# SSFN – Building a secure communication network for the financial community

## SSFN Regulations

Version 1.3, valid from 01.11.2026

SCION

ELEVATING SECURE COMMUNICATION

Version 1.3 – 01.07.2026

# Document history

All the changes carried out in this handbook are listed below with the version designation, the change date, a brief description of the change and the specification of the chapters affected.

| Version | Date | Change description | Chapter |
|---|---|---|---|
| 1.3 | 01.06.2026 | Additions (for details, see Annex B: Change history) | All |
| 1.2 | 01.06.2024 | Clarifications and expansion (for details, see Annex B: Change history) | |
| 1.1 | 03.06.2022 | Clarifications and expansion | All |
| 1.0 | 30.11.2021 | First edition | |

*Table 1: Document history*

**Change history**

All future changes from Version 1.3 will be listed in the change documentation.

Please address all suggestions, corrections, and proposed improvements to this document to:

**SIX BBS Ltd**
Hardturmstrasse 201
CH-8005 Zurich
E-mail: pm-ssfn@six-group.com
www.six-group.com

# General information

This document is licensed under the Creative Commons Attribution 4.0 International (CC BY 4.0).

The contents may be copied, distributed, modified or used commercially, provided that SIX is credited as the author.

This document has been prepared with utmost care, but errors and inaccuracies cannot be completely ruled out. SIX BBS Ltd cannot assume any legal responsibility or any liability for errors in this document or their consequences.

To improve readability, the use of masculine and feminine forms of language are avoided wherever possible. All personal designations are to be regarded as gender neutral.

Should you encounter any errors in this document or have any suggestions for improvements, we would be grateful if you e-mailed your feedback to **pm-ssfn@six-group.com**.

SIX provides this English translation of this document. Should there be any differences in content, the German version shall prevail.

SSFN Regulations © 2026 by SIX BBS Ltd is licensed under Creative Commons Attribution 4.0 International. To view a copy of this license, visit creativecommons.org/licenses/by/4.0

# Table of contents

**Document history** ..... **2**
**General information** ..... **3**
**Table of contents** ..... **4**
**List of tables** ..... **6**
**List of figures** ..... **7**
**1 Basics of the SSFN** ..... **8**
1.1 SSFN and participants ..... 8
1.2 Purpose of the SSFN regulations ..... 9
1.3 Recipients of the SSFN regulations ..... 9
1.4 Reference documents ..... 9
**2 SSFN system overview** ..... **10**
2.1 SCION technology ..... 10
2.2 SCION network group ..... 12
2.3 SSFN classification ..... 13
2.4 SSFN ISD ..... 13
2.5 SSFN specifications ..... 16
2.6 Function as a network ..... 18
**3 Governance** ..... **19**
3.1 Formal structure ..... 19
3.2 Product owner ..... 19
3.3 SSFN voting members ..... 20
3.4 Governance regulations ..... 20
3.5 Committees ..... 22
3.6 SSFN services/Service provisioning ..... 22
**4 Admission requirements** ..... **23**
4.1 Fulfilment of admission criteria ..... 23
4.1.1 SSFN users ..... 23
4.1.2 SSFN service providers ..... 23
4.1.3 SIX as the primary certificate issuer ..... 24
4.2 SSFN certificate ..... 24
**5 Tasks of the SSFN participants** ..... **25**
5.1 SSFN service providers ..... 25
5.1.1 SSFN certificate issuers ..... 25
5.1.2 SSFN core members ..... 26
5.1.3 SSFN carriers ..... 26
5.1.4 SSFN endpoint providers ..... 27
5.1.5 SSFN providers for SCION solutions ..... 27
5.2 SSFN users ..... 28
5.3 Exchange of information for troubleshooting ..... 28
**6 Responsibilities** ..... **29**
**7 Onboarding process for SSFN service providers** ..... **30**
**8 Corrective action, suspension or exclusion of an SSFN participant** ..... **32**
**9 Change management of the SSFN regulations** ..... **35**

**10 Contracts ..... 36**
**Annex A: Admission criteria for SSFN service providers ..... 37**
**Annex B: Change history ..... 41**
**Annex C: Glossary ..... 43**

# List of tables

Table 1: Document history ..... 2
Table 2: Reference documents ..... 9
Table 3: Links to relevant internet pages ..... 9
Table 4: Governance regulations ..... 21
Table 5: Onboarding process for SSFN service providers ..... 31
Table 6: Process for corrective action, suspension or exclusion of an SSFN participant ..... 34
Table 7: Overview of contracts in the SSFN ..... 36
Table 8: Requirements for SSFN service providers ..... 40
Table 9: Change history, version 1.3 ..... 41
Table 10: Change history, version 1.2 ..... 42

# List of figures

Figure 1: Elements of an ISD ..... 11
Figure 2: SCION group and contractual relationships ..... 12
Figure 3: Schematic representation of an SSFN, including roles in an ISD ..... 13
Figure 4: SSFN governance structure ..... 19

# 1 Basics of the SSFN

## 1.1 SSFN and participants

The Secure Swiss Finance Network ("**SSFN**") is an independent SCION-based communications network provided for the Swiss financial marketplace which allows all players, primarily the authorised users of the Swiss financial marketplace ("**SSFN users**"), to communicate with each other in a secure fashion within a self-contained system to reduce the cyber risks associated with the public internet, without requiring them to be connected to the same telecommunications provider.

The SSFN is based on a SCION network and technically represents its own isolation domain ("**ISD**"). Thus, a distinction is made between a SCION network group of the infrastructure providers (here "**SSFN service providers**") and the SSFN as a specific SCION isolation domain.

SSFN service providers may have the following roles:

1. SSFN certificate issuers
2. SSFN carriers with core services ("core members")
3. SSFN carriers
4. SSFN endpoint providers
5. SSFN SCION solution providers

SSFN service providers are able to offer comparable services to participants of other SCION isolation domains, independent of the SSFN.

SSFN participants are either pure SSFN users or can also be SSFN service providers at the same time. They are collectively referred to as "**SSFN participants**".

SIX BBS Ltd ("**SIX**") is the "**product owner**" of the SSFN. The control and steering structure (governance) of SSFN is jointly exercised by the Swiss National Bank ("**SNB**"), Switch and SIX ("**SSFN voting members**"). SIX has defined these regulations for the SSFN ISD together with the SSFN voting members ("**SSFN regulations**"). SIX additionally acts as a certificate issuer for the SSFN ("**SSFN certificate issuer**"). In this function, SIX performs the initial issuing and renewal of the AS certificates necessary for admission to the SSFN ("**SSFN certificate**") for all SSFN participants.

## 1.2 Purpose of the SSFN regulations

The SSFN regulations:

1. Describes what the overall SSFN system entails (e.g. based on the specifications)
2. Defines the governance of SSFN
3. Specifies which criteria an SSFN participant must meet as an SSFN service provider or as an SSFN user in order to be admitted to the SSFN
4. Identifies the roles and responsibilities of all SSFN participants
5. Defines the process in the event of breaches of the SSFN regulations
6. Explains the process for amending the SSFN regulations
7. Provides an overview of the relevant contracts for the SSFN.

## 1.3 Recipients of the SSFN regulations

The SSFN regulations are intended for SSFN participants who access the SSFN either as SSFN service providers and/or as SSFN users.

## 1.4 Reference documents

| Ref | Document/schema | Title | Source |
|---|---|---|---|
| [1] | Agreement for SSFN service providers | Agreement for SSFN service providers | SIX |
| [2] | Best practice document (general sections) | Best Practices for SCION ISD Operations for ISPs | Anapaya |
| [3] | Best practice document (SSFN-specific sections) | ISD Operations Manual for SSFN Core ISPs | Anapaya, SIX |
| [4] | SSFN certificate agreement | Agreement regarding SSFN certificates | SIX |

*Table 2: Reference documents*

| Organisation | Link |
|---|---|
| GitHub | github.com/scionproto/scion |
| SCION Association | www.scion.org |
| SIX | www.six-group.com/ssfn |

*Table 3: Links to relevant internet pages*

# 2 SSFN system overview

## 2.1 SCION technology

SCION is a technology that was developed at ETH Zurich.

SCION organises existing Autonomous Systems[1] ("**AS**") into groups of independent routing levels called Isolation Domains ("**ISD**"), enabling trusted communication between members in that group, irrespective of which participating network provider they are connected to.

In order to set up an ISD, a valid Trust Root Configuration ("**TRC**") issued by the voting members is required. This TRC designates the governance principles and essential authorised service providers (core members [for routing] and certificate issuers [for AS certificates]) of this ISD. The issuing of an AS certificate (see below) by the certificate issuers as designated in the TRC is based on the admission criteria defined in the governance principles. The TRC thus forms the "Root of Trust" for the corresponding ISD. The trust, i.e. the TRC, is therefore also renewed annually.

The core element of a SCION-based network is control over the path that data uses from the sender to the receiver (routing). Here, all possible paths to the receiver are shown in real time to the sender at any given moment. The path here includes all intermediate nodes, i.e. the SCION gateways, which can be used between sender and receiver.

The control that the data packets follow on the path to the receiver, as selected by the sender, is secured based on cryptographic processes using certificates. The SCION gateways forward the data packets to the subsequent SCION gateway in accordance with the sender's instructions stored in the respective package, without the possibility of choosing a different path. Thanks to this information being real-time, a new path can be determined and used almost without any interruption if a SCION gateway was to become unavailable or fail. The sender can store path selection priorities in its SCION gateways for this purpose.

Each AS stores a certificate on its SCION gateways that identifies the respective AS as a member of an ISD ("**AS certificate**"). As stipulated in the SCION specification, an AS certificate has a short validity period (usually 72 hours) for security reasons. It must therefore be renewed periodically via an application to the certificate issuer. These application and renewal processes are fully automated and do not require any manual intervention by the participants. The validity period of the current AS certificate and that of the new AS certificate overlap, so that there is a valid AS certificate available at all times.

