

CA SIC

Directives de certification

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

Notes

Les informations de ce document vous sont fournies sans garantie et peuvent être modifiées à tout moment sans avertissement préalable.

Tous les droits de ce document sont réservés, y compris leur reproduction photomécanique, leur mémorisation sur des médias électroniques et leur traduction en langues étrangères.

Le document a été élaboré avec le plus grand soin mais des erreurs et des imprécisions ne peuvent être exclues à 100 %.

Par conséquent, SIX Interbank Clearing SA ne peut être tenu responsable des erreurs ou de leurs conséquences et décline toute responsabilité à cet effet.

Contrôle de version

Version	Date	Commentaire
1.0	23 mai 2002	Première édition
1.1	16 août 2002	Nouveau logo, nouvelle police de caractères, nouvelle designations de produit
1.2	23 sept. 2005	Précisé que SIC CA n'est pas un bureau de certification public.
2.0	8 février 2007	Transfert du secteur d'activité LSV de Swiss Interbank Clearing SA à PayNet (Schweiz) AG à partir du 1er janvier 2007 et mises à jour
2.1	1 avril 2007	À partir du 1er avril 2007 la société PayNet (Schweiz) AG aura comme nouvelle raison sociale Telekurs PayNet SA
2.2	27 jan. 2009	À partir du 1er janvier 2009 les sociétés Swiss Intebank Clearing SA et Telekurs PayNet SA auront comme nouvelle raison sociale SIX Interbank Clearing SA et SIX Paynet SA; Telekurs Group aura comme nouvelle raison sociale SIX Group

Copyright SIX Group. Tous droits réservés.

© Droits de copie 2002-09 par SIX Interbank Clearing SA, CH-8021 Zurich

Table des matières

1	Introduction	5
1.1	Vue d'ensemble	5
1.2	Champ d'application.....	5
1.3	Définition des termes	5
1.4	Abréviations	5
2	Certificats SIC.....	7
2.1	Hiérarchie des certificats.....	7
2.2	Types de certificats	7
2.2.1	Informations générales	7
2.2.2	Matrice de certificat	7
2.2.3	Certificat du CA.....	7
2.2.3.1	Codes utilisés	8
2.2.3.2	Destination	8
2.2.3.3	Période de validité.....	8
2.2.3.4	Empreinte digitale	8
2.2.3.5	Extensions.....	8
2.2.4	Certificat de participant pour personnes privées (Private Certificate).....	9
2.2.4.1	Codes utilisés	9
2.2.4.2	Destination	9
2.2.4.3	Période de validité.....	9
2.2.4.4	Extensions.....	9
2.2.5	Certificat personnel de participant pour entreprises (Staff Certificate)	10
2.2.5.1	Codes utilisés	10
2.2.5.2	Destination	10
2.2.5.3	Période de validité.....	10
2.2.5.4	Extensions.....	10
2.2.6	Certificat de participant pour entreprises (Corporate Certificate).....	11
2.2.6.1	Codes utilisés	11
2.2.6.2	Destination	11
2.2.6.3	Période de validité.....	11
2.2.6.4	Extensions.....	11
3	Infrastructure du CA	12
3.1	Exploitant	12
3.2	Clé du CA.....	12
3.2.1	Création.....	12
3.2.2	Distribution de la clé publique du CA	12
3.3	Services de répertoire	12
3.4	Arrêt de l'activité.....	13
3.4.1	Obligation de garde	13
3.5	Sécurité	13
3.5.1	Sécurité du système.....	13
3.5.2	Sécurité personnelle	13

3.6	Audit	13
4	Directives de certification	14
4.1	Enregistrement des participants	14
4.2	Création des clés de participants	14
4.3	Demande de certificat	14
4.4	Distribution des clés et des certificats	14
4.5	Obligations des participants	15
4.5.1	Destination des certificats de participants.....	15
4.5.2	Obligations des détenteurs de clés	15
4.6	Annulation de certificats	16
4.6.1	Raisons côté participant pour une annulation	16
4.6.2	Raisons côté émetteur pour une annulation	16
4.6.3	Raisons côté sociétés du groupe SIX pour une annulation	16
4.6.4	Listes d'annulation (CRL).....	16
4.7	Responsabilité.....	17
4.8	Modification des directives	17
4.9	Transfert du prestation de service dans le groupe SIX	17

1 Introduction

1.1 Vue d'ensemble

Le présent document décrit les types de certificats et directives de certification (CPS) du bureau de certification de SIX Interbank Clearing SA (CA SIC).

