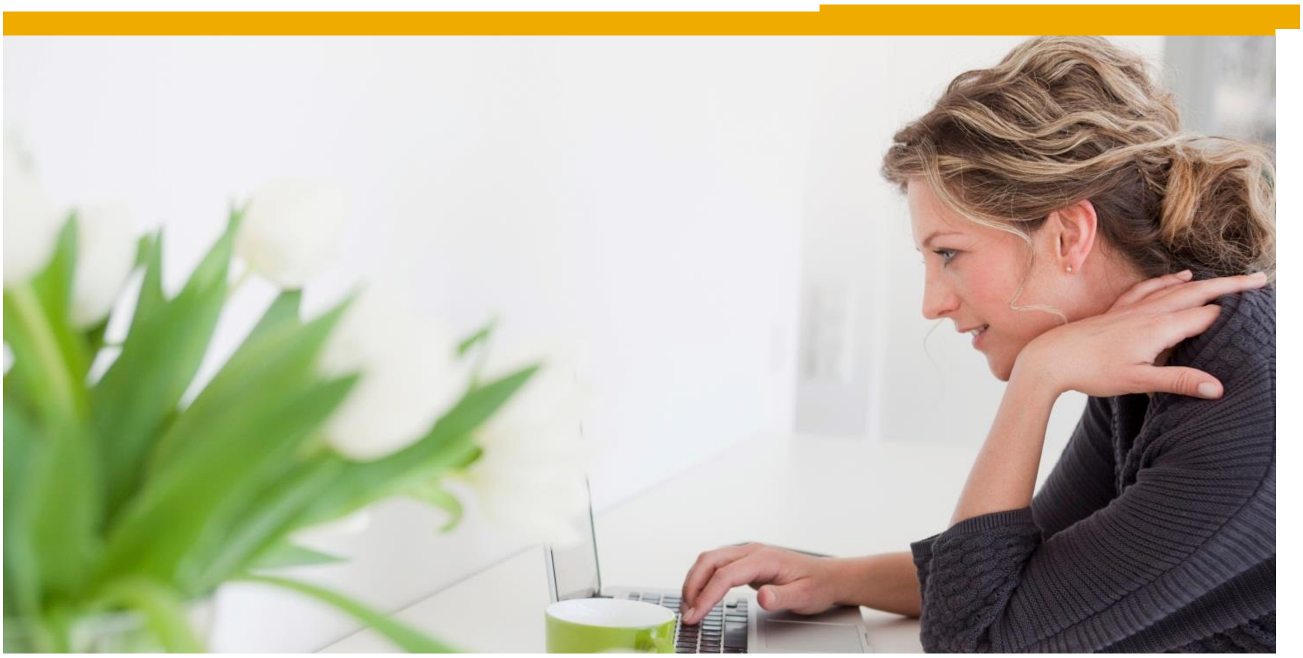


SAP Global PKI Zertifizierungsrichtlinie (Certificate Policy – CP)

INFORMATION ABOUT THE DOCUMENT

Overview

Title of Document	SAP Global PKI Zertifizierungsrichtlinie (Certificate Policy – CP)
File name	SAP-PKI-CP-v1-English.docx
Description	Certificate Policy of SAP Global PKI Based on RFC 3647
Version	1.1
Object Identifier	OID 1.3.6.1.4.1.694.4.100.2
Retired documents	None
Authors	Walther, Ralf; Hackenschmidt, Chrstopher; Rothländer, Christian
Responsible contacts at SAP	Christian Rothländer

Document History

Version	Date	Comment
0.1	1/23/2013	Complete new version in German based on the English document from Mr. Höltkemeier (Microsoft)
0.91	September 16, 2013	Final version (without LEGAL involvement Ch. 9.x)
0.95	April 29, 2014	Final version (with LEGAL agreed)
1.0	13.05.2014	For publishing (including Code Signing Topic)
1.1	December 9th, 2016	Updates: Org unit Security 1.5, CA housing 5.1, Validity of Certificates 6.3.2

TABLE OF CONTENTS

1 INTRODUCTION 10
1.1 Overview 10
1.2 Document Name and Identification 11
1.3 Participants in the Certification Infrastructure (PKI) 11
1.3.1 Certification Authorities 11
1.3.2 Registration Authorities 11
1.3.2.1 Online Registration 12
1.3.2.2 Offline Requirement 12
1.3.3 Certificate Subscribers 12
1.3.4 Relying Parties 12
1.3.5 Other Participants 12
1.4 Application Area 12
1.4.1 Suitable Certificate Usage 13
1.4.2 Restricted Certificate Usage 13
1.4.3 Forbidden Certificate Usage 13
1.5 Administration of the Certificate Policy 13
1.5.1 Change Management 13
1.5.2 Contacts 13
1.5.3 Checking Suitability for Regulations Governing the Certification Practice Statement (CPS) in Accordance with the Certificate Policy 14
1.5.4 Procedures for Recognizing Regulations for the Certification Practice Statement (CPS) 14
1.6 Definitions and Abbreviations 14
1.6.1 Abbreviations 14
1.6.2 Definitions 14
2 PUBLICATIONS AND DIRECTORY SERVICE 15
2.1 Directory Services 15
2.2 Publication of Certificate Information 15
2.3 Updating of the Information (Time, Frequency) 15
2.4 Controlling Access to Directory Services 15
3 IDENTIFICATION AND AUTHENTICATION 16
3.1 Names 16
3.1.1 Name Forms 16
3.1.1.1 CA Certificates 16
3.1.1.2 Domain Controller Certificates 16
3.1.1.3 Server Certificates (incl. DC and OCSP) 16
3.1.1.4 Code Signing Certificates (SAP internal) 17
3.1.1.5 User Certificates 17
3.1.2 Informativeness of Names 17
3.1.3 Anonymity or Pseudonyms of Subscribers 18
3.1.4 Rules for Interpretation of Different Name Formats 18

3.1.5 Uniqueness of Names 18
3.1.6 Recognition, Authentication, and Function of Trademarks 18
3.2 Identify Check in New Applications 18
3.2.1 Verification of the Ownership of a Private Key 18
3.2.2 Authentication of an Organization 18
3.2.3 Authentication of Natural Persons 18
3.2.4 Non-Verified Participant Information 18
3.2.5 Checking Authorization 18
3.2.6 Criteria for Collaboration 19
3.3 Identification and Authentication during Certificate Renewal 19
3.3.1 Routine Certificate Renewal 19
3.3.2 Certificate Renewal after a Block 19
3.4 Identification and Authentication of Block Applications 19
4 PROCESS ORGANIZATION (Certificate Lifecycle) 20
4.1 Certificate Application 20
4.1.1 Who Can Apply for a Certificate? 20
4.1.2 Procedures and Responsibilities 20
4.2 Processing Certificate Applications 20
4.2.1 Execution of the Identification and Authentication 20
4.2.2 Acceptance or Rejection of Certificate Applications 20
4.2.3 Processing Time for Certificate Applications 20
4.3 Certificate Issuance 21
4.3.1 Tasks of the Certification Authority 21
4.3.2 Notifying the Applicant 21
4.4 Certificate Acceptance 21
4.4.1 Acceptance of the Certificate 21
4.4.2 Publication of the Certificate by the Certification Authority 21
4.4.3 Notification of Further Instances by the Certification Authority 21
4.5 Use of the Key Pair and Certificate 21
4.5.1 Use by the Subscriber 21
4.5.2 Use of the Certificate by the Relying Party 21
4.6 Certificate Renewal on Retention of the old Key (Re-Certification) 22
4.6.1 Reasons for Certificate Renewal 22
4.6.2 Who Can Apply for a Certificate Renewal? 22
4.6.3 Expiry of the Certificate Renewal 22
4.6.4 Notification of Subscriber Following Certificate Renewal 22
4.6.5 Acceptance of a Certificate Renewal 22
4.6.6 Publication of a Certificate Renewal by the Certification Authority 22
4.6.7 Notification of Further Instances by the Certification Authority 22
4.7 Key and Certificate Renewal (Re-Key) 22
4.7.1 Reasons for a Key and Certificate Renewal 22

4.7.2 Who Can Apply for a Key and Certificate Renewal? 22

4.7.3 Process for Key and Certificate Renewal 22

4.7.4 Notifying the Subscriber 22

4.7.5 Acceptance of the Key and Certificate Renewal 22

4.7.6 Publication of a Certificate Renewal by the Certification Authority 23

4.7.7 Notification of Further Instances by the Certification Authority 23

4.8 Certificate Modification 23

4.8.1 Reasons for Certificate Modification 23

4.8.2 Who Can Apply for a Certificate Modification? 23

4.8.3 Process of Certificate Modification 23

4.8.4 Notifying the Subscriber 23

4.8.5 Acceptance of the Certificate Modification 23

4.8.6 Publication of a Certificate Modification by the Certification Authority 23

4.8.7 Notification of Further Instances by the Certification Authority 23

4.9 Revocation/Blocking and Suspension of Certificates 23

4.9.1 Reasons for Revocation/Blocking 23

4.9.2 Who Can Apply for a Revocation/Block? 23

4.9.3 Process for Revocation / Block 24

4.9.4 Deadlines for the Subscriber 24

4.9.5 Processing Deadlines for the Certificate Authority 24

4.9.6 Request for Block Checks by a Relying Party 24

4.9.7 Frequency of Block List Publication 24

4.9.8 Maximum Latency Time for Block Lists 24

4.9.9 Availability of Online Status Requests 24

4.9.10 Requirements for Online Status Requests 24

4.9.11 Other Available Forms of Announcing Revocations 25

4.9.12 Requirements in the Event of Compromise of Private Keys 25

4.9.13 Reasons for Suspension 25

4.9.14 Who Can Apply for a Suspension? 25

4.9.15 Process for a Suspension 25

4.9.16 Maximum Block Duration for a Suspension 25

4.10 Service for Status Request of Certificates (OCSP) 25

4.10.1 Operation-Specific Attributes 25

4.10.2 Availability of the Service 25

4.10.3 Other Features 25

4.11 Termination of the Contractual Relationship 25

4.12 Key Escrow and Recovery 25

4.13 Policies and Practices for Key Escrow and Recovery 25

4.14 Policies and Practices for Protecting and Recovering Session Keys 25

5 INFRASTRUCTURAL, ORGANIZATIONAL, AND PERSONNEL SECURITY MEASURES 26

5.1 Infrastructural Security Measures 26

5.1.1 Area of Deployment and Design 26
5.1.2 Access 26
5.1.3 Power Supply and Air-Conditioning Systems 26
5.1.4 Risk of Water Damage 26
5.1.5 Fire Prevention 26
5.1.6 Storage of Data Carriers 26
5.1.7 Disposal 26
5.1.8 External Data Backup 26
5.2 Organizational Security Measures 27
5.2.1 Roles Concept 27
5.2.2 Number of Persons Involved per Task 27
5.2.3 Identification and Authentication of each Role 27
5.2.4 Roles that Require Separation of Tasks 27
5.3 Personnel Security Measures 27
5.3.1 Requirements for Employees 27
5.3.2 Security Check of Employees 27
5.3.3 Training Requirements 27
5.3.4 Frequency and Requirements of Further Training 27
5.3.5 Frequency and Process of Work Center Switches 28
5.3.6 Penalties for Unauthorized Actions 28
5.3.7 Requirements for Independent Suppliers 28
5.3.8 Documentation for Personnel 28
5.4 Monitoring / Logs 28
5.4.1 Monitored Events 28
5.4.2 Frequency of the Log Analysis 29
5.4.3 Storage Period for Log Data 29
5.4.4 Protecting Log Data 29
5.4.5 Backup of Log Data 29
5.4.6 Monitoring System (Internal or External) 29
5.4.7 Notification of the Event Trigger 29
5.4.8 Weakpoint Analysis 29
5.5 Archiving 29
5.5.1 Archived Data 29
5.5.2 Storage Period for Archived Data 30
5.5.3 Protection of the Archive 30
5.5.4 Backup of the Archive (Data Backup Concept) 30
5.5.5 Requirements for Time Stamps 30
5.5.6 Archiving System (Internal or External) 30
5.5.7 Procedures for Retrieving and Checking Archived Data 30
5.6 Change of Key of the Certification Authority 30
5.7 Compromise and Recovery (Disaster Recovery) 30