AS certificates can only be issued and renewed by those certificate issuers that have been designated and thus authorised by the voting members in the TRC. Real-time information on the status of possible paths is also determined by the core members as designated in the TRC.

Each SCION gateway requires special SCION software to function. They all must be compatible with each other within the ISD. The SCION software is open source (see github.com/scionproto/scion).

In particular, ETH Zurich and Anapaya Systems, a spin-off of ETH Zurich and commercial provider of SCION solutions, contribute significantly to the further development of the SCION software. In addition, the SCION Association was founded in 2023, which is also committed to standardising SCION at IETF and striving for certification of SCION providers.

[1] An autonomous system ("**AS**") is understood to be a network that is independently detectable and addressable from the outside. As a rule, a company (or a group of companies) maintains such a network in order to be able to manage it with a common routing policy.

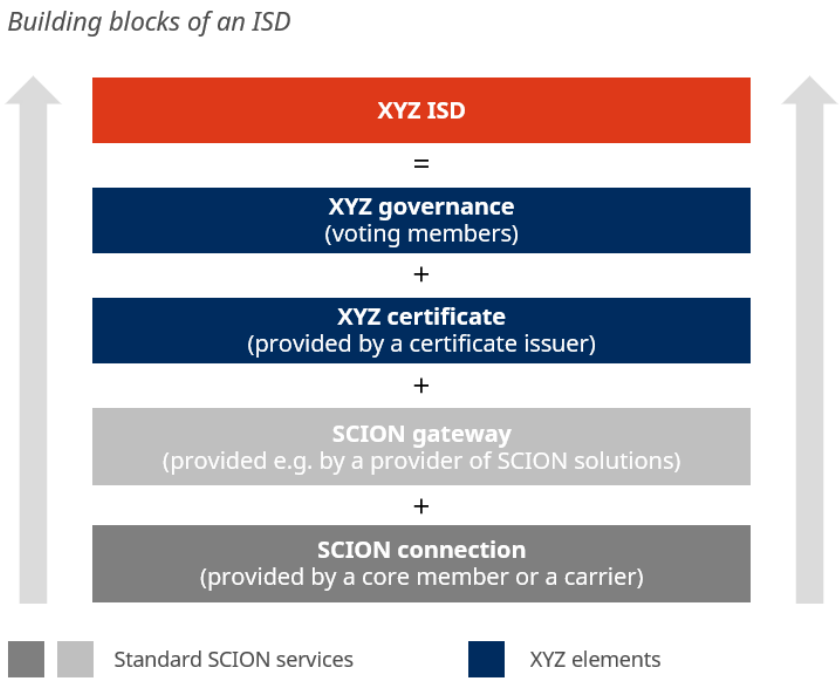



*Figure 1: Elements of an ISD*

The SCION technology is designed in such a way that hardware components used, such as the SCION gateways, can be used simultaneously in different ISDs. For this purpose, the corresponding certificates for the respective ISDs must be stored on the gateways.

Consequently, this means that core members, carriers and SCION solution providers in particular can define their services largely independently of the individual ISDs and can therefore offer standardised SCION services.

For each ISD, it must be determined who a voting member is, and which rules shall apply with regard to participation in that ISD. Compliance with these rules for participation is ensured by the voting members and the respective certificate issuer of an ISD.

Special Core Members may provide interconnection services into several ISDs for the provision of a SCION-based network and for the ISDs based on it. In order to ensure the necessary services of the respective core members within the scope of the interconnection service, they need to adhere to increased requirements.

The SCION technology does not define a fixed number of voting members, certificate issuers or core members. However, any change in these three roles requires an update of the TRC. As the number increases, the complexity also increases but without the availability being improved to the same extent.

## 2.2 SCION network group

The SCION network group forms the basic network infrastructure on which various ISDs are operated. The SCION network group is the amalgamation of all core members that comply with the SCION specification and thereby enable communication for any ISD (see Figure 2).

In conjunction with the telecommunications providers and CAs that constitute the "**SCION Community**", Anapaya defines the guidelines for activities and processes in a SCION network group in a "**Best practice document (general sections)**" [2] – based on past experience. The regulations contained therein define the best practices for secure, technically correct and resilient operations of a SCION network group and regulate the rules of conduct, namely:

1. The redundant connection between the carriers to guarantee a high network availability (redundant peering)
2. The redundant connection between the carriers to the corresponding CA service providers (certificate issuer) in order to guarantee high availability (redundant CA connection)
3. Group-wide operational regulations such as a company-wide management of security incidents (incident management).

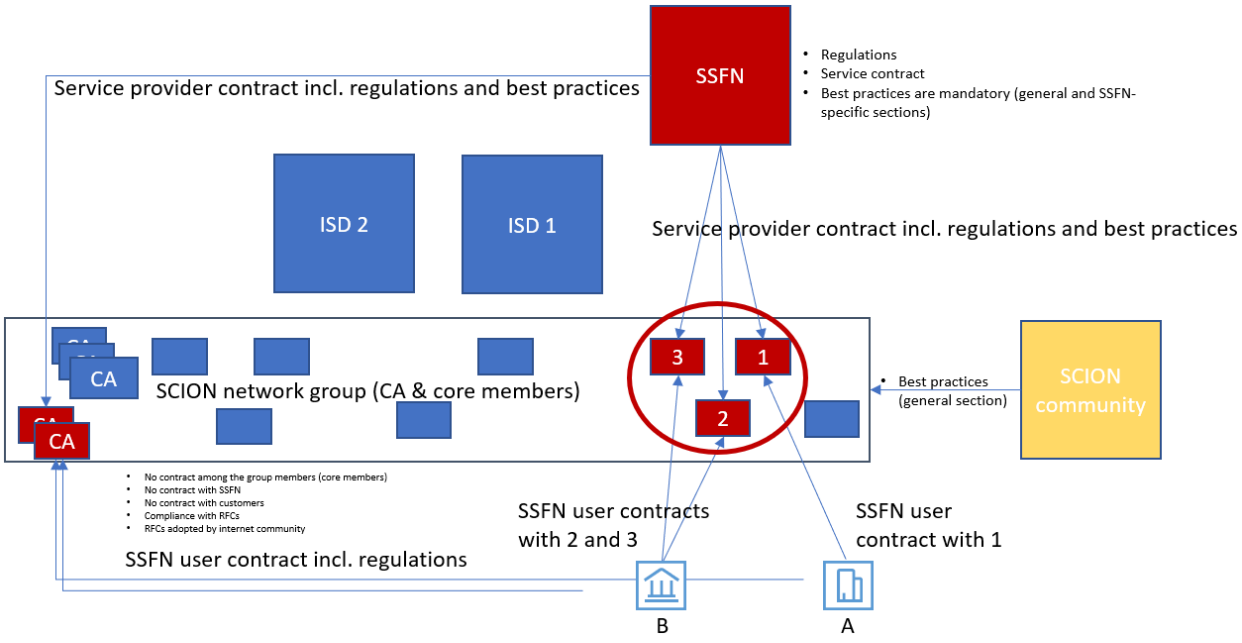



*Figure 2: SCION group and contractual relationships*

For SCION group members offering the SSFN, the best practice document (general part) [2] as well as the specifications for SSFN (best practice document (SSFN-specific sections) [3]) must be followed. In the SSFN, the best practice document (SSFN-specific sections) [3] has priority over the best practice document (general sections) [2].

## 2.3 SSFN classification

The SSFN is an independent communication network based on the SCION technology which is provided for the Swiss financial marketplace. This allows authorised SSFN users to communicate with each other in a protected manner in a self-contained network while reducing the cyber risks associated with the public internet, without needing to be connected to the same SSFN carrier.

The functional description of the SSFN deliberately avoids any technological aspects. The SSFN is based on the cooperation of infrastructure providers, which in turn use the SCION technology as a routing architecture (see chapter 2.2).

The separation between the SCION-based network group and the SSFN as an ISD happens at the so-called service access point. This separation allows the specification and responsibility to be clearly assigned to either the SCION-based network or the SSFN.

Accordingly, SSFN service providers regulate and define their technical and operational aspects as well as processes amongst themselves.

## 2.4 SSFN ISD

The SSFN is a communication network based on a SCION-based network group and as such represents an independent ISD with its own TRC. An AS certificate in the SSFN is referred to as an "**SSFN certificate**".

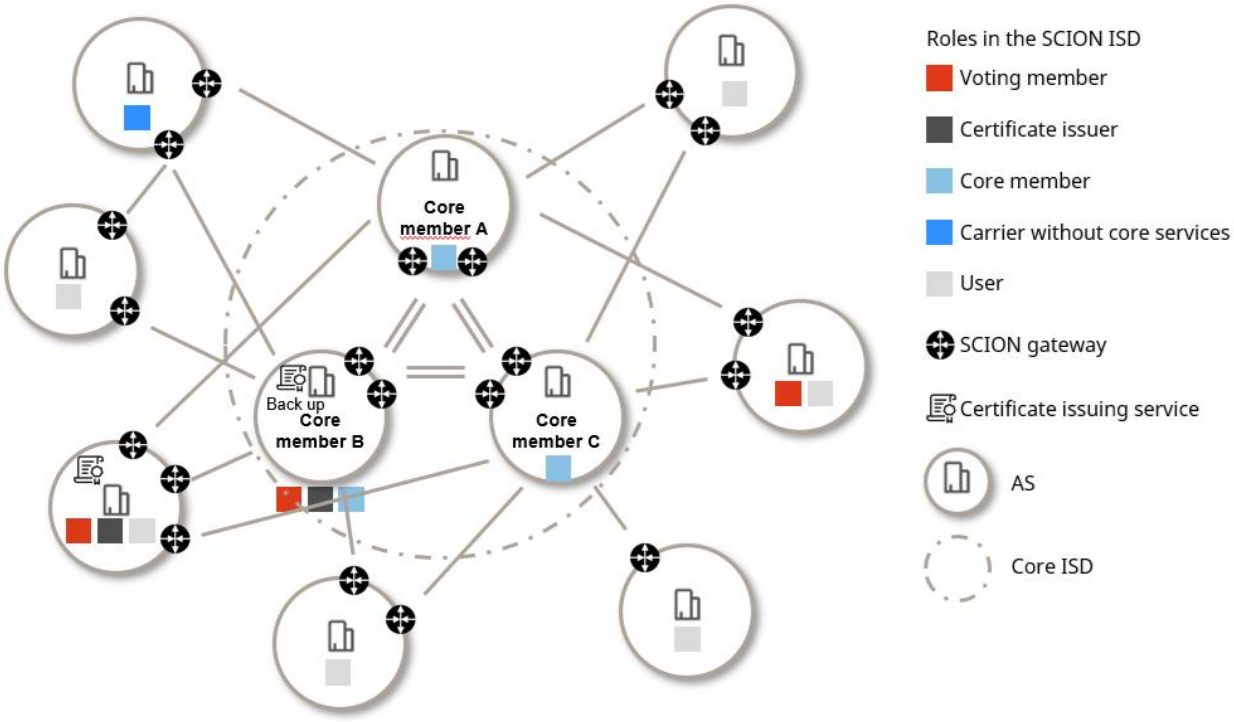



*Figure 3: Schematic representation of an SSFN, including roles in an ISD*

In an ISD, here using SSFN as an example (as illustrated in *figure 3*), the following roles must be performed by the associated AS (see chapter 4 "*Admission requirements*"):

