Payment Services

SIC CA

Zertifizierungsrichtlinien

Certificate Practice Statement (CPS)
der SIC Customer ID CA 1024 Level 2

Hinweise

Die in diesem Dokument enthaltenen Angaben sind ohne Gewähr und können jederzeit ohne vorherige Benachrichtigung geändert werden.

Dieses Dokument ist mit grösster Sorgfalt erstellt worden, doch können Fehler und Ungenauigkeiten nicht vollständig ausgeschlossen werden.
SIX kann für Fehler und deren Folgen weder eine juristische Verantwortung noch irgendwelche Haftung übernehmen.

Inhaltsverzeichnis

1 Einführung

1.1 Überblick

Das vorliegende Dokument beschreibt die Zertifikatstypen und die Zertifizierungsrichtlinien (CPS) der Zertifizierungsstelle von SIX Interbank Clearing (SIC CA).

Die Zertifizierungsrichtlinien enthalten ein Regelwerk, das den Einsatzbereich von Zertifikaten für eine bestimmte Benutzergruppe und/oder Anwendungsklasse mit gemeinsamen Sicherheitsanforderungen definiert.

Die vorliegenden Zertifizierungsrichtlinien gelten für Zertifikate für Dienstleistungen wie sie im Kapitel 1.2 beschrieben werden und richten sich an die Teilnehmer dieser Dienste.

1.2 Anwendungsbereich

Diese Zertifizierungsrichtlinien gelten ausschliesslich für Zertifikate, welche von der SIC Customer ID CA 1024 Level 2 für die sichere Client-Authentifizierung im Rahmen des SSL-Protokolls für die Dienstleistungen der Gruppengesellschaften von SIX ausgestellt werden.

SIX Payment Services AG:

- payCOM^{web}
- Web-Applikationen (LSV^{+}/BDD-Aufträge und -Stammdaten)

SIX Interbank Clearing AG:

- remoteGATE
- SIC-Extranet

Die SIC CA ist keine öffentliche CA. Die Teilnehmerzertifikate können nicht für verbindliche elektronische Signaturen (gemäss Signaturgesetz) verwendet werden.

1.3 Sprachregelung

In diesem Dokument werden die Ausdrücke «Teilnehmer» bzw. «Schlüsselinhaber» für männliche, weibliche und juristische Personen verwendet.

Der Ausdruck «Aussteller» bezeichnet die juristische Person des CA Betreibers.

1.4 Abkürzungen

In diesem Dokument werden folgende Abkürzungen verwendet:

CA **C**ertification **A**uthority (Zertifizierungsstelle)

CPS **C**ertificate **P**ractice **S**tatement (Zertifizierungsrichtlinien)

CRL **C**ertificate **R**evocation **L**ist (Sperrliste)

DN **D**istinguished **N**ame (Name des Zertifikatinhabers (Subject DN) bzw. des Zertifikatausgebers (Issuer DN))

ID **Id**entifikation

PIN **P**ersönliche **I**dentifikations-**N**ummer

PKI **P**ublic **K**ey **I**nfrastruktur

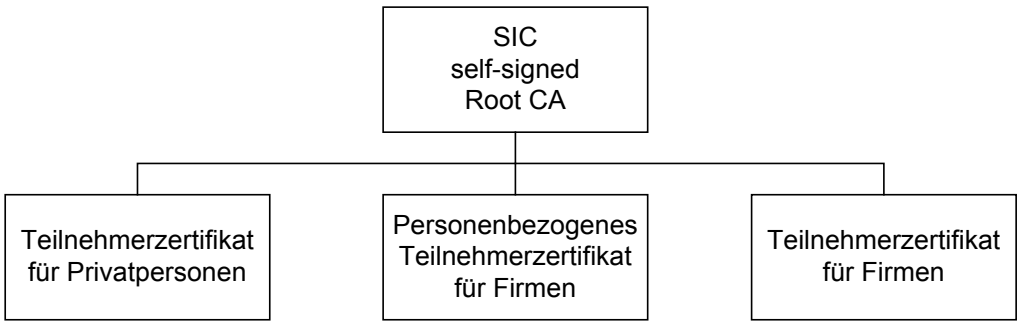
RDN **R**elative **D**istinguished **N**ame (O=Organisation, OU=Organsiational Unit, L=Locality, ST=State or Province, CN=Common Name, C=Country)

RSA Name des von **R**ivest, **S**hamir und **A**dleman entwickelten Public-Key Systems

2 SIC Zertifikate

2.1 Zertifikatshierarchie

Die Zertifikatshierarchie besteht aus einer self-signed Root CA, welche unmittelbar die Teilnehmerzertifikate zertifiziert:



Innerhalb der verschiedenen Zertifikatstypen gibt es jeweils nur eine Klasse von Zertifikaten.