Les directives de certification sont un ensemble de règles qui définissent le domaine d'utilisation des certificats pour un groupe donné d'utilisateurs et/ou une catégorie donnée d'application ayant des exigences de sécurité communes.

Les présentes directives de certification s'appliquent aux certificats pour les prestations de services comme décrit au chapitre 1.2, et sont destinées aux participants à ces services.

1.2 Champ d'application

Les présentes directives de certification s'appliquent exclusivement aux certificats qui sont établis par le SIC Customer ID CA 1024 Level 2 (CA SIC) pour l'authentification fiable du client dans le cadre du protocole SSL pour les prestations de services des sociétés du groupe SIX.

SIX Paynet SA:

- payCOM^{web}
- Applications Web de SIX Paynet SA

SIX Interbank Clearing SA:

- remoteGATE
- SIC Extranet
- Application Web de SIX Interbank Clearing SA

Le SIC CA n'est pas un bureau de certification public. Les certificats de participants ne peuvent pas être utilisés comme signatures électroniques légales (selon la Loi sur la signature numérique).

1.3 Définition des termes

Dans le présent document, les termes "participant" ou "détenteur de clé" sont employés pour des personnes physiques, hommes ou femmes, ainsi que pour des personnes juridiques.

Le terme "émetteur" désigne la personne juridique de l'exploitant du CA.

1.4 Abréviations

Le présent document utilise les abréviations suivantes:

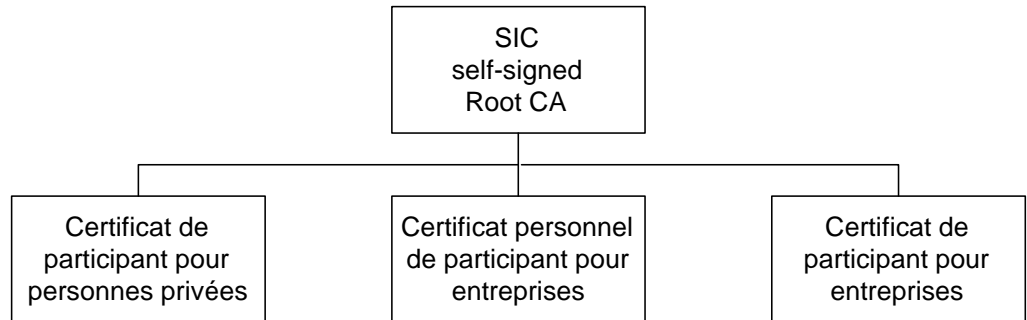
CA	C ertification A uthority (bureau de certification)
CPS	C ertificate P ractice S tatement (directives de certification)
CRL	C ertificate R evocation L ist (liste d'annulation de certificats)
DN	D istinguished N ame (nom du détenteur du certificat (Subject DN) ou de l'émetteur du certificat (Issuer DN))

ID	I dentification
PIN	N uméro d' I dentification P ersonnel
PKI	I nfrastructure P ublic K ey
RDN	R elative D istinguished N ame (O=Organisation, OU=Unité Organisationnelle, L=Localité, ST=État ou Province, CN=Nom Commun, C=Pays)
RSA	Nom du système de Public Key développé par R ivest, S hamir et A dleman

2 Certificats SIC

2.1 Hiérarchie des certificats

La hiérarchie des certificats consiste en un self-signed Root CA, qui certifie directement les certificats de participants:



Pour chaque type de certificats, il n'existe qu'une seule catégorie de certificats.

2.2 Types de certificats

2.2.1 Informations générales

Tous les certificats établis par le CA de SIC sont basés sur la norme X.509v3. On établit exclusivement des certificats pour clé RSA 1024 bits avec exposant public 65537 et SHA-1 comme algorithme de Hash.

2.2.2 Matrice de certificat

Le tableau suivant montre, quels types de certificats sont utilisés pour les différents prestations de services.

