Certification Practice Statement

Revision R4

2017-06-02

Copyright

Printed: June 2, 2017

Responsible for the content:

SBS Software Ges.m.b.H.
Weiserhofstraße 18
A-5020 Salzburg

Table of Revision

Version	Author	Date	Changes
R0	Andreas Hoheneder, Christoph Meinhart	2012-09-01	Initial Version.
R1	Andreas Hoheneder	2013-01-09	ISSUER is now called SBS-ISSUER. Added OID for CPS.
R2	Andreas Hoheneder	2015-11-04	New issuer SBS-ISSUER-3. ROOT-CA-2 (SHA1) is not supported.
R3	Andreas Hoheneder	2016-10-21	Corrected text errors; no change in content.
R4	Christoph Meinhart, Andreas Hoheneder	2017-06-02	Corrected text errors. Special certificates may be valid up to 3 years. New issuer TEST-ISSUER-2 replaces TEST-ISSUER-1.

Contents

1. Introduction

This Certification Practice Statement (CPS) defines the PKI security model of Salzburger Banken Software (SBS). It describes the requirements for issuance, usage, destruction and revoking of certificates within the PKI in accordance with SBS security policy to ensure a secure operation of the PKI.

The structure of this document follows RFC 3647 "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework".

1.1. Overview of the PKI Architecture

The PKI uses a root certificate, which signs issuer certificates. No certificates will be signed by ROOT-CA-1 which use SHA1 for hashing, as this algorithm has cryptographic limitations[1].

1.2. Document Name and Identification

Description:	Certification Practice Statement (CPS)
Version:	R4 EN
Object-ID:	2.5.29.32.0[2]

This document is rated "public" in accordance with our Quality Management System (QMS).

[1] http://csrc.nist.gov/groups/ST/hash/statement.html
[2] 4.2.1.5 from http://www.ietf.org/rfc/rfc3280.txt

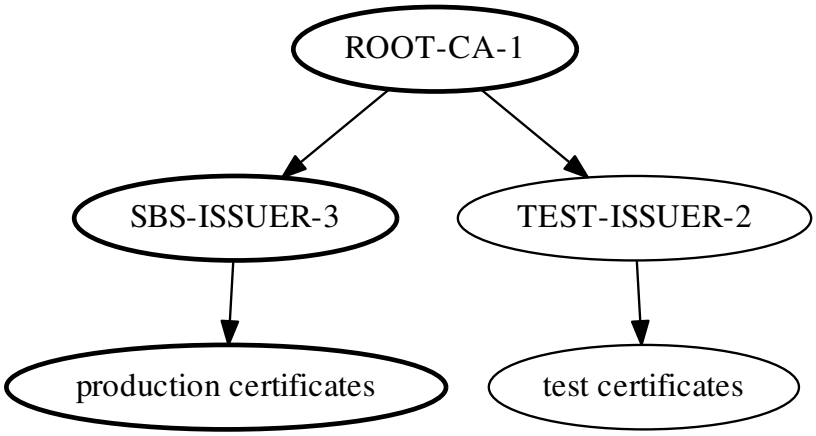

Figure 1: PKI Architecture

1.3. Usage of Certificates

1.3.1. Certificates for Access to VPN

The VPN certificates are used to authenticate authorized access by employees and customers of SBS from external devices to the company network. These certificates also ensure the integrity and encryption of this communication.

1.3.2. Use in Software Development

Certificates issued by the PKI are also used in software development. Thus, digital signatures protect the integrity of the software, and special test certificates are used for software tests.

1.3.3. Protection of Electronic Mail

The e-mail correspondance between SBS and its customers is protected by the use of certificates encrypting the communication between mail servers. The e-mails themselves can be digitally signed and encrypted to prevent unauthorized reading and altering.

1.3.4. Protection of Internal Infrastructure

Additionally to the aforementioned ones, the PKI issues certificates for internal use.

These are deployed on network components and systems of SBS for ensuring confidentiality and integrity of internal communication.

1.4. Administration of the CPS

This document is managed and versioned within the certified QMS of SBS. Additionally, the current version is available to the public on the SBS website.

The security officer is in charge of maintaining the document

1.5. Contacts

Information about the PKI of SBS can be obtained here:

- on the SBS website via `http://pki.sbs.co.at`
- via email to info@sbs.co.at
- via written request to:
  SBS Software Ges.m.b.H.
  Weiserhofstraße 18
  5020 Salzburg
  Austria

2. Identification and Authentication

2.1. Identification of Certificates

2.1.1. Certificate Names

The issued certificates use Distinguished Names according to X.501. The possible symbols are restricted to the letters of the English alphabet, "space" and the special characters "_", "-", "." and "@".