2.2 Zertifikatstypen

2.2.1 Allgemeine Informationen

Alle von der SIC CA ausgestellten Zertifikate basieren auf dem X.509v3 Standard. Es werden ausschliesslich Zertifikate für 1024 Bit RSA Schlüssel mit öffentlichem Exponent 65537 und SHA-1 als Hash-Algorithmus ausgestellt.

2.2.2 Zertifikatsmatrix

Die nachstehende Tabelle zeigt, welche Zertifikatstypen für die verschiedenen Dienstleistungen zum Einsatz kommen.

	Private Certificate	Staff Certificate	Corporate Certificate
Web-Applikationen	–	x	–
payCOM^{web}	x	x	x
remoteGATE	–	x	–
SIC-Extranet	–	x	–

2.2.3 CA Zertifikat

Das CA Zertifikat ist mit dem korrespondierenden privaten Schlüssel signiert (self-signed). Die Überprüfung des CA Zertifikats erfolgt durch Vergleich des Hash-Wertes (Fingerprint) des Zertifikats mit dem offiziell von der SIX Interbank Clearing AG publizierten Wert. Die Schlüssellänge des CA Zertifikats beträgt 1024 Bit.

2.2.3.1 Namensgebung

Das SIC Root Zertifikat hat folgenden Subject- und Issuer-DN:

RDN	Beschreibung
O	Swiss Interbank Clearing AG
OU1	CA Services
OU2	Level 2 (Hardware Token Based Client Certificates)
C	CH
CN	SIC Customer ID CA 1024 Level 2

2.2.3.2 Verwendungszweck

Der CA Schlüssel wird für das Ausstellen von Teilnehmerzertifikaten und das Ausstellen von Sperrlisten (CRL) verwendet. Zusätzlich wird mit dem öffentlichen CA Schlüssel ein symmetrischer Schlüssel für die Verwaltung der CA Datenbank geschützt.

2.2.3.3 Gültigkeitsperiode

Die Gültigkeitsperiode des CA Zertifikats beträgt zehn (10) Jahre. Das CA Zertifikat ist gültig von 31. Oktober 2011 bis 31. Oktober 2021.

2.2.3.4 Fingerprint

Hash Algorithmus	Fingerprint
MD5	`32B1 87D7 861E 85D6 5ADD 1B4C BF86 9B87`
SHA-1	`CB2F 6004 69C4 DA8B D028 5068 A736 0FFE 0BD1 B896`

2.2.3.5 Erweiterungen

Das CA Zertifikat enthält die folgenden X.509v3 kompatiblen Erweiterungen.

Name	Wert
Basic Constraints	• CA: true • Pathlength: 0
Key Usage	• Certificate Signing • CRL Signing
Subject Key Identifier	`569F 5AFA B52B 8E07 D92A 458A 0D59 D538 27D0 54FB`

Alle Erweiterungen sind non-critical.

2.2.4 Teilnehmerzertifikat für Privatpersonen (Private Certificate)

Die Registrierung der Teilnehmer erfolgt gemäss den Vertragsbedingungen der entsprechenden Dienstleistung.

2.2.4.1 Namensgebung

RDN	Beschreibung	Zwingend
O	Privatperson	Ja
OU1	BPID	Ja
OU2		Nein
OU3		Nein
C	Land	Ja
ST	Kanton	Nein
L	Ort	Nein
CN	Name der Privatperson	Ja
Email	E-Mail der Privatperson	Ja

2.2.4.2 Verwendungszweck

Das Teilnehmerzertifikat wird ausschliesslich für die sichere Client-Authentifizierung im Rahmen des SSL-Protokolls des entsprechenden Teilnehmers verwendet.

2.2.4.3 Gültigkeitsperiode

Die Gültigkeitsperiode beträgt drei (3) Jahre.

2.2.4.4 Erweiterungen

Das Teilnehmerzertifikat enthält die folgenden X.509v3 kompatiblen Erweiterungen.

