

SAP Cloud Root CA Certificate Policy (CP)

Requirements for SAP Cloud PKI

PUBLIC

June 18th, 2020
Version: 1.0



THE BEST RUN



www.sap.com/contactsap

© 2018 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies. See <http://www.sap.com/corporate-en/legal/copyright/index.epx> for additional trademark information and notices.

THE BEST RUN



TABLE OF CONTENTS

1	INTRODUCTION	5
1.1	Overview	5
1.2	Document Name and Identification.....	6
1.3	PKI Participants	7
1.4	Certificate Usage	7
1.5	Policy Administration	7
1.6	Definitions and Acronyms.....	8
2	PUBLICATION AND REPOSITORY RESPONSIBILITIES	10
2.1	Repositories.....	10
2.2	Publication of certification information	10
2.3	Time or frequency of publication.....	10
2.4	Access controls on repositories.....	10
3	IDENTIFICATION AND AUTHENTICATION.....	11
3.1	Naming.....	11
3.2	Initial identity validation	12
3.3	Identification and authentication for re-key requests	13
3.4	Identification and authentication for revocation request.....	13
4	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	14
4.1	Certificate Application.....	14
4.2	Certificate application processing.....	15
4.3	Certificate issuance.....	15
4.4	Certificate acceptance.....	16
4.5	Key pair and certificate usage	16
4.6	Certificate renewal.....	16
4.7	Certificate re-key	17
4.8	Certificate modification	17
4.9	Certificate revocation and suspension.....	17
4.10	Certificate status services.....	19
4.11	End of subscription	19
4.12	Key escrow and recovery.....	19
5	FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS.....	20
5.1	Physical Security Controls.....	20
5.2	Procedural Controls	21
5.3	Personnel Controls.....	21
5.4	Audit Logging Procedures	22
5.5	Records Archival	23
5.6	Key Changeover	24
5.7	Compromise and Disaster Recovery	24
5.8	CA or RA Termination	25
6	TECHNICAL SECURITY CONTROLS.....	26
6.1	Key Pair Generation and Installation	26
6.2	Private Key Protection and Cryptographic Module Engineering Controls	27
6.3	Other aspects of key pair management.....	29
6.4	Activation data.....	29

6.5	Computer security controls	29
6.6	Life cycle technical controls	30
6.7	Network security controls	30
6.8	Time-stamping	30
7	CERTIFICATE, CRL, AND OCSP PROFILES	31
7.1	Certificate profile	31
7.2	CRL profile	32
7.3	OCSP profile	33
8	COMPLIANCE AUDIT AND OTHER ASSESSMENTS	34
8.1	Frequency or circumstances of assessment	34
8.2	Identity/qualifications of assessor	34
8.3	Assessor's relationship to assessed entity	34
8.4	Topics covered by assessment	34
8.5	Actions taken as a result of deficiency	34
8.6	Communication of results	34
9	OTHER BUSINESS AND LEGAL MATTERS	35
9.1	Fees	35
9.2	Financial Responsibility	35
9.3	Confidentiality of business information	35
9.4	Privacy of personal information	35
9.5	Intellectual property rights	36
9.6	Representations and warranties	36
9.7	Disclaimers of warranties	37
9.8	Limitation of liability	37
9.9	Indemnities	37
9.10	Term and termination	37
9.11	Individual notices and communications with participants	37
9.12	Amendments	37
9.13	Dispute resolution provisions	38
9.14	Governing Law	38
9.15	Compliance with the applicable law	38
9.16	Miscellaneous Provisions	38
9.17	Other Provisions	38

1 INTRODUCTION

This *certificate policy* (CP) document states the requirements of the SAP Cloud Root CA regarding the operation of subordinate CAs. In order to achieve the predetermined security level and trustworthiness of the whole infrastructure, these requirements must be fulfilled by each CA that wants to be certified by the SAP Cloud Root CA.

Subordinate CAs are required to have a *Certification Practice Statement* (CPS) that describes how the requirements of the CP are implemented. Thus, the CP defines what should be done, whereas the CPS describes how it should be done. Since some content of a CPS might be confidential, a CPS does not need to be published. If requested, a verifying body may access the document after signing a Non-Disclosure Agreement (NDA).

This document describes the certificate policy for the SAP Cloud PKI of SAP SE with basic protection requirements.

Certificates for applications that require basic protection include server and client authentication certificates. Other areas of application such as data encryption and document signing are currently not covered by this certificate policy.

This document was created in accordance with the policies in RFC 3647. It is targeted at subscribers/relying parties, the operators of the PKI and their auditors.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

1.1 Overview

The SAP Cloud PKI may have up to three CA layers followed by the end entity:

- SAP Cloud Root CA
- optional SAP Cloud Intermediate CA
- SAP Cloud Issuing CA
- End entity

A SAP Cloud Issuing CA must not issue another CA certificate. It is only allowed to issue certificates to end entities.

Each CA operated by SAP SE is subject to certain requirements in terms of structure and implementation. The following list provides an overview which basic prerequisites must be met:

- **Hierarchy:** A PKI must comprise a minimum of a two-tier but no more than a three-tier hierarchy of certification authorities with a Root CA on top that is operated offline.
- **Purpose:** Issuing CAs must be assigned to a certain scope.
- **Certificate Restrictions:** As far as feasible, the purpose must be defined in the restrictions of the certificates. *Basic Constraints* are necessary to distinguish between end user and CAs. Only a CA can issue a certificate to another certification authority.
- **Revocation Information:** Information about the status of a certificate must be made available to relying parties via the standard channels (CRL download and OCSP), except when using short-lived certificates. The validity of short-lived certificates within the SAP Cloud PKI must not exceed 1 week.
- **Availability:** All components of a PKI must be highly available to ensure that the failure of an individual component does not cause the service to fail.
- **Key Protection:** In order to protect the private keys of an online CA from being compromised, its private key must be protected by a hardware-side mechanism (HSM, SmartCards, TPM, etc.). Exceptions need explicit approval by SAP IT Security.
- **6-eyes-Principle:** All SAP Cloud Root CA operations performed with its private key must be monitored and documented via a triple control system (6-eyes-principle).

- **System Security:** All systems involved in the SAP Cloud PKI must be protected in accordance with their role based on the SAP policies.
- **Audits:** The system environment must be audited regularly, and immediately after any extensive changes. This may be performed by an external service provider or internally e.g. via an HASI (Hacking Simulation).

1.2 Document Name and Identification

Document name: SAP Cloud PKI Certificate Policy (CP) – Requirements for SAP Cloud PKI

Version: 1.0

Date: 18.06.2020

Policy OID Depending on its version, it is referenced via the following *Object Identifier* (OID):

X.509 OID	Description
1.3.6.1.4.1.694.4	SAP PKI Base of the SAP PKI Namespace
1.3.6.1.4.1.694.4.200	SAP Cloud PKI production environment
1.3.6.1.4.1.694.4.200.1	SAP Cloud Root CA - Certificate Policy (CP)
1.3.6.1.4.1. 694.4.200.1.1	SAP Cloud Root CA - Certificate Policy Version 1.0
1.3.6.1.4.1. 694.4.200.1.1.1	SAP Cloud Root CA - Certificate Policy Version 1.1
1.3.6.1.4.1. 694.4.200.1.2	SAP Cloud Root CA - Certificate Policy Version 2.0
1.3.6.1.4.1. 694.4.200.2	SAP Cloud Root CA Certification Practice Statement (CPS)
1.3.6.1.4.1. 694.4.200.2.1	SAP Cloud Root CA CPS Version 1.0
1.3.6.1.4.1. 694.4.200.2.1.1	SAP Cloud Root CA CPS Version 1.1
1.3.6.1.4.1. 694.4.200.2.2	SAP Cloud Root CA CPS Version 2.0
1.3.6.1.4.1. 694.4.200.3	SAP <Cloud CA> Certification Practice Statement (CPS)
1.3.6.1.4.1. 694.4.200.3.1	SAP <Cloud CA> CPS Version 1.0
1.3.6.1.4.1. 694.4.200.3.1.1	SAP <Cloud CA> CPS Version 1.1
1.3.6.1.4.1. 694.4.200.3.2	SAP <Cloud CA> CPS Version 2.0

The certificate policy of the SAP Cloud Root CA is publicly accessible via the following Web site:
<http://www.pki.co.sap.com/>



1.3 PKI Participants

1.3.1 Certification Authorities

The *SAP Cloud PKI* consists of an offline SAP Cloud Root CA and multiple issuing Sub-CAs that issue server and client authentication certificates.

1.3.2 Registration Authorities

A Registration Authority confirms the identity of end entities, if required. Alternatively, an existing repository of identities can be utilized. A Registration Authority can also be inherent to a Certification Authority.