5.7.1 Procedure for Security Incidents and Compromised Certificates 30
5.7.2 Resources, Software, and/or Data are Corrupted 30
5.7.3 Compromised Private Key 31
5.7.4 Resumption of Operations after an Emergency 31
5.8 Suspension of Operations 31
6 TECHNICAL SECURITY MEASURES 32
6.1 Key Generation and Installation 32
6.1.1 Key Generation 32
6.1.2 Transferring the Private Key to the Subscriber 32
6.1.3 Transfer of Public Key to the Certificate Issuer 32
6.1.4 Transfer of Public CA Key to Relying Parties 32
6.1.5 Key Lengths 32
6.1.6 Generating the Public Key Parameters and Quality Assurance 32
6.1.7 Key Usage Purposes (X.509v3) 33
6.2 Protection of Private Keys and Use of Cryptographic Modules 33
6.2.1 Standard of Cryptographic Modules 33
6.2.2 Distributing Private Keys across Multiple Persons (n-from-m) 33
6.2.3 Depositing Private Keys (Key Escrow) 33
6.2.4 Backup of Private Keys 33
6.2.5 Archiving of Private Keys 33
6.2.6 Transfer of Private Keys to or from a Cryptographic Module 34
6.2.7 Storage of Private Keys in a Cryptographic Module 34
6.2.8 Activation of Private Keys 34
6.2.9 Deactivation of Private Keys 34
6.2.10 Destruction of Private Keys 34
6.2.11 Quality of Cryptographic Modules 34
6.3 Other Aspects of Key Management 34
6.3.1 Archiving Public Keys 34
6.3.2 Validity of Certificates and Key Pairs 35
6.4 Activation Data 36
6.4.1 Generating and Installing the Activation Data 36
6.4.2 Protection of Archiving Data 36
6.4.3 Other Aspects 36
6.5 Security Measures for Computers 36
6.5.1 Specific Requirements for Technical Security Measures 36
6.5.2 Quality of Security Measures 36
6.6 Technical Measures in the Lifecycle 37
6.6.1 Measures in System Development 37
6.6.2 Measures in Security Management 37
6.6.3 Lifecycle of Security Measures 37
6.7 Security Measures for the Network 37

6.8 Time Stamps 37

7 PROFILES FOR CERTIFICATES, BLOCK LISTS AND ONLINE STATUS QUERIES 38

7.1 Certificate Profile 38

7.1.1 Version Numbers 38

7.1.2 Certificate Extensions 38

7.1.3 Algorithm Identifier (OID) 38

7.1.4 Name Forms 38

7.1.5 Name Restrictions 38

7.1.6 Identifiers for Certification Policies (OID) 38

7.1.7 Use of Extensions to the Policy Constraints 38

7.1.8 Syntax and Semantics of Policy Qualifiers 38

7.1.9 Processing of Critical Extensions for Certificate Policies 38

7.2 Block List Profile 39

7.2.1 Version Numbers 39

7.2.2 Block Lists and Block List Entry Extensions 39

7.3 OCSP Profile 39

7.3.1 Version Numbers 39

7.3.2 OCSP Extensions 39

8 CONFORMITY CHECK (Compliance Audit, Assessments) 40

8.1 Frequency and Circumstances of the Check 40

8.2 Identity and Qualification of the Auditor 40

8.3 Relation of the Auditor to the Audited Material 40

8.4 Audited Areas 40

8.5 Resolving Defects 40

8.6 Publication of Results 40

9 OTHER BUSINESS AND LEGAL MATTERS 41

9.1 Fees 41

9.1.1 Fees for Creating or Renewing Certificates 41

9.1.2 Fees for Accessing Certificates 41

9.1.3 Fees for Blocks or Status Requests 41

9.1.4 Other Fees 41

9.1.5 Fee Compensation 41

9.2 Financial Responsibility 41

9.2.1 Compulsory Cover 41

9.2.2 Other Assets 41

9.2.3 Insurance or Guarantee for End Participants 41

9.3 Confidentiality of Business Information 41

9.3.1 Confidential Data 41

9.3.2 Non-Confidential Data 41

9.3.3 Responsibility for Protecting Confidential Information 41

9.4 Protection of Personal Data 41

9.4.1 Policy for Processing Personal Data 41
9.4.2 Data to be Treated in Confidence 41
9.4.3 Non-Confidential Data 41
9.4.4 Responsibility for Protecting Personal Data 42
9.4.5 Consent and Usage of Personal Data 42
9.4.6 Publication Following Legal Order or as Part of Court Evidence 42
9.4.7 Other Circumstances of Publication 42
9.5 Copyrights 42
9.6 Obligations 42
9.6.1 Obligation of Certification Authorities 42
9.6.2 Obligation of the Registration Authorities 42
9.6.3 Obligation of the Subscriber (Subscriber Party Agreement) 42
9.6.4 Obligation of the Relying Party (Relying Party Agreement) 42
9.6.5 Obligation of Other Participants 43
9.7 Warranty (Exclusion of Liability) 43
9.8 Limitation of Liability 43
9.9 Exemption of Liability 43
9.10 Effective Date and Termination 43
9.10.1 Effective Date 43
9.10.2 Termination 43
9.10.3 Consequences of Termination 43
9.11 Individual Notifications and Communication with Participants 43
9.12 Changes to the Policy 43
9.12.1 Procedure in the Case of Changes 43
9.12.2 Notification Mechanism and Deadlines 43
9.12.3 Circumstances that Require a Change to the Policy ID (OID) 43
9.13 Conflict Resolution 43
9.14 Governing Law 43
9.15 Compliance with the Governing Law 43
9.16 Other Provisions 44
9.16.1 Completeness 44
9.16.2 Assignment of Rights 44
9.16.3 Severability 44
9.16.4 Legal Disputes / Place of Performance 44
9.16.5 Forces Majeures 44
9.17 Other Provisions 44
10 Supporting Documents 45

1 INTRODUCTION

A *Certificate Policy* (CP) is a publicly accessible document that describes the suitability of a certificate for given application areas. The CP defines the security requirements on which the operation of the infrastructure is based, and which govern how certificates are handled. Based on the CP, users can assess whether a certificate is trustworthy for the specific area of application or not.

In addition to the certificate policy is the *Certification Practice Statement* (CPS), which describes how the requirements of the CP are implemented. As such, the CP defines what should be done, whereas the CPS describes how it should be done. Since the content of a CPS is completely trustworthy, only extracts need to be published as a summary. If requested, a verifying body may access the entire document.

This document describes the certificate policy for PKIs of SAP SE with basic protection requirements. It forms part of the SAP security policy and standards, and is directly based on the "*General Certificate Policy for Production Certificate Hierarchies*" (Fig. 1).

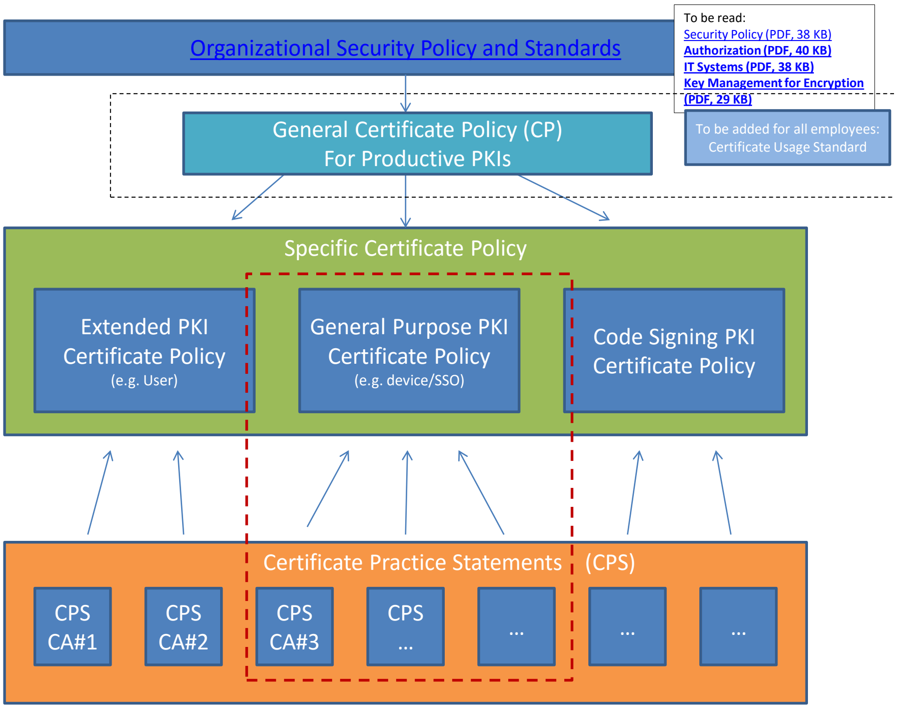

Organizational Security Policy and Standards
To be read:
Security Policy (PDF, 38 KB)
Authorization (PDF, 40 KB)
IT Systems (PDF, 38 KB)
Key Management for Encryption (PDF, 29 KB)
General Certificate Policy (CP)
For Productive PKIs
To be added for all employees:
Certificate Usage Standard
Specific Certificate Policy
Extended PKI
Certificate Policy
(e.g. User)
General Purpose PKI
Certificate Policy
(e.g. device/SSO)
Code Signing PKI
Certificate Policy
Certificate Practice Statements (CPS)
CPS
CA#1
CPS
CA#2
CPS
CA#3
CPS
…
…
…
…

Fig. 1 – Overview of SAP Certificate Policies

Certificates for applications that require basic protection include server certificates for SSL/TLS and certificates for user authentication (SSO). Other areas of application such as data encryption and signing are not covered by this certificate policy.