| ISD role | Description | Parties in the SSFN |
|---|---|---|
| Voting members | Creation and updating of the TRC, including establishing governance for the ISD as well as approving adjustments (e.g. regulatory adjustments, admission criteria, etc.). | SIX, Swiss National Bank (SNB), Switch (see chapter 3) |
| Certificate issuer | Creation and renewal of all AS certificates required in the ISD (based on the governance of the ISD), with the exception of those for the TRC. | SIX, (see chapter 5.1.1); Switch acts as backup for certificate renewal. |
| Core member (carrier with core services) | Provision of core services (e.g. path finding / beaconing for the real-time determination of the status of every possible path, TRC dissemination) for the ISD, provision of connectivity (based on the governance of the ISD). The core member is usually a telecommunications provider with significant own network infrastructure (e.g. Internet Service Provider). | Sunrise, Swisscom, Switch (see chapter 5.1.2) |
| Carrier | Provision of connectivity (based on the governance of the ISD). Note: this role is not mandatory for the functioning of an ISD. The carrier is usually also an Internet Service Provider or telecommunications provider, but without significant own network infrastructure or the provider is domiciled abroad. | Other carriers (see chapter 5.1.3) |
| User | User of a SCION ISD. | Authorised actor (in accordance with chapter 4.1.1) in the Swiss financial marketplace (e.g. participant in SIC) |
| Provider of SCION solutions (not illustrated in Figure 3: Schematic representation of an SSFN, including roles in an ISD, but also essential for the functioning of an ISD) | Creation, provision/distribution and maintenance of commercial SCION-based software (possibly including hardware). | Anapaya Systems Ltd (currently the only provider; see chapter 5.1.5) |
| SCION endpoint provider (not illustrated in Figure | "Service providers" which enable users who are NOT directly connected to the ISD to access services via the ISD or offer other services to these users via the ISD (e.g. managed services for the SCION connection). In contrast to "carrier", these service | Service providers for SIX customers (e.g. service bureaux for SIC participants) which require an SSFN connection in |

| ISD role | Description | Parties in the SSFN |
|---|---|---|
| 3: Schematic representation of an SSFN, including roles in an ISD) | providers are not telecommunications providers, but, for example, e.g. outsourcing providers (such as service bureaux). | order to enable indirectly authorised SSFN users to access the SSFN or to offer them other services via SSFN (e.g. managed services for the SSFN connection). See also chapter 5.1.4 |

The SSFN as an independent ISD has defined its own governance, independent of other ISDs (see chapter 3). This governs the tasks and responsibilities within the SSFN ISD.

In order to maintain high availability while minimising the impact on technical complexity, a ratio of two SSFN certificate issuers to three SSFN core members appears to be optimal in the SSFN ISD with respect to the number of SSFN certificate issuers and SSFN core members.

**SIX as the product owner** defines the governance of the SSFN together with the other SSFN voting members (chapter 3).

## 2.5 SSFN specifications

The SSFN represents an ISD based on the existing SCION network group. As such, certain specifications of the communication network are provided by the SCION protocol, and others are specified by the SSFN voting members.

The specifications outside the general SCION protocol are listed below.

**Operational requirements for SSFN participants**: The tasks and responsibilities of each SSFN participant are defined in accordance with their roles. This specifically includes requirements for security. Violation of the requirements may result in exclusion from the SSFN or other appropriate measures may be taken (e.g. path restrictions, firewall rules). The operational requirements to the SSFN service providers are ensured within the scope of the *Admission criteria for SSFN service providers* in accordance with Annex A.

**Availability/reliability**: In principle, the availability or reliability of the SSFN is determined by the SSFN service providers involved. These define the corresponding service aspects in their customer contracts (e.g. availability, response times in the event of incidents, operating times). The reliability of the relevant SCION components (e.g. core services, connections between SSFN core members, SSFN certificate issuers) is achieved through a high level of redundancy among the SSFN service providers and is ensured within the framework of the *Admission criteria for SSFN service providers* in accordance with Annex A.

**Performance/capacity**: The performance and capacity of the SSFN arises from the interaction of the SSFN service providers involved. These providers define the corresponding characteristics (such as bandwidth, latency, availability) in their customer contracts and deliver the corresponding quality and performance in their own networks based on those characteristics. Quality and performance in their own networks are therefore ensured within the scope of the *Admission criteria for SSFN service providers* in accordance with Annex A.

**Error handling, BCM, BCP and DR**: These aspects of the SSFN result from the interaction of the SSFN service providers involved. All SSFN service providers shall ensure that suitable processes, systems and resources are in place to detect and handle faults or failures, as part of the *Admission criteria for SSFN service providers* in accordance with Annex A. Similarly, individual rules on this are specified in the best practice documents (general and SSFN-specific sections).

**"Best practice document" for activities within the SCION group:** Based on empirical values, there are guidelines for activities and procedures in a SCION network group (e.g. incident/problem management) established under the leadership of Anapaya and with the assistance of the SSFN core members and SIX. All SSFN service providers confirm within the scope of the *Admission criteria for SSFN service providers* as per Annex A that they comply with the provisions detailed in documents[2] and [ [3]] or have implemented equivalent measures.

**Monitoring**: Each SSFN participant needs to monitor the state of all its visible paths as well as its SSFN-specific services in order to be able to take appropriate measures if necessary. There is no central monitoring for the SSFN.

**Geofencing**: There are no specific requirements regarding geofencing. SSFN service providers inform the SSFN voting members where their SSFN-related SCION gateways are located. SSFN service providers must also announce if cross-border "hops" are used. Within the network of an SSFN service provider, it cannot be specified that only data lines in Switzerland are used for the transfer of SSFN data. However, SSFN users can ask their respective contractual partner and SSFN service providers at any time where the SSFN-related SCION gateways are actually located. The SSFN service providers are obliged to provide this information.

**Authorised participants**: The SSFN sets high requirements for admission and thus for obtaining an SSFN certificate. Only parties that meet the criteria set out in the SSFN regulations can apply to SIX for an SSFN certificate (chapter 4.2).

**Use of the SSFN certificate**: Use of the SSFN certificate is only permissible in the context of the SSFN.

**Protection against cyber risks/(D)DoS**: The SSFN is logically separated from all other networks (including the public internet). Within SSFN, however, an authorised SSFN participant could intentionally or unintentionally overload other authorised SSFN participants with traffic. Protective mechanisms based on the SCION protocol exist for this purpose. Affected SSFN participants can take measures themselves (e.g. informing the sender via the receiver, blocking paths from the sender to the receiver via the receiver, adapting their own firewall rules). In addition, the SSFN certificate issuer can refuse to renew a sender's SSFN certificate in the event of violations of the SSFN regulations (see chapter 8).

**Network protocols used by the SSFN service provider**: It is expected that SSFN service providers offer native SCION connections. However, it is also possible to design the SCION traffic as an overlay (e.g. on the individual IP backbone). Regardless, the SSFN service provider must demonstrably ensure that there is no unauthorised transfer to another ISD or to the public internet at any time. This is ensured within the scope of the *Admission criteria for SSFN service providers* in accordance with Annex A.

**Exclusive use of publicly registered IP addresses**: All SSFN participants exclusively use registered public IP addresses. The SSFN participants ensure that the addresses are not accessible from the internet (or from other public networks).

**Segregation from the public internet:** *For SCION connections to the SSFN ISD, the SSFN access links provided by the SCION provider between the customer premises equipment ("**CPE**") and the provider's core must not be addressable and accessible from the provider's public internet or the public internet.*

**SCION solutions, including associated software deployment:**

SSFN participants shall implement SCION solutions as follows:

1. The SCION solution used by an SSFN participant must comply with the currently valid SCION specifications. The decisive factor is the compatibility of the SCION solution used with the reference implementation of the technology provider, currently only Anapaya Systems AG. This must be ensured independently by each SSFN participant.
2. The connection architecture and software deployment process must meet standard business security requirements and ensure integrity and authorisation at all times.

**Protection of cryptographic keys**: The following requirements apply depending on the cryptographic materials used:

1. SSFN certificates: SSFN certificates and the associated keys (public and private keys) are stored on the SCION gateways in accordance with the SCION protocol (no HSM). The SCION gateways must be hardened and access to cryptographic data must be especially restricted via the defined regulations.
2. Certificates of the SSFN certificate issuers (e.g. issuer keys): By default, the SSFN certificate issuers should store their private cryptographic data (private keys) in the HSMs with the usual business protection measures. This is mandatory for the root certificate private keys. Storage in an HSM can be dispensed with if short certificate durations (<10 days for intermediate certificates) are used instead. In such a case, the device used (e.g. server) must be hardened and access restricted via defined regulations.
3. Trust Root Configuration (TRC): In this case, the private cryptographic data (private keys) must be stored in the HSMs with the usual business protection measures.

