Certificate Policy

BASF PKI Root CA

Document Sign-Off

PETERSEH Digital unterschrieben von PETERSEH Datum: 2020.07.17 17:04:50 +02'00'

Key Management
Process Owner

BernatS1 Digital unterschrieben von BernatS1 Datum: 2020.07.20 09:02:19 +02'00'

Certificate Management
Product Manager

KIEFERA Digitally signed by KIEFERA Date: 2020.07.20 16:39:43 +02'00'

Certificate Management
Product Owner

Contents

1 Introduction

1.1 Overview

This document summarizes the requirements for the multiple BASF certification authorities (CA) when issuing, managing, revoking, and renewing or re-keying certificates for users and machines based on the X.509 version 3 certificate format. The structure of this Certificate Policy (CP) adheres to the framework outlined in RFC 3647.

The BASF Public Key Infrastructure (PKI) is operated for the private BASF business environment only. There is no connection to other PKI infrastructures. It consists of a Root CA, and subordinate CAs for specific use cases such as user encryption or machine authentication. Business partners and contractors can be enrolled in the BASF PKI too, if a valid business need and contractual relationship exist.

1.1.1 Types of Certificates

Within this CP and all corresponding documents within this PKI, different types of certificate holders are covered. Other types are not part of this CP, but can be part of the underlying PKI and must be defined by the introducing CA. In the following, the different types of certificate holders are described.

[TYPE_CA] - A certification authority issues other CAs or end entity certificates, as well as validation information of certificates managed by the respective CA (e.g. CRLs, OCSP responses)

[TYPE_PKI_SERVICE] - A PKI service provides required functionality to the PKI itself or a CA system. E.g. OCSP Responder, Registration Authority

[TYPE_USER] - A user is an individual, who interacts with other individuals and technical solutions in the context of business purposes. The individual can be an internal employee, a contractor or a business partner.

[TYPE_DEVICE] - A device is a physical or virtual instance with an operating system to provide basic operation functionality. Devices can interact with individuals or other devices and have an own identifier in the technical environment where they are working.

[TYPE_SERVICE] - A service can be a software component of a technical user account, which is used by software components in order to execute operations autonomously without interaction of individuals.

Where required in the document, the types will be referenced to define specific requirements, which are not applicable to all types.

1.1.2 Conventions

If chapters in this CP contain “No stipulation”, this CP does not specify requirements. If nevertheless, there exist requirements in Sub CAs within this PKI, the CPS of the affective CA **MUST** include a description of the requirements and implementation controls.

This CP uses different terms to outline the obligation of requirements. The terms are written in capital letters:

“MUST” / “MUST NOT”	Obligatory requirement which has to be fulfilled.
“SHOULD” / “SHOULD NOT”	Requirement, exception can be implemented with justification and approval.
“CAN” / “NEED NOT”	Optional.

1.2 Document name and identification

Name: Certificate Policy of the BASF Root CA.

Version: 3.0

Date: 01.07.2020

OID: 1.3.6.1.4.1.21220.3.2.1.3

1.3 PKI Participants

1.3.1 Certification Authorities

The BASF PKI has a three-layer certification structure with a self-signed root certificate. The Root CA certifies only Policy CAs and Issuing CAs. The Policy CAs are allowed to certify Issuing CAs, while Issuing CAs are allowed to issue leaf certificates to certificate subscribers.

1.3.2 Registration Authorities

The registration authorities (RA) verify a subscriber’s identity and authenticity. They validate certificate signing request information, which is provided by certificate subscribers and authorize certificate subscribers for the request of certificate profiles.

1.3.3 Subscribers

The subscribers who receive certificates from the BASF PKI can be

- natural persons [TYPE_USER],
- machines [TYPE_DEVICE],
- software components [TYPE_SERVICE],
- technical accounts [TYPE_SERVICE].

Every CA within the BASF PKI **MUST** document in their Certificate Practice Statement (CPS) which identities may be subscribers.

1.3.4 Relying Parties

The PKI **MUST** only be used for business related use cases within BASF Group and between BASF Group and external business partners. Thus, the relying parties are identical to the subscribers.

A detailed definition of allowed relying parties must be defined in the CPS of any respective Issuing CA.

1.3.5 Other participants

No stipulation.

1.4 Certificate Usage

1.4.1 Appropriate Certificate uses

Issued certificates must only be used for purposes according to the defined KeyUsage and ExtendedKeyUsage extensions, as defined in RFC 5280.

Additional details on certificate usage definitions can be prescribed in the relevant Issuing CAs' CPS.

1.4.2 Prohibited certificate uses

Any usage, which is not linked to a business purpose of BASF is prohibited.