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

1.1 Overview

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

- **Hierarchy**: A PKI must comprise a minimum of a two-stage but no more than a three-stage hierarchy of certification authorities with a root CA based on their root and operated offline.
- **Purpose**: Issuing CAs must be purposeful, i.e. they must have a dedicated design for machines or user certificates.
- **Certificate Restrictions**: As far as is feasible, the purpose must be defined in the restrictions of the certificates. *Basic Constraints* are necessary to ensure that only the root CA can issue certificates for certification authorities.

- **Revocation Information**: Information about the validity of a certificate must be made available to relying parties via the standard channels (CRL download and OCSP).
- **Availability**: All components of a PKI available must be highly available to ensure that the failure of an individual component does not cause the service to fail.
- **Key Protection**: The private keys of all online certification authorities must be protected against attack by hardware-side mechanisms (HSM, SmartCards, TPM, etc.). Exceptions need explicit Approval by SAP IT Security.
- **Dual Control Principle**: All operations performed with or on the private key of the root CA must be monitored and documented via a dual control system.
- **System Security**: All systems involved in a 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.

1.2 Document Name and Identification

This document is titled ***SAP Global PKI Certificate Policy – CP***, and is referenced via its own *Object Identifier* (OID).

x.509 OID	Description
1.3.6.1.4.1.694.4	SAP Global PKI Base of the SAP Global PKI Namespace
1.3.6.1.4.1.694.4.100	Production environment Base of the SAP Global PKI production environment
1.3.6.1.4.1.694.4.100.1	PKI Policy SAP Global PKI Certificate Policy / Certification Practice Statement Policy Reference
1.3.6.1.4.1. 694.4.100.2	Current CP documentation SAP Global PKI Certificate Policy Version 1.0
1.3.6.1.4.1. 694.4.100.3	Current CPS documentation SAP Global PKI Certification Practice Statement Version 1.0

The certificate policy and the CPS are publicly accessible via the following Web site:

http://www.pki.co.sap.com/

1.3 Participants in the Certification Infrastructure (PKI)

This certificate policy describes:

1.3.1 Certification Authorities

The hierarchy of an SAP PKI with basic protection requirements.

The *SAP Global PKI* is a two-stage PKI hierarchy. The offline root CA controls two issuing sub-CAs where one of these sub-CAs issues only user certificates, and the other issues only machine certificates.

1.3.2 Registration Authorities

The SAP AD and WEB-RA are registration authorities.

1.3.2.1 Online Registration

- SAP AD
- Authentication / identification (AD membership and associated processes (hardware/software in the SAP distribution process))
- No verification, but restrictions via AD information and the defined values
  (Microsoft: autoenrollment)

1.3.2.2 Offline Requirement

- WEB-RA
- Authentication / Identification
- Verification (manual)

1.3.3 Certificate Subscribers

Subscribers are the entities listed in the certificate. This might be users, systems, (computers, appliances, etc.) or even services.

Users are always people with a valid SAP user ID at the time of the request, or a valid ID of a company that has a contractual relationship with SAP.

Only devices with a valid SAP Asset Management entry or an equivalent identifier of a partner company of SAP are regarded as machines or systems.

Services can only be performed on the above systems designated as machines, and operated by persons designated as users as defined above.

Subscribers are also always the owners of the private cryptographic key belonging to the certificate. Such ownership comes with additional responsibilities (see 9.6.3)

1.3.4 Relying Parties

A relying party is the party that is informed about the validity of a certificate in order to verify and assess the trustworthiness of a subscriber based on the certificate policy.

The checker or relying party of a certificate depends on its application. This could be either a machine or person. Although certificates may only be issued to a restricted group, any system or any person, even outside SAP may potentially check the validity of a certificate.

By using the certificate, every person implicitly agrees to this policy.

1.3.5 Other Participants

Another component of the PKI are the storage directories for the information behind the entries in the certificates for the *Authority Information Access* (AIA), the *Certificate Revocation Lists* (CRL), and certificate policies. As a minimum, these must provide a Web server via HTTP. The same applies for the *Online Certificate Status Protocol* (OCSP) service.

Microsoft-based PKIs also contain the *Active Directory* (AD) as a repository; PKI environments of other manufacturers often use an LDAP directory or similar database in its place. These are equally as much part of the PKI environment as any *Hardware Security Module* (HSM), as are also required here, and which must be considered separately.

Other participants such as a bridge CA are not considered in this CP.

1.4 Application Area

The certification authorities of an SAP PKI with basic protection requirements are what is known as “basic validation” CAs, i.e. when the subscriber is authenticated, the existing mechanisms are used (password, certificate, e-mail, dual control, and so on). This is not the same as the enhanced verification of subscribers, where applicants apply in person, and have to identify themselves using a photo ID.

Since certificates for signatures (nonrepudiability) and for encryption (key recovery) must satisfy far higher requirements, only certificates for the authentication of end participants and transport encryption may be issued under this certificate policy.

This ensures that PKIs of this type cannot issue any qualified certificates under this signature ruling.

Any certificates issued by these PKIs are intended for SAP-internal use only, that is for authenticating internal systems for SAP employees or partners (and vice versa), and for encrypting the network traffic between documents or systems operated by SAP or partners.

1.4.1 Suitable Certificate Usage

The usage areas of the issued certificates are derived directly from the validation of the subscriber. This results in the following suitable usage scenarios:

- Machine certificates
  - Authentication
  - Transport encryption
  - Code signing
- PKI-related machine certificates
  - CA signatures
  - OCSP response signatures
- User certificates
  - Authentication
  - Encryption

1.4.2 Restricted Certificate Usage

All certificates issued by SAP PKIs with basic protection requirements are used only by SAP-internal systems, 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.

Note that the fundamental nature of the validation of the subscriber identity suggests the same assumptions of trust as the validation processes themselves. As such, identification via a certificate of this PKI type is the same as a logon using a user name and password.

1.4.3 Forbidden Certificate Usage

All types of use not listed under 1.4.1 and 1.4.2 are forbidden. In particular, this includes:

- Use of end participant certificates as a CA certificate
- Use of end participant certificates for other purposes than specified in the application
- Use of end participant certificates beyond their validity
- Use of end participant certificates after they have been revoked by the PKI
- Use of machine certificates on non-SAP systems and non-certified partner systems
- Use for non-SAP-internal or non-SAP partner processes

1.5 Administration of the Certificate Policy

1.5.1 Change Management

The policy is managed and changed by the *SAP Global Security - Secure Operations* team.
This team is referred to as SAP *"IT Security"* department in the document in order to avoid and simplify repeated updates of the document due to organizational name changes.

p.9.12

1.5.2 Contacts

SAP SE
SAP Global Security - Secure Operations
Dietmar-Hopp-Allee 16
69190 Walldorf
Germany

Voice:	+49 6227-7-47474
Fax:	+49 6227-7-57575
E-mail:	sap.it.security@sap.com

Web: http://www.sap.com

1.5.3 Checking Suitability for Regulations Governing the Certification Practice Statement (CPS) in Accordance with the Certificate Policy

The body specified in 1.5.2 checks that a *Certification Practice Statement* (CPS) agrees with this certificate policy (CP).

1.5.4 Procedures for Recognizing Regulations for the Certification Practice Statement (CPS)

The regulations for operating a certification authority must be provided by the authority's operator, and provided to the IT security department for inspection and checking before productive use.

IT Security will confirm that the CPS conforms with this policy. Any changes to the CPS must be notified to IT Security immediately, and require a new acceptance process.

1.6 Definitions and Abbreviations

1.6.1 Abbreviations

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
HSM	Hardware Security Module
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
RA	Registration Authority
SSL/TLS	Secure Socket Layer / Transport Layer Security
SSO	Single Sign On

1.6.2 Definitions

The description of this certificate policy assumes the reader is familiar with terms such as "certificate", "PKI", "directory service", and so on, which are used in relation to the operation of a certification authority. The following terms are also important:

End participant Under this policy, an end participant may represent a system, a service, a user, or a group of these. An end participant is either a subscriber or relying party.

Machine/System A machine or system refers to any objects that can be uniquely identified by an equipment number or *Asset Management* entry or similar identifier of an SAP partner.

User Users are any individuals that are maintained in the official HR systems of SAP or a partner, and which have a unique ID.

Autoenrollment This term is synonymous with an automated and event-driven process concerning the distribution and renewal of end participant certificates.

Basic Protection Requirements

Registration Authority (RA) A *Registration Authority (RA)* denotes an instance located upstream of a CA, which is tasked with the authentication and authorization of end participants, and reviewing and ensuring the correctness of the certificate and blacklist entries.

2 PUBLICATIONS AND DIRECTORY SERVICE

2.1 Directory Services

Certain data must be stored and saved to operate an SAP basic protection CA. This means the use of one or more directories that are precisely specified in the CPS. Directories may contain information about elements such the end participants, certificates, and their validity.

Directory services must be operated so that they satisfy the same availability requirements as the PKI service itself. All directories used by the PKI and their logs must be listed in the CPS.

2.2 Publication of Certificate Information

The operators of an SAP CA must make certain information about the certification authority and their issued certificates publicly available or internally within SAP in accordance with the purpose of use. Above all, this includes the certificate policy, the corresponding CPS abstract, and any agreement between the subscribers and relying parties. The location at which this information can be retrieved must be entered in the issued certificates using “CP qualifier”.

Validity information about the issued certificates must also be published so the relying parties can easily access up-to-date information about blocked certificates. Publications of block lists and individual information about the *Online Certificate Status Protocol* (OCSP) is required. Providing the policies outlined here are maintained, it is possible to provide the public section of the issued certificates and replicate these even in non-SAP directories.

2.3 Updating of the Information (Time, Frequency)

The CP and CPS and their corresponding documentation should be revised as little as possible. Minor changes should therefore be collected and saved, and added to updated versions of the documentation no more than once a year. Extensive changes on the other hand should be incorporated and published immediately.

Depending on the underlying technology, validity information regarding certificates must be kept as up-to-date as possible, and must not be stored for longer than 14 days. Further details are provided in the CRL and Certificates sections.

2.4 Controlling Access to Directory Services

Read access to information in the directories that is relevant for the PKI 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 Names

SAP PKIs are 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).

Information about the end participants is relatively free in form, and depends on how the certificates are used and the processing instances. Nevertheless, names must be chosen that allow a certificate to be uniquely and unambiguously assigned to an end participant.

CA and CRL signature certificates are special cases. In these cases, RFC 5280 specifies that the *Subject* and Issuer must match in the certificate.