## 2.6 Function as a network

SSFN participants can be either SSFN users or SSFN service providers that fulfil the correspondingly defined admission criteria in advance (see chapter 4 "Admission requirements").

The SSFN participants are permitted to exchange data with each other via the SSFN ISD. The SSFN participants define unilaterally, bilaterally or multilaterally which data can be exchanged via which paths.

- SSFN, in its function as a network, does not specify the usage of that data. However, use of the SSFN is only permissible for the exchange of data legitimised by the SSFN participants involved: each participant remains responsible for compliance with the laws applicable to its own domain.
- If parties have chosen their path preferences in such a way that they contradict each other and therefore data cannot be exchanged, the parties concerned must resolve this contradiction bilaterally.

In order to be able to use the SSFN ISD as an SSFN participant, the following infrastructure must also be provided by each SSFN participant:

a) a data connection (or several data connections) to the SSFN (usually a SCION connection to an SSFN core member or an SSFN carrier). A redundant connection via different carriers (SSFN core member or SSFN carrier) is recommended.

b) the availability of at least one SCION gateway.

c) SSFN participants must also have a valid SSFN certificate (see chapter 4.2) and are obliged not to take any actions that have a negative impact on other SSFN participants or on the SSFN ISD.

d) SSFN participants must carry out the necessary work per each service in their roles as SENDER and RECEIVER (e.g. setting up/recording the IP address of the service for SSFN, DNS settings, firewall rules).

# 3 Governance

## 3.1 Formal structure

In the SSFN, governance is provisioned by the SSFN voting members: SIX, SNB and Switch. SIX also fulfils the role of product owner and SSFN certificate issuer.

The requirement of an uneven number of SSFN voting members ensures a quorum (majority decision). The number of three voting members reduces complexity and guarantees that, in the event of a failure of one voting member, the two remaining SSFN voting members could continue to manage and keep the TRC up to date (at least two parties are required to make changes to the TRC).

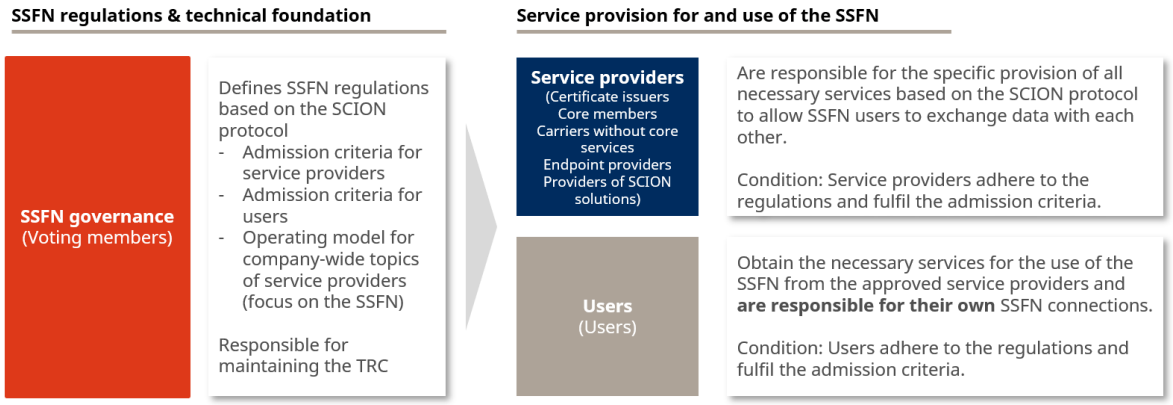



*Figure 4: SSFN governance structure*

## 3.2 Product owner

As the product owner, SIX defines the rules of the SSFN regulations and the best practice document (SSFN-specific sections) [3] in coordination with the two other SSFN voting members. It can also make recommendations to the SCION Community for the adaptation of the best practice document (general sections) [2].

The product owner performs all the delegable tasks of the SSFN voting members (except for those tasks that require the involvement of the other SSFN voting members (e.g. resolutions, updating the TRC)).

Further tasks of the product owner include:

- Acting in this role externally for the SSFN and at the same time representing the other SSFN voting members
- Coordinating and reviewing the results of assessments by external auditors of applications for admission to the SSFN as a service provider or service bureau. Applicants deemed by the product owner to be eligible for the SSFN are submitted to the voting members for voting
- Coordinating the verification of compliance by the SSFN participants of the admission criteria (chapters 4.1.1 and 4.1.2), including all related contractual obligations
- Coordinating central risk management for SSFN on behalf of and with the participation of the voting members
- Carrying out procedures in the event of a breach of the SSFN regulations by SSFN participants (chapter 8) in coordination with the other SSFN voting members

- Delivering change requests to the other SSFN voting members, updating the SSFN regulations in coordination with the other SSFN voting members and guaranteeing an information distribution channel to the SSFN participants (chapter 9)
- Assisting SSFN participants with issues related to the SSFN regulations or participation in SSFN in general
- Coordinating activities relating to TRC updates
- Coordinating the SSFN committees (chapter 3.5).

## 3.3 SSFN voting members

The three SSFN voting members have the core task of defining the SSFN regulations and thus establishing the rules for the proper functioning of the SSFN and updating them (chapter 9). This also includes active participation in SSFN risk management under the leadership of the product owner.

They also support the product owner in questions regarding the SSFN regulations from SSFN service providers and SSFN users in the context of participation in the SSFN. Upon request, the SSFN voting members will support the product owner in the performance of its duties; the SSFN voting members may also take on special tasks by mutual agreement.

Furthermore, they regulate aspects related to the TRC (chapter 2.1) and ensure that the TRC is kept up to date. They make final decisions on the further development of the SSFN ISD (chapter 2.5). This includes in particular the initial creation of the TRC, its revisions in accordance with the rules, including sufficient lead times, and modifications as required (including the admission of SSFN core members and SSFN certificate issuers).

The SSFN voting members jointly decide on the admission (or exclusion) of service providers in the SSFN and their role.

## 3.4 Governance regulations

Governance is organised as follows:

| Element | Specific regulation |
|---|---|
| Number | SSFN is established and defined by three SSFN voting members. The number may fall below three for a short time (e.g. due to a resignation), but a new SSFN voting member must be recruited to the committee as soon as possible. Voting members are institutions (not persons); however, a person acting as a voting member must be defined by the respective institution. |
| Admission criteria | Only those who actively support the goals of SSFN, are willing to perform the duties and responsibilities defined in the SSFN regulations, bring added value to the SSFN and are confirmed by the existing SSFN voting members shall be eligible as SSFN voting members. There are no automatic rights of admission. |
| Resignation | Resigning SSFN voting members must actively assist in the search for a replacement. It is expected that the resigning SSFN voting member will only resign after the successful election of a new SSFN voting member. The notice period is 12 months effective from the end of a quarter. During this period, the tasks and responsibilities must continue to be performed. |

| Element | Specific regulation |
|---|---|
| Product owner | The SSFN voting members elect the product owner.<br>The product owner is SIX, which is also an SSFN voting member and certification authority.<br>If the product owner resigns from its duties, it must observe a notice period of 12 months from the end of a quarter, as in the case of resignation as a voting member, and must continue to fulfil its duties in full during this period. In the event of a handover, all necessary information/data must be handed over to the new product owner in full and without prior request.<br>The SSFN voting members are responsible for finding a replacement within this period. |
| Resolutions | Resolutions are generally passed by the SSFN voting members, and as a rule are usually made unanimously (in the sense of a consensus decision). If no common position can be found, a simple majority is valid. In principle, the SSFN voting members have equal rights; in the event of a tie (e.g. an abstention), SIX has the casting vote in its role as the product owner.<br>***Caveats concerning resolutions on the exclusion procedures (see chapter 8)***:<br>• If a potentially excludable SSFN participant is simultaneously connected to a systemically important financial market infrastructure pursuant to the Financial Market Infrastructure Act ("**FinMIA**"), only the operator of the systemically important infrastructure shall decide on the further participation of such a participant within the scope of a procedure pursuant to chapter 8. The product owner must obtain this decision and continue or terminate the procedure accordingly.<br>• If a potentially excludable SSFN participant is simultaneously connected to the SIC system as a systemically important infrastructure, only the SNB shall decide on the further participation of such a participant within the scope of a procedure pursuant to chapter 8. The SNB's decision regarding participation in the SIC system takes precedence over the decision of the financial market infrastructure operator.<br>Decisions within the SSFN are considered final, i.e. there are no possibilities for appeal within the SSFN governance.<br>Furthermore, the affected SSFN parties shall have no legal or financial claims against the decision-making body or against any other party within the SSFN for any damages as a result of a procedural decision pursuant to chapter 8. |
| Compensation | The SSFN voting members shall not receive any financial compensation for their roles as SSFN voting members.<br>SIX is exempt from this rule in its role as the product owner. The expenses resulting from this role are compensated via fee income pursuant to the "Agreement regarding SSFN certificates". |

*Table 4: Governance regulations*

## 3.5 Committees

The following three committees exist in the SSFN:

- **SSFN governance board**: The SSFN voting members meet on an ad hoc basis, as required. Function: Exchange among the SSFN voting members and making fundamental decisions (e.g. further development of SSFN, acceptance of system tests, modifications to the SSFN regulations, renewal of the TRC, changes of a technical nature, handling of requests from other committees, etc.)
- **SSFN provider meeting**: Meets periodically, but at least twice a year, chaired by the product owner . The participants are the SSFN service providers that have the roles of SSFN certificate issuer, SSFN core members, SSFN carriers and optionally the SSFN voting members. Other SSFN service providers such as SSFN endpoint providers and SSFN providers for SCION solutions can be invited to individual sessions as required.