Certificates must only be used to the extent permitted with applicable laws. CA Certificates MAY not be used for any functions except CA functions. In addition, end-user Subscriber Certificates SHOULD NOT be used as CA Certificates.

1.5 Policy Administration

1.5.1 Organization administering the document

This CP is maintained by the Product Owner of the BASF Corporate PKI.

Any change in the CP triggers a review of underlying CPs and CPS to make sure required changes are reflected.

1.5.2 Contact Person

Name: PKI Operations Team
Email: key-management@basf.com

1.5.3 Person determining CPS suitability for the policy

CPS are verified by the Key Management Process Owner in the Cybersecurity organization. The responsible unit operating a CA must ensure that each CPS complies with the guidelines in the respective CP

1.5.4 CPS approval procedures

The CA operation unit assures that the applicable CPS complies with the guidelines in the respective CP and takes responsibility and accountability for it. There is no formal approval process applied before a CPS change becomes effective.

1.6 Definitions and acronyms

AD	Active Directory
BGD	BASF Group Directory
CA	Certification Authority - The entity that issues certificates
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DNS	Domain Name Service
FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
Policy CA	An intermediate certification authority within a PKI, which details policy requirements for Issuing CAs it certifies
RA	Registration Authority - The entity that performs identification and authentication of certificate applicants.
RFC	Request For Comments
Root CA	Trust anchor of a PKI, which cryptographically signs its digital certificate with its own private key
Sub CA	A certification authority within a PKI, which is allowed to issue certificates and was signed by another CA in the PKI hierarchy
UPN	User Principal Name
X.500	An ISO and ITU standard that defines how global directories should be structured
X.509	Standardized format of digital certificates, described in RFC 5280

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Repositories providing information about issued certificates and validation information shall be high-available to certificate validators and users. Access requirements and permissions must be defined in the CPS of any respective CA in the PKI hierarchy.

It must be ensured that security and data privacy requirements of BASF Group are followed for PKI related information made available to information consumers.

If external communication partners need access to a repository, access must be limited to required information for the necessary PKI-related action. Externally available namespaces of repostories and attributes in certificates must differ from BASF internal namespaces and prevent disclosure of internal organization and IT service information. Controls to ensure this requirement must be defined and implemented in the applicable Sub CAs and their CPS.

2.2 Publication of certification information

CA certificates must be made available to certificate consumers and validators in order to allow the validator to proof the certificate chain.

Validation information, such as OCSP responses and CRLs shall be published in a way that certificate consumers and validators are able to proof the validity prior to perform a cryptographic operation.

Individual requirements on publication of certificate information must be defined and implemented by the respective Sub CA and their CPS.

2.3 Time or frequency of publication

Information about issued certificates and their validity status shall be published in a timely manner and with a sufficient frequency.

Individual requirements on publication frequency of information must be defined in any CA's CPS.

2.4 Access controls on repositories

Access to PKI information shall be limited by applying a need-to-know principle.

CAs shall implement controls to prevent unauthorized adding, modifying or deleting of repository entries.

If external communication partners need access to a repository, access must be limited to required information for the necessary PKI-related action. Externally available namespaces of repositories and attributes of certificates must differ from BASF internal namespaces and prevent disclosure of internal organization and IT service information. Controls to ensure this requirement must be defined and implemented in the applicable Sub CAs and their CPS.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

The issuer Distinguished Name (DName) **MUST** be identical to the subject DName in the issuer's certificate to allow chain building.

3.1.1 Types of names

Certificates **MUST** be issued in accordance with the X.509 standard. The following types of names shall be used in digital certificates.

[ALL_TYPES] - X.500 distinguished names **MUST** be used for the subject DN of a certificate holder

[TYPE_USER] - RFC-822 names **MUST** be used for email address identifiers, when added to a digital certificate.

[TYPE_DEVICE] - DNS fully qualified domain name (FQDN) of another equivalent identifier for the device (e.g. IP address).

The X.500 name **MUST** be contained in the subject and issuer field of the certificate. The other name types are to be used in the subjectAlternativeName extension of the X.509 certificate.

3.1.2 Need for names to be meaningful

Names **MUST** be meaningful to allow for determination of the certificate holders.

It must be possible to identify the certificate holder uniquely by querying the certificate holder's name identifier in an authoritative source of BASF.

Sub CAs are requested to define in their CPS which authoritative sources are used to define and link the name identifiers with the respective authoritative source entry.

3.1.3 Anonymity or pseudonymity of subscribers

The use of pseudonyms is permitted, if individuals and technical components with access to the certificate can be identified uniquely with an additional information source (e.g. a data source mapping the pseudonym and an individual with restrictive access controls).

