Network Access Control technology to check the security posture of the remote machine prior to connecting it to the network. Remote Management of the CA system shall be the only use of Remote Access.

6.7.6.7 Authentication

Any machine used to access CA systems remotely shall require two or more factors of authentication. In particular, a 2FA according to the Roche Password Management Standard is required. Authentication shall occur between the remote machine and the jump station.

6.7.6.8 Communications security for remote access

All communications between the remote access host and the CA system shall be protected by [FIPS 140], or some other equivalent standard, validated cryptography, as required for CA to RA communications in Section 6.7.4.5. Session identifiers shall be invalidated at logout to preserve session authenticity, as described in section 6.7.4.6, Session Authentication.

6.7.7 Penetration testing

Penetration testing exercises both physical and logical security controls. Regularly performing this testing will allow a CA to mitigate and avoid vulnerabilities in their systems.

The CA System shall biannually, or whenever major system changes occur, conduct external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems. Penetration testing shall occur from outside the network perimeter (i.e. the Internet or wireless frequencies around an organization) as well as from within its boundaries (i.e. on the internal network) to simulate both outsider and insider attacks.

A standard method for penetration testing consists of:

- Pretest analysis based on full knowledge of the target system.
- Pretest identification of potential vulnerabilities based on pretest analysis.
- Testing designed to determine exploitability of identified vulnerabilities.

Detailed rules of engagement shall be agreed upon by all parties before the commencement of any penetration testing scenario. These rules of engagement are correlated with the tools, techniques, and procedures that are anticipated to be employed by threat-sources in carrying out attacks. An organizational assessment of risk guides the decision on the level of independence required for penetration agents or penetration teams conducting penetration testing. Vulnerabilities uncovered during penetration testing shall be incorporated into the vulnerability remediation process.

6.8 Time-stamping

Asserted times shall be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events (see Section 5.4.1).

7. Certificate, CRL and OSCP profiles

7.1 Certificate profile

Certificates issued by a CA under this policy shall conform to the following documents:

G3 PKI Standard Computer Certificate Templates - PL ID 20318988
G3 PKI CMAR Certificate Templates - PL ID 20318987
G3 PKI CMS Enrolled Certificate Templates - PL ID 19685264
G3 PKI NDES Certificate Templates - PL ID 18865535
G3 PKI Standard User Certificate Templates - PL ID 20317831

Each certificate issued by a CA shall be given a serial number consisting of a unique, positive integer, not longer than 20 octets. Serial numbers must have at least 20 random bits added to ensure adequate entropy. Each certificate issued by a CA shall be given a serial number consisting of a unique, positive integer, not longer than 20 octets.

7.1.1 Version number(s)

The CA shall issue X.509 v3 certificates (populate version field with integer “2”).

7.1.2 Certificate extensions

The key usage extension (keyUsage) shall be marked as critical. Certificates shall assert the minimum number of key usages required for functionality. Signature certificates shall assert *digitalSignature*. Encryption certificates shall assert either *keyEncipherment* or *keyAgreement*. CA certificates shall assert *keyCertSign* and *cRLSign*.

Certificates shall assert the minimum number of extended key usages (extKeyUsage) required for functionality. The *anyExtendedKeyUsage* key purpose shall not be asserted.

The basic constraints extension (basicConstraints) shall be marked critical in CA certficates, and the path length constraint should be set to 2.

7.1.3 Algorithm object identifiers

Certificates issued under this CP shall use the following OIDs for signatures:

sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}

7.1.4 Name forms

The subject field in certificates issued under this policy shall be populated with an X.500 distinguished name as specified in section 3.1.1.

The issuer field of certificates issued under this policy shall be populated with a non-empty X.500 Distinguished Name as specified in section 3.1.1.

7.1.5 Name constraints

The CAs should assert name constraints in CA certificates.

7.1.6 Certificate policy object identifier

Certificates issued under this CP shall assert the following OID(s):

2.16.840.1.113995.2.1.1

By including this policy identifier in a certificate, the CA states conformance to the policy.

7.1.7 Usage of policy constraints

The CAs may assert policy constraints in CA certificates.

Issued certificates will not support legally binding digital signatures/non-repudiation.

Issued certificates have no legal binding to the subscriber/subjects and imply no liability.

7.1.8 Policy qualifiers syntax and semantics

Not applicable.

7.1.9 Processing semantics for the critical certificate policies extension

Certificates issued under this policy shall not contain a critical certificate policies extension.

7.2 CRL profile

CRLs issued by a CA under this policy shall conform to the CRL profile specified in the document PKI G3 CRL Publishing.

7.2.1 Version number(s)

The CAs shall issue X.509 Version two (2) CRLs.

7.2.2 CRL and CRL entry extensions

Detailed CRL profiles addressing the use of each extension are specified in the document PKI G3 CRL Publishing.

7.3 OCSP profile

OCSP Responses issued by a CA under this policy shall conform to the OCSP profile specified in the PKI OCSP installation TOP document of the references section.

Certificate status servers (CSSs) operated under this policy shall sign responses using algorithms designated for CRL signing.