  Function: Exchange among the operators of the SCION core infrastructure regarding the operational aspects of the network, especially its stability, availability and extraordinary incidents. Requirements for improvements and further developments of the SCION network group shall also be discussed. Modifications that result in changes within the SSFN ISD must be requested from the SSFN voting members
- **SSFN risk management**: The risk delegates of the voting members meet every six months and manage the SSFN risks from the risk inventory and, if necessary, take on new risks for processing.

## 3.6 SSFN services/Service provisioning

- Approved SSFN Services ("**SSFN Services**")

  SSFN Services are basically the services of the SIX Group that comply with Swiss financial market regulations or financial market standards. In addition, these services must include formal proof of identification as part of the contractual agreement with the clients (e.g. SIC). The SSFN voting members have exclusive decision-making power over admissions to services on the SSFN. The following services currently qualify as "SSFN services": SIC, euroSIC and SECOM.
- Services that are reachable via the SSFN ("**reachable services**")

  Any service that can be reached by an SSFN user or an SSFN endpoint provider via the SSFN.

  **Note:**

  In addition to using the SSFN for reachable services, an SSFN user may also use the SSFN to network its own sites via the SSFN (e.g. branch offices and its own data centres) that are not in the same network (= same AS). At the time of writing, this excludes IoT devices, in particular card terminals and individual ATMs. Each site that is not in the same network of an SSFN participant is technically regarded as an independent SSFN user; accordingly, a separate SSFN certificate with its own AS number is required for each such site. This SSFN certificate is issued to the same legal entity as the initially issued SSFN certificate. Customers of SSFN users may not be connected via the SSFN ISD, but may communicate with their service provider, the actual SSFN user, via the SCION protocol using another ISD (e.g. the SwissISD). However, this communication takes place outside the SSFN.

# 4 Admission requirements

## 4.1 Fulfilment of admission criteria

### 4.1.1 SSFN users

Operators in the Swiss financial marketplace who meet one of the following criteria are generally admitted to the SSFN as SSFN users:

a) Participant is an SSFN voting member or

b) Participant is a contractual partner of SIX Group Ltd or a group company of SIX Group Ltd and makes use of an SSFN service (see chapter 3.6).

The product owner has the right at any time to verify the admission criterion for the SSFN user pursuant to b) above.

Furthermore, the SSFN user must confirm to the SSFN certificate issuer that it acknowledges and complies with the SSFN regulations within the scope of the "Agreement regarding SSFN certificates" (chapter 4.2).

### 4.1.2 SSFN service providers

In order to be admitted to participate in the SSFN as an SSFN service provider, the SSFN service provider must confirm to the product owner within the scope of the separate agreement "Participation in the SSFN as an SSFN service provider" that it complies with the SSFN regulations and will continually fulfil the admission criteria in accordance with Annex A of these regulations ("***Acknowledgment of the SSFN regulations***", chapter 7). Annex A of these regulations is otherwise identical to Annex 2 of the aforementioned agreement. Annex A determines the respective valid version of Annex 2 of the agreement "Participation in the SSFN as an SSFN service provider"[2].

The admission criteria to be fulfilled are assigned to the respective role of the SSFN service provider in the SSFN. Examples of possible evidence to document the fulfilment of the admission criteria are listed in Annex A (or Annex 2 of the agreement "Participation in the SSFN as an SSFN service provider").

If the SSFN service provider has multiple roles (e.g. SSFN core member and SSFN certificate issuer), it must comply with the requirements in accordance with Annex A for all applicable roles and must note this accordingly in Annex 2 of the agreement "Participation in the SSFN as an SSFN service provider" as part of its acceptance of the *Acknowledgment of the SSFN regulations*.

In accordance with the agreement "Participation in the SSFN as an SSFN service provider", the product owner has the right to check the fulfilment of the admission criteria of the SSFN service provider at any time or to have this checked by an appropriately commissioned third party. Therefore, the electronic evidence regarding the fulfilment of the admission criteria in accordance with Annex A must be always kept available by the SSFN service provider in a complete and up-to-date manner.

If an SSFN participant fulfils the criteria as an SSFN user (e.g. SIC participant) but also acts as an SSFN service provider (e.g. service bureau for other SIC participants), the agreement "Participation in SSFN as an SSFN service provider" must also be signed. Technically, the same SCION connection can be used for both roles. The SSFN service provider may engage subcontractors for the

[2] Differences may arise from the further development of Annex A in contrast with the wording of Annex 2 at the time of signing the contract. Changes in Annex A are always announced with modifications to the SSFN regulations and therefore automatically accepted as valid.

provision of its services. In doing so, it shall always remain responsible for compliance with the admission criteria applicable to its role and must enforce this vis-à-vis the subcontractor at all times.

### 4.1.3 SIX as the primary certificate issuer

SIX is admitted to the SSFN as the exclusive Primary Certificate Issuer and thus, in addition to its role as the product owner and as an SSFN voting member, also assumes the role of the SSFN service provider (see chapter 5.1.1).

The initial issue of a valid SSFN certificate is considered a special task within the SSFN. The provision of a valid SSFN certificate must therefore be ensured by an SSFN voting member. In its role as the primary certificate issuer, SIX is therefore exempt from signing the agreement "Participation in SSFN as an SSFN service provider". Notwithstanding the above, SIX as the primary certificate issuer is also bound by the rules of the SSFN regulations (including compliance with the relevant requirements of Annex A) and must perform specifically defined tasks and responsibilities (chapter 5.1.1 and chapter 6).

## 4.2 SSFN certificate

To participate in the SSFN, each SSFN participant requires an SSFN certificate, (chapter 2.6), which is initially issued to them by the SSFN certificate issuer under the "Agreement regarding SSFN certificates" [4] and upon fulfilment of the admission criteria in accordance with chapter 4.1.1 and/or chapter 4.1.2.

To maintain security, the validity of the SSFN certificate must be continually renewed by the SSFN certificate issuer (chapter 5.1.1). Renewing the certificate requires that the SSFN participant continues to fulfil the admission criteria in accordance with chapter 4.1.1 and/or chapter 4.1.2.

The process of SSFN certificate renewal is as follows:

SSFN certificates generally have a validity period of 72 hours, with the exception of the initial SSFN certificate, which has a validity of 30 days. Before the validity of a "normal" SSFN certificate expires, the renewal must be initiated by the SSFN participant 18 hours after using the currently valid SSFN certificate (as part of a fully automated process). This results in a time overlap of the active SSFN certificate with the already renewed SSFN certificate, so that the SSFN participant has a valid SSFN certificate even in the event of technical problems.

# 5 Tasks of the SSFN participants

There are the following categories of SSFN participants with specific tasks:

- **SSFN service providers**: SSFN certificate issuers, SSFN core members, SSFN carriers, SSFN endpoint providers, SSFN providers of SCION solutions; see chapter 5.1
- **SSFN users**, see chapter 5.2.

An SSFN participant may have more than one role, and the tasks and requirements to be fulfilled are cumulative.

All SSFN participants are responsible for their SSFN connection and thus for the proper operation of their SSFN connection. This also includes taking appropriate protection measures.

## 5.1 SSFN service providers

SSFN service providers provide services for the SSFN ISD in the SCION network group. Via the agreement "Participation in the SSFN as an SSFN service provider", they undertake vis-à-vis the product owner to continually fulfil the admission criteria in accordance with Annex A.

SSFN service providers ensure that their SW-deployment processes (see admission criteria, Annex A) include adequate prior testing.

Before leaving the SSFN ISD, an SSFN service provider must comply with the notice period in accordance with the agreement "Participation in the SSFN as an SSFN service provider" so that a possible replacement can be found in due time.

Furthermore, an SSFN user has no claim that an SSFN service provider participates in a contractual relationship with it.

### 5.1.1 SSFN certificate issuers

SIX serves as the **primary certificate issuer** and Switch as the **secondary certificate issuer**, Switch thus fulfils an important backup function for SIX in the context of continuity in the renewal of SSFN certificates.

As the **primary certificate issuer** (chapter 4.1.3), SIX has the exclusive authorisation to issue *initial* SSFN certificates for SSFN participants within the scope of the separate "Agreement regarding SSFN certificates". SIX ensures the necessary process or can outsource this to a third party.

As the current SSFN certificate issuers, both SIX and Switch maintain the infrastructure required for the renewal of SSFN certificates, including the associated resources.

Certificate renewal is generally performed by SIX unless its infrastructure is not functioning properly. In this case, the certificate renewal is carried out automatically by Switch as the failover. The expenses incurred by Switch for its services as the secondary certificate issuer are compensated by SIX as the primary certificate issuer based on a separate agreement between SIX and the secondary certificate issuer.

The SSFN certificate issuers must also perform the following tasks:

- SIX: Verify the SSFN participant’s eligibility for the initial issue of an SSFN certificate in accordance with the "Agreement regarding SSFN certificates"
- SIX and Switch: Verify the SSFN participant’s authorisation for SSFN certificate renewals
- SIX and Switch: Obligation to faithfully issue certificates in a timely manner, provided that the SSFN participant is not suspended

- SIX and Switch: Suspend SSFN certificates (temporary or final) based on the decision of the SSFN voting members (chapter 8) including cross-checking of relevant information
- SIX and Switch: Inform the other SSFN voting members about any operational problems.

### 5.1.2 SSFN core members

The SSFN core members together form a SCION network group, consisting of their autonomous networks including the provision of associated core services (see also chapter 2).

In addition to the core service these also offer carrier services to their customers (SSFN participants).

SSFN core members must also perform the following tasks:

- Provide SCION services in the SSFN-to-SSFN users and SSFN endpoint providers. They also accept and comply with the "ISD operations manual for SSFN core ISPs" and the "Best Practices for SCION ISD Operations for ISPs"
- Provide non-discriminatory connectivity for SSFN carriers
- Cooperate with SSFN voting members, the product owner, other SSFN core members and SSFN certificate issuers as well as inform them in case of technical problems in a timely manner
- Support their SSFN customers in case of technical problems.