1.3.3 Certificate Subscribers

Certificate Subscribers are always the owners of the private cryptographic key belonging to the certificate. They are the entities listed in the certificate in the subject or the subjectAltName field. This might be personal users, service users, technical users, clients or servers.

1.3.4 Relying Parties

A relying party is the party that uses a certificate in order to verify and assess the trustworthiness of a subscriber based on the given certificate policy. By using the certificate, the Relying Party implicitly agrees to this policy.

1.3.5 Other Participants

Other components of the SAP Cloud PKI might be OCSP responders and the PKI repository where the CA certificate, the Certificate Revocation Lists (CRL) and the Certificate Policy are stored. At least this certificate policy document must be published on a Web server. If a CA issues certificates with a validity of more than one week (i.e. no short-lived certificates), a CRL must be provided on a Web server via HTTP or an *Online Certificate Status Protocol* (OCSP) service must be offered.

1.4 Certificate Usage

1.4.1 Appropriate certificate uses

SAP Cloud Intermediate CA certificates may be used to issue subordinate CA certificates and certificates to OCSP responders. In addition, it may be used to issue CRLs.

SAP Cloud Issuing CA certificates may be used to issue certificates to OCSP responders and certificates to end entities like personal users, service users, technical users, clients and servers. In addition, it may be used to issue CRLs.

An end entity may use his certificate for authentication and transport encryption.

1.4.2 Prohibited certificate uses

All certificates issued by SAP Cloud PKI may only be used by SAP-internal systems, SAP landscapes, employees, and partners. Use in external scenarios is not permitted. In other words, certificates may not be issued to or checked by entities that do not have a contractual relationship with SAP.

A SAP Cloud Issuing CA must not issue certificates to other CAs. Only SAP Cloud Intermediate CAs are allowed to issue CA certificates.

End entities must not use their certificate for private purposes. Their certificate use is restricted to authentication and transport encryption. They must not issue certificates to other end entities.

1.5 Policy Administration

1.5.1 Organization administering the document

The certificate policy is managed and changed by the SAP IT Security department. This team is referred to as SAP IT Security in the whole document in order to avoid and simplify repeated updates of the document due to organizational name changes.

1.5.2 Contact person

SAP SE
Petra Barzin
SAP Global Security
Dietmar-Hopp-Allee 16
69190 Walldorf, Germany
E-Mail: petra.barzin@sap.com

1.5.3 Person determining CPS suitability for the policy

SAP IT Security checks that a Certification Practice Statement (CPS) adheres to the requirements of this certificate policy.

1.5.4 CPS approval procedures

The regulations for operating a CA must be provided by the service owner of the CA in form of a CPS to SAP IT Security for inspection and approval before productive use of the CA.

IT Security will check if the CPS conforms with the requirements laid out in this policy. In case of essential changes to the CPS, IT Security must be notified immediately, and a new acceptance process is required.

1.6 Definitions and Acronyms

1.6.1 Abbreviations

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation Lists
CSR	Certificate Signing Request
DN	Distinguished Name
FIPS	Federal Information Processing Standard
FQDN	Fully-Qualified Domain Name
HASI	Hacking Simulation
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure
IDS/IPS	Intrusion Detection System/Intrusion Prevention System
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
SAN	SubjectAltName
SLA	Service Level Agreement
TLS	Transport Layer Security

1.6.2 Definitions

CA	A trusted entity that issues and revokes public key certificates
Certificate	A data structure that contains an entity identity(s), the entity's public key and possibly other information, along with a signature on that data set that is generated by a trusted party, i.e. a CA, thereby binding the public key to the included entity identity.

CRL	A list of revoked public key certificates created and digitally signed by a CA.
Client	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server
CPS	A statement of the practices that a CA employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements i.e., requirements specified in this Certificate Policy.
CSR	Request that is sent to a CA in order to get enrolled. It contains the public key of the end entity that is requesting a Certificate.
Cross Certificate	A certificate issued from a CA that signs the public key of another CA that is not within its trust hierarchy and thus establishes a trust relationship between the two CAs and extends trust relationships
Distinguished Name	An identifier that uniquely represents an object in the X.500 directory information tree. The subject and issuer of a certificate use Distinguished Names for historical reasons. DN are defined by the X.500 standard of the International Telecommunication Union (ITU-T), specifically the recommendations of X.501 and X.520.
End entity	Under this policy, end entities may be personal users, service users, technical users, clients and servers. An end entity is either a subscriber or a relying party.
FQDN	The hostname and domain name for a specific system
HSM	A physical computing device that safeguards and manages digital keys for strong authentication and provides cryptographic operations processing
Key	A value used to control cryptographic operations, such as signature generation or signature verification.
User	Users are any individuals that are maintained in the official HR systems of SAP or a partner, and which have a unique ID.
OID	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class.
OCSP	The OCSP protocol is used to check on the status of a certificate. This is a more scalable alternative compared to the use of CRLs.
PKI	The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates.
Private Key	The key in Asymmetric Cryptography that is kept secret by the owner (end entity).
Public Key	The key in Asymmetric Cryptography that is widely distributed.
RA	An RA denotes an instance located upstream of a CA, which is tasked with the authentication and authorization of end entities, as well as with reviewing and ensuring the correctness of the CSRs and optionally the issued certificates.
Repository	A database service capable of storing information, such as certificates and CRLs, allowing unauthenticated information retrieval.
Revocation	Revocation of a certificate invalidates a previously signed certificate and is listed in the next published CRL by its serial number.
Root CA	The Root CA is the topmost CA in a PKI hierarchy and acts as the trust anchor for certificates issued by CAs in this PKI hierarchy.
Server	A system entity that provides a service in response to requests from clients.
Sub-CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA.
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party.



2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

If an existing repository is utilized to retrieve identity information of end entities, this repository must be listed in the CPS of an Issuing CA.

2.2 Publication of certification information

The own CA certificate should be published on an internet facing Web server and a link to the CA certificate must be added in all issued certificates.

If a CA issues certificates with a validity of more than one week (i.e. no short-lived certificates), a CRL must be provided on an internet facing Web server via HTTP or an *Online Certificate Status Protocol* (OCSP) service must be offered. In this case, the URL of the CRL, the OCSP responder, or both must be added to all issued certificates.

The web server must be operated so that it satisfies the same availability requirements as the PKI service itself.

This CP document of the SAP Cloud Root CA must be published by the Root CA's operator.

2.3 Time or frequency of publication

If CRLs are issued by a CA they must be published immediately after they have been issued, at least within four hours of a working day. The CRL issuance frequency is given in section 4.9.7.

2.4 Access controls on repositories

All relying parties must be able to retrieve data from the PKI repository. Read access to information in PKI repository is non-critical and can be carried out anonymously and unauthorized. However, access not required for the purposes stated in this document should be avoided.

Only authorized roles of the PKI may be given write access or allowed to add or delete data records. The latest logical and physical protective measures must be taken to ensure that unauthorized access is not possible.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

The SAP Cloud PKI is designed according to the X.509 standard and must therefore meet corresponding requirements. This applies to the format of the certificates including the names contained in the certificates, which may appear in the fields *Subject* and *Subject Alternate Name* (SAN).

Naming information about end entities depends on how the certificates are used by the processing instances. Names must be chosen that allow a certificate to be uniquely and unambiguously assigned to an end entity.

3.1.1 Types of names

All names that appear in the subject field of a certificate must use the format of a *Distinguished Names* (DN).

The details regarding the necessary and optional attributes of the DN and other name forms must be specified in the respective CPS.

The minimum requirements for the individual certificate types are defined below.

3.1.1.1 CA Certificates

RFC 5280 states precise requirements for certificates from certification authorities and those that are used for signing certificate revocation lists (CRL). As such, the *Subject* and *Issuer* must match, and the DN in accordance with the X.500 standard must not be empty.

The following attributes and values must be specified as a minimum in the Subject of a CA certificate:

- **CN** (commonName)
The contents must contain enough information to indicate the function of the CA.
- **O** (organization)
The organization, that is the company that operates the CA, in most cases "SAP SE"
- **C** (country)
The country according to ISO3166-1, Alpha2 (2 country codes) in which the CA is operated

3.1.1.2 Server Certificates (incl. OCSP)

It must be ensured that the server can be uniquely identified by the name.

TLS Server certificates must include, but not be limited to, at least one FQDN or IP address in the certificate's SubjectAltName (SAN) extension. Wildcard FQDNs are permitted to the extent regulated by SAP Security Policy.

The following minimum requirements apply to the Subject if it is not empty:

- **CN** (commonName)
If present, this field **MUST** contain a single IP address or FQDN that is one of the values contained in the certificate's subjectAltName extension
- **OU** (organizationalUnit)
Any value can be entered, but it must describe as accurately as possible an existing SAP service, SAP department or equivalent organizational structure. Multiple OU attributes may be used.
- **O** (organization)
The organization that operates the server, which is normally "SAP SE"
- **C** (country)
The country in accordance with ISO3166-1, Alpha2 (2 country codes) in which the service is operated

3.1.1.3 User/Client Certificates

This certificate type is used to identify a personal user, service user, technical user or client. The reference to the subscriber must be able to be derived from the *Common Name* of the *Subject* and/or the *Subject Alternate Name*.