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

2.2.3 Certificat du CA

Le certificat du CA est signé avec la clé privée correspondante (self-signed). Le contrôle du certificat du CA s'effectue en comparant la valeur Hash (empreinte digitale) du certificat à la valeur officiellement publiée par SIX Interbank Clearing SA. La longueur de clé du certificat du CA est de 1024 bits.

2.2.3.1 Codes utilisés

La Subject DN et l'Issuer DN du certificat Root SIC sont les suivantes:

RDN	Description
O	Swiss Interbank Clearing SA
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 Destination

La clé du CA est utilisée pour l'établissement de certificats de participants et l'établissement de listes d'annulation (CRL). De plus, la clé publique du CA protège une clé symétrique pour la gestion de la base de données du CA.

2.2.3.3 Période de validité

La période de validité du certificat du CA est de dix (10) ans. Le certificat du CA est valable du 18 janvier 2002 au 18 janvier 2012.

2.2.3.4 Empreinte digitale

Algorithme de Hash	Empreinte digitale
MD5	94B6 190E C563 556E 1DE3 8013 F6B0 18C5
SHA-1	6D44 7C83 6DD5 0528 277B 8498 CC4F 7CFB 7B52 EDAF

2.2.3.5 Extensions

Le certificat du CA comporte les extensions suivantes, compatibles X.509v3.

Désignation	Valeur
Basic Constraints	<ul style="list-style-type: none"> CA: true Pathlength: 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

Les extensions sont toutes non critiques.

2.2.4 Certificat de participant pour personnes privées (Private Certificate)

L'enregistrement des participants s'effectue suivant les conditions contractuelles de la prestation de service correspondante.

2.2.4.1 Codes utilisés

RDN	Description	Obligatoire
O	Personne privée	Oui
OU1	BPID	Oui
OU2		Non
OU3		Non
C	Pays	Oui
ST	Canton	Non
L	Localité	Non
CN	Nom de la personne privée	Oui
Email	E-mail de la personne privée	Oui

2.2.4.2 Destination

Le certificat de participant est utilisé exclusivement pour l'authentification fiable du client dans le cadre du protocole SSL du participant correspondant.

2.2.4.3 Période de validité

La période de validité est de trois (3) ans.

2.2.4.4 Extensions

Le certificat de participant comporte les extensions suivantes, compatibles X.509v3.

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

Les extensions sont toutes non critiques.

2.2.5 Certificat personnel de participant pour entreprises (Staff Certificate)

Un certificat personnel de participant pour entreprises est délivré à une personne spécifique qui souhaite utiliser les prestations de services comme décrit au chapitre 1.2 pour le compte d'une entreprise.

L'enregistrement des participants s'effectue suivant les conditions contractuelles de la prestation de service correspondante.

2.2.5.1 Codes utilisés

RDN	Description	Obligatoire
O	Nom de l'entreprise	Oui
OU1	BPID	Oui
OU2	Nom de la division/du groupe	Non
OU3		Non
C	Pays	Oui
ST	Canton	Non
L	Localité	Non
CN	Nom du participant	Oui
Email	E-mail de la personne privée	Oui

2.2.5.2 Destination

Un certificat personnel de participant pour entreprises peut être utilisé pour l'utilisation commerciale des prestations de services selon le chapitre 1.2. Le certificat de participant est utilisé exclusivement pour l'authentification fiable du client dans le cadre du protocole SSL du participant correspondant.

2.2.5.3 Période de validité

La période de validité est de trois (3) ans.

2.2.5.4 Extensions

Le certificat de participant comporte les extensions suivantes, compatibles X.509v3.

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

Les extensions sont toutes non critiques.

2.2.6 Certificat de participant pour entreprises (Corporate Certificate)

Un certificat de participant pour entreprises est délivré à des participants qui souhaitent utiliser les prestations de services comme décrit au chapitre 1.2 pour le compte d'une entreprise. Le certificat de participant pour entreprises peut être utilisé simultanément par plusieurs participants. L'enregistrement des participants s'effectue suivant les conditions contractuelles de la prestation de service correspondante.

Il est recommandé de utiliser des certificats de participant pour entreprises en principe.