If Sub CAs issue pseudonymized end entity certificates they shall define in their CPS which information sources are used for mapping the pseudonym to identifiable certificate holders.

3.1.4 Rules for interpreting various name forms

When the name contains an RFC-822 name it shall be the email address of the certificate holder and written into the subjectAlternativeName extension of the certificate. If the certificate holder is a shared mailbox, requirements from chapter 3.1.3 apply.

3.1.5 Uniqueness of names

CAs shall generate certificates with unique subject and issuer DNs over the entire life cycle of the CA. The CA defines in its CPS how the unique name is established.

3.1.6 Recognition, authentication, and role of trademarks

There shall be no infringement of trademarks certificate information.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The method to prove possession of a private key by the issuing CA shall be a secure protocol where the certification request shall be signed. The requirement to prove the possession of the private key **SHOULD NOT** apply where the key pair is generated by the issuing CA itself.

3.2.2 Authentication of organization identity

If certificates are issued to organizations, the identification and authentication of the organization must be conducted according to the requirements, defined by the responsible BASF Group function.

Sub CAs, which issue certificates for BASF external organizations must define and implement effective processes according to internal and external regulatory requirements in cooperation with the responsible function within BASF Group.

3.2.3 Authentication of individual identity

Individuals' authentication **MUST** happen according to BASF's Identity and Access Management Policy requirements [3] and processes, defined by the responsible Process Owner.

Sub CAs must define the applicable processes and the responsible Process Owners must approve the use of the defined processes prior to productive use.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

Sub CAs must implement effective controls to ensure that only authorized requesters submit certificate signing requests, which are issued by the CA. The controls must be defined in the respective CPS of the CA.

[TYPE_CA] - New Sub CAs must be approved by the Product Owner of PKI within BASF Group before productive implementation.

3.2.6 Criteria for interoperation

CAs **SHOULD** only issue RFC 5280 compliant certificates.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Re-keying of certificates is allowed in the following ways:

- The process is conducted following the requirements of chapter 3.2 Initial identity validation
- The re-key request is digitally signed with the certificate, which shall be re-keyed. The signing certificate must be valid at the time of re-keying. The issuing CA must proof that the subject of the signing certificate is equivalent to the subject in the certificate signing request provided.

[TYPE_CA], [TYPE_PKI_SERVICE] - CA and PKI Service certificates **MUST NOT** be re-keyed.

3.3.2 Identification and authentication for re-key after revocation

Re-keying of revoked certificates is **NOT** allowed.

3.4 Identification and authentication for revocation request

Prior to revocation of certificates authentication of the revocation request according to requirements of the Identity and Access Management Policy [3] must be performed. After successful authentication, the requester's authorization to revoke the respective certificate must be proofed before executing the revocation.

CA's and PKI Service components' digital certificates' revocation require the approval of the respective CA owner and documentation in the incident and change management system.

Sub CAs must define and implement effective process and technical controls to enforce the policy requirements and describe such processes in their CPS.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Requesters of certificates must be authorized for this operation. The CA Owner must specify and implement effective controls to limit the ability to only authorized requesters and describe those controls in the CPS of the CA.

Request authorization must respect the applicability of certificate types to requesters defined in chapter 1.1.1 of this CP.

No individual or entity listed on a BASF list of prohibited persons or other list that prohibits doing business with such organization or person under the laws of Federal Republic of Germany CAN submit an application for a Certificate.

4.1.2 Enrollment process and responsibilities

The registration and enrollment process must be documented in the CPS of the affected CA. Requirements from chapters 3.2 and 4.1.1 **MUST** be fulfilled.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The process must be defined and documented in the respective CA CPS. Requirements from chapter 3.2 **MUST** be fulfilled.

4.2.2 Approval or rejection of certificate applications

The CA shall approve the certificate application if a valid certification request is provided and the requester is in an active business relationship with BASF Group.

Otherwise it shall reject the certificate application.

Details on validation acceptance criteria **MUST** be specified in the respective CA CPS and must be approved prior to productive implementation by the CA Owner.

4.2.3 Time to process certificate applications

The issuing CA should process the certificate request in a timely manner. Details on processing times **SHOULD** be documented in the respective CA CPS.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The source of the Certificate Request SHALL be verified before issuance. Certificates are generated, issued and distributed only after the CA or RA performs the required identification and authentication steps in accordance with Section 3.

The CA shall issue the requested certificates and return them to the requestor. The CA certificate and the chain to this Root CA should have been distributed in advance or together with the issued certificate.

