



Payment Services

SIC CA

Certification Guidelines

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



Information

No guarantee can be given for the information contained in this document which is subject to change without notice.

SIX reserves all rights for this document including the rights of photomechanical reproduction, storage on electronic media and the translation into foreign languages.

Although great care has been taken in the compilation and preparation of this work to ensure accuracy, errors and omissions cannot be entirely ruled out.

SIX cannot be held liable for any decision made or action taken in reliance on the information in this document or for any consequential, special or similar damages.

Table of Contents

1	Abstract	5
1.1	Overview	5
1.2	Scope of application	5
1.3	Conventions	5
1.4	Abbreviations	5
2	SIC Certificates	7
2.1	Certificate hierarchy	7
2.2	Types of certificate	7
2.2.1	General information	7
2.2.2	Certificate matrix	7
2.2.3	CA certificate	7
2.2.3.1	Naming conventions	8
2.2.3.2	Intended purpose	8
2.2.3.3	Period of validity	8
2.2.3.4	Fingerprint	8
2.2.3.5	Extensions	8
2.2.4	Personal certificate for private persons (Private Certificate)	9
2.2.4.1	Naming conventions	9
2.2.4.2	Intended purpose	9
2.2.4.3	Period of validity	9
2.2.4.4	Extensions	9
2.2.5	Employee certificate for companies/businesses (Staff Certificate)	10
2.2.5.1	Naming conventions	10
2.2.5.2	Intended purpose	10
2.2.5.3	Period of validity	10
2.2.5.4	Extensions	10
2.2.6	Certificate for companies/businesses (Corporate Certificate)	11
2.2.6.1	Naming conventions	11
2.2.6.2	Intended purpose	11
2.2.6.3	Period of validity	11
2.2.6.4	Extensions	11
3	CA Infrastructure	12
3.1	Operator	12
3.2	CA Keys	12
3.2.1	Generation	12
3.2.2	Distribution of the public CA key	12
3.3	Directory service	12
3.4	Suspension of activities	12
3.4.1	Safe custody obligation	12
3.5	Security	13
3.5.1	System security	13
3.5.2	Personal security	13
3.6	Auditing	13

4	Certification Guidelines	14
4.1	Registration of parties	14
4.2	Generation of party keys	14
4.3	Application for a certificate	14
4.4	Distribution of keys and certificates	14
4.5	Obligations of the parties	15
4.5.1	Intended purpose of the party certificates	15
4.5.2	Obligations of key owners	15
4.6	Blocking of certificates	15
4.6.1	Party-related reasons for revocation	15
4.6.2	Issuer-related reasons for revocation	16
4.6.3	SIX-related reasons for revocation	16
4.6.4	Certificate Revocation List (CRL)	16
4.7	Liability	16
4.8	Changes to the certificate practice statement	16
4.9	Transfer of the service within SIX	16

1 Abstract

1.1 Overview

This document describes the types of certificate and the certification guidelines (Certificate Practice Statement, CPS) for SIX Interbank Clearing as a certification authority (SIC CA).

The certification guidelines comprise regulations defining the use of certificates for a specified group of users and/or class of application having common security requirements.

This certificate practice statement applies to certificates for services as described in chapter 1.2 and are solely intended for persons taking advantage of these services.

1.2 Scope of application

These certification guidelines apply solely to certificates issued by SIC Customer ID CA 1024 Level 2 for secure client authentication when using the SSL protocol in conjunction with services of the companies of SIX.

SIX Payment Services Ltd:

- payCOM^{web}
- Web applications (LSV⁺/BDD orders and master data)

SIX Interbank Clearing Ltd:

- remoteGATE
- SIC Extranet

The SIC CA is not a public CA and the party certificates cannot be used for binding electronic signatures (based on the law governing signatures).

1.3 Conventions

In this document, the terms "Party" and "Key Owner" apply equally to persons of both sexes and legal entities.

The term "Issuer" refers to the certification authority (CA) as a legal entity.