Name	Wert
Key Usage	• keyEncipherment • digitalSignature
Authority Key Identifier	`569F 5AFA B52B 8E07 D92A 458A 0D59 D538 27D0 54FB`

Alle Erweiterungen sind non-critical.

2.2.5 Personenbezogenes Teilnehmerzertifikat für Firmen (Staff Certificate)

Ein personenbezogenes Teilnehmerzertifikat für Firmen wird an eine spezifische Person ausgegeben, welche die Dienstleistung wie im Kapitel 1.2 beschrieben im Auftrag einer Firma nutzen möchten.

Die Registrierung der Teilnehmer erfolgt gemäss den Vertragsbedingungen der entsprechenden Dienstleistung.

2.2.5.1 Namensgebung

RDN	Beschreibung	Zwingend
O	Name der Firma	Ja
OU1	BPID	Ja
OU2	Name der Abteilung / Gruppe	Nein
OU3		Nein
C	Land	Ja
ST	Kanton	Nein
L	Ort	Nein
CN	Name des Teilnehmers	Ja
Email	E-Mail der Privatperson	Ja

2.2.5.2 Verwendungszweck

Ein personenbezogenes Teilnehmerzertifikat für Firmen kann für die geschäftliche Nutzung der Dienstleistung gemäss Kapitel 1.2 genutzt werden. Das Teilnehmerzertifikat wird ausschliesslich für die sichere Client-Authentifizierung im Rahmen des SSL-Protokolls des entsprechenden Teilnehmers verwendet.

2.2.5.3 Gültigkeitsperiode

Die Gültigkeitsperiode beträgt drei (3) Jahre.

2.2.5.4 Erweiterungen

Das Teilnehmerzertifikat enthält die folgenden X.509v3 kompatiblen Erweiterungen.

Name	Wert
Key Usage	• keyEncipherment • digitalSignature
Authority Key Identifier	`569F 5AFA B52B 8E07 D92A 458A 0D59 D538 27D0 54FB`

Alle Erweiterungen sind non-critical.

2.2.6 Teilnehmerzertifikat für Firmen (Corporate Certificate)

Ein Teilnehmerzertifikat für Firmen wird an Teilnehmer ausgegeben, welche die Dienstleistung wie im Kapitel 1.2 beschrieben im Auftrag einer Firma nutzen möchten. Das Teilnehmerzertifikat für Firmen kann von mehreren Teilnehmern gleichzeitig genutzt werden. Die Registrierung der Teilnehmer erfolgt gemäss den Vertragsbedingungen der entsprechenden Dienstleistung.

Es empfiehlt sich, grundsätzlich personenbezogene Teilnehmerzertifikate für Firmen zu verwenden.

2.2.6.1 Namensgebung

RDN	Beschreibung	Zwingend
O	Name der Firma	Ja
OU1	BPID	Ja
OU2	Name der Abteilung / Gruppe	Ja
OU3		Nein
C	Land	Ja
ST	Kanton	Nein
L	Ort	Nein
CN	*Corporate Certificate*	Ja
Email		Nein

2.2.6.2 Verwendungszweck

Ein Teilnehmerzertifikat für Firmen kann für die geschäftliche Nutzung der Dienstleistung gemäss Kapitel 1.2 genutzt werden. Das Teilnehmerzertifikat wird ausschliesslich für die sichere Client-Authentifizierung im Rahmen des SSL-Protokolls des entsprechenden Teilnehmers verwendet.

2.2.6.3 Gültigkeitsperiode

Die Gültigkeitsperiode beträgt drei (3) Jahre.

2.2.6.4 Erweiterungen

Das Teilnehmerzertifikat enthält die folgenden X.509v3 kompatiblen Erweiterungen.

Name	Wert
Key Usage	• keyEncipherment • digitalSignature
Authority Key Identifier	`569F 5AFA B52B 8E07 D92A 458A 0D59 D538 27D0 54FB`

Alle Erweiterungen sind non-critical.

3 CA Infrastruktur

3.1 Betreiber

Der Betreiber der CA ist die SIX Interbank Clearing:

SIX Interbank Clearing AG
Hardturmstrasse 201
Postfach
8021 Zürich

3.2 CA Schlüssel

3.2.1 Generierung

Die Erzeugung der CA Schlüsselpaare wurde in einer gesicherten Umgebung durchgeführt. Die Schlüsselpaare wurden mehrfach redundant auf verschiedenen Hardware Token gespeichert. Die Hardware Token sind über Zugriffcodes geschützt und in Sicherheitstresoren abgelegt.