4.3.2 Notification to subscriber by the CA of issuance of certificate

No stipulation. There is no requirement on notification. If additional notification is required, the CA CPS **MUST** include the description of such processes.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

No stipulation.

If a certificate use case requires specific acceptance confirmation by the requestor, the CPS of the respective CA **MUST** include the description of such process.

4.4.2 Publication of the certificate by the CA

[TYPE_CA] - CA certificates **MUST** be published in the HTTP location, which is added to the AIA extension of the CA certificate. Publication to additional locations **CAN** be done, if the access to the CA certificate is then easier for the certificate consumer.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The subscriber **MUST** be allowed to use the private key and certificate only for appropriate applications as specified by the certificate template and documented in the respective CA CPS.

4.5.2 Relying party public key and certificate usage

A relying party is obligated to rely on certificates only for appropriate applications as documented in the respective CA CPS and in consistency with applicable certificate content.

It **MUST** perform public key operations as a condition of relying on a certificate and it **MUST** check the status of a certificate prior to using the certificate for the respective operation.

4.6 Certificate renewal

Certificate renewal **SHOULD NOT** be used.

In case of strict reasons, why certificate renewal is required, the CA CPS **MUST** include validation means, which evaluate the sufficient security of the existing private key until the end of requested certificate validity period.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

The re-key process requires the generation of a new key pair, which satisfy the policy requirements for its intended use at the time of generation.

During certificate request process, the new certificate request **SHOULD** be digitally signed with an existing and valid certificate of the requester. The signing certificate and the one being issued **MUST** contain the same certificate holder information and **SHOULD** have the same key usage and extended key usage purposes.

Deviations from these requirements **MUST** be documented in the respective CPS and be approved by the PKI Owner.

4.7.2 Who may request certification of a new public key

The initiation of the re-key process **SHOULD** only be allowed for the affected certificate holder.

Any process deviation, where not the certificate holder itself starts this process, needs to be documented in the respective CPS of the certificate issuing CA and **MUST** be approved by the respective CA Owner.

4.7.3 Processing certificate re-keying requests

Re-key process that contain a digital signature of the existing certificate, which is intended to be re-keyed, are allowed to be processed automatically by the issuing CA, if the affected RA component validates the digital signature and the validity of the signing certificate.

Any other process must follow the requirements of chapter 4.2.

4.7.4 Notification of new certificate issuance to subscriber

The definitions of chapter 4.3.2 apply.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No stipulation.

4.7.6 Publication of the re-keyed certificate by the CA

The definitions of chapter 4.4.2 apply.

4.7.7 Notification of certificate issuance by the CA to other entities

The definitions of chapter 4.4.3 apply.

4.8 Certificate modification

Certificate modification is not supported. Any desired change to certificate content requires the issuance of a new certificate.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A certificate must be revoked for one of the following reasons:

- Key compromise of the certificate holder;
- Loss of private key by certificate holder;
- Private key protection facilities become insecure and cannot protect the private key as required;
- Cryptographic algorithms and methods become insecure and do not protect the target business data as required;
- Subscriber leaves BASF or contract is discontinued in case of certificates for individuals;
- Machine or technical account is decommissioned in case of non-individual subscribers;

- Certificate content is not valid anymore and must be changed;
- The affected issuing CA terminates its operation permanently

4.9.2 Who can request revocation

Revocation can be requested by the certificate owner and by an authorized body. The definition of the authorized bodies is documented in the CPS of the respective issuing CA.

4.9.3 Procedure for revocation request

The responsible RA and issuing CA define the process of performing certificate revocation.

4.9.4 Revocation request grace period

After a reason for certificate revocation has occurred the certificate revocation process **SHOULD** be conducted timely.

Detail process specifications are defined by the respective issuing CA.

4.9.5 Time within which CA must process the revocation request

Certificate revocation **MUST** be conducted timely and without culpable delay.

Details about sufficient timeframes for certificate revocation **MUST** be documented in the respective Issuing CA CPS.

4.9.6 Revocation checking requirement for relying parties

Issuing CAs **MUST** provide valid revocation information as signed CRLs to target certificate consumers via an available HTTP link resource. Additional CRL download resources, e.g. via LDAP **CAN** be provided in addition.

Revocation information in form of OCSP responses **CAN** be provided.

4.9.7 CRL issuance frequency (if applicable)

The definitions of chapter 2.3 apply.

4.9.8 Maximum latency for CRLs (if applicable)

CRLs **MUST** be published in a timely manner.

Detailed latency definitions **MUST** be documented in the respective CPS of the corresponding issuing CA.