1.4 Abbreviations

The following abbreviations are used in this document:

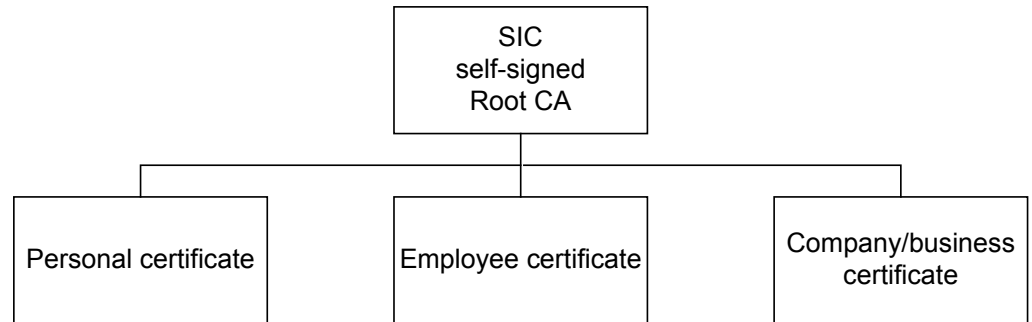
CA	C ertification A uthority
CPS	C ertificate P ractice S tatement
CRL	C ertificate R evocation L ist
DN	D istinguished N ame (name of the certificate owner (Subject DN) or certificate issuer (Issuer DN))
ID	I dentification
PIN	P ersonal I dentification N umber

- PKI** **P**ublic **K**ey **I**nfrastructure
- RDN** **R**elative **D**istinguished **N**ame (O=Organisation, OU=Organisational Unit, L=Locality, ST=State or Province, CN=Common Name, C=Country)
- RSA** Name of the public key system developed by **R**ivest, **S**hamir and **A**ldeman

2 SIC Certificates

2.1 Certificate hierarchy

The certificate hierarchy comprises a self-signed root CA which immediately validates the party certificates.



Only one class is represented within the different types of certificate.

2.2 Types of certificate

2.2.1 General information

All certificates issued by SIC are based on the X.509v3 standard. Only certificates for 1024 bit RSA keys with the public exponent 65537 and SHA-1 as hash algorithm are issued.

2.2.2 Certificate matrix

The following table shows which certificate types have to be used for the different services.

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

2.2.3 CA certificate

The CA certificate is signed using the corresponding private key (self-signed). The certificate is verified by comparing the hash value (fingerprint) of the certificate with the official value published by SIX Interbank Clearing Ltd. The length of the CA certificate key is 1024 bits.

2.2.3.1 Naming conventions

The SIC root certificate has the following subject and issuer DN:

RDN	Description
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 Intended purpose

The CA key is used to issue party certificates and publish certificate revocation lists (CRL). In addition, the public CA key is used to protect a symmetrical key for CA database administration.

2.2.3.3 Period of validity

The CA certificate is valid for a period of ten (10) years. The CA certificate is valid from 31 October 2011 until 31 October 2021.

2.2.3.4 Fingerprint

Hash algorithm	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 Extensions

The CA certificate contains the following X.509v3 compatible extensions:

Name	Value
Basic Constraints	<ul style="list-style-type: none"> • CA: true • Path length: 0
Key Usage	<ul style="list-style-type: none"> • Certificate Signing • CRL Signing
Subject Key Identifier	569F 5AFA B52B 8E07 D92A 458A 0D59 D538 27D0 54FB

All extensions are non-critical.

2.2.4 Personal certificate for private persons (Private Certificate)

The person is registered in accordance with the contract conditions applying to the service involved.

2.2.4.1 Naming conventions

RDN	Description	Mandatory
O	Private person	Yes
OU1	BPID	Yes
OU2		No
OU3		No
C	Country	Yes
ST	Canton	No
L	Place	No
CN	Name of the private person	Yes
Email	E-mail address of the private person	Yes

2.2.4.2 Intended purpose

The private certificate is used solely for secure client authentication in conjunction with the SSL protocol for the party involved.

2.2.4.3 Period of validity

The certificate is valid for three (3) years.

2.2.4.4 Extensions

The party certificate contains the following X.509v3 compatible extensions:

Name	Value
Key Usage	<ul style="list-style-type: none"> • keyEncipherment • digitalSignature
Authority Key Identifier	569F 5AFA B52B 8E07 D92A 458A 0D59 D538 27D0 54FB

All extensions are non-critical.