The following minimum information is required in the Subject:

- **CN** (common Name)
Any value can be entered, but must uniquely identify the personal user, service user, technical user or client
- **OU** (organizationalUnit)
Any value can be entered, but it must describe as accurately as possible an existing SAP service, SAP department or equivalent organizational structure. Multiple OU attributes may be used.
- **O** (organization)
The organization to which the subscriber belongs, which is normally “SAP SE”
- **C** (country)
The country in accordance with ISO3166-1, Alpha2 (2 country codes) in which the organization is registered for which the subscriber is active.

3.1.2 Need for names to be meaningful

Based on the subject and/or the SAN, it must be possible to assign a certificate unambiguously to an organization and the corresponding end entity.

Names shall be meaningful in order to allow for determination of the certificate holders.

3.1.3 Anonymity or pseudonymity of subscribers

Subscribers may not be anonymous. Pseudonyms and aliases, however, are possible if they are unique in the CA namespace.

3.1.4 Rules for interpreting various name forms

The certificate holder/subscriber of a certificate must be either named in the *Subject* and/or in the *Subject Alternate Name* field in the certificate.

The name forms used by a CA must be declared in its CPS.

3.1.5 Uniqueness of names

Names in the *Subject* and/or *Subject Alternate Name* must be unique within the namespace of a CA. Certificates with the same names are possible providing that they are assigned to the same subscriber and have different serial numbers.

3.1.6 Recognition, authentication, and role of trademarks

Use of legally protected names is not permitted. The applicant (subscriber or RA) is responsible for ensuring that no naming rights of third parties are violated.

3.2 Initial identity validation


3.2.1 Method to prove possession of private key

An X.509 certificate binds a public key to the identity of a certificate holder. Thus, the identity must be verified and it must be assured that the certificate applicant possesses the private key which belongs to the public key. Thus, an applicant must employ suitable methods to show that he is the owner of the corresponding private key. Certificate applications using PKCS#10 (RFC 2986) or CMC (RFC 5272) meet this requirement.

3.2.2 Authentication of organization identity

There are two different scenarios for authenticating organization identity:

1. The organization identity information originates from the applicant himself
In this case, the CA, an RA or some upstream processes must validate the applicant's organization identity according to the CA's naming concept.
In case of a TLS server certificate the ownership or control of the domain must be verified.
In case of a client certificate, where the subscriber/holder of the certificate acts on behalf of an organization e.g. is part of a customer's tenant, the affiliation of the subscriber to this organization/tenant must be verified.

- 
2. The certificates are issued based on information from a data source
In this case, no unchecked sources may be used for information in the certificate. It must be ensured that this information is correct when the data records are entered into the data source.
Prior to using any data source as a reliable data source, the CA must evaluate the source for its reliability, accuracy, and resistance to alteration or falsification.

3.2.3 Authentication of individual identity

If the applicant is a natural person, then the CA, an RA or another upstream process must verify the applicant's name and the authenticity of the certificate request.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

The CA must check authorization and assess the authenticity of the certificate request before issuing a certificate.

3.2.6 Criteria for interoperation

Collaboration with external PKIs (for example, cross-certification) requires thorough revision of this policy. No collaboration is planned currently.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

In case the current certificate is still valid, the new CSR may be signed with the current key and certificate for the purpose of identification and authentication. Otherwise the identification and authentication must be carried out the same way as for the initial request (cf. 3.2.2).

3.3.2 Identification and authentication for re-key after revocation

The process for renewing a certificate following a previous revocation must be the same process as for the initial request (cf. 3.2.2). The keys may not be reused, new keys must be generated.

3.4 Identification and authentication for revocation request

If a CA issues certificates with a validity of more than one week (i.e. no short-lived certificates), a CA must offer a revocation service where certificates can be revoked.

Revocation requests must be verified by the CA with regards to the identity of the applicant and the legitimacy of the revocation request before the certificate will be revoked.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

A certification application for a subordinate CA issued by the SAP Cloud Root CA may only be submitted by the service owner of the new CA.

Certification applications for end entity certificates must be submitted by a SAP user, client or server. Registration authorities (RA) can also take over this function if they ensure that only legitimate end entities become certified. A certificate application of an external company is not allowed.

4.1.2 Enrollment process and responsibilities

Two procedures are possible for a certificate application: An automated, event-triggered process that runs without user interaction, and a manual process in which an end entity generates the key and the certificate application and submits these to the CA or an RA online or offline.

Three roles can be differentiated in these procedures, which do not necessarily have to be assumed by different parties:

- **CA Operators**
The operators of the CA must provide suitable interfaces that support one or both procedures (automated and manual).
- **Applicant**
This role describes the person that submits the application to the CA following a successful check and authentication of the subscriber. The applicant may be the actual subscriber or a registration authority (RA). An RA must provide the necessary interfaces to allow applications to be submitted to and received by the CA.
- **Subscriber**
The owner of a private key is the holder or subscriber of the corresponding certificate. He should trigger the process for a certificate application.

Enrollment of a Sub-CA (SAP Cloud Intermediate CA or SAP Cloud Issuing CA)


If a CA wants to be certified by the SAP Cloud Root CA, the service owner of this new CA must describe in a Certification Practice Statement how the CA is going to fulfill the requirements of this CP document. The CPS document must be created in accordance with [RFC 3647](#) and sent to SAP IT Security for approval. SAP IT Security must check that the CPS adheres to the requirements of this CP. The approval must be given in written form, must contain the name of the service owner as the contact person and must be archived by SAP IT Security.

Once the CPS is approved by SAP IT Security, the service owner of the new CA must open a SAP IT Ticket to the SAP PKI team who operate the SAP Cloud Root CA. The ticket must contain the following information:

- Reference to the approved CPS (name, OID, version, date)
- Subject name of the certificate request
- Certificate request of the Sub CA
- Contact name and SAP internal phone number or messenger and user ID that shall be used by the SAP PKI team for an out-of-band verification of the CSR's public key fingerprint

Before issuing a Sub-CA certificate, the PKI administrator of SAP Cloud Root CA must check the existing approval of the CPS and verify the fingerprint of the public key, as well as the content of the CSR with respect to:

- Distinguished name of the Subject as named in the SAP IT ticket
- Public Key Length as required in section 6.1.5



He must confirm the successful out-of-band fingerprint verification and affirmed CPS approval in the SAP IT Ticket. Operation of the SAP Cloud Root CA is only allowed according to a six-eyes principle (triple control) where employees from the SAP PKI team and from SAP IT Security must be present. The certification reply must then be returned in the SAP IT ticket response to the service owner of the new subordinate CA.

If a Sub-CA itself issues another subordinate CA certificate, it must ensure that the subordinate CA also fulfils all the requirements that are described in this CP document.

In case of a Sub-CA, key generation must be done decentralized by the certificate applicant.

Enrollment of an end entity

In case of an end entity, key generation should be done decentralized by the certificate applicant.

Only authorized applicants are allowed to request certificates. For automated processes, all certificate applicants must be granted privileges in order to submit a certificate application. It must be ensured that the privileges – e.g. authorization tokens – cannot be eavesdropped or misused.

The CA, an RA or some upstream processes must check the authentication of organization identity (cf. 3.2.2) and individual identity (cf. 3.2.3), where applicable. Subject names and SANs must not be re-used by a CA for different subscribers.

4.2 Certificate application processing

After a certificate application has been submitted to the CA/RA, an authorization check must be performed and the information must be verified. This can be performed automatically or manually.

All requests must be traceable, i.e. processing information must be stored e.g. in an appropriate database or in a log file for a period to be defined in the CPS. This period must be consistent with the retention period for audit logs (cf. 5.4.3).

4.2.1 Performing identification and authentication functions

The requirements for identification and authentication are described in section 3.

4.2.2 Approval or rejection of certificate applications

The decision about approval or rejection of a certificate application must be made a RA or by the CA who processes the certificate application.

Certificate requests must be rejected in case of missing signatures, failed verification of the certificate request, insufficient proof of identity, missing CPS or insufficient qualification of the PKI administrator of the Sub-CA.

4.2.3 Time to process certificate applications

A certificate application of a Sub-CA must be processed within ten working days at the latest, if all input requirements are met.

A certificate application of an end entity must be processed within two working days at the latest, if all input requirements are met.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The CA must issue the requested certificate and return it to the requestor or provide a certificate retrieval function.

All data generated in relation to the issuing of Sub-CA certificates as well as the Sub-CA certificate itself must be archived for a period to be defined in the CPS and consistent with the retention period for audit logs (cf. 5.4.3).

