Certification Practice Statement

Revision R4

2017-06-02

Copyright

Für den Inhalt verantwortlich:

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

Änderungsverzeichnis

Version	Autor	Datum	Änderungen
R0	Andreas Hoheneder, Christoph Meinhart	2012-09-01	Initiale Version.
R1	Andreas Hoheneder	2013-01-09	ISSUER lautet nun SBS-ISSUER. OID für die CPS hinzugefügt.
R2	Andreas Hoheneder	2015-11-04	Neuer Issuer SBS-ISSUER-3. ROOT-CA-2 (SHA1) wird nicht unterstützt.
R3	Andreas Hoheneder	2016-10-21	Textfehlerkorrektur; keine inhaltliche Änderung.
R4	Christoph Meinhart, Andreas Hoheneder,	2017-06-02	Textfehlerkorrektur. Spezielle Zertifikate dürfen bis zu 3 Jahre gültig sein. Neuer Issuer TEST-ISSUER-2 löst TEST-ISSUER-1 ab.

Inhaltsverzeichnis

1. Einführung

Dieses Certification Practice Statement (CPS) legt das Sicherheitskonzept der PKI der Salzburger Banken Software (SBS) fest. Es beschreibt die Anforderungen an die Ausstellung, Verwendung, Vernichtung und den Rückruf von Zertifikaten innerhalb der PKI in Übereinstimmung mit der Sicherheitsleitlinie der SBS um einen sicheren Betrieb der PKI zu gewährleisten.

Hinsichtlich der Gliederung orientiert sich dieses Dokument am RFC-Standard 3647 "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework".

1.1. Übersicht des PKI-Aufbaus

Die PKI betreibt ein Root-Zertifikat, dem die Issuer-Zertifikate unterstellt sind. Es werden von der ROOT-CA-1 keine Zertifikate signiert die den Hashalgorithmus SHA1 verwenden, da dieser kryptographische Schwächen[1] aufweist.

1.2. Dokumentenname und Identifikation

Bezeichnung:	Certification Practice Statement (CPS)
Version:	R4 DE
Objekt-ID:	2.5.29.32.0[2]

Dieses Dokument wurde laut Qualitätsmanagementsystem (QMS) als "öffentlich" eingestuft.

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

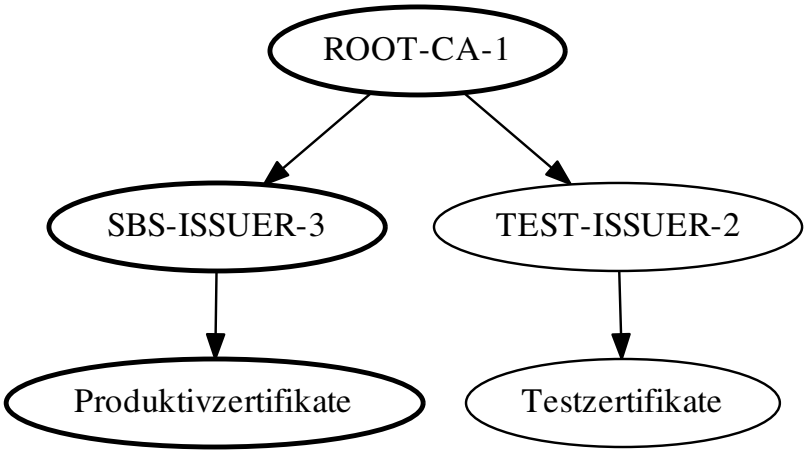

Abbildung 1: Aufbau der PKI

1.3. Anwendung der Zertifikate

1.3.1. Zertifikate zur Nutzung des VPN-Zugangs

Die VPN-Zertifikate dienen zur Authentifizierung autorisierter Zugriffe von SBS-Mitarbeitern und Kunden von externen Geräten auf das Unternehmensnetzwerk. Durch diese Zertifikate wird auch eine Verschlüsselung und Integritätssicherung dieser Kommunikation erreicht.

1.3.2. Nutzung zum Einsatz in der Softwareentwicklung

Von der PKI ausgestellte Zertifikate kommen auch in der Softwareentwicklung zum Einsatz: So wird die Integrität von Softwarelieferungen durch den Einsatz digitaler Signaturen geschützt und es werden spezielle Testzertifikate in den Softwaretests verwendet.