2.2.5 Employee certificate for companies/businesses (Staff Certificate)

An employee certificate for companies/businesses is issued to a specific individual who wishes to take advantage of the services as described in chapter 1.2 on the instructions of the company in question.

The parties are registered in accordance with the contract conditions applying to the service involved.

2.2.5.1 Naming conventions

RDN	Description	Mandatory
O	Name of the company/business	Yes
OU1	BPID	Yes
OU2	Name of the department/group	No
OU3		No
C	Country	Yes
ST	Canton	No
L	Place	No
CN	Name of the party	Yes
E-mail	E-mail address of the private person	Yes

2.2.5.2 Intended purpose

An employee certificate for companies/business can be used to take advantage of the service according to chapter 1.2 for business purposes. The party certificate is used solely for secure client authentication in conjunction with the SSL protocol for the individual involved.

2.2.5.3 Period of validity

The certificate is valid for three (3) years.

2.2.5.4 Extensions

The party certificate contains the following X.509v3 compatible extensions:

Name	Value
Key Usage	<ul style="list-style-type: none"> • keyEncipherment • digitalSignature
Authority Key Identifier	569F 5AFA B52B 8E07 D92A 458A 0D59 D538 27D0 54FB

All extensions are non-critical.

2.2.6 Certificate for companies/businesses (Corporate Certificate)

A party certificate for companies/businesses is issued to individuals who wish to take advantage of the service as described in chapter 1.2 on the instructions of the company in question. The party certificate for companies/businesses can be used simultaneously by several employees within the company. Persons are registered in accordance with the contract conditions applying to the service involved.

It is advisable to use in principle personal certificates for companies and businesses.

2.2.6.1 Naming conventions

RDN	Description	Mandatory
O	Name of the company/business	Yes
OU1	BPID	Yes
OU2	Name of the department/group	Yes
OU3		No
C	Country	Yes
ST	Canton	No
L	Place	No
CN	<i>Corporate Certificate</i>	Yes
E-mail		No

2.2.6.2 Intended purpose

A party certificate for companies/businesses can be used to take advantage of the service according to chapter 1.2 for business purposes. The party certificate is used solely for secure client authentication in conjunction with the SSL protocol for the individual involved.

2.2.6.3 Period of validity

The certificate is valid for three (3) years.

2.2.6.4 Extensions

The party certificate contains the following X.509v3 compatible extensions:

Name	Value
Key Usage	<ul style="list-style-type: none"> • keyEncipherment • digitalSignature
Authority Key Identifier	569F 5AFA B52B 8E07 D92A 458A 0D59 D538 27D0 54FB

All extensions are non-critical.

3 CA Infrastructure

3.1 Operator

SIX Interbank Clearing is the operator of the CA:

SIX Interbank Clearing Ltd
Hardturmstrasse 201
Postfach
8021 Zurich

3.2 CA Keys

3.2.1 Generation

Generation of the CA key-pair is undertaken in a secure environment. A number of redundant copies of key-pairs are stored on different hardware tokens which are protected by access codes and stored in secure vaults.

The key generation process guarantees that the CA private key is only stored on the hardware token intended for this purpose. The private key cannot be separated from the hardware token.

3.2.2 Distribution of the public CA key

- Together with the SmartCard user PIN, each party receives the fingerprint of the CA certificate by post (included in the Starter Kit)
- Each party receives the SmartCard by registered post
- The CA certificate can be obtained at SIX Interbank Clearing Ltd.

3.3 Directory service

No public directory service exists.

3.4 Suspension of activities

SIX Interbank Clearing Ltd will inform all parties if its CA activities are going to be suspended.

3.4.1 Safe custody obligation

SIX Interbank Clearing Ltd undertakes to safeguard party data for a specific length of time:

- Agreement
- Party data
- Certificate with the relevant status information

3.5 Security

3.5.1 System security

The SIC CA is operated on a dedicated system. Access to the CA system is subjected to physical access checks.

3.5.2 Personal security

Access to the SIC CA system is restricted to a defined group of persons. All critical operations are undertaken using the principle of duplicate checking.

3.6 Auditing

The SIC CA is subject to a periodic audit undertaken by SIX auditors.