### 5.1.3 SSFN carriers

SSFN carriers are carriers that do not provide their own core services in the SCION group.

They offer SCION connectivity to their customers in order to enable them to connect to the SSFN ISD, and where necessary, supplemented by "managed services". For example, it may be a carrier acting principally as a "connector" to the SSFN for cross-border users.

SSFN carriers must also perform the following tasks:

- Provide SCION services in the SSFN-to-SSFN users and SSFN endpoint providers
- Cooperate with SSFN voting members, the product owner, other SSFN core members and SSFN certificate issuers as well as inform them in case of technical problems in a timely manner
- Support their SSFN customers in case of technical problems.

### 5.1.4 SSFN endpoint providers

SSFN endpoint providers enable a contracted user to either

a) access SIX services via the SSFN (e.g. as a service bureau for SIC participants), or

b) provide managed services for the SSFN connection of an SSFN participant.

In order for a service provider to become an SSFN endpoint provider, a pre-existing contract on the part of the service provider is required with at least one SSFN user.

In case a) applies:

- The pre-existing contract must be substantially related to an SSFN service provided by the SSFN user (e.g. service bureau for SIC participants, service provider for SECOM customers).
- If no customer of the service provider is yet an SSFN user, the service provider may still participate in the SSFN as an SSFN endpoint provider during a period of six months (with possible extension upon justified written request). This period is used to acquire an SSFN user as a customer and thus fulfil requirement a).

In case b) applies:

- The pre-existing contract is explicitly and exclusively set up for maintenance and monitoring services for the SSFN connection of the SSFN participant.

SSFN endpoint providers must also perform the following tasks:

- Cooperate with SSFN voting members, the product owner, other SSFN core members and SSFN certificate issuers as well as inform them in case of technical problems in a timely manner
- Connect customers and ensure that their customers can communicate via the SSFN at any time
- Provide secure access to its infrastructure for its customers, who are SSFN users, via the SSFN communication network.

### 5.1.5 SSFN providers for SCION solutions

SSFN providers for SCION solutions create and maintain SCION-based software for use in a SCION-based network. They provide scalable SCION solutions that can be used in SCION networks.

Note: SSFN providers for SCION solutions do not receive SSFN certificates.

SSFN providers for SCION solutions must perform the following tasks:

- Further develop and maintain the SCION software and appliances in compliance with the SCION protocol and use the SCION open source
- Distribute SCION solutions (such as software, support, management, hardware, licences) to SSFN participants
- Provide timely and complete information to the product owner regarding major changes (e.g. release upgrades, hot fixes)
- Support its SSFN customers in case of problems
- Cooperate with SSFN voting members, the product owner, other SSFN core members and SSFN certificate issuers as well as inform them in a timely manner in case of problems.

## 5.2 SSFN users

SSFN users use the SSFN to connect to the services of SIX Group and to exchange data with other SSFN participants (SSFN service providers or SSFN users) as required.

For this purpose, SSFN users obtain the services necessary for their needs from SSFN service providers (see chapter 5 at the beginning).

SSFN users must also perform the following tasks:

- Procure the SCION connection(s) and corresponding SCION gateways according to their own needs (redundancy, bandwidth, BCM, availability, etc.) and taking into account any service-specific rules (e.g. SIC).
- Securely operate its SSFN connection (e.g. monitoring, configuration, access protection, certificates, path redundancy, firewalls, current SCION software, expertise). In addition to operating current SCION software, the SSFN user is obliged to take account of the instructions in the developer's release notes in a timely manner.
- Decide with which other SSFN users they want to exchange data via the SSFN
- If the SSFN connection is operated (in whole or in part) by a third party, the SSFN user nevertheless always retains responsibility and must fulfil its consequent obligations at all times. This may also include a recurring adequate risk assessment of the commissioned third party in the sense of reviewing an outsourcing-relevant service in accordance with FINMA.

## 5.3 Exchange of information for troubleshooting

SSFN service providers and SSFN users shall support each other to resolve incidents and faults. SSFN service providers and SSFN users must therefore be aware that information necessary for troubleshooting (e.g. gateway software version, port settings, IP address, recording of network traffic) may be shared with other SSFN participants. Each SSFN user shall therefore be responsible for all such information that it might share.

The information exchanged in the aforementioned context of malfunctions is to be handled according to the need-to-know principle and is to be used only in the context of troubleshooting.

# 6 Responsibilities

The product owner, the SSFN voting members, both individually and as a committee, and the other decision-making entities and committees in the SSFN, do not make any guarantees or assurances to the SSFN participants due to the provision of SSFN as a group service (chapter 1.1). Any claims of the SSFN participants against these parties in connection with their participation in the SSFN are excluded to the extent permitted by law.

If an SSFN participant breaches the SSFN regulations, the procedure in accordance with chapter 8 shall be applied.

In all other respects, each SSFN participant, whether that be as an SSFN service provider or as an SSFN user, is responsible for the services provided to its contractual partners. Any guarantees or assurances are to be regulated in the bilateral contractual relationships between the SSFN participants. If contractual services between the SSFN participants are not provided or are provided inadequately, this must be clarified exclusively within the framework of the respective contractual relationship between them.

For the SSFN certificate issuers, the specific regulations as specified in the "Agreement regarding SSFN certificates" shall apply.

In the event of disputes regarding SSFN among SSFN participants, the product owner may only be requested to mediate. The product owner shall decide at its own discretion (e.g. based on its expertise) whether it appears expedient to mediate in the requested dispute. However, the product owner will in no way take a party position or make a legal assessment with regard to the dispute but will only seek to find a consensus between the SSFN participants concerned.

# 7 Onboarding process for SSFN service providers

New SSFN service providers are accepted using the following process:

| # | Step | Description |
|---|---|---|
| 1 | Interest as an SSFN service provider | A service provider expresses interest to the product owner as a potential SSFN service provider. |
| 2 | Product owner:<br>Preliminary check | Based on the following criteria, an objective preliminary check of the service provider's suitability is performed by the product owner with subsequent coordination with the SSFN voting members.<br>Criteria relevant to the review include:<br>– degree of support in the application of SCION technology<br>– complexity in the integration into the SSFN<br>– impact on operations<br>– technical expertise<br>– reputation in the market.<br>The result of the preliminary check is valid for a maximum of 12 months. |
| 3 | Product owner:<br>Decision on preliminary check; information about admission criteria | The result of the preliminary check is communicated to the service provider in writing by the product owner. There are no possibilities for appeal against this decision on the part of the service provider concerned (chapter 1.1).<br>If approved, the service provider will be informed by the product owner about the admission criteria to be fulfilled and the corresponding necessary evidence (Annex A) as a prerequisite for access to the SSFN. |
| 4 | Service provider:<br>Provision of evidence and acceptance of the SSFN regulations | After the service provider has provided the relevant evidence, it confirms to the product owner by signing the agreement "Participation in the SSFN as SSFN service provider" that it complies with the SSFN regulations and will permanently fulfil the admission criteria in accordance with Annex A of these regulations (see chapter 4.1.2). |
| 5 | Product owner:<br>Check fulfilment of admission criteria | The product owner or a third party commissioned by the product owner checks the fulfilment of the admission criteria in accordance with Annex A (see chapter 4.1.2).<br>The future SSFN service provider prepares for this check by:<br>– providing all available evidence (documents, process descriptions, test results, etc.) in accordance with the admission criteria;<br>– naming contact person(s) in case of questions during the check for the sake of efficiency. |

| # | Step | Description |
|---|---|---|
| 6 | Product owner:<br>Recommendation to SSFN voting members<br><br>SSFN voting members:<br>Final decision | The product owner prepares a recommendation for the attention of the other SSFN voting members for admission or rejection of participation in the SSFN (including reasons, e.g. non-fulfilment of individual admission criteria). The SSFN voting members make the final decision regarding admission to the SSFN (see chapter 3.4). There are no possibilities for appeal against this decision on the part of the service provider. |
| 7 | Product owner:<br>Communication of decision | The result of the final decision is communicated to the affected service provider in writing by the product owner. |
| 8 | Admission to participation in the SSFN | In case of a positive admission decision, the necessary measures for the admission of the SSFN service provider to the SSFN are implemented. |

*Table 5: Onboarding process for SSFN service providers*

# 8 Corrective action, suspension or exclusion of an SSFN participant

In the event of a breach of the SSFN regulations by an SSFN participant, the following procedure can be initiated after the product owner consults with the other SSFN voting members.

| # | Step | Description |
|---|---|---|
| 1 | Allegation of breaches of the SSFN regulations<br>Product owner:<br>Examination of the allegations | The Product Owner becomes aware of an allegation (e.g. by an SSFN participant) that another SSFN participant is not complying with the SSFN regulations and that this could result in a potential risk or damage. The product owner reviews the allegations of a possible violation of the SSFN regulations. |
| 2 | Product owner:<br>Opportunity to make a statement;<br>Opening of corrective action procedure<br><br>Service provider:<br>Preparation of procedure plan with defined measures to remedy the unsatisfactory situation<br><br>Product owner<br>Confirmation of procedure plan and measures, setting a deadline | If an allegation appears to be justified, the product owner contacts the affected SSFN participant and gives them the opportunity to make a written statement about the alleged misconduct. Depending on this, the product owner opens the corrective action procedure or adapts the procedure process in coordination with the SSFN voting members (e.g. waives opening the procedure or waives the corrective action plan or decides to suspend an SSFN voting member due to possible bias, etc.).<br>If the SSFN participant must be assumed to be in breach and/or this is deemed justified by the product owner, the affected SSFN participant is given the opportunity to create a plan of action with defined and scheduled measures to remedy the unsatisfactory situation. The product owner can adjust this plan in consultation. The procedure plan with the defined measures is then confirmed by the product owner to the participant with a deadline for its complete implementation.<br>If an SSFN participant is simultaneously connected to a systemically important financial market infrastructure in accordance with FinMIA, the product owner shall inform the FMI operator about the status of the ongoing procedure in connection with the SSFN participant.<br>If an SSFN participant is simultaneously connected to the SIC system as a systemically important infrastructure, the product owner shall inform the SNB about the status of the ongoing procedure in connection with the SSFN participant. |