2.2.6.1 Codes utilisés

RDN	Description	Obligatoire
O	Nom de l'entreprise	Oui
OU1	BPID	Oui
OU2	Nom de la division/du groupe	Oui
OU3		Non
C	Pays	Oui
ST	Canton	Non
L	Localité	Non
CN	<i>Corporate Certificate</i>	Oui
Email		Non

2.2.6.2 Destination

Un certificat de participant pour entreprises peut être utilisé pour l'utilisation commerciale des prestations de services selon le chapitre 1.2. Le certificat de participant est utilisé exclusivement pour l'authentification fiable du client dans le cadre du protocole SSL du participant correspondant.

2.2.6.3 Période de validité

La période de validité est de trois (3) ans.

2.2.6.4 Extensions

Le certificat de participant comporte les extensions suivantes, compatibles X.509v3.

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

Les extensions sont toutes non critiques.

3 Infrastructure du CA

3.1 Exploitant

L'exploitant du CA est SIX Interbank Clearing SA:

SIX Interbank Clearing SA
Hardturmstrasse 201
Postfach
8021 Zurich

3.2 Clé du CA

3.2.1 Création

La création des paires de clés du CA a été effectuée dans un environnement sécurisé. Les paires de clés ont été mémorisées plusieurs fois, de façon redondante, sur différents hardware token. Les hardware token sont protégés par des codes d'accès et déposés dans des coffres-forts.

Le processus de création des clés garantit que la clé privée du CA est enregistrée uniquement sur le hardware token prévu à cet effet. La clé privée ne peut pas quitter le hardware token.

3.2.2 Distribution de la clé publique du CA

- Chaque participant reçoit par courrier, conjointement avec le PIN d'utilisateur de la SmartCard, l'empreinte digitale du certificat du CA (contenus dans le kit de démarrage).
- Chaque participant reçoit la SmartCard par courrier recommandé.
- Le certificat du CA peut être obtenu chez SIX Interbank Clearing SA.

3.3 Services de répertoire

Il n'y a pas de service public de répertoire.

3.4 Arrêt de l'activité

SIX Interbank Clearing SA informe tous les participants si un arrêt des activités du CA est prévu.

3.4.1 Obligation de garde

SIX Interbank Clearing SA s'engage à conserver les données des participants pendant une période donnée:

- contrat
- données sur les participants
- certificat avec les informations d'état correspondantes

3.5 Sécurité

3.5.1 Sécurité du système

Le CA de SIC est exploité sur un système dédié. L'accès au système du CA est soumis à des contrôles d'accès physiques.

3.5.2 Sécurité personnelle

L'accès au système du CA de SIC est limité à un cercle défini de personnes. Les opérations critiques sont toutes exclusivement exécutées suivant le principe du contrôle par deux personnes différentes.

3.6 Audit

Le CA de SIC est soumis à un audit périodique par des contrôleurs du groupe SIX.

4 Directives de certification

4.1 Enregistrement des participants

L'enregistrement des participants s'effectue suivant le droit contractuel en vigueur de la prestation de service correspondante selon le chapitre 1.2.

4.2 Création des clés de participants

Les paires de clés RSA sont créées chez SIX Interbank Clearing SA. Le processus de création des clés garantit que la clé privée est enregistrée uniquement sur le hardware token. La clé privée ne peut pas quitter le hardware token. SIX Interbank Clearing SA ne possède pas de copie de la clé privée.

4.3 Demande de certificat

Toute personne ou entreprise qui a conclu un contrat valable selon le chapitre 4.1 peut poser une demande de certificat de participant. La demande est contrôlée par SIX Interbank Clearing SA. Il appartient à SIX Interbank Clearing SA d'établir un certificat de participant conformément à la demande ou de rejeter la demande.

4.4 Distribution des clés et des certificats

La SmartCard avec la clé de participant et le certificat associé ainsi que le numéro personnel d'identification d'utilisateur (PIN) sont envoyés au participant par voies séparées.