1.3.3. Absicherung des E-Mail-Verkehrs

Der E-Mail-Verkehr zwischen der SBS und Kunden wird einerseits durch den Einsatz von Zertifikaten zum Aufbau gesicherter Verbindungen auf den E-Mail-Servern und andererseits durch die Verwendung digitaler signierter E-Mails vor unbefugtem Mitlesen oder Änderung geschützt.

1.3.4. Absicherung unternehmensinterner Infrastruktur

Zusätzlich zu den oben genannten Zertifikaten werden auch noch weitere zur unternehmensinternen Verwendung von der PKI ausgestellt. Diese kommen auf Netzwerkkomponenten und Systemen der SBS zur Sicherstellung der Vertraulichkeit und Integrität der Kommunikation zum Einsatz.

1.4. Administration des CPS

Dieses Dokument wird innerhalb des zertifizierten QMS der SBS verwaltet und versioniert. Darüber hinaus ist die aktuelle Version öffentlich auf der SBS-Website abrufbar.

Die Wartung des Dokuments obliegt dem Sicherheitsverantwortlichen.

1.5. Ansprechpartner

Informationen zur PKI der SBS erhält man auf folgenden Wegen:

- auf der SBS-Website unter `http://pki.sbs.co.at`
- per E-Mail an info@sbs.co.at
- auf schriftliche Anfrage an:
  SBS Software Ges.m.b.H.
  Weiserhofstraße 18
  5020 Salzburg
  Österreich

2. Identifizierung und Authentifizierung

2.1. Identifikation von Zertifikaten

2.1.1. Zertifikatsnamen

Die ausgestellten Zertifikate sind mit Distinguished Names nach X.501 versehen, wobei in diesem nur die Verwendung von Buchstaben des englischen Alphabets, Leerzeichen und die Sonderzeichen „_“, „-“, „.“ und „@“ erlaubt sind.

Bei Zertifikaten für natürliche Personen müssen Kontaktinformationen (wie eine E-Mail-Adresse) enthalten sein. Jedes dieser Zertifikate ist genau einer Person zugeordnet, es werden keine Sammelzertifikate für natürliche Personen ausgestellt.

2.1.2. Algorithmus zur Vergabe der X.509-Seriennummern

Die Vergabe der X.509-Seriennummern in den Zertifikaten wird nach folgendem Schema durchgeführt:

xx yy yy yy yy zz zz zz zz

xx ... 1 Byte fortlaufende Nummer der Root-CAs:
01 ... SBS Root-CA-1 mit sha256 und 4096 Bit

yy ... 4 Byte fortlaufende Nummer der Issuer-CAs:
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 Byte fortlaufende Nummer der eigentlichen Zertifikate

2.1.3. Technische Details der ausgestellten Zertifikate

Von der PKI werden digitale Zertifikate nach X.509 Version 3 (RFC 3280) ausgestellt. Als Signaturalgorithmus wird SHA256 in Verbindung mit RSA verwendet. Sämtliche ausgestellte Zertifikate werden mit den Erweiterungen „X509v3 Subject Key Identifier“ (Fingerabdruck des Zertifikats) und alle nicht-CA-Zertifikate mit „X509v3 Authority Key Identifier“ versehen. Darüber hin-

aus werden bei allen Zertifikaten die erlaubten Anwendungsbereiche über die Erweiterung „X509v3 Key Usage“ eingegrenzt.

2.2. Identitätsüberprüfung von Personen

Zertifikate werden nur an Mitarbeiter oder Kunden der SBS ausgestellt, die sich in der unternehmensinternen Notes-Datenbank befinden. Bei Neuanstellung eines Mitarbeiters wird über Vorlage eines amtlichen Lichtbildausweises die Identifizierung abgewickelt.

3. Veröffentlichungen und Verteilung der Zertifikate

Die Zertifikate werden bei Anschluss an das Notes-System der SBS verschlüsselt über E-Mail zugestellt. Handelt es sich bei dem Empfänger um einen Kunden, der nicht über dieses System angeschlossen ist, so wird entweder über persönliche Übergabe oder Abruf per Website mit anschließender telefonischer Verifikation des Zertifikat-Fingerabdrucks die Authentizität des übermittelten Zertifikats sichergestellt.

4. Lebenszyklus der Zertifikate

4.1. Beantragung

Ein Zertifikat kann beim Sicherheitsverantwortlichen der SBS unter Angabe des Grundes beantragt werden. Zertifikate werden grundsätzlich nur an Mitarbeiter oder Kunden der SBS und nicht an unternehmensfremde Personen ausgestellt.