| # | Step | Description |
|---|---|---|
| 3 | Product owner:<br>Review of implemented measures and possible end of the corrective action procedure or granting of an extension of the deadline. | The product owner checks and documents the implementation of the defined measures, at the latest immediately upon expiry of the set deadline. It may also commission a third party to carry out the review.<br>If, in the view of the product owner, the measures have been fully implemented and the unsatisfactory situation has been remedied, the scheduled corrective action procedure is terminated.<br>If, in the view of the product owner, the measures have not been implemented or have only been implemented incompletely or if the unsatisfactory situation still exists, the product owner can grant an extension of the deadline with any newly defined measures. |
| 4 | Product owner:<br>End of the corrective action procedure or<br>Recommendation to SSFN voting members for temporary or permanent exclusion from SSFN | If, after the grace period has been set, the product owner considers that the defined measures – those from the procedure plan or, if necessary, newly defined with the setting of a grace period – have been implemented and the unsatisfactory situation has been remedied, the corrective action procedure is terminated.<br>If the defined measures have not been implemented or have only been implemented incompletely, or if the unsatisfactory situation continues to exist, and if it appears that<br>– a further extension of the deadline seems ineffective from the point of view of the product owner and/or<br>– keeping the SSFN participant in the SSFN seems unreasonable from the point of view of the network group,<br>then the product owner makes a recommendation to the SSFN voting members on how to proceed as follows:<br>→temporary or final revocation of the affected SSFN participant's admission to the SSFN by suspending the renewal of the SSFN certificate (chapter 5.1.2). |
| | **Caveat:**<br>Separate decision must be obtained if systemically important infrastructure is affected (pursuant to FinMIA) | **Caveat:**<br>If an SSFN participant is simultaneously connected to a systemically important financial market infrastructure in accordance with FinMIA, only the operator of the systemically important infrastructure shall decide on the further participation of such a participant. The product owner must obtain this decision and continue or terminate the procedure accordingly.<br>If an SSFN participant is simultaneously connected to the SIC system as a systemically important infrastructure, only the SNB shall decide on the further participation of such a participant. The SNB's decision regarding participation in the SIC system shall take |

| # | Step | Description |
|---|---|---|
| | | precedence over the decision of the financial market infrastructure operator. |
| 5 | Final decision | The SSFN voting members usually make decisions by unanimous vote (chapter 3.4). The result of the decision of the SSFN voting members is communicated to the SSFN participant in writing. The decision is considered final and the SSFN participant has no possibility to appeal against this decision within the SSFN governance.<br>The decision made under the caveat in step 4 is considered final within the SSFN governance. |
| 6 | SSFN certificate issuers:<br>Suspension of the SSFN certificates | Based on the decision of the SSFN voting members or based on a decision under the caveat in step 4, the SSFN certificate issuers temporarily or permanently suspend the renewal of the SSFN certificate of the offending SSFN participant and inform any affected SSFN service providers. |
| 7 | Consequences of the suspension | The SSFN participant affected by the suspension has no legal or financial claims against the decision-making body or against any other party within the SSFN for any damages as a result of the suspension of the SSFN certificate. |

*Table 6: Process for corrective action, suspension or exclusion of an SSFN participant*

# 9 Change management of the SSFN regulations

Significant changes to the SSFN regulations, i.e., those that impact SSFN participants, are made as follows:

1. Submission to the product owner of the proposed changes by SSFN voting members or by SSFN participants.
2. Compilation and initial assessment by the product owner of the proposals (e.g. in terms of meaningfulness, benefits, costs, impacts).
3. Consultation of the proposed adjustments with SSFN Risk Management.
4. Opening of a consultation of the proposed substantial changes with all SSFN participants by the product owner (review)
5. Evaluation of the comments received by the SSFN voting members (coordination/preparation by the product owner) and a joint decision by the SSFN voting members as to which of the proposed changes shall be finally implemented.
6. As a rule, the SSFN participants are to be informed in an appropriate manner by the product owner about the new version of the SSFN regulations at least three months before they come into effect.
7. The moment when the modified SSFN regulations come into effect is at the discretion of the SSFN voting members; generally, this takes place in the middle of the year. In the case of urgent adjustments for the SSFN, according to the assessment of the SSFN voting members, an entry into effect is possible after a reasonable period of time after the SSFN participants have been informed.

Formal modifications to the SSFN regulations can be made by the SSFN voting members through the product owner at any time and do not require consultation with the SSFN participants. However, the SSFN participants must be informed appropriately before such regulations come into effect.

# 10 Contracts

The following overview shows the main contractual relationships in connection with participation in the SSFN:

| # | Party 1 | Party 2 | Content of contract |
|---|---|---|---|
| 1 | Telecommunication provider (SSFN core members, SSFN carrier) | SSFN participant (exception: SSFN core members) | SCION connection |
| 2 | SSFN provider for SCION solutions or SSFN core members or SSFN | SSFN participant (exception: SSFN core members) | SCION solution (software and/or hardware)<br>→ for own purposes or for resale to own customers |
| 3 | SSFN certificate issuer (SIX) | SSFN participant | "Agreement regarding SSFN certificates" |
| | | | SSFN certificate |
| 4 | Product owner | SSFN service provider | "SSFN Services Agreement" [1] |
| | | | Acknowledgment of and compliance with the SSFN regulations, in particular the fulfilment of the admission criteria in accordance with the agreement |
| 5 | SIX | Switch | Switch as the secondary certificate issuer |
| 6 | SNB | Anapaya | Measures to ensure the operation of the SSFN, including governance |
| 7 | SIX | Anapaya | Service provisioning for SSFN as well as rules of conduct |

*Table 7: Overview of contracts in the SSFN*

# Annex A: Admission criteria for SSFN service providers

Annex A lists the admission criteria that SSFN service providers must demonstrably meet in accordance with chapter 4.1.2 of the SSFN regulations. Different criteria must be met depending on the role. An SSFN service provider may have more than one role, and the criteria to be fulfilled are cumulative. The SSFN service provider may engage subcontractors for the provision of its services. In doing so, it shall always remain responsible at all times for compliance with the admission criteria applicable to its role and must enforce this vis-à-vis the subcontractor.

| # | Relevant for: | | | | | Admission criteria | Recommendations regarding possible verifications |
|---|---|---|---|---|---|---|---|
| | SSFN core members | SSFN carriers | SSFN certificate issuers | SSFN endpoint providers | SSFN providers for SCION solutions | | |
| 1 | x | x | | | | The party is listed in the OFCOM register as a telecommunications service provider with an entry in category 5.1 or 5.2 or in a corresponding register of the national licensing authority in the IT and telecommunications sector (if domiciled abroad) OR the party can demonstrate a permanent activity within the scope of IT network/telecommunications services (analogous to OFCOM categories 5.1 or 5.2) for third parties (e.g. by dint of the "company's purpose" as per a recent extract from the commercial register). | SSFN core member: print screen of OFCOM register excerpt with time stamp<br>SSFN carrier: print screen of OFCOM register excerpt or equivalent confirmation (if domiciled abroad), with time stamp |
| 2 | x | x | x | x | x | Audit of the party's accounts by an FAOA-approved auditor (www.rab-asr.ch/#/publicregister), or equivalent if domiciled abroad. | - Copy of last year's auditor's report (e.g. from annual report)<br>- Print screen of FAOA register extract with time stamp<br>- or equivalent, if domiciled abroad |
| 3 | x | x | x | x | | Access to own AS certificate and associated key is adequately protected (at rest, at processing). | - Process documentation with roles (if applicable), RACI matrix (if applicable), segregation of duties according to industry best practices (e.g. ITIL), access based on the least privilege principle and access rights are checked at regular intervals<br>- Audit trail/access log |
| 4 | | | x | | | Access to and custody of the CP root key and CP CA key are protected with an HSM and adequate processes (at rest, at processing). | - Process documentation with roles (if applicable), RACI matrix (if applicable), segregation of duties according to industry best practices (e.g. ITIL), access based on the least privilege principle and access rights are checked at regular intervals<br>- Audit trail/access log |
| 5 | x | x | x | x | x | Granting of access rights to certificates and keys is regulated. | - Process documentation with roles (if applicable), RACI matrix (if applicable), segregation of duties according to industry best practices (e.g. ITIL), access based on the least privilege principle<br>- Audit trail/access log |

| # | Relevant for: SSFN core members | SSFN carriers | SSFN certificate issuers | SSFN endpoint providers | SSFN providers for SCION solutions | Admission criteria | Recommendations regarding possible verifications |
|---|---|---|---|---|---|---|---|
| 6 | x | x | x | x | x | If data are stored by the party or accessed by authorised persons of the party from outside the country in which it is located (e.g. Switzerland), their customers must be clearly and comprehensively informed and appropriate consent must be demonstrably obtained. | - Compliance with data protection provisions as part of the contract (e.g. GTC) |
| 7 | x | x | x | x | | The list of locations of the SSFN gateways (street, house number, postal code, city, country) is complete and correct. | - List with locations (address) including designation of the data centre (e.g. extract from the CMDB with timestamp) |
| 8 | x | x | | | | The SSFN ISD is used exclusively for SSFN traffic (data and control plane), the SSFN traffic (data and control plane) flows exclusively within the SSFN ISD.<br>There is transparent disclosure of geofencing and cross-border hops (if applicable) to own customers. | - Network plan with all SSFN elements for which a transition to another network is possible (with timestamp)<br>- Penetration test<br>- (Screenshot of disclosure of geofencing/cross-border hops with timestamp) |
| 9 | x | x | x | x | x | No unauthorised (by SSFN voting members) interconnection with foreign networks (incl. other SCION networks and the global Internet) (to/from SSFN) exists or will be built. | - Penetration test<br>- Process documentation with roles (if applicable), RACI matrix (if applicable), segregation of duties according to industry best practices (e.g. ITIL) |
| 10 | | | x | | | An audit log of access to certificates is kept. | - Process documentation with roles (if applicable), RACI matrix (if applicable), segregation of duties according to industry best practices (e.g. ITIL), access based on the least privilege principle<br>- Audit trail/access log |
| 11 | x | x | x | x | | A security operations centre is operated, including associated processes for handling security-relevant incidents. | - Process documentation with roles (if applicable), RACI matrix (if applicable), segregation of duties according to industry best practices (e.g. ITIL) |
| 12 | x | x | x | | | Security-relevant network services (especially network time) are protected, including associated detection and removal of deviations. | - Process documentation with roles (if applicable), RACI matrix (if applicable), segregation of duties according to industry best practices (e.g. ITIL)<br>- Penetration test |
| 13 | x | | | | | SCION core services (especially SCION control services) are offered redundantly. | - List of hostnames and locations of servers with control services (e.g. extract from CMDB with timestamp)<br>- Network drawing |
| 14 | | | x | | | Issuing services are offered redundantly (does not apply to initial certificate). | - List with hostnames and locations of servers with issuing services (e.g. extract from CMDB with timestamp)<br>- Network drawing |