4.9.9 On-line revocation/status checking availability

The revocation information **CAN** be provided via an OCSP service. In case of an existing OCSP service the responder connection information **SHOULD** be added to the affected certificates in the AIA extension.

4.9.10 On-line revocation checking requirements

If a conforming certificate consumer is not capable of performing validation checks via CRL, they **SHOULD** perform those validation checks via a provided online validation service.

4.9.11 Other forms of revocation advertisements available

The revocation of the by this CP affected Root CA will be communicated in a different manner.

4.9.12 Special requirements re-key compromise

No stipulation.

4.9.13 Circumstances for suspension

Certificate suspension **SHOULD NOT** be used.

If certificate suspension is used by an issuing CA due to strict business requirements, it **MUST** only be used for non-critical cases, where affected security protection of business information is not endangered.

4.9.14 Who can request suspension

No stipulation.

4.9.15 Procedure for suspension request

The procedure **MUST** be documented in the CPS of the implementing issuing CA.

4.9.16 Limits on suspension period

No stipulation.

4.10 Certificate status services

4.10.1 Operational Characteristics

Certificate revocation information **MUST** be available through an HTTP service within and outside BASF Group network infrastructure for legitimate certificate consumers.

For certificate consumers inside BASF Group network, revocation information **CAN** be accessible via LDAP protocol, too.

Information about available certificate revocation services **MUST** be added to the CDP and AIA extension of applicable certificates.

4.10.2 Availability of Status Services

Revocation information **SHOULD** be available for 24 hours on 7 days per week. Allowed downtimes of such services are documented in the respective CPS of the affected issuing CA.

4.10.3 Optional Features

No stipulation.

4.11 End of subscription

The subscription of a certificate subscriber ends with the end of the business purpose of the certificate usage.

The issuing CA’s CPS **MUST** define detailed criteria for such end of subscription events.

As soon as a subscription end trigger is identified, the affected certificate **MUST** be revoked. Requirements of chapter 4.9 apply.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Private keys of non-repudiation certificates **MUST NOT** be archived. Private keys of authentication certificates **SHOULD NOT** be archived. If legal obligations exist, private keys of encryption certificates **MUST** be archived. Business reasons might stipulate that private keys of encryption certificates SHOULD be archived.

Any private key **MUST NOT** be stored or transferred in an unencrypted form. During recovery, the affected private key **SHOULD NOT** be cached by an intermediary component between the key recovery solution and the target device.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

Root and Policy CAs **MUST** be set up and operated with physical protection measures against unauthorized access. Technical equipment which may change the behavior of CA configuration **MUST** be locked away from daily operation personnel in managed IT infrastructure environments.

For any physical protection requirements of the PKI components, the requirements from [1] apply.

5.2 Procedural controls

The access to CA functions **MUST** be limited by following the least privilege principle and **MUST** be defined in an access control concept per CA. This concept **MUST** be approved by the CA Owner prior to productive implementation.

Operations on the Root CA **SHOULD** be conducted with 4-eye principle and documentation for the performed actions **MUST** be created and archived.

5.3 Personnel controls

The personnel filling trusted roles **MUST** be skilled in their job, this **MUST** be ensured by the respective CA owners.

5.4 Audit logging procedures

All events that are related to the security of the CA system and cryptographic material used by the CA **MUST** be automatically recorded in audit log files and provided timely to the central security logging service of BASF Group.

Audit logs **SHOULD** be protected against unauthorized and unnoticed change and protected with digital signatures.

5.5 Records archival

Paper-based documents as well as electronic messages **MUST** be recorded in a way that their storage, preservation, and reproduction is always accurate and complete according to legal regulations and BASF Group policy requirements.

5.6 Key changeover

[TYPE_CA] - The change of key material **MUST** follow documented and approved processes.

[TYPE_CA] - CA keys **MUST** be created within a key ceremony and a complete documentation of all performed steps. A register of secrets holders **MUST** be created.

[TYPE_CA] - Affected certificate subscribers **SHOULD** be informed upfront with sufficient lead time to evaluate fulfillment of new CA's process and technology requirements.

5.7 Compromise and disaster recovery

[TYPE_CA] - If a CA key is compromised, it **MUST** be revoked immediately.

[TYPE_CA] - In case of CA key compromise, the affected CA owner **MUST** report a security incident according to the BASF Incident Management [2] requirements. Affected certificate subscribers **SHOULD** be informed according to guidelines of the opened incident.

[TYPE_CA] - Conforming CAs **MUST** have a disaster and recovery plan to allow timely recovery of the CA in case of loss of key material or CA data. The recovery procedure **SHOULD** be tested regularly.