3.1.1 Name Forms

All names that appear in certificates issued by an SAP CA follow the format of the *Distinguished Names* (DN) of the X.500 standard of the International Telecommunication Union (ITU-T), specifically, the recommendations of X.501 and X.520.

The details regarding the necessary and optional attributes of the DN are specified in the respective CPS; no differentiation is made as to whether the DN was created from manual entries or automatically, for example following a directory reconciliation. Since the latter case means the applicant and name source are separated, the minimum requirements may differ slightly here.

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 block 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*:

- **CN** (commonName)
  The CA can be assigned any name, but 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

No specifications are given for the SAN; the information for this element is unusual and is not recommended.

3.1.1.2 Domain Controller Certificates

Domain controller certificates are the same as server certificates (see 3.1.1.3)

3.1.1.3 Server Certificates (incl. DC and OCSP)

Certificates of this type are generally used to authenticate a service for a client. The *Common Name* (CN) in the *Subject* and the *DNS Name* or *IP* in the SAN are the key elements here. A CN alone may be sufficient for an automatic issuing process that derives its information from a directory, although it must be ensured that the service and therefore the operator can be uniquely identified by the name.

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

- **CN** (commonName)
  Any value can be entered, but it must contain the host/service name or host header of the Web site, and conform with the relevant standard (X.400, X.500, RFC822, etc.)
- **OU** (organizationalUnit) – for manual application only
  Any value can be entered, but it must describe as accurately as possible an existing SAP department or equivalent organizational structure of a partner
- **O** (organization) – manual application only
  The organization that operates the service, which is normally “SAP SE” or a partner company
- **C** (country) – manual application only
  The country in accordance with ISO3166-1, Alpha2 (2 country codes) in which the service is operated

For **SANs** (if relevant), the following minimum information is required:

- **DNSName**
  Same as the *Common Name **of the** Subject*
- **IP** (iPAddress) – manual application only
  the IP addresses of the system

3.1.1.4 Code Signing Certificates (SAP internal)

Certificates of this Type are used for authentication of Software / Code origin to a Client. Relevent here is the *Common Name* (CN) in the *Subject* and the *Timestamp*. It must be ensured that the producer of the Software (especially the SAP internal Department) can be identified.

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

- **CN** (commonName)
  Any value can be entered, but it must describe the use case of this code signing, and conform with the relevant standard (X.400, X.500, RFC822, etc.)
- **OU** (organizationalUnit)
  Any value can be entered, but it must describe as accurately as possible an existing SAP department or equivalent organizational structure of a partner, if available, insert also email address of the department
- **O** (organization)
  The organization that operates the service, which is normally “SAP SE” or a partner company
- **C** (country)
  The country in accordance with ISO3166-1, Alpha2 (2 country codes) in which the service is operated

For **SANs** (if relevant), the following minimum information is required:

- **rfc822Name**
  A name in the format of a Web e-mail address (Responsible Contact Person for this Signing Certificate)

3.1.1.5 User Certificates

This certificate type is used to identify and authenticate an individual or group of individuals. The reference to the subscriber must 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 user or group
- **O** (organization) – manual application only
  The organization for which the subscriber(s) are active.
- **C** (country) – manual application only
  The country in accordance with ISO3166-1, Alpha2 (2 country codes) in which the organization is registered for which the subscriber is active.

If specified, ***Subject Alternate Names*** (SANs) require the following minimum information:

- **rfc822Name**
  A name in the format of a Web e-mail address
- **x400Address**
  A name in the form of an x.400 address
- **otherName**
  Where required, a name in a different format required by the application.

3.1.2 Informativeness of Names

Based on the *Subject* and/or the SAN, it must be possible to assign a certificate uniquely and transparently to an organization and the corresponding person or service. Names must also be chosen that are generally comprehensible and contain relevant information.

3.1.3 Anonymity or Pseudonyms of Subscribers

Subscribers may not be anonymous. Pseudonyms and aliases, however, are possible for such time that these are unique in the SAP namespace, and for which it is possible to combine as an administrative contact during the application.

3.1.4 Rules for Interpretation of Different Name Formats

Standardized name types such as X.500 *Distinguished Names* are preferable. In exceptional cases where this is not possible, proprietary name formats may also be used, but these must be sufficiently documented.

The used formats or references to the documentation must be listed in the CPS at this point.

3.1.5 Uniqueness of Names

Names in the *Subject* and/or *Subject Alternate Name* must be unique in the namespace of SAP or the partner. 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 Function of Trademarks

Conscious use of legally protected names is not permitted. The CA operator is not allowed to explicitly check the name of an applicant. The applicant is responsible for ensuring that no naming rights of third parties are violated.

No claims for compensation resulting from wrongly used names may be submitted against the operator of the certification authority.

3.2 Identify Check in New Applications

3.2.1 Verification of the Ownership of a Private Key

An applicant must employ suitable methods to show that he is the owner of the corresponding private key; this also means further responsibilities regarding the protection of this key (see 9.6.3). Certificate applications using PKCS#10 (RFC 2986) or CMC (RFC 5272) meet this requirement.

3.2.2 Authentication of an Organization

If an applicant acts on behalf an organization, that is, a partner, the applicant must be able to demonstrate affiliation via appropriate mechanisms. This is possible, for example, via a specific group affiliation in automated processes. The procedure must be released by IT Security:

3.2.3 Authentication of Natural Persons

One of the features of SAP CAs with basic protection requirements is that the authentication is not performed directly by the CA, but based on already existing mechanisms. This may be, for example, a user name and password as entered when logging onto the PC, or a process similar to an e-mail handshake where access to a mailbox can serve as sufficient identification.

Authentication of persons may be required in different scenarios. In all cases, the applicant must be identifiable by suitable means, and described in the CPS.

Exceptions are possible, but require confirmation by IT Security.

3.2.4 Non-Verified Participant Information

There are two different scenarios for verifying participant information:

1.) The **information** for the certificate originates **from the applicant** himself
In this case, the fields specified in 3.1.1 are checked. Additional information in the *Subject*, SAN, or other certificate enhancements are transferred to the certificate without checking, provided that no further policies have been defined for the sub-CA or the special certificate type.

2.) The certificates are **automatically** created with information from a directory
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 directory.

3.2.5 Checking Authorization

Different conditions apply for authorizing the process depending on whether an application is intended for the actual applicant or for another entity:

Self-Application

Verifying group membership of an official SAP directory or similar system of a partner company is deemed sufficient authorization.

Application for Another Person

A certificate is always issued to the holder of a private key, the ownership of which has already been proven as described in 3.2.1.

Application for a Service or Machine

The applicant must be able to show permission of an administrative contact for the service or machine (service owner, project management, etc.). Group-based or workflow-based approaches are possible.

Certificates may only be issued for devices with an entry in SAP Asset Management or a similar ID of a partner company, or in the case of loaned equipment, official permission must be provided by the project manager.

3.2.6 Criteria for Collaboration

Collaboration with external PKIs (for example, cross-certification) requires thorough revision of this policy, and is not planned at the current time.

3.3 Identification and Authentication during Certificate Renewal

3.3.1 Routine Certificate Renewal

Routine renewal of a certificate, i.e. in the case of a certificate that is still valid, the certificate can be renewed with the classic method, that is, in the same way as for a new application or by signing the existing, valid certificate. In the latter case, the contents can be transferred from the existing certificate. However, if the information from the request does not originate from the certificate itself, this is not possible.

3.3.2 Certificate Renewal after a Block

The process for renewing a certificate following a previous block is the same as the process for a new application. The keys may not be reused, and new keys must be generated.

3.4 Identification and Authentication of Block Applications

To prevent unnecessary delays when deactivating compromised identities, any SAP employee or partner can apply for temporary blocks with minimal requirements for identifying the block applicant. Requirements may include, for example, knowledge of a telephone number, e-mail address, or similar personal data.

A temporary block always follows a process where the final aim is the block or its revocation. This process must be performed at the same time as the temporary block, and includes an extended check of the identity of the applicant and the legitimacy of the application.

Server certificates cannot be blocked temporarily, and must always run through the complete blocking process.

The following or similar authentications are possible for a rapid temporary block:

- Knowledge of details from the address book
- Block application signed with certificate
- Digital signatures of a *Registration Authority (RA)*

The extended authentication must always be a verifiable documented process with the consent of the subscriber or subscriber’s manager or the service owner or project manager.

4 PROCESS ORGANIZATION (CERTIFICATE LIFECYCLE)

4.1 Certificate Application

4.1.1 Who Can Apply for a Certificate?

Systems or users that meet the definitions as specified in section 1.6.2 can apply for certificates. Registration authorities (RA) can also assume this function if they ensure checks are performed in accordance with these definitions.

4.1.2 Procedures 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 participant (see 4.1.1) generates the key and 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 both procedures (automated and manual). The option of an external RA must also be possible.
  A contact person must also be specified in the event of any questions.

- **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.
  A contact person must also be nominated in this case.

- **Subscriber**
  The owner of a private key is the holder or subscriber of the corresponding certificate. The requirements of this role trigger the process for a certificate application. The *Subscriber Party Agreement* in section 9.6.3 describes the relevant responsibilities; these include the following in particular:

  - Truthful information
  - Key generation
  - Proof of ownership of the private key as defined by 3.2.1

4.2 Processing Certificate Applications

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 by a person.

All requests must be stored in an appropriate database for period to be defined in the CPS.

4.2.1 Execution of the Identification and Authentication

The authentication requirements differ depending on whether an application is made by the actual subscriber or by a third party. In all cases, it must be possible to clearly identify the applicant by suitable means. This may include, for example, existing methods such as a user name/password, a client certificate, e-mail handshake, or a workflow process with similar characteristics.

If the application is submitted in the name of an end participant, this person must also authorize the process, and confirm that he (the person) or the subscriber (service/machine) owns the private key for the certificate. This process must be fully transparent (e.g. a workflow in the ticket system).

4.2.2 Acceptance or Rejection of Certificate Applications

The CPS must define the prerequisites for the authorization required to receive a certificate, and these prerequisites must be implemented in operation. If the application also corresponds to the policies in this document, and if the official interfaces have been used for the application, the certificate can be issued by the CA.

In all other cases, and in particular if the applicant does not respond to requests, an application should be rejected. This must be sent in the form of an informal message to the specified contact (if specified), and does not require any comments to be given if the system supports this.

4.2.3 Processing Time for Certificate Applications

The duration required for a certificate application to be processed through to its acceptance or rejection should be set to a reasonable time, and specified in the CPS document.

4.3 Certificate Issuance

An automatic process such as Microsoft's autoenrollment, i.e. the issuing of a certificate without further checks by a person, is subject to stricter requirements than the manual process.