Bei der Antragstellung kann ein Certificate Signing Request (CSR) eingereicht werden.

4.2. Ausstellung

Nach der Prüfung der Identität und Berechtigung des Antrags wird ein Zertifikat ausgestellt. Wenn kein CSR eingebracht wurde, wird ein neues Schlüsselpaar erstellt und für das Zertifikat verwendet.

Im Falle der Einreichung eines CSR werden zusätzlich noch folgende Überprüfungen durchgeführt:

- Korrektheit der Angaben im CSR
- Korrektheit der verwendeten Zeichen für den Zertifikatsnamen
- Übereinstimmung der verwendeten Algorithmen und Schlüssellängen für das Schlüsselpaar mit den Sicherheitsbestimmungen

Wurden alle Überprüfungen erfolgreich abgeschlossen, wird dem Antragsteller das Zertifikat (und gegebenenfalls der dazugehörige private Schlüssel) verschlüsselt per E-Mail zugestellt. Anderenfalls wird er über E-Mail von der Ablehnung und den Gründen dafür informiert.

4.3. Erneuerung

Für die von der PKI ausgestellten Zertifikate gelten folgende Gültigkeitsdauern:

- ROOT-CA-1: 15 Jahre (bis 2. September 2026)

- Issuer-Zertifikate: 5 Jahre
- Endnutzer-Zertifikate (E-Mail, VPN, Webserver): 2 Jahre (in gut begründeten Ausnahmefällen bis zu 3 Jahre)

Jeweils nach dem Ablauf der Hälfte der Gültigkeitsdauer wird das Nachfolge-Zertifikat ausgerollt. So sind im Normalfall immer zwei Zertifikate jeden Typs gültig.

4.4. Widerruf

Der Widerruf eines Zertifikats kann entweder durch den Zertifikatsinhaber oder die PKI veranlasst werden.

Gründe für den Widerruf umfassen:

- Die im Zertifikat enthaltenen Daten entsprechen nicht mehr den Tatsachen.
- Der zum Zertifikat gehörende geheime Schlüssel wurde kompromittiert oder es Besteht der Verdacht einer Kompromittierung.
- Das Zertifikat wird nicht mehr länger benötigt.
- Einer oder mehrere der eingesetzten Algorithmen des Zertifikats ist gebrochen oder gilt als nicht mehr sicher. Hier obliegt es dem Sicherheitsverantwortlichen, das Zertifikat sofort zu widerrufen oder es je nach Gefährdungslage innerhalb einer angemessenen Frist auszutauschen.
- Die ausstellende CA wurde kompromittiert.

- Die ausstellende CA stellt die Dienste ein.

Der Grund für den Zertifikatswiderruf wird in der Certification Revocation List (CRL) laut RFC 2459 angegeben. Die im Standard definierten Werte werden laut der Microsoft Security Guidance [3] interpretiert.

4.4.1. Ablauf eines Widerrufs

Ein Widerruf kann durch Antrag bei dem Sicherheitsbeauftragten gestellt werden. Der Antragsteller muss entweder eine Signatur des entsprechenden Zertifikats über den Antrag vorweisen, den Antrag über die im Unternehmen verwendete Notes-Datenbank einbringen oder sich durch Vorlegung eines amtlichen Lichtbildausweises identifizieren.

Der Widerruf erfolgt unverzüglich, spätestens aber innerhalb von drei Arbeitstagen nach Zugang des Widerrufantrags durch Einträge in den CRLs. Der Inhaber des widerrufenen Zertifikats wird über den Widerruf per E-Mail in Kenntnis gesetzt.

4.4.2. Änderung von Zertifikaten

Eine Änderung von Zertifikaten (das Ändern und neue Signieren eines Zertifikats basierend auf demselben privaten Schlüssel) wird bei Vorliegen entsprechender Gründe (beispielsweise entsprechen die im Zertifikat angegeben Daten nicht mehr den Tatsachen) nach vorgenommener Prüfung durchgeführt.

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

4.4.3. Suspendierung von Zertifikaten

Die PKI nimmt keine Suspendierung (befristetes Aussetzen der Gültigkeit) von Zertifikaten vor. Wird ein Zertifikat vorübergehend nicht benötigt, wird es widerrufen und es muss ein neues Zertifikat beantragt werden, sobald es benötigt wird.