Certificates issued for natural persons must include contact information (e.g. an e-mail address). Every certificate is assigned to one specific person. This PKI will not issue group certificates to natural persons.

2.1.2. Algorithm Used to Construct X.509 Serial Numbers

X.509 serial numbers are issued according to the following schema:

xx yy yy yy yy zz zz zz zz

xx ... 1 byte consecutive number of the root certificates:
01 ... SBS ROOT-CA-1 using sha256 and 4096 bit

yy ... 4 bytes consecutive number of the issuer certificates:
01 00 00 00 04 ... SBS-ISSUER-1
01 00 00 00 05 ... SBS-ISSUER-3
01 00 00 00 06 ... TEST-ISSUER-2

zz ... 4 bytes consecutive number of the actual user certificates

2.1.3. Technical Details of Issued Certificates

The PKI issues certificates according to X.509 version 3 (RFC 3280). The signature algorithm used is SHA256 in combination with RSA. All issued certificates carry the extension "X509v3 Subject Key Identifier" (fingerprint of the certificate) and all non-CA-certificates carry the extension "X509v3 Authority Key Identifier". Additionally, the use of all certificates is restricted via the extension "X509v3 Key Usage".

2.2. Verifying the Identity of Individuals

Certificates are only issued to employees or customers of SBS who are registered in the company-internal Lotus Notes database. Newly recruited employees are identified by an official photo identification.

3. Publication and Distribution of Certificates

Provided the receiving party is connected to SBS's Lotus Notes system the certificate will be delivered by encrypted email. If the recipient is not connected to this system the authenticity of the certificate has to be guaranteed either by personal delivery or download from a website combined with the verification of the fingerprint via telephone.

4. Life Cycle of Certificates

4.1. Application

A Certificate can be requested from the SBS security officer. The reason for needing a certificate has to be stated. Certificates are only issued to employees or customers of SBS and not to people unrelated to the company.

A Certificate Signing Request (CSR) can be submitted when filing an application.

4.2. Issuance

After verifying the identity and eligibility of the application a certificate will be issued. If no CSR was submitted, a key pair is generated and used to build the certificate.

If a CSR was handed in the following will be verified:

- correctness of the information stated in the CSR
- correctness of the characters used for certificate name
- conformity of the algorithms and key lengths with security policy

Once all verifications are completed, the applicant will receive the certificate (and the corresponding private key if necessary) via encrypted e-mail. Otherwise, they are informed about their rejection and the reasons for it via e-mail.

4.3. Renewal

The lifetime of the certificates issued by the PKI is defined as:

- ROOT-CA-1: 15 years (until September 2, 2026)
- Issuer certificates: 5 years
- End-user certificates (e-mail, VPN, web server): 2 years (in well justified exceptional cases up to 3 years)

After half of the lifetime a new certificate is issued. This implies that usually

two certificates of a kind are valid at any time.

4.4. Revocation

Either the PKI or the certificate owner can initiate the revocation of a certificate.

Reasons for a certificate revocation include:

- Information contained in the certificate is no longer true.
- The private key of the certificate is compromised or there is suspicion of compromise.
- The certificate is no longer needed.
- One or more algorithms used to create the certificate are cryptographically broken or are no longer regarded as safe. It is the security officer's choice to either revoke the certificate immediately or within a time span adequate to the threat level.
- The issuance CA has been compromised.
- The issuance CA ceases operation.

The reason for a certificate revocation is specified in the Certification Revocation List (CRL) according to RFC 2459. The values mentioned in the standard are interpreted corresponding to the Microsoft Security Guidance[3].

[3] http://technet.microsoft.com/en-us/library/cc700843.aspx

4.4.1. Revocation Process

The request for a certificate revocation is to be submitted to the security officer. The applicant either has to show a valid signature of the certificate in question, bring in the request via the Notes database used in the company or identify himself presenting official photo identification.

The revocation is executed as soon as possible but not later than three days after the revocation request through entries in the CRLs. The owner of the certificate is notified via e-mail.

4.4.2. Modification of Certificates

The modification of existing certificates (the modification and signing of a certificate based on the same private key) will be carried out if there are reasons that suggest to do so. The reasons (for instance the information in the certificate is no longer true) will be reviewed and checked prior to certificate issuance.

4.4.3. Certificate Suspension

The PKI does not suspend certificates (interrupt the validity for a limited period of time). If a certificate is temporarily not used it will be revoked and a request for a new certificate has to be placed as soon as it is needed again.

4.4.4. Private Key Escrow

The PKI does not save user's private keys on principle. If a private key is lost or rendered unusable (e.g. through a forgotten password), the security officer has to be notified. The certificate belonging to the private key will be revoked and a new one has to be applied for.