The following points are required in order to ensure that a certificate can be issued immediately without the intervention of a person:

- The values of the certificate attributes must not be read from the certificate application, but must be taken from a third-party independent and verified instance (repository such as AD, LDAP, DB, etc.).
- In the event of a request without an upstream RA, certificates may only be issued for the actual requestors and not on behalf of a requestor.
- In the event of an RA that always makes requests on behalf of another requestor, it must be possible to clearly verify the validation process by the subscriber or subscriber's manager in the RA.

Manual issuing of certificates, i.e. with information for certificate attributes within the application, must be set to "Pending", and requires the involvement of an authorized person. Following a successful check, the certificate can be issued via the available methods (e.g. Microsoft CA Management Console)

4.3.1 Tasks of the Certification Authority

A CA must be able to complete all tasks associated with the issuing of a certificate. In particular, this includes:

- Creating and signing the certificate
- Providing a retrieval or issuing function for the certificate
- All data generated in relation to the issuing of the certificate as well as the certificate itself must be archived for a period to be defined in the CPS

4.3.2 Notifying the Applicant

The subscriber or the administrative contact to be specified in the application must be informed of the successful issuing of the certificate. In an automated scenario, the issuing of a certificate is sufficient notification.

4.4 Certificate Acceptance

4.4.1 Acceptance of the Certificate

The subscriber or corresponding administrative contact must check the certificate for correctness following receipt. In the event of errors, the certificate must be blocked immediately (see 4.9)

If the format and information in the certificate are in order, the certificate is regarded as accepted.

In automated processes, a certificate is deemed accepted following successful issuing.

4.4.2 Publication of the Certificate by the Certification Authority

The certificates of the PKI itself, that is, the individual CAs, which are required to complete the chain of trust, must at least be published via the authorities specified in the certificate.

Furthermore, the root certificate of the PKI must be available as a trustworthy root certification authority certificate on all systems that perform a certificate check in order to ensure trust can be established without the involvement of the user.

End user certificates can be published to central directories in accordance with the technical requirements of the application.

4.4.3 Notification of Further Instances by the Certification Authority

No rulings.

4.5 Use of the Key Pair and Certificate

4.5.1 Use by the Subscriber

Usage of the certificate and the corresponding cryptographic keys is subject to the *Subscriber Party Agreement*, as defined in 9.6.3. Any other usage is not permitted.

4.5.2 Use of the Certificate by the Relying Party

Certificates of this CA type are used in the authentication of services, systems, and users by relying parties that implicitly agree to usage conditions as set out in the *Relying Party Agreement* (see 9.6.4).

4.6 Certificate Renewal on Retention of the old Key (Re-Certification)

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

This type of certificate extension is only permissible for certificates protected by special hardware (HSM, SmartCards, TPM, etc.). Any hardware used must not be compromised by this process.

4.6.1 Reasons for Certificate Renewal

Reasons for renewing the certificate may include the normal expiry of the certificate's validity, or premature extension owing to insufficient time periods in the certificate.

4.6.2 Who Can Apply for a Certificate Renewal?

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

4.6.3 Expiry of the Certificate Renewal

The process is the same as a certificate application as described in sections 4.1, 4.2, and 4.3.

If a certificate that is still valid signs the application, there is no need to check the information for the certificate. In this case, the values must be transferred completely from the existing certificate, and must not be changed.

4.6.4 Notification of Subscriber Following Certificate Renewal

See 4.4.3

4.6.5 Acceptance of a Certificate Renewal

See 4.4.1

4.6.6 Publication of a Certificate Renewal by the Certification Authority

See 4.4.2

4.6.7 Notification of Further Instances by the Certification Authority

No rulings.

4.7 Key and Certificate Renewal (Re-Key)

When a certificate is renewed by means of a "*re-key*", only the validity and corresponding cryptographic key of a certificate change, while retaining the hash and signature algorithms, that is, the *Cryptographic Service Providers* (CSP). More extensive changes than this are described in section 4.8.

If the algorithms used in the CSP are deemed sufficiently secure for the entire time the certificate is used, a "*re-key*" is permissible, otherwise a completely new certificate must be issued (see 4.1). The certificate to be renewed must also still be valid, and must not be blocked. Otherwise a completely new application will also be required here.

4.7.1 Reasons for a Key and Certificate Renewal

The same reasons that apply to a certificate renewal without "*re-key*" (section 4.6.1) also apply here. In addition to these reasons, however, the expected problems with the selected key lengths also apply. If an algorithm with the original key length is no longer deemed to be secure, and if increasing the key length can fix the problem, a certificate renewal using a "*re-key*" is recommended.

4.7.2 Who Can Apply for a Key and Certificate Renewal?

See 4.1.1

4.7.3 Process for Key and Certificate Renewal

The process is the same as a certificate application as described in sections 4.1, 4.2, and 4.3.

If a certificate that is still valid signs the application, there is no need to check the information for the certificate. In this case, the values must be transferred completely from the existing certificate, and must not be changed.

4.7.4 Notifying the Subscriber

See 4.4.3

4.7.5 Acceptance of the Key and Certificate Renewal

See 4.4.1

4.7.6 Publication of a Certificate Renewal by the Certification Authority

See 4.4.2

4.7.7 Notification of Further Instances by the Certification Authority

No rulings.

4.8 Certificate Modification

If changes to the certificate information are necessary, for example a name change following a marriage, this can be done using the existing key pair or a new key pair. If a new key is required, this is equivalent to a new application (see 4.1). Only modifications with the same key will be described below.

For a certificate modification, the existing certificate must still be valid, and must not be blocked. Also, the private key must be protected by hardware (HSM, SmartCard, TPM, etc.), and must not be compromised. If this is not the case, a new application must be submitted.

Changes to the underlying cryptographic algorithms require a new application, or a renewal by "*re-key*" (see 4.7). This cannot be achieved through certificate modification.

4.8.1 Reasons for Certificate Modification

A certificate modification while retaining the cryptographic key is required when changes to the *Subject* or SAN are required. This may be the case, for example, following a marriage or after a restructuring of the organization.

4.8.2 Who Can Apply for a Certificate Modification?

See 4.1.1

4.8.3 Process of Certificate Modification

The process is the same as a certificate application as described in sections 4.1, 4.2, and 4.3. It is not possible to circumvent the validation processes for the certificate information by using the existing valid key for the signature.

4.8.4 Notifying the Subscriber

See 4.4.3

4.8.5 Acceptance of the Certificate Modification

See 4.4.1

4.8.6 Publication of a Certificate Modification by the Certification Authority

See 4.4.2

4.8.7 Notification of Further Instances by the Certification Authority

No rulings.

4.9 Revocation/Blocking and Suspension of Certificates

4.9.1 Reasons for Revocation/Blocking

Reasons for blocking a certificate include:

- 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

4.9.2 Who Can Apply for a Revocation/Block?

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

Direct line managers or their managers can also apply for a revocation in the name of the end participant. In exceptional cases that are particularly relevant to the persons and companies involved, the responsible *Security Officer* can request a block.

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

4.9.3 Process for Revocation / Block

The operator of an SAP basic protection CA must provide an option for round-the-clock (24/7) entering and processing of block applications. This could be provided as a “Self Service” that automatically makes the necessary checks (see 3.4.) and offers a sufficiently secure interface (digital signature of the block application, etc.).

Block applications must be supported via a minimum of the following interfaces:

- Telephone call or e-mail to the SAP Helpdesk
- Additional written form such as the IT helpdesk Web portal

4.9.4 Deadlines for the Subscriber

If a subscriber suspects a certificate has been compromised, he must inform the PKI operator as soon as possible, and request the block.

4.9.5 Processing Deadlines for the Certificate Authority

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

Processing times are defined in the CPS, and may be based on the criticality of the certificate, that is, the certificate class.

4.9.6 Request for Block Checks by a Relying Party

Relying parties of the certificates of an SAP PKI with basic protection must be able to review the entire chain of trust including block information about the individual certificates.

SAP PKIs with basic protection offer both CRLs and OCSP services for this purpose, with the OCSP services always taking priority, and CRLs only being used if OCSP is not supported by the application.

If the application is not able to perform a block list check, the verifying instance must not assume a valid SAP authentication.

4.9.7 Frequency of Block List Publication

Block lists of an offline root CA can have far longer periods than issuing CAs:

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

Block lists 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 that are not within the validity of the certificate can be deleted.

4.9.8 Maximum Latency Time for Block Lists

The defined publication periods must be maintained as far as is possible, and the CRLs should be transferred to the directories as quickly as possible. It must be ensured at all times that there is one valid CRL in the directories.

4.9.9 Availability of Online Status Requests

Block lists and the OCSP service must be available 7x24 to ensure that status requests can be processed at any time.

4.9.10 Requirements for Online Status Requests

All PKI participants, subscribers and relying parties must be able to evaluate one of the available block list methods (block lists or OCSP requests).

4.9.11 Other Available Forms of Announcing Revocations

No rulings.

4.9.12 Requirements in the Event of Compromise of Private Keys

No ruling has been defined here because the scenario is already sufficiently covered by existing processes and regulations.

4.9.13 Reasons for Suspension

A certificate is suspended if a certificate block application cannot be verified securely enough (see 3.4), but the situation requires a certificate to be invalidated immediately. A suspension can be subsequently reversed, which minimizes the effects of an incorrect block.

4.9.14 Who Can Apply for a Suspension?

See 4.1.1

4.9.15 Process for a Suspension

See 4.9.3

The extended check of the block application and investigation, where necessary, of the reasons for the block must be performed as soon as possible to ensure that the suspension can be transferred converted into a block or reactivated.

4.9.16 Maximum Block Duration for a Suspension

A certificate may not be suspended for more than one year or the period of the certificate. If the maximum suspension time is reached without the issues having been clarified, the certificate must be blocked.

4.10 Service for Status Request of Certificates (OCSP)

In addition to publication of the block lists, an *Online Certificate Status* service must also be provided.

4.10.1 Operation-Specific Attributes

In general, the OCSP service is a preferable service for requesting block information than a simple CRL check because the information is provided via OCSP almost in real time, and is therefore more up-to-date.

4.10.2 Availability of the Service

See 4.9.9.

4.10.3 Other Features

OCSP information is signed with OCSP certificates, which means users should use hardware protection (HSM/TPM/SmartCard) to protect the private key of the OCSP instance.

4.11 Termination of the Contractual Relationship

If the certificate is no longer required before its validity expires, the subscriber must apply for a block.

If the PKI or CA need to be deactivated or disassembled prior to the end of the lifetime for economic or security reasons, all certificates that are still valid may be revoked.

However, the PKI operator is also able to revoke individual certificates for security reasons.

4.12 Key Escrow and Recovery

No rulings.

4.13 Policies and Practices for Key Escrow and Recovery

No rulings.

4.14 Policies and Practices for Protecting and Recovering Session Keys

No rulings.