4.3.2 Notification to subscriber by the CA of issuance of certificate

No stipulation.



4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

No stipulation.

4.4.2 Publication of the certificate by the CA

No stipulation.

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 is only allowed to use its private key and certificate for appropriate applications as set forth in section 1.4 “Certificate Usage” and in consistency with applicable certificate content.

4.5.2 Relying party public key and certificate usage

A relying party is obligated to rely on certificates only for appropriate applications as set forth in section 1.4 “Certificate Usage” and in consistency with applicable certificate content. Before trusting a certificate with a validity of more than one week (i.e. no short-lived certificates), the relying party must check the status of the certificate using CRLs or OCSP.

4.6 Certificate renewal

Certificate renewal only extends the period of a certificate without changes being made to the cryptographic keys or any other information in the certificate. Such a process is only possible if the existing certificate is still valid and not revoked. Otherwise a new certificate application must be submitted as described in section 4.1.

This type of certificate extension is only allowed for CAs where the private key is protected by special hardware (HSM, SmartCards, TPM, etc.).

Certificate renewals for end entities are prohibited, new keys must always be generated (cf. 4.7).

4.6.1 Circumstance for certificate renewal

A certificate renewal may replace a regular key renewal of a CA before the CA certificate expires.

4.6.2 Who may request renewal?

Certificate renewals are possible by the same instances as described in section 4.1.1.

4.6.3 Processing certificate renewal requests

Processing certificate renewal requests shall be carried out the same way as for processing an initial request (cf. 4.1.2).

4.6.4 Notification of new certificate issuance to subscriber

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

No stipulation.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

There must be a regular key renewal in time before the public keys expires. Additionally, certificate re-key must take place when a certificate is revoked for reasons of key compromise, when information contained in a certificate has changed, when any of the cryptographic algorithm being used is no longer valid, or the key size has become too short.

4.7.2 Who may request certification of a new public key

A certificate request of a new public key must be submitted the same way as for the initial certificate application (cf. 4.1.1). Also, the enrollment process and responsibilities must be the same as for the initial request (cf. 4.1.2).

4.7.3 Processing certificate re-keying requests

Processing certificate re-keying requests must be carried out the same way as for processing an initial request (cf. 4.2).

In case of an end entity whose current certificate is still valid, the new certificate application may be signed with the current key and certificate for the purpose of identification and authentication of the subscriber (cf. 3.3.1).

4.7.4 Notification of new certificate issuance to subscriber

No stipulation.

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

No stipulation.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate modification

Certificate modification means that information needs to be changed that is contained in a certificate, for example a name change following a marriage.

Pure certificate modification is prohibited. New keys must always be generated when certificate content changes (cf. 4.7).

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

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

- Suspicion that the private key has been compromised
- Suspicion that a CA in the chain of trust has been compromised
- Reinstallation of systems
- Replacement of a valid certificate with a new one
- Operational shutdown of the system using the certificate
- Deactivation of a user or machine account
- Loss of a system or key
- Cessation of CA operation or the agreement between the SAP Cloud Root CA and a subordinate CA has been terminated

4.9.2 Who can request revocation

Any user can request revocation of his own certificate or the certificate of a device or service assigned to him (administrative contact, service owner, project manager, etc.).

Direct line managers or their managers may also apply for a revocation in the name of the end entity. In exceptional cases the responsible Security Officer may request revocation of an end entity certificate, too.

An HR process (person leaves the company, instant dismissal, etc.) can also lead to the justified revocation of a certificate.

4.9.3 Procedure for revocation request

If a Sub-CA issues end entity certificates with a validity of more than one week (i.e. no short-lived certificates), it must provide an option for round-the-clock (24x7) entering of revocation requests.

In order to revoke a Sub-CA certificate, the system owner of the Sub-CA must inform the PKI administrator of the SAP Cloud Root CA (SAP PKI team) via mail or telephone.

4.9.4 Revocation request grace period

After a reason for certificate revocation has occurred, the subscriber, i.e. a Sub-CA or an end entity has to request revocation as soon as possible.

4.9.5 Time within which CA must process the revocation request

A request to revoke a certificate has the highest processing priority as defined in the SAP internal standard SLAs for incident management.

Processing times must be defined in the CPS. They depend on the criticality of the certificate.

4.9.6 Revocation checking requirement for relying parties

Except of short-lived certificates, a relying party must rely on certificates only after checking the status of the certificate using CRLs or OCSP.

A CA must provide Relying Parties with information how to find the appropriate CRL or OCSP responder service in order to check certificates for their revocation status (cf. 7.1.2).

4.9.7 CRL issuance frequency (if applicable)

CRLs of an offline root CA may have far longer validity periods than issuing online CAs:

Publication Interval	Maximum six months
Overlap Period	Maximum two months
Life	Maximum eight months (publication interval + overlap period)

CRLs of issuing online CAs must be published far more often:

Publication Interval	Maximum seven days
Overlap Period	Maximum four days
Life	Maximum eleven days (publication interval + overlap period)

CRL entries of expired certificates can be deleted.

4.9.8 Maximum latency for CRLs (if applicable)

Within the operating hours the latency between the generation of CRLs and posting the CRLs to the PKI repository must be no more than 4 hours. It must be ensured at all times that there is one valid CRL in the PKI repository.



4.9.9 On-line revocation/status checking availability

Except for short-lived certificates, CRLs or an OCSP responder service must be available 24x7 to ensure that status requests can be processed at any time.

4.9.10 On-line revocation checking requirements

All relying parties must be able to evaluate one of the available status checking mechanisms.

4.9.11 Other forms of revocation advertisements available

There must not be any other form of revocation advertisements available.

4.9.12 Special requirements related to key compromise

If a subordinate CA suspects key compromise of its private key, the CA must request certificate revocation immediately and notify potential Relying Parties of an actual or suspected CA private key compromise.

4.9.13 Circumstances for suspension

Not applicable. Certificate suspension must not be used.

4.9.14 Who can request suspension

Not applicable. Certificate suspension must not be used.

4.9.15 Procedure for suspension request

Not applicable. Certificate suspension must not be used.

4.9.16 Limits on suspension period

Not applicable. Certificate suspension must not be used.

4.10 Certificate status services

4.10.1 Operational Characteristics

Revocation entries on a CRL or OCSP Response must not be removed until after the expiry date of the revoked certificate.

4.10.2 Service Availability

The CA must operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions. The CA must maintain an online 24x7 repository that application software can use to automatically check the current status of all unexpired certificates issued by the CA.

4.10.3 Optional Features

The private key of an OCSP responder must be protected by secure hardware (HSM, SmartCards, TPM, etc.).

4.11 End of subscription

if the SAP Cloud Root CA terminates its service, a confirmation of the end of subscription shall be sent via mail to the service owners of all Sub-CAs as soon as the end of subscription is known. The subordinate CA is requested to revoke all certificates, that are still valid, and issue a new CRL before its own CA certificate will be revoked by the SAP Cloud Root CA. After all subordinate CA certificates have been revoked the SAP Cloud Root CA must issue a new CRL.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

No stipulation.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable. There is no session key encapsulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

This section deals with non-technical security measures of the SAP Cloud PKI for applications with basic protection requirements. This includes building security, administrative and operational controls.

5.1 Physical Security Controls

The SAP Cloud PKI must be operated in a physically protected environment in order to prevent or at least detect unauthorized access to sensitive systems and loss of sensitive data.

The trust anchor of the SAP Cloud PKI (SAP Cloud Root CA & related HSM & related private key) must be kept “on premise” in the SAP data center.

Subordinate CAs of this PKI may be operated in SAP data center or at service provider data centers, if they have implemented adequate physical and infrastructure security measures according to this policy.

5.1.1 Site location and construction

All CAs operated by and for SAP must satisfy the highest security requirements. This also applies to building security. Systems of a PKI can only be operated in “*SAP Tier IV Level*” or comparable data center of a service provider. This is the highest security level under which SAP data centers operate.

5.1.2 Physical access

All data centers that house PKI components must be physically secured to ensure that only authorized personnel are granted access to the building.

The PKI components of the SAP Cloud Root CA must in addition be physically protected within the SAP data center to ensure that only those roles listed in section 5.2.1. can access the components. Appropriate measures may include specially secured cages or racks. These must not be protected by the same system that protects access to the building, but must be protected by a different concept (e.g. biometric system). Any exceptions, for example to allow manufacturers access to SAP Cloud Root CA for support purposes require an authorized person to be present at all times.

5.1.3 Power and air conditioning

Data centers must be equipped with a primary and a backup power system and a primary and backup air conditioning system in order to ensure access to electric power and to control the temperature in the data center.

5.1.4 Water exposures

Data centers must be constructed and equipped in a way preventing floods or other damaging water exposures.