7.3.1 Version number(s)

CSSs operated under this policy shall use OCSP version 1.

7.3.2 OCSP extensions

Detailed CRL profiles addressing the use of each extension are specified in the PKI OCSP installation TOP document of the references section.

8. Compliance audit and other assessments

CAs shall have a compliance audit mechanism in place to ensure that the requirements of this Certificate Policy are being implemented and enforced.

8.1 Frequency or circumstances of assessment

CAs and RAs shall be subject to a periodic compliance audit at least once every two years.

8.2 Qualifications of assessor

The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the CA’s Operational documents and this CP. The compliance auditor must perform such compliance audits as a regular ongoing business activity. In addition to the previous requirements, the auditor must be a certified information system auditor (CISA) or IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

8.3 Assessor’s relationship to assessed entity

The compliance auditor either shall be a private firm that is independent from the entities (CA and RAs) being audited, or it shall be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation. To insure independence and objectivity, the compliance auditor must not have served the entity in developing or maintaining the entity’s CA Facility or certificate practices statement. The Policy Authority shall determine whether a compliance auditor meets this requirement.

8.4 Topics covered by assessment

The purpose of a compliance audit is to verify that a CA and its recognized RAs comply with all the requirements of the current versions of the CA’s Operational documents. All aspects of the CA/RA operation shall be subject to compliance audit inspections.

8.5 Actions taken as a result of deficiency

When the compliance auditor finds a discrepancy between the requirements of this CP or the stipulations in the Operational documents and the design, operation, or maintenance of the PKI, the following actions shall be performed:

- The compliance auditor shall note the discrepancy
- The compliance auditor shall notify the parties identified in section 8.6 of the discrepancy
- The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to the appropriate PKI Authorities, as defined in Section 1.5.1.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the Policy Authority may decide to temporarily halt operation of the CA or RA, to revoke a certificate issued to the CA or RA, or take other actions it deems appropriate. The Policy Authority shall provide to the CA its procedures for making and implementing such determinations.

8.6 Communication of the results

An Audit Compliance Report shall be provided to the entity responsible for CA operations. The Audit Compliance Report and identification of corrective measures shall be provided to the appropriate PKI Authorities within 30 days of completion. A special compliance audit may be required to confirm the implementation and effectiveness of the remedy.

9. References

9.1 Roche Documents

PL ID 1327020	Roche Global Information Security Policy
PL ID 4779514	Roche Global Information Security Directive
PL ID 6305535	Roche Password Management Standard
PL ID 20318988	G3 PKI Standard Computer Certificate Templates
PL ID 20318987	G3 PKI CMAR Certificate Templates
PL ID 19685264	G3 PKI CMS Enrolled Certificate Templates
PL ID 18865535	G3 PKI NDES Certificate Templates
PL ID 20317831	G3 PKI Standard User Certificate Templates
PL ID 18878681	PKI G3 CRL Publishing
PL ID 18878681	FI G3 PKI RLS Publishing TOP
PL ID 17084248	Solution Architecture
PL ID 22877879	PKI OCSP installation TOP

9.2 External References

[1] ETSI TS 102 042 V2.1.1 (2009-05)
Policy requirements for certification authorities issuing public key certificates

[2] RFC3647
S. Chokhani, etc al., Certificate Policy and Certification Practices Framework, November 2003

[3] ETSI EN 319 411-2 v2.1.1 (2016-02)
Policy and security requirements for Trust Service Providers issuing certificates.

[4] NISTIR 7924 – Reference Certificate Policy

[5] NIST SP 800-147B
BIOS Protection Guidelines for Servers

[6] NIST SP 800-147
BIOS Protection Guidelines

Electronic Signature Page

Roche Certificate Policy

This document has been signed by:

Meaning: Sign for Review
Function: Author
User Name: Muinos, Julio (muinosj)
Date: 09-Jun-2020 18:10 Basel Server Time

Meaning: Sign for Review
Function: Enterprise Security Architecture
User Name: Koster, Carl (kosterc)
Date: 09-Jun-2020 21:58 Basel Server Time

Meaning: Sign for Review
Function: Head of Secure Access Operations
User Name: Heimburger, Cedric (heimburc)
Date: 10-Jun-2020 09:46 Basel Server Time

Meaning: Sign for Review
Function: Head of monitoring and Incident Response
User Name: Ehrhart, Tim (ehrhartt)
Date: 10-Jun-2020 12:52 Basel Server Time

Meaning: Sign for Review
Function: Head of Information Security and Privacy Governance
User Name: West, Dan (westd1)
Date: 10-Jun-2020 14:21 Basel Server Time

Meaning: Sign for Review
Function: Head of Secure Access Engineering
User Name: De La Torre, Enrique (delatore)
Date: 11-Jun-2020 11:43 Basel Server Time

Meaning: Sign for Approval
Function: Vice President, Global Head, Group Information Security/Privacy, Quality, Process & Risk Management
User Name: Imber, Vicky (imberv)
Date: 16-Jun-2020 16:25 Basel Server Time

The unique PL id (left) identifies this document within Project Library. The individually numbered signature page(s) created by Project Library and the signed document are combined and rendered into this PDF.