5 INFRASTRUCTURAL, ORGANIZATIONAL, AND PERSONNEL SECURITY MEASURES

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

5.1 Infrastructural Security Measures

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

See also: http://www.sapdatacenter.com

Issuing CA’s of this PKI may be operated in SAP datacenter or at PKI Service provider datacenters (if they have implemented adequate physical and infrastructure Security measures according to this policy).

5.1.1 Area of Deployment and Design

All *Public Key Infrastructures* 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 centers of a PKI provider (precise details available on request). This is the highest security level under which SAP data centers operate.

All operations-relevant components have a redundant design, including the buildings. Moreover, these components must also be operated by SAP itself, or by a SAP authorized PKI service provider.

5.1.2 Access

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

The actual PKI components within the DC must also be physically protected 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 for support purposes require an authorized person to be present at all times.

5.1.3 Power Supply and Air-Conditioning Systems

All components satisfy the redundant designs as required by “*SAP Tier IV Level*”.

5.1.4 Risk of Water Damage

SAP data center locations are chosen so as to minimize the risk of flooding.

5.1.5 Fire Prevention

All fire prevention measures satisfy the requirements of “*SAP Tier IV Level*” and comply with the applicable conditions.

5.1.6 Storage of Data Carriers

Data carriers that contain information related to an SAP PKI, must be stored with the same physical and logical access controls that are used for the systems themselves. The rooms must also provide protection against damage from hazards such as fire, water, and radiation.

5.1.7 Disposal

Confidential documentation and data carriers that contain 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 manufacturers instructions must be followed.

The general SAP disposal policies must also be observed.

5.1.8 External Data Backup

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

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

5.2 Organizational Security Measures

5.2.1 Roles Concept

Employees that ensure operation of the PKI, particularly those with access to and control of the cryptographic keys and operations, have a special and trusted role. With trusted roles, tasks that are assigned to the role and which are incorrectly completed represent a security risk. It is immaterial whether this was done intentionally or by accident.

The following roles must be defined by the PKI manager:

- PKI Operator
- Information Security Officer
- Service Owner and Manager
- Auditors (Log Review)

5.2.2 Number of Persons Involved per Task

Most tasks associated with SAP PKIs with basic protection requirements do not require several people to complete the task. This is not the case, however, for actions that directly apply to the root CA or secure key containers (HSM). In these cases, there must be at least one other person to implement the principle of dual control. Examples of such tasks include issuing a new root CRL or critical security changes to the HSM systems.

5.2.3 Identification and Authentication of each Role

During their previous activities at SAP, employees are assigned the requisite status that allows them to perform work on an SAP PKI. SAP ensures that the relevant persons have trusted status.

If in the course of audits or similar processes it is necessary to grant persons access without this status, such persons must be approved and monitored by IT Security.

Technical barriers must be put in place to ensure that only the holders of trusted roles are able to access the system.

5.2.4 Roles that Require Separation of Tasks

SAP PKIs that correspond to the basic level of protection do not require separation of certain tasks. If key recovery is required in any of the sub-CAs, then roles with this authorization should where possible be distinguished from normal PKI admin roles, otherwise a dual-control principle should be applied.

5.3 Personnel Security Measures

5.3.1 Requirements for Employees

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, and which demands compliance with the described process and knowledge of the certificate policy.

5.3.2 Security Check of Employees

All employees of SAP and partners will be subjected to a high duty of care standard that differs from region to region when they are hired or contracted.

Beyond these requirements, employees will not be subjected to any further security checks.

5.3.3 Training Requirements

Those who perform PKI-related activities must regularly take part in further training courses, and SAP must provide all the necessary tools to ensure the requisite tasks can be performed satisfactorily by employees in the long-term. The following qualifications in particular are necessary:

- Basic knowledge of IT security and data protection
- PKI administration in general, and Microsoft PKI expertise in particular
- HSM administration (manufacturer-specific and if applicable)

5.3.4 Frequency and Requirements of Further Training

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 Frequency and Process of Work Center Switches

It is not necessary to analyze current work centers or how frequently these are switched. It is in the general operational interest of the PKI to minimize the frequency of changes to the personnel and partners responsible for PKIs by ensuring the personnel who fill these positions are carefully selected beforehand.

5.3.6 Penalties for Unauthorized Actions

If individual persons or groups act contrary to the requirements of the SAP PKI environment, the interests of SAP SE in general, or the PKI environments in particular, measures will be taken in accordance with the standard SAP policies. These may differ from region to region.

Furthermore, any persons knowingly and seriously violating SAP policies will have to be released from their PKI-related roles.

5.3.7 Requirements for Independent Suppliers

In principle, the same requirements that apply to employees also apply to suppliers who perform tasks in the PKI environment, that is, they are required to have an SAP User ID including all related obligations. 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 for Personnel

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

5.4 Monitoring / Logs

In the course of operating the PKI, data is generated that must be monitored and stored for later analysis. 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 Monitored Events

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

Manually created logs must be countersigned by the persons involved, and transferred to the archiving system provided by IT Security.

5.4.2 Frequency of the Log Analysis

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.

Manually created logs must be checked and read by IT Security when sent to the archiving system.

5.4.3 Storage Period for Log Data

Log files must be stored for at least 1 year.

5.4.4 Protecting Log Data

Measures must be taken to ensure that event logs cannot be changed or adjusted by unauthorized persons. Such measures may include log systems that are operated by trustworthy administrators who are not operating the PKI at the same time. If this cannot be implemented for the standard methods, a copy of the log data must be transferred to another system (forking) that meets these requirements.

In the case of manually created logs, IT Security must create a storage system in a central location that offers secure storage of and protected access to the information.

Any persons whose operational roles require it will receive read access.

5.4.5 Backup of Log Data

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 Monitoring System (Internal or 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 of the Event Trigger

Any events that trigger an alarm must be appropriately notified and made accessible 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 Weakpoint Analysis

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 Archiving

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 Archived Data

The data to be archived includes all information regarding the lifecycle of the issued certificates including the PKI certificates themselves, as well as all hand-written logs (see 5.4.1). Other data relating to the system does not need to be archived.

Information about the certificates includes:

- The certificate itself
- Applicant
- Time of request and issue

- In the case of CA certificates, the last complete CRL issued

5.5.2 Storage Period for Archived Data

Information about the lifecycle of the certificates must be stored for one year longer than their validity. Written logs must be stored for one year longer than the validity of the PKI. If data is included that relates to components split between services, this data must be stored for the lifetime of the components plus one year.

5.5.3 Protection of the Archive

See 5.4.4

5.5.4 Backup of the Archive (Data Backup Concept)

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

Special mention must also be made of the archiving of possible cleanup processes, which remove invalid certificates from the production system. Ensure that the deadlines specified in 5.5.2 are maintained.

If the PKI operation is suspended, the shutdown plan must describe what should happen to the archive (5.8).

5.5.5 Requirements for Time Stamps

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 Archiving System (Internal or External)

See 5.4.6

5.5.7 Procedures for Retrieving and Checking Archived Data

See 5.4.4

5.6 Change of Key of the Certification Authority

A normal expiry of a certification authority certificate does not necessarily require a change to the cryptographic keys. In this case, the same procedure may be used as for renewing a certificate as described in section 4.6.

If changes are required only to the certificate, and not the keys, however, this is a certificate modification as described in 4.8.

Other reasons for a change of key such as a compromised key, a change to the cryptographic algorithms, changes to the key lengths, i.e. all operations that relate to the cryptography of the certificate and key, require a certificate renewal using a "*re-key*".

Such a process in a certification authority requires what is known as a *key ceremony*. See section 6.1. Essentially, the information that applies to the lifecycle of certificates from section **6.3.2** also applies to CA certificates.

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. This may be the case, for example, in the event of long replication processes.

If such a situation is planned, the respective cross certificates must also be published to the relevant authorities (4.4.2) in addition to the actual root certificates.

5.7 Compromise and Recovery (Disaster Recovery)

PKI failures must be resolved as quickly as possible to ensure that the service can resume normal operations. All measures suitable in a business environment must be taken (clusters, HSM, etc.).

5.7.1 Procedure for Security Incidents and Compromised Certificates

If a security-relevant incident is registered in connection with the 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 Resources, Software, and/or Data are Corrupted

If it is ever suspected that the system or parts of it are corrupt, contact IT Security and ensure an open communication structure.

The time and the severity of the loss of integrity must also be established, and the following procedure will be based on this information:

- If the time of the incident is known, and only the system is affected but not the key (because this is in the 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 5.7.3.

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

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

5.7.3 Compromised Private Key

If it is ever suspected that the system or parts of it are corrupt, contact IT Security and ensure an open communication structure.

If the incident affects a key stored in the 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 only the key of a subordinate CA is affected, all valid certificates that it has issued must be revoked, followed by the certificate issued by the root CA for the CA itself.

In the case of the root CA key, all valid end entity certificates must be revoked by the respective sub CAs, and all sub CA certificates 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 also be returned to a clean state of integrity, and the cause of the incident 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 Resumption of Operations after an Emergency

The PKI operator must create an emergency plan that allows the fastest-possible recovery of the service. This must be regularly tested by the operator.

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

If a region becomes impossible to use following a natural catastrophe or similar event, remote restoration must be established at another location in accordance with a globally distributed backup 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 Suspension of Operations

If SAP is required to suspend operation of the PKI, all affected parties (subscribers, relying parties, etc.) must be informed in plenty of time to ensure they can respond adequately.

SAP also guarantees the storage periods will be observed for the PKI archives and logs as described in sections 5.4.3 and 5.5.2.

At the given time, SAP will create a shutdown plan that among other things:

- Notifies the affected parties and trusted third parties of the suspension of operations
- Describes the continued support services
- Describes whether and how certificate information will continue to be issued
- Provides information about the blocking of valid CA 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 MEASURES

6.1 Key Generation and Installation

In general, a key is generated when a certificate signature request is created, and always whenever an existing certificate has to be renewed by the re-key method. This applies both to the PKI certificates themselves (CA, RA, OCSP) and end entity certificates.

- Note that wherever avoidable, keys should not be transported between systems unnecessarily (PCs, SmartCard, HSM, etc.). Since SAP PKIs with basic protection requirements cannot back up keys, a new certificate is automatically requested for services that are used again following a recovery process even though the previous certificate is not yet invalid. In such a case, the old certificate must be blocked.

6.1.1 Key Generation

Keys must be generated by the subscribers or by their operators or supervisors. As a minimum, software-based modules, but ideally, hardware-based cryptographic modules should be used to generate the keys. These must at least comply with the requirements of the FIPS 140-2 Level 1 standard.

When operating PKI solutions, Hardware Security Modules (HSMs) with security level FIPS 140-2 Level 2 must be used to protect the CA 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 ensure that the keys and their protective measures are never compromised by individuals at any point. The result must be signed by all persons involved.