Der Prozess der Schlüsselgenerierung garantiert, dass der private Schlüssel der CA nur auf den dafür vorgesehenen Hardware Token gespeichert ist. Der private Schlüssel kann den Hardware Token nicht verlassen.

3.2.2 Verteilung des öffentlichen CA Schlüssels

- Jeder Teilnehmer erhält zusammen mit der Benutzer-PIN der SmartCard den Fingerprint des CA Zertifikats per Post (im Starter Kit enthalten).
- Jeder Teilnehmer erhält die SmartCard per eingeschriebener Post.
- Das CA Zertifikat kann bei der SIX Interbank Clearing AG bezogen werden.

3.3 Verzeichnisdienste

Es gibt keinen öffentlichen Verzeichnisdienst.

3.4 Einstellung der Tätigkeit

Die SIX Interbank Clearing AG informiert alle Teilnehmer, falls eine Einstellung der Tätigkeiten der CA vorgesehen ist.

3.4.1 Aufbewahrungspflicht

Die SIX Interbank Clearing AG verpflichtet sich, die Daten der Teilnehmer für eine bestimmte Zeitdauer aufzubewahren:

- Vertrag
- Teilnehmerdaten
- Zertifikat mit den entsprechenden Statusinformationen

3.5 Sicherheit

3.5.1 Systemsicherheit

Die SIC CA wird auf einem dedizierten System betrieben. Der Zugang zum CA System unterliegt physischen Zugangskontrollen.

3.5.2 Personelle Sicherheit

Der Zugriff auf das SIC CA System ist auf einen festgelegten Personenkreis beschränkt. Alle kritischen Operationen werden ausschliesslich im Vieraugenprinzip durchgeführt.

3.6 Auditing

Die SIC CA unterliegt einem periodischen Audit durch Revisoren von SIX.

4 Zertifizierungsrichtlinien

4.1 Registrierung der Teilnehmer

Die Registrierung der Teilnehmer erfolgt gemäss geltendem Vertragsrecht der entsprechenden Dienstleistung gemäss Kapitel 1.2.

4.2 Generierung der Teilnehmerschlüssel

Die RSA Schlüsselpaare werden bei der SIX Interbank Clearing AG erzeugt. Der Prozess der Schlüsselgenerierung garantiert, dass der private Schlüssel nur auf dem Hardware Token gespeichert ist. Der private Schlüssel kann den Hardware Token nicht verlassen. Die SIX Interbank Clearing AG hat keine Kopie des privaten Schlüssels.

4.3 Zertifikatsantrag

Jeder Person oder Firma, die einen gültigen Vertrag gemäss Kapitel 4.1 abgeschlossen hat, kann einen Antrag auf ein Teilnehmerzertifikat stellen. Die Prüfung des Antrags erfolgt durch die SIX Interbank Clearing AG. Es liegt in der Verantwortung der SIX Interbank Clearing AG, ein Teilnehmerzertifikat gemäss Antrag auszustellen oder den Antrag abzuweisen.

4.4 Verteilung der Schlüssel und Zertifikate

Die SmartCard mit dem Teilnehmerschlüssel und dem dazugehörenden Zertifikat sowie der Benutzer-PIN werden dem Teilnehmer auf getrenntem Weg zugestellt.

Lieferung per normaler Post:

- Benutzer-PIN für die SmartCard
- Fingerprint des SIC Root CA Zertifikats

Lieferung per eingeschriebener Post:

- SmartCard mit dem Teilnehmerschlüssel und dem Teilnehmerzertifikat

4.5 Verpflichtungen der Teilnehmer

4.5.1 Verwendungszweck der Teilnehmerzertifikate

Die Teilnehmerzertifikate sind ausschliesslich für die Dienstleistungen gemäss Kapitel 1.2 und den vertraglich vereinbarten Bedingungen einzusetzen. Der alleinige Verwendungszweck ist die Client-Authentisierung im Rahmen des SSL-Protokolls für die Dienstleistungen gemäss Kapitel 1.2.

Die SIC Customer ID CA 1024 Level 2 ist keine öffentliche CA. Die Teilnehmerzertifikate können nicht für verbindliche elektronische Signaturen (gemäss Signaturgesetz) verwendet werden.

SIX Interbank Clearing AG lehnt jede Haftung ab, falls die Teilnehmerzertifikate für andere Zwecke als die Client-Authentisierung im Rahmen des SSL-Protokolls für die Dienstleistungen gemäss Kapitel 1.2 eingesetzt werden.