Livraison par courrier normal:

- PIN d'utilisateur pour la SmartCard
- Empreinte digitale du certificat SIC Root CA

Livraison par courrier recommandé:

- SmartCard avec la clé de participant et le certificat de participant

4.5 Obligations des participants

4.5.1 Destination des certificats de participants

Les certificats de participants doivent être exclusivement utilisés pour les prestations de services selon le chapitre 1.2 dans le cadre des conditions contractuellement convenues. Leur unique destination est l'authentification du client dans le cadre du protocole SSL pour les prestations de services selon le chapitre 1.2.

Le SIC Customer ID CA 1024 Level 2 n'est pas un bureau de certification public. Les certificats de participants ne peuvent pas être utilisés comme signatures électroniques légales (selon la Loi sur la signature numérique).

SIX Interbank Clearing SA décline toute responsabilité pour le cas où les certificats de participants seraient utilisés à d'autres fins que l'authentification du client dans le cadre du protocole SSL pour les prestations de services selon le chapitre 1.2.

4.5.2 Obligations des détenteurs de clés

Le détenteur de clé est responsable de la sécurité des éléments de clé privée en sa possession. Afin de garantir cette sécurité, le détenteur de clé doit notamment respecter les consignes suivantes:

- modification du PIN d'utilisateur de la SmartCard dès la réception de la SmartCard
- pour des certificats personnels, ne pas remettre la SmartCard et/ou le PIN à des tiers
- pour des certificats non personnels, remettre la SmartCard et/ou le PIN uniquement à des personnes autorisées de sa propre entreprise
- utiliser la clé privée exclusivement pour la destination prescrite dans le chapitre 1.2
- prendre des mesures appropriées pour protéger le système sur lequel les clés sont utilisées (protection antivirus, limitation d'accès, etc.)
- si la clé est compromise ou en cas de perte de la SmartCard, faire annuler le certificat le plus rapidement possible

4.6 Annulation de certificats

La CA SIC permet d'annuler définitivement des certificats. L'annulation est un achèvement prématuré irréversible de la validité d'un certificat. Les certificats annulés ne peuvent plus être utilisés pour les prestations de services des sociétés du groupe SIX selon le chapitre 1.2. L'annulation d'un certificat peut être le fait aussi bien des participants que de l'émetteur.

4.6.1 Raisons côté participant pour une annulation

Tout participant doit demander une annulation de son certificat de participant en cas de:

- soupçons fondés de ce que la clé de participant a été compromise
- vol ou perte de la SmartCard
- résiliation du contrat

4.6.2 Raisons côté émetteur pour une annulation

SIX Interbank Clearing SA est autorisé à annuler des certificats de participants sans demande spécifique du participant en cas de

- soupçons fondés de ce que la clé de participant a été compromise
- usage abusif des systèmes et/ou des prestations de services des sociétés du groupe SIX selon le chapitre 1.2 par le participant
- arrêt de l'exploitation de l'infrastructure PKI

4.6.3 Raisons côté sociétés du groupe SIX pour une annulation

Le propriétaire de la prestation de service est autorisé à annuler des certificats de participants sans demande spécifique du participant en cas de

- soupçons fondés de ce que la clé de participant a été compromise
- usage abusif des systèmes et/ou des prestations de services des sociétés du groupe SIX par le participant
- achèvement de la relation contractuelle

4.6.4 Listes d'annulation (CRL)

Les listes d'annulation établies par le CA sont basées sur la norme X.509 v2. Les extensions "par certificat" (Reason Codes par exemple) ne sont pas supportées. Un numéro de série en ordre croissant dans la liste d'annulation apparaît comme extension "par CRL".

Les listes d'annulation établies par le CA ne sont pas rendues publiques. Les listes d'annulation sont utilisées par les systèmes du groupe SIX pour vérifier la validité des certificats lors de l'authentification.

4.7 Responsabilité

Pour l'utilisation des certificats de participants selon le chapitre 1.2, on appliquera les clauses de validité des contrats correspondants.

Toute responsabilité est déclinée pour le cas où les certificats de participants seraient utilisés à d'autres fins que celles définies au chapitre 1.2.

4.8 Modification des directives

SIX Interbank Clearing SA se réserve le droit de changer les présentes directives de certification sans avertissement préalable.

4.9 Transfert du prestation de service dans le groupe SIX

SIX Interbank Clearing SA se réserve le droit de transférer le bureau de certification (CA SIC) à une autre société du groupe SIX sans avertissement préalable.