6.1.2 Transferring the Private Key to the Subscriber

The keys for the actual PKI, that is, for the CAs, RAs, or OCSP 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 (HSM) must be chosen that enable such a transport to be performed without affecting the integrity of the key. Keys may not be transferred using software-based protection. PKI certificates must be marked as non-exportable.

The same rules apply for private keys of the end entities. In this case, however, keys may be transferred between systems using software-protected processes between systems. Keys in the actual systems themselves must be identified as non-exportable, and the exported variant must be protected against misuse.

6.1.3 Transfer of Public Key to the Certificate Issuer

The most important element of transferring the public key and the certificate request is that the identity of the requesting party must be indisputable, and that the information cannot be changed in any way during the transfer.

The public key must be contained in a standardized format for certificate requests that is supported by the CA.

6.1.4 Transfer of Public CA Key to Relying Parties

It is possible to distribute the public elements of the CA keys via several mechanisms, and restrictions are not necessary. However, the certificates for all CAs must be accessible via one of the locations defined in the *Authority Information Access* (AIA) field. The following is also recommended:

- Also including all certificates of the chain of trust in the certificates themselves
- Implementing an automated distribution system, at least for internal users (e.g. AD group policies, logon scripts, etc.)

6.1.5 Key Lengths

SAP follows the recommendations of the NIST and BSI for key lengths. If the recommendations differ or if the information for encryption and signatures are different, the most cryptographically strong variant must always be selected.

Key lengths must be selected so that the certificates can be accepted as being secure for the entire period. As such, certificates with long periods (root CAs) must have longer key lengths than end entity certificates.

Ultimately, the SAP Security Policy determines the precise procedure, and the information must be outlined in the CPS.

Any exceptions must have valid reasons, and must be documented and assigned a risk appraisal.

6.1.6 Generating the Public Key Parameters and Quality Assurance

As with the key lengths, the current values and algorithms as recommended by the above-mentioned bodies must be used. The key issuers must ensure this is the case, and guarantee that the cryptographic providers and tools used are the latest state of the art.

The PKI does not perform quality assurance for the end entity certificates.

6.1.7 Key Usage Purposes (X.509v3)

For all certificates issued by the PKI, either the key usage extension must be used or the extended key usage, and at least one of these must be marked as "critical".

The information provided in these fields must limit the usage of the certificate to such an extent that the certificates cannot be used for any other purpose. In the case of a CA, this includes:

- keyCertSign
- cRLSign

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

6.2 Protection of Private Keys and Use of Cryptographic Modules

SAP protects cryptographic keys using physical, organizational, and process-specific methods. End participants 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.).

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

6.2.1 Standard of Cryptographic Modules

With regard to the requirements of cryptographic modules, SAP follows publication 140-2 of the *Federal Information Processing Standard* (FIPS). This applies both to software-based (140-2 Level 1) and hardware-based modules (140-2 Level 2 and higher).

Cryptographic Service Providers (CSPs) for software-based modules must meet the requirements of FIPS 140-2 Level 1. Certificates of an SAP PKI with basic protection for end participants must meet this protection level as a minimum.

Any used hardware modules must at least comply with FIPS 140-2 Level 2 or higher. Private keys of certification authorities must always be protected by systems of this category.

6.2.2 Distributing Private Keys across Multiple Persons (n-from-m)

In the case of end participants and issuing subordinate CAs, it is not necessary to split the private key across multiple persons to ensure that the key cannot be used by individuals.

The private keys of root CAs must be distributed across at least two persons from different departments to ensure the principle of dual control. This must be ensured through technical measures (SmartCards, split passwords, etc.).

For reasons of practicality, it is recommended splitting the key across as many people as is necessary to ensure that an adequate response is still possible in the event of one of the people responsible being unavailable. It is also recommended that security-critical and complex technical actions be performed together by two expertly trained persons, while being accompanied by another person from a different department so that at least three people are available for such tasks.

6.2.3 Depositing Private Keys (Key Escrow)

Private keys may not be deposited with a third-party non-SAP instance.

6.2.4 Backup of Private Keys

Private keys do not need to be backed up for end participants because full functionality can be fully restored by revoking the lost certificate, and issuing a new one.

In the case of keys from certification authorities, the backup must be equally as well protected as the live key. Among other things, this means:

- Dual control, or ideally triple control for root CAs in order to recover the key. The key must never be accessible to individual persons at any time in the procedure
- The key must only be accessible by authorized roles of the PKI
- The must always be backed up in encrypted form
- The backup must be stored at a geographically different location of the CA

6.2.5 Archiving of Private Keys

It is not necessary to archive private keys beyond the period of their usage.

6.2.6 Transfer of Private Keys to 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 Storage of Private Keys in a Cryptographic Module

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 Activation of Private Keys

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

- **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 (see 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 on the part of 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 Participants**
  Keys for end participants 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 Deactivation of Private Keys

- **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 hardware module, the key access must be blocked.

- **Subordinate CAs**
  Access to the key must be deactivated if the cryptographic module becomes unavailable or following a logoff of shutdown of the system.

- **End Participants**
  Access must be deactivated when a user session ends.

6.2.10 Destruction of Private Keys

No special procedure is planned for the destruction of keys of end participants. However, subscribers must always ensure the security of the private key; a standard, system-specific deletion process is deemed sufficient.

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

6.2.11 Quality of Cryptographic Modules

See 6.2.1

6.3 Other Aspects of Key Management

6.3.1 Archiving Public Keys

Public keys for the entire PKI must be archived and securely usable for at least one year (see 5.5.2) beyond the validity of the certificates. This is an operational requirement. 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 *Validity of Certificates and Key Pairs*

When choosing the validity period of certificate, both operational aspects and security aspects play a role. The aim is to ensure the security of certificates for as long as possible with the least amount of effort or costs. The purpose for which the certificates are used is also important because the costs for renewing the certificate of a certification authority are generally higher than in the case of an end participant.

Generally, the lifetime of a certificate must never be longer than the expected security of the used cryptographic keys and key lengths (see 6.1.5). However, even if keys are regarded as being secure for a very long period, restricting the validity is still recommended so that systems are regularly renewed and appraised. SAP defines the maximum period for root certification authorities (root CAs) as 20 years. This value indicates the maximum periods for the certificates issued in the hierarchy.

SAP PKIs with basic protection must follow the “onion principle”, that is, a CA must never issue certificates that are valid for longer than the issuing certificate itself. For example, if a root CA is only valid for two more years, and issuing CAs normally have a five-year term, the root CA may only issue a certificate valid for two years. This ensures that all issued certificates of a PKI always have a completely valid chain of trust with regard to lifetimes. This rule is replicated to other CAs in the hierarchy.

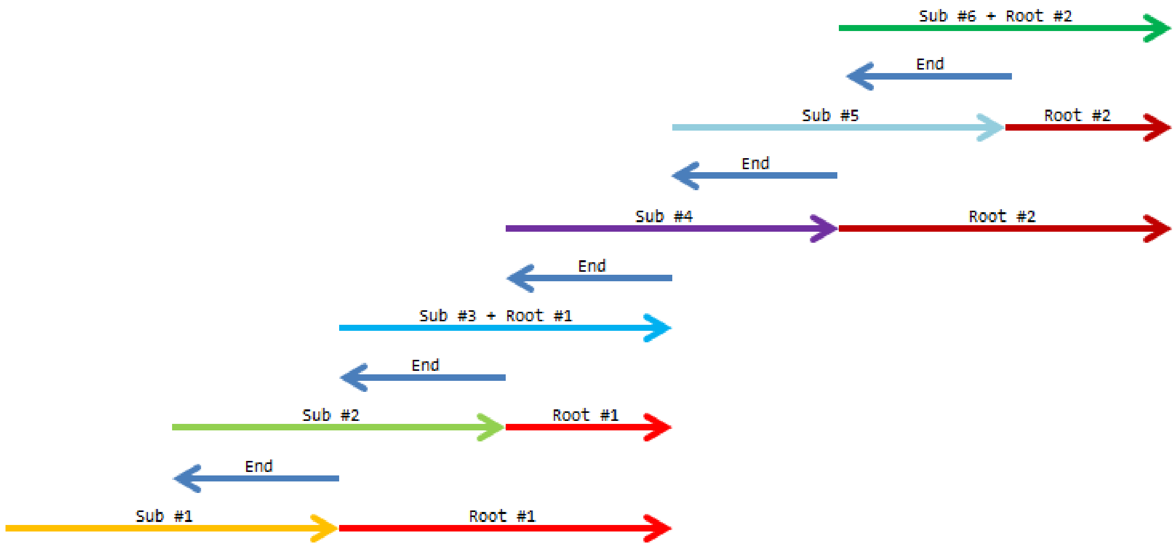
Despite this, it is important to try and ensure that certificates are issued with the maximum possible validity. This results in the following formula that indicates the latest possible time for renewing the certificate of an issuing body:

```
Time of renewal <= certificate period – maximum period of the offered certificates
```

In other words, in order to ensure that both the issuing certificate and possibly all certificates in the chain of trust do not also have to be renewed every time a new certificate is issued, the maximum periods of the certificates issued by a CA must be no more than 50% of the period of the CA itself. In the case of end participant certificates, choosing periods of even less than 50% of the period of the issuing CA is recommended.

```
Max Root = 20 years ➔ Max Sub = 0.5 * RootCA  = 10 years ➔ Max End Participant = 0.5 * SubCA = 5 years
```

This formula is central in determining the point for renewing CA certificates because this can be long before the end of the actual validity of the certificate. To ensure an issuing CA can issue valid certificates for five years, it must be renewed again after five years in the case of a ten year period, and the associated root must be renewed no later than after 15 years, and no earlier than a little after ten years if a new issuing CA is to be issued at this time.



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 4.6 is possible. However, for the next renewal of the same renewed CA, a re-key renewal as described in 4.7 is recommended. 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. OCSP response must be rebuild for the renewed CA. In case of a root CA renewal with re-key, both root CAs must also be available as trusted resources on the clients for this overlap period.

The company is free to accept the issuing of shorter certificate periods, and thereby minimize as far as possible the costs for renewals on the part of the PKI. However, the “onion principle” must always be maintained.

For CA certificates, the renewal process should be started at least one year before the actual expiry of the certificate. The complete chain of trust must be valid at all times.

In the case of certificates of end participants, short periods are preferable in order to prevent defaults in certificate management. The following maximum periods are specified:

Root CA	Maximum 20 years
SUB CA	Maximum 10 years
Server/Services	Maximum 5 years (with IT Security approval, else recommended: 2 years)
Code Signing	Maximum one year
User	Maximum one year
OCSP	Maximum four weeks The short period is due to the lack of CRL information in the certificate

6.4 Activation Data

6.4.1 Generating and Installing the Activation Data

For CA-specific data, the key fragments must be generated by hardware, and protected by the fragment owner using a private PIN (personalized fragments).