5.8 CA or RA termination

If a CA terminates its operation, all subscribers' certificates **MUST** be revoked. Afterwards the CA certificate **MUST** be revoked and its private key including back-up **MUST** be securely destroyed. The Sub CA's archival records **SHOULD** be maintained by another CA of the same hierarchy.

If the Root CA terminates its operation, all Sub CAs **MUST** be informed with sufficient lead time. The lead time is documented in the CPS of the Root CA.

5.9 Outsourcing / Outtasking

The BASF PKI **MUST** be treated as a trust anchor. In case of outsourcing or outtasking, a risk assessment according to BASF's Risk Assessment process **MUST** be performed prior to implementation.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

Key pair generation **MUST** be performed using trustworthy systems and processes that provide the cryptographic strength and attack resistance, required by Security Policy Framework's Cryptography Standard.

[TYPE_CA] - Private keys of CAs **MUST** be generated on HSM devices, which are approved for this purpose.

[TYPE_PKI_SERVICE] - Private keys **MUST** be created and maintained on approved HSMs.

[TYPE_USER] - Non-repudiation keys **MUST** only be generated in approved hardware protected key stores. Approval must be given by the PKI Owner.

6.1.2 Private key delivery to subscriber

Private keys **SHOULD** be generated in the destination, where they are going to be used.

If private keys are generated by a CA or an RA, the key **MUST** be encrypted during delivery. Credentials for decryption **MUST** be securely transferred to the certificate subscriber's device, where the private key will be used.

[TYPE_USER] - Encryption keys, which are recovered from a central key archival solution **SHOULD** be provided to the end user's device in a different channel than the decryption credentials.

6.1.3 Public key delivery to certificate issuer

If private keys are generated by the certificate subscriber, effective controls for proof of possession of the private key of the certificate subscriber **MUST** be implamented. The use of PKCS#10 requests **SHOULD** be implemented.

6.1.4 CA public key delivery to relying parties

The public key of the Root CA and all required subordinate CA certificates in the affected chain **SHOULD** be transmitted to the subscriber as part of the certificate delivery after issuance or made available for download with an accessible URL for the subscriber.

Inside BASF Group network trusted CA certificates **SHOULD** be also published in enterprise directory services.

6.1.5 Key sizes

Certificates issued by this PKI **MUST** comply with requirements and key sizes defined in the Key Management Process register of approved cryptographic solutions.

6.1.6 Public key parameters generation and quality checking

The quality of the generated key parameters **SHOULD** meet the requirements of at least FIPS 186-4 and BSI TR-02102. The applicability of other standards is not excluded for Sub CAs according to additional legal requirements.

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

The definitions of chapter 1.4.1 apply.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The private key of the CA **MUST** be protected in a hardware storage module (HSM).

The subscribers' private keys may be generated and stored on a smart card or in software.

6.2.1 Cryptographic module standards and controls

Hardware protection for private keys **SHOULD** meet the requirements of FIPS 140-2 Level 2 or higher.

[TYPE_CA] - HSMs used for CAs in this PKI **SHOULD** have an EAL4 certification.

[TYPE_USER] - Hardware protected key containers for end users **MUST** fulfill the requirements of FIPS 140-2 Level 2 or higher.

6.2.2 Private key (n out of m) multi-person control

[TYPE_CA] - Activities on the Root CA **MUST** enforce 4-eye control.

[TYPE_CA] - Activities, which may affect the security of the private key or the behavior of a Sub CA **SHOULD** be protected by 4-eye controls.

[TYPE_PKI_SERVICE] - Activities, which may impact the security of certificate request or validation behavior **SHOULD** be protected with 4-eye controls.

6.2.3 Private key escrow

[TYPE_CA] - The escrow of CA private keys **MUST NOT** be done.

[TYPE_USER] - The escrow of authentication and non-repudiation keys **MUST NOT** be supported.

[TYPE_USER] - The escrow of end user's encryption keys for authorized legal bodies or in case of company spin-offs **MUST** be strictly controlled and described in the CPS of the affected CA or a separate document, which is referenced by the corresponding CPS.

[TYPE_USER] - If escrow of end user's encryption keys in order to make them available to different authorized end users than the certificate subscriber should be allowed, the processes and security controls **MUST** be documented in the corresponding issuing CA CPS.

6.2.4 Private key backup

[TYPE_CA], [TYPE_PKI_SERVICE] - The backup of CA and central PKI service' private keys **SHOULD** be hardware protected and **SHOULD** support 4-eye control enforcement for backup and restore operations.