4.4.4. Hinterlegung und Wiedererlangen von privaten Schlüsseln

Die PKI hinterlegt grundsätzlich keine privaten Schlüssel von Zertifikatsinhabern. Gerät ein privater Schlüssel in Verstoß bzw. kann dieser nicht mehr verwendet werden (etwa durch Vergessen des Passworts) so muss dies gemeldet werden. Das zugehörige Zertifikat wird widerrufen und es muss ein neues beantragt werden.

4.4.5. Veröffentlichung von Widerrufslisten

Widerrufslisten (CRLs) werden auf der Website der SBS-PKI veröffentlicht. Unabhängig von Zertifikatswiderrufen beträgt die Gültigkeitsdauer der Widerrufslisten drei Monate. Eine Neuausstellung der Widerrufsliste wird spätestens eine Woche vor Ablauf der letzten noch gültigen Widerrufsliste durchgeführt. Falls ein Zertifikat widerrufen wurde, wird innerhalb von 8 Stunden eine neue Widerrufsliste publiziert.

Die aktuellen CRLs sind unter folgenden Webadressen hinterlegt:

- `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. Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen

5.1. Infrastrukturelle Sicherheitsmaßnahmen

5.1.1. Zugangskontrollen

Die Gebäuden der SBS sind mit Alarmanlagen gesichert, wobei sich die PKI-Komponenten in abgetrennten, gesondert gesicherten Zonen befinden, zu denen nur Berechtigte Zutritt haben.

5.1.2. Geeignete Ausstattung der Serverräume

Die Systeme der PKI werden durch eine Unterbrechungsfreie Stromversorgung (USV) vor Spannungsschwankungen und Stromausfällen geschützt um einen kontinuierlichen Betrieb oder ein ordnungsgemäßes Abschalten sicherzustellen. Darüber hinaus sind die Systeme entsprechend klimatisiert und durch eine Brandmeldeanlage überwacht.

5.1.3. Notfallvorsorge

Die PKI verfügt über regelmäßige, außerhalb des Betriebsgeländes verwahrte Datensicherungen, redundant ausgelegte Anlagen und Geräte sowie definierte

Notfallpläne um einen schnellen Anlauf nach einer Katastrophe zu gewährleisten.

5.2. Anforderungen an die Mitarbeiter

Die Mitarbeiter der PKI verfügen durch eine entsprechende Ausbildung über das benötigte Fachwissen und sind in den sicherheitsrelevanten Aspekten des PKI-Betriebs besonders geschult. Sie erfüllen die erforderlichen Ansprüche an Verlässlichkeit und Vertrauenswürdigkeit, neue Mitarbeiter werden anhand eines Auszugs aus dem Strafregister auf ihre Unbescholtenheit überprüft. Darüber hinaus sind alle Mitarbeiter laut Datenschutzgesetz und Arbeitsvertrag zur Verschwiegenheit über Daten, die ihnen im Zusammenhang mit ihrer Tätigkeit zugänglich gemacht werden, verpflichtet.

5.3. Einstellung der Zertifizierungsdienste

Sollte die PKI aus betrieblichen oder sonstigen Gründen den Betrieb einstellen, werden die Inhaber von gültigen Zertifikaten rechtzeitig benachrichtigt. Mit der Einstellung des Betriebs werden alle Zertifikate widerrufen.

6. Technische Sicherheitsmaßnahmen

6.1. Sichere Ausstellung der Zertifikate

Die Ausstellung neuer Zertifikate wird ausschließlich auf speziell gesicherten, nicht an das Unternehmensnetzwerk oder das Internet angeschlossenen Systemen durchgeführt. Der Transport von Daten zu und von diesen Systemen wird nur durch dedizierte Speichermedien und nur von autorisiertem Personal durchgeführt.

6.2. Schutz der privaten Schlüssel

Der private Schlüssel des CA-Root-Zertifikats ist in mehrfacher Ausführung auf verschlüsselten Speichermedien verwahrt. Die privaten Schlüssel der Issuer-Zertifikate befinden sich auf Smartcards die durch PINs geschützt sind. Diese Datenträger werden in gegen physischen Einbruch gehärteten und durch Alarmanlagen geschützten Bereichen aufbewahrt.

Werden private Schlüssel nicht mehr benötigt, werden sie durch sicheres Löschen der Dateien, beziehungsweise mechanische Zerstörung der Smartcard, sicher vernichtet.