5.1.5 Fire prevention and protection

Data centers must be secured in a way to prevent or extinguish fire and to protect against any other damaging exposure to flame or smoke.

5.1.6 Media storage

Media that contains critical information related to SAP Cloud PKI must be stored with the same physical and logical access controls that are used for the systems themselves.

5.1.7 Waste disposal

Confidential documentation and media that contains confidential information must be destroyed in such a way that they can longer be read or restored.

In the case of special cryptographic devices such as Hardware Security Modules (HSM) and SmartCards, the manufacturer’s instructions must be followed.

The general SAP disposal policies must also be followed.

5.1.8 Off-site backup

Regular backups must be made of all PKI-relevant components so that operation can be restored after failure of one or all components.



At least one copy must be kept in a separate location so that a destruction of the entire local infrastructure does not cause irreparable damage.

5.2 Procedural Controls

5.2.1 Trusted Roles

An authorization concept must distinguish between different trusted roles for technical PKI administration, CA operations, auditors and the service owner of the CA.

5.2.2 Number of Individuals Required per Task

The tasks associated with SAP Cloud Sub-CAs with basic protection requirements do not require several people to complete the task, i.e. no dual control.

This is not the case, however, for actions that directly apply to the SAP Cloud Root CA. In these cases, there must be at least three people to implement a six-eyes-principle. Examples of such tasks include issuing a Sub-CA certificate, a new CRL or critical security changes to the HSM systems.

5.2.3 Identification and Authentication for Trusted Roles

No stipulation.

5.2.4 Roles Requiring Separation of Duties

Auditing of a CA must be carried out by a role separate from configuration and operation of the CA.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Persons that assume a trusted role must be demonstrably qualified for this activity. Only internal employees of SAP or partners with several years history of working with SAP in long-term contracts may be considered.

All individuals must sign a declaration in which they agree to employ due care and attention when handling confidential data. This declaration also demands compliance with the described processes and knowledge of this certificate policy document.

5.3.2 Background Check Procedures

No stipulation.

5.3.3 Training Requirements and Procedures

Those who perform PKI-related activities must regularly participate in training courses. The following qualifications are particularly necessary:

- Basic knowledge of IT security and data protection
- PKI administration in general
- HSM administration (if applicable)

5.3.4 Retraining Frequency and Requirements

Ideally, training courses should be held annually to refresh employees' knowledge and to develop skills. It is important, however, that training is held as often as is necessary to ensure employees remain up-to-date with the latest developments and requirements.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Sanctions for unauthorized actions of a PKI administrator must be taken in accordance with the standard SAP policies. Any persons knowingly and seriously violating SAP policies must be released from their PKI-related roles.

5.3.7 Independent Contractor Controls

Suppliers contracted by SAP for short-term work on the PKI infrastructure must be accompanied and monitored by PKI employees and/or IT security personnel.

5.3.8 Documentation Supplied to Personnel

All persons with an SAP Cloud PKI role are required to read this certificate policy and all associated documentation (CPS, system documentation, operating guidelines, etc.). Other documentation relating to the role may also be required.

5.4 Audit Logging Procedures

All events that are related to the security of a CA system shall be recorded in audit log files. This includes the following data:

- Events related to operational processes
- Log data of the underlying system (network, operating system, appliances, etc.)
- Event logs of the application (CA, Web server, HSM, etc.)

This information must be stored and accessible in a central location. This data must be captured using suitable methods and technologies, which, in the case of processes, may even include handwriting.

5.4.1 Types of Events Recorded

All security-relevant events generated in systems of the PKI must be logged. These include, but are not limited to, the following information:

- Logon and logoff processes in the systems
- System logs in accordance with SAP hardening policies
- Events concerning lifecycle operations in the certificates of the CA itself and end entities. The lifecycle of a certificate includes:
 - Issue and extension
 - Revocation and deletion
 - Backup and archiving
- Special “key ceremony” of the root CA
- Backup/recovery of the systems and private PKI keys
- Events on cryptographic hardware modules
- Operationally-triggered changes to the systems in accordance with SAP change management processes
- Audit logs and results

All logs shall contain the date and time of the event, and the identity of the entity that caused the event, if possible.

Manually created logs must be countersigned by the persons involved.

5.4.2 Frequency for Processing and Archiving Audit Logs

All events with a criticality of at least “Warning” level (manufacturer’s classification) must trigger an alarm in the monitoring system on all systems of the PKI and must be checked and assessed by the PKI administrators. This ensures permanent event-driven monitoring of the log data.

5.4.3 Retention Period for Audit Logs

Log files of SAP Cloud Root CA must be stored for at least 1 year. Log files of Sub-CAs must be stored for at least 6 months.

5.4.4 Protection of Audit Log

Measures must be taken to protect the audit logs from unauthorized viewing, modification, or deletion.

5.4.5 Audit Log Backup Procedures

Event logs for online systems must be designed to ensure that there can never be more than one day's data loss at most.

Offline systems (root CA) must be backed up according to a defined process, and before or after any changes to the offline system.

5.4.6 Audit Log Accumulation System (internal vs. external)

The system for storing and monitoring events must be an external system, that is, it must be completely separate from the PKI system. Information can be collected via a locally installed agent or by a suitably remote readout process. Whichever method is used, however, the information must be protected from any manipulation.

5.4.7 Notification to Event-Causing Subject

Any events that trigger an alarm must be communicated to operators of the PKI.

In very serious cases, such as a compromised system or a failure of the service which makes the service unusable (e.g. the CRL publication failed), the SAP IT Emergency Management Process must be followed.

5.4.8 Vulnerability Assessments

The security of the system must be checked using both manual and automatic means. This must include:

- Port or Security Scans: The services available over the network must be subjected to regular and thorough security testing. Ideally, this will be automated using software.
- Network IDS/IPS: Systems that can be accessed from insecure network zones such as the Internet must also be secured by systems that monitor unauthorized access.
- Regular Audits: The system and operational processes must be regularly checked by external or internal audits.

5.5 Records Archival

Unlike logging, which also deals with general events, archiving concerns the entire history of service-relevant items in the system. Archiving for forensic analyses is not relevant here.

5.5.1 Types of Records Archived

The CA certificate, the last complete CRL and the CPS must be archived.

If the underlying use case of the issued certificates requires archival of information regarding the lifecycle of the issued certificates, the additional types of records to be archived must be defined in the CPS.

Paper-based documents as well as electronic data must be recorded in a way that their storage, preservation, and reproduction is always accurate and complete.

For the SAP Cloud Root CA the following data must additionally be archived:

- Backup of the CA private key
- Certificate and revocation requests from subordinate CAs

5.5.2 Retention Period for Archive

A Root CA must retain all documentation relating to certificate requests and the verification thereof, and all certificates and revocation thereof, for at least one year after any certificate based on that documentation ceases to be valid.

A Sub-CA must retain its CA certificate, the last complete CRL and the CPS for at least 6 months after its CA certificate ceases to be valid. In case of additional types of records to be archived their retention period must be defined in the CPS.



5.5.3 Protection of Archive

The archived records shall be protected against unauthorized viewing, modification, or deletion.

5.5.4 Archive Backup Procedures

If all of the data to be archived is covered by the general backup procedure for the CA, additional backup is not necessary. Otherwise, an archiving system must satisfy the additional requirements.

In case of possible cleanup processes, which remove invalid certificates from the production system, it must be ensured that the deadlines specified in section 5.5.2 are maintained.

If a CA terminates its service, the shutdown plan must describe what should happen to the archive.

5.5.5 Requirements for Time-stamping of Records

Event logs, archived data records, certificates, CRLs, and other entries must contain reliable time and date information. As such, all involved systems must coordinate their time keeping or synchronize with a central instance.

There are no requirements for a cryptographic time service in accordance with [RFC3161](#).

5.5.6 Archive Collection System (internal or external)

No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

No stipulation.

5.6 Key Changeover

The private key of a CA may only be used to issue certificates as long as the validity of the issued certificates is still within the validity timeframe of the issuing CA. Afterwards the certificate and the key of the CA must be renewed (re-key).

Special Case of Cross Certification of Root CA Certificates

When renewing a root CA certificate, it may be necessary for the old and new certificate to countersign each other (cross certification), so that the relying party can still accept certificates of the new root CA as being valid even if the new root CA certificate has not yet been added to the trusted root certification authorities.

5.7 Compromise and Disaster Recovery

CA failures must be resolved as quickly as possible to ensure that the service can resume normal operations.

All measures applicable for safeguarding operations (redundancy, HSM, geographic distribution, etc.) must be taken to minimize the risk of emergencies.

5.7.1 Incident and Compromise Handling Procedures

If a security-relevant incident is registered that is related to the SAP Cloud PKI, this must be escalated to the contact specified in section 1.5.2. Thereafter, the defined SAP processes for Incident and Emergency Management must be followed.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

If it is suspected that the CA system or parts of it are corrupted, SAP IT Security must be informed.