[TYPE_USER], [TYPE_DEVICE], [TYPE_SERVICE] - Backup of private keys to fulfill operational availability requirements **MUST** provide min. the same protection capabilities

than the primary key container. Restore operating procedures **SHOULD** be centrally documented and approved by the affected CA owner. Private keys **SHOULD** only be restored into environments, which fulfill the same minimum security requirements, like the environment, where the private key was enrolled.

6.2.5 Private key archival

As a standard behavior, private keys of certificate subscribers **MUST NOT** be archived with the following exceptions:

[TYPE_USER] - Encryption keys **SHOULD** be securely archived if otherwise availability of business information cannot be ensured. Archival and recovery procedures **MUST** be documented in the implementing CA's CPS and **MUST** be approved by the CA owner prior to productive implementation.

[TYPE_DEVICE], [TYPE_SERVICE] - The archival of encryption and authentication keys **CAN** be allowed, if strict business requirements require its implementation. The procedures **MUST** be documented in the affected CA's CPS and affected business owners **SHOULD** approve their use prior to productive implementation.

6.2.6 Private key transfer into or from a cryptographic module

A private key **SHOULD** not be transferred to a solution, which supports a lower security level than the origin. Private keys **SHOULD NOT** be saved at rest or cached in software during transit.

[TYPE_CA], [TYPE_PKI_SERVICE] - Private keys, which have been created by an HSM **MUST NOT** be transferred to a solution that supports less security protection capabilities.

6.2.7 Private key storage on cryptographic module

[TYPE_CA] - Private keys MUST be stored on approved HSMs.

[TYPE_PKI_SERVICE] - Private keys **SHOULD** be stored on approved HSMs and **MUST** implement mitigating controls, if the use of HSMs is not possible.

[TYPE_USER], [TYPE_DEVICE], [TYPE_SERVICE] - Private keys for high assurance certificates **SHOULD** be stored in hardware protected key containers.

6.2.8 Method of activating private key

[TYPE_CA] - Private keys **MUST** be activated by using a 4-eye control enforcing process.

[TYPE_PKI_SERVICE] - Private keys **SHOULD** be activated by using a 4-eye control enforcing process.

[TYPE_USER], [TYPE_DEVICE], [TYPE_SERVICE] - Private keys **SHOULD** only be activated by the certificate subscriber. The issuing CA describes the activation process for affected certificates in its CPS.

6.2.9 Method of deactivating private key

If a private key is secured by a hardware module, this module **MUST** support effective lock mechanisms to block the access to the private key usage after too many failed authentication attempts. Lock and unlock procedures **MUST** be defined and documented in the corresponding CA's CPS.

6.2.10 Method of destroying private key

[TYPE_CA], [TYPE_PKI_SERVICE] - If HSMs are used to protect the private key, affected CAs **MUST** implement effective processes to destroy the private key permanently as soon as it is not required anymore.

6.2.11 Cryptographic Module Rating

The definitions of chapter 6.2.1 apply.

6.3 Other aspects of key pair management

6.3.1 Public key archival

CAs **MUST** ensure archival of public keys for min. the duration of required use by internal and external regulations. Every CA must evaluate this duration for its provided certificates and implement effective solutions, which **MUST** be described in the CA's CPS.

6.3.2 Certificate operational periods and key pair usage periods

The duration of permitted use of public keys is defined in the Register of Approved Cryptographic Solutions.

6.4 Activation data

6.4.1 Activation data generation and installation

The responsible Registration Authority function of a CA defines sufficient activation data processes.

[TYPE_CA] - If a private key of a CA must be transferred, an activation process **MUST** be implemented to ensure a 4-eye control process to activate the CA private key.

6.4.2 Activation data protection

The issuing CA **SHOULD** provide supporting information for subscribers, how to prevent loss or unauthorized disclosure of their activation data.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

No stipulation.

6.6 Life cycle technical controls

No stipulation.

6.7 Network security controls

No stipulation.

6.8 Time-stamping

No stipulation.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

Certificate profiles **SHOULD** be compliant to RFC 5280.

7.1.1 Version Numbers

Issued certificates **MUST** be compliant to the X.509 v3 standard.

7.1.2 Certificate Extensions

The following extensions SHOULD be set to critical:

- KeyUsage (OID 2.5.29.15)
- BasicConstraints (OID 2.5.29.19)

as few extensions as possible **SHOULD** be marked as critical.

[TYPE_CA] - CA certificates **MUST** have the extension “BasicConstraints” with OID 2.5.29.19 set.

[TYPE_CA] - Issuing CAs **MUST** contain a pathlength constraint in the extension BasicConstraints, which is set to 0.