In the case of deposited fragments, the PIN must be generated independently by three individuals, and merged together in a blind process. The deposit process must be secure, and requires a dual control principle at all times.

PINs must satisfy the maximum possible complexity requirements, and must contain at least letters and numbers.

See "*Key Ceremony*".

For end participants, the creation of the activation data forms part of the underlying systems and applications, which must satisfy the generally applicable trust stages.

6.4.2 Protection of Archiving Data

The administrators of an SAP PKI and its subscribers must ensure that any activation data (SmartCards, PINs, passwords, and so on) is kept confidential for the private keys, and never disclosed to third parties.

In the case of root certificates, the fragments must be protected by a PIN stored in a secure location (safe, deposit box, or similar).

Unprotected activation data must always be secured by two persons (dual control principle), and must be converted into a secure state as soon as possible during a transport.

6.4.3 Other Aspects

No rulings.

6.5 Security Measures for Computers

All systems of the 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 Requirements for Technical Security Measures

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 Quality of Security Measures

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

6.6 Technical Measures in the Lifecycle

6.6.1 Measures in System Development

No rulings.

6.6.2 Measures in Security Management

All PKI systems must be regularly checked by the SAP IT department to ensure 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

Monitoring and / or auditing is used to ensure that systems and networks are operated in compliance with the SAP internal IT Department and SAP Global PKI specified security policies.

This includes the following tasks: Event monitoring and collection, regular penetration test for externally visible components, central system configuration (for example, AD Group Policies) and refreshing.

6.6.3 Lifecycle of Security Measures

No rulings.

6.7 Security Measures for the Network

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 partitioned from the actual 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 Stamps

Certificates, CRLs, and event logs, as well as other relevant information are time-stamped. The time stamps must be determined by a central service that derives its time from a reliable source to ensure that the data can be correlated. It is recommended using an external source (radio clock, time server, or similar) to provide the central time service with the correct time.

It is sufficient if the systems are configured so that they reconcile their system time with the time service, ensuring that all systems have the same time. Cryptographically secure time stamps provided by a corresponding service are not necessary.

7 PROFILES FOR CERTIFICATES, BLOCK LISTS AND ONLINE STATUS QUERIES

7.1 Certificate Profile

The SAP PKI with basic protection issues certificates in accordance with the following standards:

- ITU-T recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997.
- RFC 5280 (obsolete RFC 3280): Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008

7.1.1 Version Numbers

Certificates correspond to X.509 certificates, version 3.

7.1.2 Certificate Extensions

Certificate extensions strictly follow the requirements of RFC 5280. All extensions used must be listed and explained in the CPS including criticality.

As described in 6.1.7, *Key Usage* and/or *Extended Key Usage* must be set in certificates. The latter should further restrict certificate usage as far as possible according to its intended area of use.

The following specifications apply to *Key Usage*. Values not listed here are forbidden:

Key Usage Characteristic	CA Certificate	OCSP Signature	SSO	Server	DCs	Code
digitalSignature		✓	✓	✓	✓	✓
nonRepudation						
keyEncipherment			✓	✓	✓	
dataEncipherment						
keyAgreement						
keyCertSign	✓					
CRLSign	✓					
encipherOnly						
decipherOnly						

7.1.3 Algorithm Identifier (OID)

The algorithms used must be deemed secure for the validity period of the certificates. Their OID numbers must be listed at this point in the CPS.

7.1.4 Name Forms

See 3.1.1

7.1.5 Name Restrictions

No rulings.

7.1.6 Identifiers for Certification Policies (OID)

See 1.2

7.1.7 Use of Extensions to the Policy Constraints

No rulings.

7.1.8 Syntax and Semantics of Policy Qualifiers

All end participant certificates must contain a Policy Qualifier, which corresponds to the type CPS. A Web site from which the certificate policy, the CPS, and all further corresponding documents can be procured or requested must be specified as the URL.

7.1.9 Processing of Critical Extensions for Certificate Policies

No rulings.

7.2 Block List Profile

The SAP PKI with basic protection issues block lists in accordance with the following standards:

- ITU-T recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997.
- RFC 5280 (obsolete RFC 3280): Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008

7.2.1 Version Numbers

Block lists correspond to X.509 block lists, version 2.

7.2.2 Block Lists and Block List Entry Extensions

Block list extensions must be specified in accordance with RFC 5280, and specified in the CPS. A *reason code* must always be specified in a block; the reason "*unspecified*" is not acceptable.

7.3 OCSP Profile

7.3.1 Version Numbers

OCSP requests and responses are created in accordance with RFC 2560, Version 1.

7.3.2 OCSP Extensions

No rulings.

8 CONFORMITY CHECK (COMPLIANCE AUDIT, ASSESSMENTS)

8.1 Frequency and Circumstances of the Check

SAP PKIs are regularly checked based on certain events. This is performed in coordination with the usual IT and security audits, and 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 by elements of the PKI environment or its operation
- Requirements of the planned certificates
- Entry into partnership agreements with other PKI operators, for example *Qualified Subordination* by other CAs, or *Cross Certification* with other CAs

8.2 Identity and Qualification of the Auditor

Audits of the structure and operation of the SAP PKIs are carried out both internally by SAP and independently by external auditors that do not belong to the company. These are all qualified auditors with experience in PKI environments.

8.3 Relation of the Auditor to the Audited Material

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

External audits are performed by qualified and independent third parties.

8.4 Audited Areas

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 points therein must form part of the audit. In particular, the following aspects must be checked:

- Process surrounding the lifecycle of certificates
- Physical and digital access protection including authorization and role concept
- Emergency concept

8.5 Resolving Defects

If the audit identifies deficiencies that require risk prevention measures, an action plan will be drafted by the PKI operator and/or the IT department. The individual weaknesses must be prioritized, and the action plan must provide a roadmap to restoring normal operations.

After implementing the plan, the relevant team must check whether the weaknesses have been fully resolved. The management of SAP IT, the PKI operator, and the responsible security officers will be informed of the results of the check.

Findings with average impact on the security of 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 Publication of Results

The results of all audits must be held securely. The full results or extracts thereof may be made accessible to internal departments or partners on request. The process is subject to supervision by the IT Security department.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

The usage of this PKI and related Certificates is restricted for SAP users only (Here: 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. Therefore we do not specify any other regulations.

9.1.1 Fees for Creating or Renewing Certificates

No rulings.

9.1.2 Fees for Accessing Certificates

No rulings.

9.1.3 Fees for Blocks or Status Requests

No rulings.

9.1.4 Other Fees

No rulings.

9.1.5 Fee Compensation

No rulings.

9.2 Financial Responsibility

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

See 9.1

9.2.1 Compulsory Cover

No rulings.

9.2.2 Other Assets

No rulings.

9.2.3 Insurance or Guarantee for End Participants

No rulings.

9.3 Confidentiality of Business Information

9.3.1 Confidential Data

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 Non-Confidential Data

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

9.3.3 Responsibility for Protecting Confidential Information

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

9.4 Protection of Personal Data

9.4.1 Policy for Processing Personal Data

The general SAP policy concerning data protection applies.

9.4.2 Data to be Treated in Confidence

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

9.4.3 Non-Confidential Data

See 9.3.2

9.4.4 Responsibility for Protecting Personal Data

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

9.4.5 Consent and Usage of Personal Data

No rulings.

9.4.6 Publication Following Legal Order or as Part of Court Evidence

As required by the governing legislation.

9.4.7 Other Circumstances of Publication

No rulings.

9.5 Copyrights

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 Obligations

9.6.1 Obligation of Certification Authorities

The operator of the certification authorities agrees to act in accordance with policies described in this document and the requirements of the respective CPS. This includes the publication and accessibility of these documents.

9.6.2 Obligation of the Registration Authorities

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 Obligation of the Subscriber (Subscriber Party Agreement)

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 and officially accepted by the subscriber
- 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, and the certificate must be checked for accuracy following receipt by the subscriber.

Certificates may be used only if valid and in accordance with their intended purpose (see 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.

In addition, the certificate must be blocked if it is lost, if there is suspicion of compromise, or if data 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 participants.

9.6.4 Obligation of the Relying Party (Relying Party Agreement)

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

Certificates must also be checked with regard to their revocation status using the permitted mechanisms (see 4.9). The *Online Certificate Status Protocol* (OCSP) is always preferable to CRLs. Only if the OCSP service is unavailable or unsupported by the application should CRLs be used.

The relying party agrees to trust certificates only for the purposes expressly stated in the certificate (*Key Usage* or *Extended Key Usage*) (see 1.4).

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

If the relying party suspects a certificate has been misused, he or she 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 Obligation of Other Participants

No rulings.

9.7 Warranty (Exclusion of Liability)

See 9.1

9.8 Limitation of Liability

See 9.1

9.9 Exemption of Liability

See 9.1

9.10 Effective Date and Termination

9.10.1 Effective Date

This policy is effective at the time of its publication and the commissioning of the PKIs or CAs that are based on this certificate policy.

9.10.2 Termination

The certificate policy may be terminated no earlier than the suspension of operations plus the time for which the PKI-related data must be archived. This is a minimum of one year.

9.10.3 Consequences of Termination

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

9.11 Individual Notifications and Communication with Participants

No rulings.

9.12 Changes to the Policy

9.12.1 Procedure in the Case of Changes

In all cases, the currently valid certificate policy is the policy that is published in the *Policy Qualifier* URL specified in the certificates. 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.

9.12.2 Notification Mechanism and Deadlines

No rulings.

9.12.3 Circumstances that Require a Change to the Policy ID (OID)

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 Conflict Resolution

No rulings.

9.14 Governing Law

Operation of SAP PKIs is subject to the law of the Federal Republic of Germany and the European Union (EU).
See 9.1

9.15 Compliance with the Governing Law

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

9.16 Other Provisions

9.16.1 Completeness

No rulings.

9.16.2 Assignment of Rights

No rulings.

9.16.3 Severability

Should any provision of this CP/CPS 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 lacuna.

9.16.4 Legal Disputes / Place of Performance

See 9.1

9.16.5 Forces Majeures

See 9.1

9.17 Other Provisions

No rulings.

10 SUPPORTING DOCUMENTS

SAP-internal documents referred to in the text include:

- Nondisclosure Agreement
- Data Center Certificates
- SAP Data Center Security
- SAP Server Hardening Policies
- SAP Change Management Process
- IT Emergency Management Process
- SAP Security Policy
- SAP Policies for High-Security Systems

Other, externally available documents used in the drafting of this policy:

Document title	RFC 3647
Document Name	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
Description	http://www.ietf.org/rfc/rfc3647.txt
Latest available version	
Last changed	November 2003

Document title	RFC 5280
Document Name	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
Description	http://tools.ietf.org/html/rfc5280
Latest available version	
Last changed	May 2008