The time and the severity of the loss of integrity must be analyzed. The following procedure must be based on this information:

- If the time of the incident is known, and only the system is affected but not the key (because it is in secure hardware), all certificates issued by the affected CA since the time of the incident must be revoked.
- If the time is unknown, and only the system without the key is affected, all valid certificates of the CA must be revoked.
- If the key is also affected, proceed as described in section 5.7.3.



The system must also be returned to a clean state of integrity, and the cause of the incident must be resolved.

The entire process must follow the SAP Incident/Problem Management process.

5.7.3 Entity Private Key Compromise Procedures

If it is suspected that the private CA key is compromised, SAP IT Security must be informed.

If the incident affects a private key stored in secure hardware, a detailed analysis must be performed to determine whether this is a configuration error or security loophole in the product. Where necessary, the product must be changed.

If the private key of a subordinate CA is affected, all certificates that were issued must be revoked, followed by the revocation of the CA certificate itself issued by the Root CA.

In the case of the private Root CA key, all end entity certificates must be revoked by the all Sub-CAs, afterwards all Sub-CA certificates must be revoked by the Root CA. The Root CA must then be removed from the list of trusted root certification authorities on all systems of the relying parties.

The system must be returned to a clean state of integrity, and the cause of the incident must be resolved. Ultimately, this means that a new PKI must be created.

The entire process must follow the SAP Incident/Problem Management process.

5.7.4 Business Continuity Capabilities after a Disaster

A CA must document its disaster recovery procedures in the event of a disaster or a security compromise. The emergency plan must describe the fastest-possible recovery of the service.

The plan must be regularly tested by the CA administrator.

If a region cannot be used anymore following a natural catastrophe or similar event, remote restoration must be established at another location in accordance with a globally distributed backup and recovery concept. The new location may follow the original system configuration.

Where possible, areas susceptible to catastrophes that house PKI components must be monitored by security personnel at all times.

5.8 CA or RA Termination

If SAP is required to terminate operation of a CA or RA, all affected parties (subscribers, relying parties, etc.) must be informed early enough to ensure they can respond adequately.

The retention periods must be met for the PKI archives and logs as described in sections 5.4.4. and 5.5.2.

At the given time, the CA service owner must create a shutdown plan that among other things:

- Notifies the affected parties and trusted third parties of the cessation of operations
- Describes the continued support services
- Describes whether and how certificate information will continue to be issued
- Provides information about the revocation of certificates
- Defines rules regarding a successor CA
- Describes how the private keys and cryptographic modules are to be destroyed
- Archives the documentation and logs

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 required cryptographic strength of the generated keys and prevent the loss, disclosure, modification, or unauthorized use of private keys. As a minimum, software-based modules, but ideally, hardware-based cryptographic modules should be used to generate keys. These must at least comply with the requirements of the FIPS 140-2 Level 1 standard.

When operating a CA, Hardware Security Modules (HSMs) with security level FIPS 140-2 Level 2 must be used to protect the private keys.

A Root CA key must be created as part of a key ceremony, whose process must be logged and archived. The entire procedure must protect the keys from being compromised. The key ceremony must be witnessed by observers who shall validate that the process is conducted satisfactorily.

6.1.2 Private key delivery to subscriber

The keys for the actual PKI, that is, for the CAs, RAs, or OCSP responder must be created on the systems themselves so that there is no need for the keys to be transported. However, if the keys need to be transported for technical reasons, (clusters, and so on), appropriate protective mechanisms must be chosen that protect the integrity of the key. Keys may not be transferred using software-based protection.

Whenever possible, end entities shall generate the keys themselves, too. However, private keys of end entities may be transferred between systems using software-protected processes. Appropriate security controls must be in place that protect the integrity and prevent compromise and misuse of the private keys and their corresponding certificates.

6.1.3 Public key delivery to certificate issuer

The public key must be delivered to a CA in a way that the public key cannot be altered during transit. The certificate applicant must prove that he possesses the private key corresponding to the transferred public key.

6.1.4 CA public key delivery to relying parties

The Root CA certificate and the subordinate CA certificate - that contain the CA's public key - must be transmitted to the subscriber in a secure manner during the issuance and delivery of the subscriber's certificate.

In addition, each CA should publish its CA certificate on a web server and add a link to this CA certificate in every issued certificate (cf. 7.1.2. *Authority Information Access* field).

6.1.5 Key sizes

Key pairs must be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs. SAP follows the recommendations from NIST and BSI for key sizes. If the recommendations differ, the most cryptographically strong variant must be selected.

Key sizes must be selected so that the certificates can be accepted as being secure for the entire validity period. The SAP Security Policy determines the precise requirements. The selected key sizes must be outlined in the CPS. Any exceptions from the SAP Security Policy must have valid reasons and must be documented and assigned a risk assessment and acceptance.

6.1.6 Public key parameters generation and quality checking

For CAs, the quality of the generated key parameters must meet the requirements of FIPS 140-2 or of another equivalent standard, which defines the quality for generation of key parameters.

End entities must use cryptographic providers that are state of the art.

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

The key usage information in end entity certificates must not allow signing of certificates and CRLs (cf. 7.1.2).

The information must also comply with the requirements in section 1.4.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Private keys of certification authorities must be protected using Hardware Security Modules.

End entities are required as far as possible to protect their private keys against loss, disclosure, and unauthorized use in accordance with the SAP policies. In highly critical areas, this can and should be performed using hardware-supported cryptographic modules (TPMs, SmartCards, HSM, etc.).

6.2.1 Cryptographic module standards and controls

The standard to consider regarding requirements of cryptographic modules is FIPS PUB 140-2. The requirements apply to software-based (140-2 Level 1) and hardware-based modules (140-2 Level 2 and higher).

Any secure hardware (TPM, SmartCard, HSM, etc) must at least comply with FIPS 140-2 Level 2 or higher.

Cryptographic Service Providers (CSPs) for software-based modules should meet the requirements of FIPS 140-2 Level 1 as a minimum.

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

No multi-person control is required for access to Sub-CA's or end entities private keys.

6.2.3 Private key escrow

CA's or end entities private keys may not be deposited with a third-party instance.

6.2.4 Private key backup

The private key of the SAP Cloud Root CA must be backed up. Whether Sub-CA keys need to be backed up depends on the disaster and recovery plan of a CA.

In case of backed up CA keys, the backup must be equally protected as the live key. Among other things, this means:

- The key must only be accessible by authorized roles of the PKI
- The key must always be backed up in encrypted form
- The backup must be stored at a geographically different location from the CA
- For recovery of the private key from the SAP Cloud Root CA a six-eyes-principle is required. The key must never be accessible to a single person at any time in the recovery procedure.

Private keys of end entities do not need to be backed up because authentication functionality can be fully restored by revoking the lost certificate and issuing a new one. And they should not be backed up because this unnecessarily puts the private key at risk.

6.2.5 Private key archival

Beyond the backup of a CA's private key (cf. 6.2.4) there shall be no archival of a CA private key after the CA's private key usage period.

6.2.6 Private key transfer into or from a cryptographic module

Private keys may only be transported if the target system has the same level of protection as the system in which the key is located. This security level must be maintained at all times during the entire process, which also means that transfer path must be encrypted.

6.2.7 Private key storage on cryptographic module

CA keys must never be stored outside the cryptographic modules in unencrypted form. This means that the encrypted storage must be implicit throughout the system.

6.2.8 Method of activating private key

The prerequisites for activation, that is, access for the purposes of using a private key, depends on the type of PKI participant:

- **Root CA**
Measures must be taken to ensure that an individual person cannot perform actions on the key without such an action being noticed. The key must therefore be split cryptographically. Access to the individual fragments must also be protected by personalized or random PINs, which are entered on activation (cf. 6.4).
While the key is being used, one fragment must remain in the system, and access to the key must be blocked when the fragment is removed (SmartCard remains inserted)
The system must always remain offline, i.e. without a network connection.
- **Subordinate CAs**
For reasons of availability, private keys from issuing CAs must be available on another system following a system start or failover without any actions being required by the administrator. It must therefore be ensured that the key can only be accessed on the relevant systems and cannot be copied.
In the case of network-based solutions, some type of system authentication must ensure that only the CA systems have access.
- **End entities**
Keys for end entities must be protected in such a way that at least a specific context (User, Service Account, Machine, etc.) is used to activate the key, and it should only be possible to create the context by verification (password, SmartCard, certificate, etc.).

6.2.9 Method of deactivating private key

The method of deactivating the private key depends on the type of PKI participant:

- **Root CA**
The Root CA is always accessed within an active user session. If this user session ends, access to the key must be blocked. This is generally the case following a logoff or shutdown of the system.
If the system loses access to the key fragment that is required for activation, access to the key must be deactivated.
If the system loses the connection to the HSM, key access must be blocked.
- **Subordinate CAs**
Access to the key must be deactivated if the cryptographic module becomes unavailable or following a logoff or shutdown of the system.
- **End entities**
Access must be deactivated when a user session ends.