BASF specific extensions **MUST** be registered in the BASF enterprise OID register and start with 1.3.6.1.4.1.21220.3.x.

7.1.3 Algorithm OIDs

No stipulation.

7.1.4 Name Formats

Definitions of chapters 3.1.1 and 3.1.2 apply.

7.1.5 Name Constraints

Certificates used outside BASF enterprise **SHOULD NOT** contain name spaces of internal network and service areas. The responsible CAs **MUST** define external name spaces, which do not allow conclusions of BASF internal IT and service areas.

7.1.6 OIDs of Certificate Policies

Each certificate policy **MUST** have a unique OID of BASF OID namespace. The OID of the applicable policy **SHOULD** be added to the “CertificatePolicies” extension (OID 2.5.29.32) of leaf certificates and their intermediate CAs.

7.1.7 Use of “PolicyConstraints”

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics of critical CP Extension

No stipulation.

7.2 CRL profile

7.2.1 Version number(s)

The revocation lists **MUST** be X.509 v2 CRLs.

The use of Delta CRLs **CAN** be allowed to issuing CAs.

7.2.2 CRL and CRL entry extensions

The CRL of the BASF Root CA and SUB CAs MUST contain

- CRL number,
- CRL issuer,
- Signature of the issuer,
- Date issued,
- Date for Next Update,
- List of revoked certificate serial numbers.

Other CRL extensions may be used if they are not marked as critical.

CRL entries **CAN** contain the reason code for the revocation of the respective certificate.

CRLs **SHOULD** be available in intranet and internet.

7.3 OCSP profile

An OCSP Service **SHOULD** be available and accessible from the internet.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

No stipulation.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

No stipulation.

9.2 Financial responsibility

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

The certificate application data and Certificate Practice Statements (CPS) - whether approved or disapproved – shall be kept confidential as well as the disaster recovery plans and the audit reports. The BASF CP documents **MUST** be regarded as private and BASF internal and only selectively made available to business partners either as excerpt or complete after PKI owner approval.

9.3.2 Information not within the scope of confidential information

Documents and certificates, which are made available to the public internet **SHOULD** be classified as public according to BASF information classification requirements.

9.3.3 Responsibility to protect confidential information

The certificate application data and personal information inside the application data **MUST** be treated in accordance with the German laws (“Bundesdatenschutzgesetz”, “Datenschutzgesetze der Länder”) and BASF internal security directives and guidelines to protect data privacy.

9.4 Privacy of personal information

9.4.1 Privacy plan

In the context of the CA operation personal user data is to be collected and stored. This data **MUST** be treated in accordance with the German laws (“Bundesdatenschutzgesetz”, “Datenschutzgesetze der Länder”) and BASF internal security directives and guidelines.

9.4.2 Information treated as private

No stipulation. The requirements of BASF data privacy regulations apply.

9.4.3 Information not deemed private

No stipulation. The requirements of BASF data privacy regulations apply.

9.4.4 Responsibility to protect private information

No stipulation. The requirements of BASF data privacy regulations apply.

9.4.5 Notice and consent to use private information

No stipulation. The requirements of BASF data privacy regulations apply.

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation. The requirements of BASF data privacy regulations apply.

9.4.7 Other information disclosure circumstances

No stipulation. The requirements of BASF data privacy regulations apply.

9.5 Intellectual property rights

The CA and leaf certificates and the corresponding private keys shall be in property of BASF.

[TYPE_USER] - The certificates and private keys of the end-users shall be their own property.

9.6 Representations and warranties

This CP **MUST NOT** serve as a contract and therefore **MUST NOT** contain any warranties. The information in the certificate **SHOULD** be true to the best of the issuing CA's knowledge.

9.7 Disclaimers of warranties

No stipulation. See section 9.6.

9.8 Limitations of liability

No stipulation.

9.9 Indemnities

No stipulation. See section 9.2.

9.10 Term and termination

9.10.1 Term

The CP shall become effective when the certificate is issued.

9.10.2 Termination

The CP shall never expire. There may be new versions when some certificate related issues shall be changed. But this CP shall still be valid for the certificates issued under this policy.

9.10.3 Effect of termination and survival

No stipulation.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

No stipulation.

9.13 Dispute resolution provisions

No stipulation.

9.14 Governing law

The German laws shall govern the enforceability, interpretation, and validity of this CP.

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

No stipulation.

9.17 Other provisions

No stipulation.

10 Referenced Documents

[1] Operational Systems Management Policy Intranet – Security Policy Framework

[2] Incident Management Security Policy Intranet – Security Policy Framework

[3] Identity and Access Management Policy Intranet – Security Policy Framework