4 Certification Guidelines

4.1 Registration of parties

The parties are registered in accordance with the applicable contract conditions for the service involved as per chapter 1.2.

4.2 Generation of party keys

The RSA key-pair is generated by SIX Interbank Clearing Ltd. The key generation process guarantees that the private key is only stored on the hardware token. The private key cannot be separated from the hardware token. SIX Interbank Clearing Ltd holds no copy of the private key.

4.3 Application for a certificate

Each person or company/business who has finalised a valid agreement in accordance with chapter 4.1 can apply for a party certificate. The application is checked by SIX Interbank Clearing Ltd who, at its discretion, may grant or reject the application.

4.4 Distribution of keys and certificates

The SmartCard containing the party key and the associated certificate plus the user PIN are sent to the party under separate cover.

Delivery by normal post:

- User PIN for the SmartCard
- Fingerprint of the SIC root CA certificate

Delivery by registered mail:

- SmartCard containing the party key and party certificate

4.5 Obligations of the parties

4.5.1 Intended purpose of the party certificates

Party certificates are only to be used for the services according to chapter 1.2 within the framework of the contractually agreed conditions. The sole purpose is client authentication in conjunction with the SSL protocol for the services according to chapter 1.2.

The SIC Customer ID CA 1024 level 2 is not a public CA and the party certificates cannot be used for binding electronic signatures (based on the law governing signatures).

SIX Interbank Clearing Ltd accepts no liability whatsoever for party certificates which are used for any purpose other than client authentication in conjunction with the SSL protocol for the services according to chapter 1.2.

4.5.2 Obligations of key owners

The key owner is responsible for the security of private key components in his possession. As a means of guaranteeing security, the key owner must observe the following:

- As soon as the SmartCard has been received, the user PIN must be changed
- Where personal certificates are involved, the SmartCard and/or PIN must not be communicated to third parties
- Where non-personal certificates are involved, the SmartCard and/or PIN may only be communicated to authorised persons within the same company
- The private key is only to be used for the purpose specified in chapter 1.2
- Adopt measures to ensure that the system on which the keys are used is suitably protected (virus detection, access restriction, etc.)
- If the key is compromised or the SmartCard lost, the certificate must be blocked immediately

4.6 Blocking of certificates

SIC PKI offers the possibility of irrevocably blocking certificates (revocation). This is the irreversible and premature termination of a valid certificate. Revoked certificates can no longer be used for the services of SIX companies according to chapter 1.2 and both the party concerned and the issuer are authorised to request certificates to be terminated in this manner.

4.6.1 Party-related reasons for revocation

Each party must apply for his certificate to be revoked if:

- there are grounds for suspicion that the party key has been compromised
- the SmartCard has been lost or stolen
- agreement has been terminated

4.6.2 Issuer-related reasons for revocation

SIX Interbank Clearing Ltd is authorised to block a party certificate without a special application if:

- there are grounds for suspicion that the party key has been compromised
- misuse of the SIX systems and/or services according to chapter 1.2 by the party involved
- suspension of PKI operations

4.6.3 SIX-related reasons for revocation

The service owner is authorised to block party certificates if:

- there are grounds for suspicion that the party key has been compromised
- misuse of the SIX systems and/or services by the party involved
- termination of the agreement

4.6.4 Certificate Revocation List (CRL)

The certificate revocation lists issued by the CA are based on the X.509 v2 standard. "Per-certificate" extensions (e.g. reason codes) are not supported. An incremental serial number in the certificate revocation list appears as a "per-CRL" extension.

The certificate revocation lists issued by the CA are not publicised. The certificate revocation lists are used by the SIX systems for checking the validity of certificates used for authentication purposes.

4.7 Liability

When using the party certificates in accordance with chapter 1.2, the liability clauses for the relevant agreements apply.

No liability is accepted whatsoever for party certificates used for any purposes other than those defined in chapter 1.2.

4.8 Changes to the certificate practice statement

SIX Interbank Clearing Ltd reserves the right to make changes to the certificate practice statement (these guidelines) without notice.

4.9 Transfer of the service within SIX

SIX Interbank Clearing AG reserves the right to transfer the certification authority (SIC CA) to another SIX company without notice.