4.4.5. Publication of Revocation Lists

Certificate Revocation Lists (CRLs) are published on the SBS PKI website. Regardless of certificate revocations, these lists are valid for three months. If a certificate has been revoked, a new revocation list is published within eight hours.

The current CRLs are available via:

- http://pki.sbs.co.at/sbs-root-ca-1.crl
- http://pki.sbs.co.at/sbs-issuer-1.crl
- http://pki.sbs.co.at/sbs-issuer-3.crl

5. Physical, Organizational and Human Resources Controls

5.1. Physical Security Controls

5.1.1. Access Control

SBS buildings are secured by alarm systems, while PKI components are situated in separated, specially secured zones, which only authorized personnel has access to.

5.1.2. Appropriately equipped Server Rooms

The PKI systems are protected from voltage fluctuations and power outages by means of Uninterrupted Power Supply (UPS) technology in order to ensure continuous operations. Furthermore, the systems are temperature controlled and monitored by fire alarm systems.

5.1.3. Business Resilience

PKI information is regularly backed up and stored off-site. Systems and equipment are redundant and emergency plans ensure business continuation after disasters.

5.2. Employee Requirements

All PKI staff have the necessary expertise and are trained in security relevant aspects of PKI operations. All employees fulfill the requirements regarding reliability and trustworthiness. New employees' criminal records are checked to ensure they are suited to work in trusted positions. Furthermore, the Austrian data privacy law and the contract of employment oblige employees to keep secret all information they have access to in connection with their duties.

5.3. Cease of PKI Operation

Owners of valid certificates are notified if the PKI ceases operation for business-related or other reasons. All existing certificates are revoked in this case.

6. Technical Security Measures

6.1. Secure Issuance of Certificates

Certificates are only issued within specially protected systems, which are completely isolated and unconnected to the business network and the internet. The transport of data to and from these systems is only carried out by authorized personnel using dedicated storage media.

6.2. Private Key Protection

The private key of the root certificate is saved on redundant encrypted storage media. The issuer certificates' private keys are stored on smart cards and protected by PINs. All storage media containing private keys is stored in protected areas with measures against physical access and monitored by alarm systems.

When private keys are no longer needed, they are destroyed either by securely deleting the data or mechanically destroying the smart card.

6.3. Protection of Activation Information

The activation information necessary to access private keys is protected by the following measures:

- All PKI staff are obliged to keep PINs and passwords entrusted to them secret and to not write them down.
- If an employee leaves the PKI, all passwords and PINs they knew are changed.
- The PINs used to access the issuer certificates' private keys are only saved encrypted. The passwords to use the private keys of the root certificates are not saved electronically and only stored in specially secured locations.

7. Other business-related or legal regulation

7.1. Fees

Currently, the PKI does not charge users anything for their services.

7.2. Obligations

7.2.1. Obligations of the PKI

The PKI pledges to

- work according to the principle of data saving and only to collect and use information necessary to operate the PKI,
- issue a new certificate revocation list after each certificate revocation and at least a week before the current list is invalid.

7.2.2. Obligations of Certificate Owners

Every owner of a personal certificate is obligated to

- give correct and complete information in a certificate request and to notify the PKI if information in the certificate is incorrect or no longer true,
- keep PINs and private keys safe and not pass them on to other persons

- destroy certificates which are no longer used
- comply with the certificate usage restrictions
- immediately initiate the revocation of a certificate in case the according private key is compromised.
  A private key is regarded compromised if a third party has knowledge of the PIN or the private key password or if this cannot be completely ruled out.

7.3. Warranty

SBS guarantees to a third party relying on correctness of an issued certificate, that the PKI

- complies with the X.509 standards as mentioned in this document
- performs all processes described in this document
- revokes a certificate if necessary

7.4. Liability

The company SBS is liable to the holders of the certificates and injured party for damages contractual in accordance with the regulations of the Austrian Data Protection Act, but assumes no liability under the Digital Signature Act and Signature Ordinance. The certificate holder shall indemnify and holds harmless the company on all matters relating to these certificates.

The company is not liable for damage that occurs due to

- outages or unavailability of PKI or CA services
- delay between a certificate revocation and the next planned issuance of a certification revocation list
- unauthorized use of certificates or use for purposes not specified in this document
- disclosure of private data from certificates or certificate revocation lists

7.5. Applicable Law

The general terms and conditions of the Salzburger Banken Software apply in their valid version.

Court of jurisdiction is the responsible court in Salzburg.

A. Definitions and Acronyms

VPN Virtual Private Network

QMS Quality Management System

SBS Salzburger Banken Software

PKI Public Key Infrastructure

CPS Certification Practice Statement

CRL Certification Revocation List

UPS Uninterrupted Power Supply

CSR Certificate Signing Request