| # | Relevant for: SSFN core members | SSFN carriers | SSFN certificate issuers | SSFN endpoint providers | SSFN providers for SCION solutions | Admission criteria | Recommendations regarding possible verifications |
|---|---|---|---|---|---|---|---|
| 15 | x | x | x | x | | Appropriate business continuity planning or management (BCP or BCM) measures have been taken to remain operationally available in the event of a data centre failure. | - Process documentation with roles (if applicable), RACI matrix (if applicable), segregation of duties according to industry best practices (e.g. ITIL)<br>- BCP plans, test scripts and test reports |
| 16 | x | x | x | | | "Monitoring and capacity management processes" exist in order to comply with agreed bandwidths, availabilities and latency times for customers and, if applicable, other core service providers. | - Process documentation with roles (if applicable), RACI matrix (if applicable), segregation of duties according to industry best practices (e.g. ITIL)<br>- Screenshot of monitoring/SSFN capacity management with timestamp |
| 17 | x | x | x | | | Monitoring exists to maintain the guaranteed (according to point 16) availabilities | - Process documentation with roles (if applicable), RACI matrix (if applicable), segregation of duties according to industry best practices (e.g. ITIL)<br>- Screenshot of SSFN monitoring with timestamp<br>- Service level report |
| 18 | x | x | x | x | x | All services and appliances fully cover the currently valid technical core specifications (SCION protocol) | - Confirmation by Anapaya (core specifications) or the SCION Foundation (future SCION certification authority) |
| 19 | x | | | | | Redundant peerings with other SSFN core members exist, are monitored and restored in reasonable time in case of failure. | - Process documentation with roles (if applicable), RACI matrix (if applicable), segregation of duties according to industry best practices (e.g. ITIL)<br>- Network drawing (or peering inventory) |
| 20 | | x | x | | | Redundant SCION connections (to two SSFN carriers with core services) exist, are monitored and restored in reasonable time in case of failure. | - Process documentation with roles (if applicable), RACI matrix (if applicable), segregation of duties according to industry best practices (e.g. ITIL)<br>- Network drawing |
| 21 | x | x | x | | | An incident management process is in place, incidents and security incidents are managed and security incidents are communicated. | - Process documentation with roles (if applicable), RACI matrix (if applicable), segregation of duties according to industry best practices (e.g. ITIL) |
| 22 | x | x | x | x | x | A change management process is in place and implemented, including a principle of multi-party verification for configuration changes in the SSFN ISD. | - Process documentation with roles (if applicable), RACI matrix (if applicable), segregation of duties according to industry best practices (e.g. ITIL) |
| 23 | x | x | x | x | x | SCION/SSFN network devices and other devices/services offered for SCION are adequately physically protected. | - Protection concept<br>- Process documentation with roles (if applicable), RACI matrix (if applicable), segregation of duties according to industry best practices (e.g. ITIL)<br>- Audit reports |

| # | Relevant for: SSFN core members | SSFN carriers | SSFN certificate issuers | SSFN endpoint providers | SSFN providers for SCION solutions | Admission criteria | Recommendations regarding possible verifications |
|---|---|---|---|---|---|---|---|
| 24 | x | x | | | x | Integrity and authorisation of SW deployment processes are ensured, as well as secure processes, testing and procedures for customers. | - Process documentation with roles (if applicable), RACI matrix (if applicable), segregation of duties according to industry best practices (e.g. ITIL) |
| 25 | x | x | x | x | x | The provisions of the "Best practices in the SCION group" (reference documents [2] and [3]) are complied with or implemented by equivalent measures. | - Process documentation with roles (if applicable), RACI matrix (if applicable), segregation of duties according to industry best practices (e.g. ITIL) |
| 26 | x | x | | | | SSFN voting members, or deputy product owner, are informed about the sale of a SCION connection for the SSFN. | - Extract from the SSFN customer database with timestamp |
| 27 | | | | x | | A contract exists with at least one SSFN user or, in the case of managed services for the SSFN connection, with at least one SSFN subscriber (see chapter 5.1.4) | - Valid contract (see chapter 5.1.4) |

*Table 8: Requirements for SSFN service providers*

# Annex B: Change history

**Version 1.3**

In addition to correcting any spelling and wording errors, the following significant changes have been made:

| Chapter | What |
|---|---|
| General information | Adaptation of the licence from strictly restrictive to CC BY 4.0 |
| 1.4 | ETH link removed, as information can be found directly at the SCION Association. |
| 2.1 | Role description in an ISD moved to chapter 2.4 and merged there with the naming of the specific parties in the SSFN. This increases readability in chapter 2.1 (focus on SCION) and strengthens understanding of the manifestations in SSFN in chapter 2.4. |
| | Figure for roles in ISD updated. |
| 3.5 | Adaptation of the committees to current representation |
| 3.6 | "SSFN Services" basically described as services of SIX; restriction to SIX removed for "reachable services" |
| 4.1.1 | Enumeration "b)": no longer restricted to "paid" SSFN services. |
| 4.1.2 | Detail for subcontractors added. |
| 5.1/5.2 | Obligation of service providers and users added to exercise corresponding care in software deployment and monitoring. |
| 5.1.2 | Services of the core members now also refer to carrier services. |
| 5.1.4 | For "case a)" the example "Service Provider for SECOM customers" added to loosen coupling to SIC |
| 5.2 | Addition of recommendation for risk assessment for third-party mandates |
| Annex A | Extension to take account of delegation to subcontractors |
| | Detailing of criterion 9 |
| | Detailing of criterion 24, extension of scope to SSFN CA and endpoint providers |
| Annex C | Revision of wording from "cross-connect" to "Interconnection with foreign networks..." |

*Table 9: Change history, version 1.3*

**Version 1.2**

| Chapter | What |
|---|---|
| 2.5 | Clarification: Compliance with "Best Practice Document"<br>These must be complied with or **implemented by equivalent measures**. |
| 2.5 | Clarification/new: **Exclusive use of publicly registered IP addresses.** |
| 2.5 | New: **Segregation of the SSFN from the public internet**. |
| 2.6 | New: Bilateral voting in the event of conflicting path preferences between two participants. |
| 3.2 | New: Coordination of the required external assessment by SIX as the product owner. |
| 3.2 | New: Coordination of the central risk management of SSFN voting members by SIX as the product owner. |
| 3.3 | New: Voting members jointly decide on the authorisation etc. of SSFN service providers and their role. |
| 3.6 | Clarification: Indication that SIX maintains (and publishes) an up-to-date list of authorised SSFN services. |
| 5 | New: All SSFN participants are responsible for their connection etc. |
| 7 | New: The results of a preliminary check by an SSFN service provider are valid for a maximum of 12 months. |
| 7 | New: future SSFN service providers prepare all necessary documents for the assessment in advance. |
| 8 | Clarification: If non-compliance with the regulations has resulted in e.g. a potential risk or damage, written form; commissioning of third parties; final decision lies with SNB. |
| 9 | New: Consultation of the risk management of SSFN voting members |
| Annex A | Clarification: #25 Compliance with the "Best Practice Document"<br>These must be complied with or **implemented by equivalent measures.** |

*Table 10: Change history, version 1.2*

# Annex C: Glossary

| | |
|---|---|
| **AS** | Autonomous systems |
| **AS No.** | Unique number that characterises an AS |
| **AS certificate** | Access certificate for each AS in a specific ISD |
| **BCM, BCP and DR** | Business continuity management, business continuity plan, disaster recovery |
| **CA** | Certificate authority |
| **CI** | Certificate issuer |
| **(D)DoS** | (Distributed) denial of service attack |
| **HSM** | Hardware security module |
| **Interconnection with foreign networks (incl. other SCION networks)** | In the SSFN context a connection of SSFN foreign networks with SSFN. This includes both the internet and inter-company networks, but not intra-company connections. |
| **ISD** | Isolation domain |
| **ISP** | Internet service provider |
| **ITIL** | Information technology infrastructure library |
| **Path** | Route of a data packet from sender to receiver |
| **Peering** | Establishing a network connection |
| **RACI** | Responsible, accountable, consulted, informed |
| **SCION** | Scalability, Control and Isolation On Next-generation networks |
| **SIC** | Swiss Interbank Clearing – The SIC system is a systemically important infrastructure in accordance with FinMIA and is the RTGS system for the CHF currency. It is operated by SIC Ltd (a subsidiary of SIX) on behalf of the SNB. |
| **SLA** | Service level agreement (service agreement) |
| **SNB** | Swiss National Bank |
| **SCION gateway** | Gateway and router are used synonymously |
| **SSFN** | Secure Swiss Finance Network |
| **TRC** | Trust root configuration |
| **Voting member** | Decision-making committee for SSFN; SNB, SIX, Switch |