4.5.2 Verpflichtungen der Schlüsselinhaber

Der Schlüsselinhaber ist für die Sicherheit der privaten Schlüsselkomponenten in seinem Besitz verantwortlich. Um die Sicherheit zu gewährleisten, hat der Schlüsselinhaber insbesondere folgendes zu beachten:

- Ändern des Benutzer-PIN der SmartCard sofort nach Erhalt der SmartCard
- Bei personengebunden Zertifikaten die SmartCard und/oder den PIN nicht an Dritte weiterzugeben
- Bei nicht personengebundenen Zertifikaten die SmartCard und/oder den PIN nur an berechtigte Personen im eigenen Unternehmen weitergeben
- Den privaten Schlüssel ausschliesslich für den vorgegebenen Verwendungszweck gemäss Kapitel 1.2 einzusetzen
- Geeignete Massnahmen zu treffen um das System, auf welchem die Schlüssel verwendet werden, zu schützen (Virenschutz, Zugangsbeschränkung etc.)
- Bei Kompromittierung des Schlüssels oder Verlust der SmartCard das Zertifikat unverzüglich sperren zu lassen

4.6 Sperren von Zertifikaten

Die SIC PKI bietet die Möglichkeit, Zertifikate unwiderruflich zu sperren (revozieren). Die Sperrung ist eine irreversible, vorzeitige Beendigung der Gültigkeit eines Zertifikats. Gesperrte Zertifikate können nicht mehr für die Dienstleistungen von SIX gemäss Kapitel 1.2 verwendet werden. Sowohl die Teilnehmer wie auch der Aussteller kann eine Sperrung der Zertifikate veranlassen.

4.6.1 Teilnehmerseitige Gründe für eine Sperrung

Jeder Teilnehmer muss eine Sperrung seines Teilnehmerzertifikates beantragen bei

- begründetem Verdacht, dass der Teilnehmerschlüssel kompromittiert wurde
- Diebstahl oder Verlust der SmartCard
- Vertragsauflösung

4.6.2 Ausstellerseitige Gründe für eine Sperrung

SIX Interbank Clearing AG hat das Recht, Teilnehmerzertifikate ohne spezifischen Antrag des Teilnehmers zu sperren bei

- begründetem Verdacht, dass der Teilnehmerschlüssel kompromittiert wurde
- Missbrauch der Systeme von SIX und/oder Dienstleistungen gemäss Kapitel 1.2 durch den Teilnehmer
- Einstellung des PKI Betriebs

4.6.3 SIX-gruppengesellschaftliche Gründe für eine Sperrung

Der Dienstleistungs-Owner hat das Recht, Teilnehmerzertifikate zu sperren bei

- begründetem Verdacht, dass der Teilnehmerschlüssel kompromittiert wurde
- Missbrauch der Systeme von SIX und/oder Dienstleistungen gemäss Kapitel 1.2 durch den Teilnehmer
- Beendigung des Vertragsverhältnisses

4.6.4 Sperrlisten (CRL)

Die von der CA ausgestellten Sperrlisten basieren auf dem X.509 v2 Standard. Es werden keine «per-certificate» Extensions (z. B. Reason Codes) unterstützt. Als «per-CRL» Extension erscheint eine fortlaufend aufsteigende Seriennummer in der Sperrliste.

Die von der CA ausgestellten Sperrlisten werden nicht öffentlich verfügbar gemacht. Die Sperrlisten werden von den Systemen von SIX zur Überprüfung der Gültigkeit von Zertifikaten bei der Authentifizierung eingesetzt.

4.7 Haftung

Für die Verwendung der Teilnehmerzertifikate gemäss Kapitel 1.2 gelten die Haftungsklauseln der entsprechenden Verträge.

Es wird jede Haftung abgelehnt, falls die Teilnehmerzertifikate für andere als die im Kapitel 1.2 definierten Zwecke verwendet werden.

4.8 Änderungen der Richtlinien

Die SIX Interbank Clearing AG behält sich das Recht vor, diese Zertifizierungsrichtlinien ohne Vorankündigung zu ändern.

4.9 Übertragung der Dienstleistung innerhalb von SIX

Die SIX Interbank Clearing AG behält sich das Recht vor, die Zertifizierungsstelle (SIC CA) ohne Mitteilung an eine andere Gruppengesellschaft von SIX zu übertragen.