6.2.10 Method of destroying private key

In case of CA keys, all locations at which the key is stored in any form must be deleted securely with verifiable evidence (using the latest technology).

End entities must ensure that their private keys are destroyed in a way that prevents their loss, theft, modification, or unauthorized use.

6.2.11 Cryptographic Module Rating

See section 6.2.1

6.3 Other aspects of key pair management

6.3.1 Public key archival

The operational requirements for archiving public keys are described in section 5.5.

Within the context of forensic analyses, longer archiving may be useful or even required for compliance reasons. Longer terms depend on the application and are not within the scope of this document.

6.3.2 Certificate operational periods and key pair usage periods

The lifetime of a certificate must never exceed the expected security of the used cryptographic keys and key sizes (cf. 6.1.5). The lifetime of keys is determined by SAP Security Policy.

A CA must never issue certificates that are valid for longer than the issuing certificate itself. I.e. the private key of a CA may only be used for signing subordinate certificates as long as the whole validity period of the subordinate certificates would be within the validity period of the CA certificate. Afterwards the private key may only be used for signing CRLs.

If the keys of a CA certificate are still good and there is no need for any other attribute change of the CA certificate, a renewal using re-certification as described in section 4.6 is possible. However, for the next renewal of the same renewed CA, a re-key renewal as described in section 4.7 is required. As a result of this re-key method, there is a phase of overlapping in which two CRLs must be issued; one by the certificate of the expiring, but still valid CA, and one by the new CA. The OCSP responder must be rebuilt for the renewed CA. In case of a Root CA renewal with re-key, both Root CAs must be available as trusted resources on the clients for the overlap period.

6.4 Activation data

6.4.1 Activation data generation and installation

See section 6.2.8

The requirements for the passphrase of the administrator account to access a CA are determined by SAP Security Policy.

6.4.2 Activation data protection

The administrators of SAP Cloud PKI and its subscribers must ensure that any activation data is kept confidential for private keys and is never disclosed to third parties.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

All systems of the SAP Cloud PKI must be secured using the latest technology and in accordance with the *Best Practices* information of the manufacturer for their intended purpose. The SAP-internal and general public security standards must also be followed where relevant.

6.5.1 Specific computer security technical requirements

Requirements include the following measures for ensuring the system security of the PKI components:

- Physical and digital access to the systems is permitted only for trusted persons that require such access for performing their PKI role.
- Wherever possible, antivirus and antimalware products must be installed and operated by SAP and checked regularly for irregularities.
- Complex passwords must be used for the user accounts that comply with the SAP password policies. There are no time limits for password validity for offline machines.
- All systems must be locked or shut down when not in use.

6.5.2 Computer security rating

Security measures must be applied according to the SAP policies for high-security systems.



6.6 Life cycle technical controls

6.6.1 System development controls

No stipulation.

6.6.2 Security management controls

All PKI systems must be regularly checked by SAP IT to ensure that they comply with the required policies. This includes the following methods:

- Event monitoring, collection, and inspection in a central location
- Recurring penetration test for externally visible components
- Central configuration management and regular refreshing of components wherever possible

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

The PKI systems must be operated in dedicated network segments that are separated by firewalls. As a minimum, the network segments “external”, “DMZ”, and “internal” must be differentiated, and the PKI segment must also be separated from the Office network.

Only the protocols required for the function of the PKI may be exchanged between the segments. Dedicated *Jump Hosts* that require two-factor authentication for user logons must be used for all administrative tasks.

Intrusion Detection systems must be used to monitor network traffic to the PKI systems for components that can be accessed externally.

6.8 Time-stamping

No stipulation.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

The SAP Cloud PKI with basic protection must issue certificates in accordance with the following standards:

- ITU-T recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, Oct 2016
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008

7.1.1 Version Numbers

All certificates within the SAP Cloud PKI must be compliant to X.509 version 3 (Type 0x02).

7.1.2 Certificate Extensions

According to RFC 5280 a certificate using system must reject a certificate if it encounters a critical extension it does not recognize, or a critical extension that contains information that it cannot process. A non-critical extension may be ignored if it is not recognized, but must be processed if it is recognized.

Certificate extensions must strictly follow the requirements of RFC 5280.

All extensions used must be listed and explained in the CA's CPS including criticality.

Subordinate CAs:

All CA certificates that are subordinate to the SAP Cloud Root CA must include the following X.509v3 extensions:

- *keyUsage* (2.5.29.15) with only the *keyCertSign* and *cRLSign* bits set (marked as critical)
- *basicConstraints* (2.5.29.19) with the *CA* bit set to *TRUE* and a path length constraint of 0 or 1 (marked as critical). There must be no more than two levels of Sub-CAs.
- *subjectKeyIdentifier* (2.5.29.14) containing the key identifier of the own public key (marked as non-critical)
- *authorityKeyIdentifier* (2.5.29.35) containing the reference to the *subjectKeyIdentifier* of the issuing CA (marked as non-critical)
- *cRLDistributionPoints* (2.5.29.31) with the URL(s) to retrieve the CRL (marked as non-critical)
- *authorityInfoAccess* (1.3.6.1.5.5.7.1) with the *accessMethod* *id-ad-calssuer* containing the URL(s) to retrieve the issuing CA's certificate (marked as non-critical)

Other certificate extensions may be used in CA certificates as long as their usage is described in the CA's CPS document and it complies to RFC 5280.

End entities:

All end entity certificates within the SAP Cloud PKI must not use the *keyCertSign* and *cRLSign* bits within the *keyUsage* extension and must not use the *basicConstraints* extension with the *CA* bit set to *TRUE*.

They must include the following X.509v3 extensions:

- *keyUsage* (2.5.29.15) with the *digitalSignature* and optionally the *keyEncipherment* bit set (marked as critical)
- *ExtendedKeyUsage* (2.5.29.37) containing the key usage purpose *id-kp-serverAuth* and/or *id-kp-clientAuth* (marked as either critical or non-critical)
- *authorityKeyIdentifier* (2.5.29.35) containing the reference to the *subjectKeyIdentifier* of the issuing CA (marked as non-critical)

They should include the following X.509v3 extensions:

- *subjectKeyIdentifier* (2.5.29.14) containing the key identifier of the own public key (marked as non-critical)

- *authorityInfoAccess* (1.3.6.1.5.5.7.1) with the *accessMethod* *id-ad-calssuer* containing the URL(s) to retrieve the issuing CA's certificate (marked as non-critical)

If the CA issues CRLs, it must additionally include the following X.509v3 extension:

- *cRLDistributionPoints* (2.5.29.31) with the URL(s) to retrieve the CA's CRL (marked as non-critical)

If the CA offers an OCSP service, it must additionally include the following X.509v3 extension:

- *authorityInfoAccess* (1.3.6.1.5.5.7.1) with the *accessMethod* *id-ad-ocsp* containing the URL of the OCSP responder service (marked as non-critical)

TLS Server certificates must additionally include:

- *SubjectAltName* (2.5.29.17) with at least one FQDN or IP address (marked as non-critical)

Other certificate extensions may be used in end entity certificates as long as their usage is described in the CA's CPS document and it complies to RFC 5280.

7.1.3 Algorithm Identifier (OID)

The algorithm used must be deemed secure for the validity period of the issued certificates. The name and OID number of the signature algorithm used when issuing certificates must be documented in the CA's CPS, e.g. Name = sha256WithRSAEncryption, OID = 1.2.840.113549.1.1.11

7.1.4 Name Forms

See section 3.1.1

7.1.5 Name Restrictions

No stipulation.

7.1.6 Identifiers for Certification Policies (OID)

No stipulation.

7.1.7 Use of Extensions to the Policy Constraints

No stipulation.

7.1.8 Syntax and Semantics of Policy Qualifiers

No stipulation.

7.1.9 Processing of Critical Extensions for Certificate Policies

No stipulation.

7.2 CRL profile

If CRLs are issued, the SAP Cloud PKI with basic protection must issue CRLs in accordance with the following standards:

- ITU-T recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, Oct 2016
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008

7.2.1 Version number(s)

All CRLs within the SAP Cloud PKI must be compliant to X.509 version 2 (Type 0x01).

7.2.2 CRL and CRL entry extensions

RFC 5280 requires "if a CRL contains a critical extension that the application cannot process then the application must not use that CRL to determine the status of certificates. However, applications may ignore unrecognized non-critical extensions".

CRL and CRL entry extensions must strictly follow the requirements of RFC 5280.



All CRL and CRL entry extensions used must be listed and explained in the CA's CPS including criticality.