6.3. Sicherheitsmaßnahmen für Aktivierungsdaten

Die Aktivierungsdaten für die privaten Schlüssel werden durch folgende Maßnahmen geschützt:

- Alle Mitarbeiter der PKI sind verpflichtet, die ihm anvertrauten PINs

und Passwörter geheim zu halten und nicht aufzuschreiben.

- Falls ein Mitarbeiter nicht mehr länger in der PKI tätig ist, werden die ihm bekannten PINs und Passwörter ersetzt.

- Die für die Verwendung der privaten Schlüssel der Issuer-Zertifikate notwendigen PINs werden nur verschlüsselt gespeichert. Die Passwörter zur Verwendung der privaten Schlüssel der Root-Zertifikate werden nicht elektronisch gespeichert und nur an speziell gesicherten Orten hinterlegt.

7. Weitere geschäftliche und rechtliche Regelungen

7.1. Gebühren

Durch die Nutzung der von der PKI zur Verfügung gestellten Dienste entstehen Anwendern derzeit keine Kosten.

7.2. Verpflichtungen

7.2.1. Pflichten der PKI

Die PKI verpflichtet sich,

- nach dem Grundsatz der Datensparsamkeit zu arbeiten und nur für den Betrieb der PKI notwendige Daten zu erheben und zu nutzen,

- nach jedem Zertifikatswiderruf, spätestens aber eine Woche vor Ablauf der Widerrufsliste, eine aktualisierte zu veröffentlichen.

7.2.2. Pflichten der Zertifikatsinhaber

Jeder Zertifikatsinhaber eines personenbezogenen Zertifikats ist verpflichtet,

- bei der Beantragung von Zertifikaten korrekte und vollständige Angaben zu machen und die PKI in Kenntnis zu setzen, falls Angaben in seinem Zertifikat nicht oder nicht mehr den Tatsachen entsprechen
- PINs und private Schlüssel geheim zu halten und nicht an Dritte weiterzugeben
- nicht mehr benötigte Zertifikate unbrauchbar zu machen
- die Beschränkungen hinsichtlich Verwendung der Zertifikate einzuhalten
- im Falle einer Kompromittierung des privaten Schlüssels unverzüglich den Widerruf des Zertifikats zu veranlassen.
  Ein privater Schlüssel gilt als kompromittiert, falls Dritte von PIN oder Passwort Kenntnis bekommen haben oder falls dies nicht mit Sicherheit auszuschließen ist.

7.3. Gewährleistung

Die SBS gewährleistet für die PKI gegenüber Dritten, die auf die Richtigkeit eines ausgestellten Zertifikats vertraut haben, dass

- die X.509-Standards, wie im CPS beschrieben, eingehalten werden
- die Abläufe, wie im CPS beschrieben, durchgeführt werden

- ein Zertifikat bei Vorliegen der Voraussetzungen widerrufen wird

7.4. Haftung

Die SBS haftet den Inhabern der Zertifikate und geschädigten Dritten gegenüber für vertragstypische Schäden gemäß den Bestimmungen des österreichischen Datenschutzgesetzes, übernimmt aber keinerlei Haftung im Rahmen des Signaturgesetzes bzw. der Signaturverordnung. Der Zertifikatsinhaber hat die SBS in allen Belangen im Zusammenhang mit diesen Zertifikaten schad- und klaglos zu halten.

Die SBS haftet nicht für Schäden, die durch

- den Ausfall der PKI- oder CA-Dienstleistungen entstehen
- die Verzögerung zwischen dem Widerruf eines Zertifikats und der nächsten planmäßigen Veröffentlichung einer CRL entstehen
- Schäden, die durch unberechtigte Nutzung von Zertifikaten oder durch Nutzung außerhalb der im CPS festgelegten Zwecke entstehen
- Schäden, die durch die Offenlegung persönlicher Daten aus Zertifikaten oder Widerrufslisten entstehen

7.5. Geltendes Recht

Es gelten die Allgemeinen Geschäftsbedingungen der Salzburger Banken Software in ihrer gültigen Fassung.

Gerichtsstand ist das sachlich zuständige Gericht in Salzburg.

A. Definitionen und Akronyme

VPN Virtual Private Network

QMS Qualitätsmanagementsystem

SBS Salzburger Banken Software

PKI Public Key Infrastruktur

CPS Certification Practice Statement

CRL Certification Revocation List

USV Unterbrechungsfreie Stromversorgung

CSR Certificate Signing Request