CRL extensions:

All CRLs that are issued within the SAP Cloud PKI must include the following CRL extensions:

- *authorityKeyIdentifier* (2.5.29.35) containing the reference to the subjectKeyIdentifier of the issuing CA (marked as non-critical)
- *cRLNumber* (2.5.29.20) with a monotonically increasing sequence number (marked as non-critical)

Other CRL extensions may be used as long as their usage is described in the CA's CPS document and it complies to RFC 5280.

CRL entry extensions:

All CRLs that are issued within the SAP Cloud PKI must include the following CRL entry extension:

- *Reason Code* (2.5.29.21) identifying the reason for the certificate revocation (marked as non-critical)

It's recommended to also include the following CRL entry extension:

- *Invalidity Date* (2.5.29.24) indicating the date when it was known or suspected that the private key was compromised or that the certificate otherwise became invalid

7.3 OCSF profile

7.3.1 Version number(s)

OCSF requests and responses must be created in accordance with RFC 6960. OCSF responses must use the basic response type *id-pkix-ocsp-basic*.

7.3.2 OCSF extensions

No stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

The SAP Cloud Root CA as well as subordinate CAs shall be assessed every three years. For the SAP Cloud Root CA and its directly subordinate CA this is coordinated by the IT Security department.

In addition to the normal audits, the following reasons may trigger an unplanned check:

- Suspicion of compliance violations
- Requirement coming from a business case where certificates from SAP Cloud PKI are used
- Entry into partnership agreements with other PKI operators, for example Cross Certification with other CAs

8.2 Identity/qualifications of assessor

Audits of the SAP Cloud PKI may be carried out either internally by SAP or independently by external auditors that do not belong to the company. The auditors must all be qualified auditors with PKI experiences.

8.3 Assessor's relationship to assessed entity

In the event of internal checks, the audit may not be carried out by the operator of the PKI. It must be performed by independent SAP employees.

External audits are performed by qualified and independent third parties.

8.4 Topics covered by assessment

The auditors must be able to decide freely which areas of the PKI are to be checked. At the very least, the certification policy and the requirements therein must be part of the audit. In particular, the following aspects must be checked:

- Certificate management processes
- Physical security controls
- Procedural controls, in particular authorization and role concept
- Personnel controls
- Technical security controls
- Disaster recovery plan

8.5 Actions taken as a result of deficiency

The actions to be taken as a result of a deficiency must be defined in close consultation between the auditor and the CA being audited. The CA being audited shall correct the problems causing the deficiencies within a reasonable time frame.

If a deficiency has been found at the SAP Cloud Root CA or a subordinate CA, which poses an immediate threat to the security and integrity of the whole SAP Cloud PKI, the CA service owner together with SAP IT Security must determine which steps to take and whether revocation of the respective CA is necessary.

Findings with average impact on the security of PKI operations must be addressed and resolved within a reasonable period. In serious cases, the action plan must be compiled as quickly as possible. If necessary, temporary workarounds may be implemented if the solution to the problem cannot be implemented immediately.

8.6 Communication of results

The results of a SAP Cloud PKI audit must be kept secure. However, full results or extracts thereof may be made accessible to internal departments or partners on request. The process is subject to supervision by SAP IT Security.



9 OTHER BUSINESS AND LEGAL MATTERS

The usage of this PKI and related certificates is restricted for SAP users only (SAP Employees and contractors owning a SAP userID) and is restricted for equipment which is SAP owned or provided exclusively to SAP. Generally, SAP internal regulations and standards apply, as well as agreements and contracts with affected external parties.

9.1 Fees

9.1.1 Certificate issuance or renewal fees

No stipulation.

9.1.2 Certificate access fees

No stipulation.

9.1.3 Revocation or status information access fee

No stipulation.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

No stipulation.

9.2 Financial Responsibility

SAP is not liable to third parties for financial damages caused by use of the service.

9.2.1 Insurance coverage

No stipulation.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

All information obtained during a process related to the lifecycle of a certificate, and which is not listed under section 9.3.2. must be assigned a minimum of SAP information classification "internal".

9.3.2 Information not within the scope of confidential information

All information that forms part of a certificate, of a CRL, or is publicly accessible to others is classified as non-confidential.

9.3.3 Responsibility to protect confidential information

Measures for protecting confidential data are described in the classification level in accordance with the current SAP information classification policy.

9.4 Privacy of personal information

9.4.1 Privacy plan

The general SAP policy concerning data protection applies.

9.4.2 Information treated as private

The SAP data protection policy defines which information is to be classified as personal data.

9.4.3 Information not deemed private

See 9.3.2

9.4.4 Responsibility to protect private information

Measures for protecting personal data are described in the classification level in accordance with the current SAP information classification policy.

9.4.5 Notice and consent to use private information

No stipulation.

9.4.6 Disclosure pursuant to judicial or administrative process

As required by the governing legislation.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

All rights remain with SAP.

Unmodified, free of charge, and nonexclusive distribution of all published information does not require any express prior approval by SAP.

9.6 Representations and warranties

9.6.1 CA representations and warranties

The operator of a certification authorities within SAP Cloud PKI agrees to act in accordance with the certificate policies described in this document.

9.6.2 RA representations and warranties

RAs are obliged to observe this certificate policy and to employ the necessary level of care and attention in all actions.

All information provided by subscribers and other service users must be checked for accuracy according to the best will and knowledge.

The operator of the registration authority agrees not to provide knowingly incorrect information to the CA.

9.6.3 Subscriber representations and warranties

Subscribers own the private key to the certificates. This key must be held confidential in accordance with SAP data classification policies. Subscribers agree to protect and use the private key carefully. This includes:

- Not using the key before the certificate has been issued by the CA
- Not duplicating the key or transporting it via insecure channels
- Not continuing to use the key after expiry or revocation of the certificate

Furthermore, all information submitted in the certificate application must be truthful.

Certificates may be used only if valid and in accordance with their intended purpose (cf. 1.4); in particular, the certificate may not be used as a certification authority certificate. The subscriber is forbidden from misusing or illegally using the certificate and cryptographic key and must report any such usage to the responsible body immediately.

Except for short-lived certificates, the certificate must be revoked if it is lost, if there is suspicion of compromise, or if data in the certificate is changed, for example a change of surname.

The subscriber agrees to act in accordance with this policy and will be liable for the possible legal consequences that may result from improper actions.

SAP reserves the right to enter into other agreements separate to this certificate policy with end entities.

9.6.4 Relying party representations and warranties

Relying Parties are obliged to perform an RFC 5280 compliant check of the validity of SAP Cloud PKI certificates. In particular, the entire chain of trust must be validated through to the root certification authority including all interim CAs.

Except for short-lived certificates, certificates must be checked with regard to their revocation status. The *Online Certificate Status Protocol* (OCSP) is always preferable to CRLs. Only if the OCSP service is unavailable or unsupported by the application, CRLs should be used.

The relying party agrees to trust certificates only for the purposes explicitly stated in the certificate (*Key Usage* or *Extended Key Usage*).

If the check returns a negative, i.e. invalid result, the corresponding process must be terminated.

If the relying party suspects that a certificate has been misused, he must notify the responsible bodies as soon as possible. In such a case, even a technically valid certificate must no longer be deemed trusted.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

No stipulation.

9.8 Limitation of liability

No stipulation.

9.9 Indemnities

No stipulation.

9.10 Term and termination

9.10.1 Term

This policy is effective at the time of its publication.

9.10.2 Termination

The certificate policy may become ineffective no earlier than the cessation of operations plus the time for which the PKI-related data must be archived.

9.10.3 Effect of termination and survival

All agreements on (SAP) standards, legal obligations, and so on remain unaffected by the termination.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for amendment

In all cases, the currently valid certificate policy is the policy that is published at the following Web site:
<http://www.pki.co.sap.com/>

Changes automatically invalidate any preceding policies, and the updated version must be made accessible at the same location, and given a hierarchically ascending version number and publication date.

Previous versions must continue to be available.

For more information, see section 1.5.1.

9.12.2 Notification mechanism and period

No stipulation.



9.12.3 Circumstances under which OID must be changed

Extensive changes that represent an entirely new basis for the scope of the certificate policy require a change to the OID belonging to the policy (see 1.2).

9.13 Dispute resolution provisions

No stipulation.

9.14 Governing Law

Operation of SAP Cloud PKI is subject to the law of the Federal Republic of Germany and the European Union (EU).

9.15 Compliance with the applicable law

In cases of doubt, the governing law always takes precedence over the specifications in this document.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

Should any provision of this CP document be or become ineffective or unenforceable, the validity of the remaining policy remains unaffected. The ineffective or unenforceable provision must be replaced by an effective and enforceable provision that achieves as nearly as possible the parties' intended business purposes in the ineffective or unenforceable provision. These provisions will also apply, with the necessary modifications, if this agreement has any gaps.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other Provisions

No stipulation.