SSFN – Building a secure communication network for the financial community

SSFN Reglement

Version 1.3, gültig ab 01.11.2026



Version 1.3 – 01.07.2026

Revisionsnachweis

Nachfolgend werden alle in diesem Handbuch durchgeführten Änderungen mit Versionsangabe, Änderungsdatum, kurzer Änderungsbeschreibung und Angabe der betroffenen Kapitel aufgelistet.

Version	Datum	Änderungsbeschreibung	Kapitel
1.3	15.01.2026	Ergänzungen (Details siehe Anhang B: Änderungshistorie)	Alle
1.2	01.06.2024	Präzisierungen & Ergänzung (Details siehe Anhang B: Änderungshistorie)	
1.1	03.06.2022	Präzisierungen & Ergänzung	Alle
1.0	30.11.2021	Erstausgabe	

Tabelle 1: Revisionsnachweis

Änderungskontrolle

Alle zukünftigen Änderungen gegenüber Version 1.2 werden in einer Änderungsdokumentation aufgeführt.

Bitte richten Sie sämtliche Anregungen, Korrekturen und Verbesserungsvorschläge zu diesem Dokument ausschliesslich an:

SIX BBS AG
Hardturmstrasse 201
CH-8005 Zürich
E-Mail: pm-ssfn@six-group.com
www.six-group.com

Allgemeine Hinweise

Dieses Dokument steht unter der Lizenz Creative Commons Attribution 4.0 International (CC BY 4.0).

Die Inhalte dürfen kopiert, verbreitet, bearbeitet und kommerziell genutzt werden, sofern SIX als Urheberin genannt wird.

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

Aus Gründen der besseren Lesbarkeit wird, wo immer möglich, auf die Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen sind als geschlechtsneutral zu betrachten.

Sollten Sie allfällige Fehler in diesem Dokument feststellen oder Verbesserungs-vorschläge haben, sind wir Ihnen dankbar für Ihre Rückmeldung per E-Mail an **pm-ssfn@six-group.com**.

SIX stellt eine englische Übersetzung dieses Dokuments zur Verfügung. Sollte es dabei zu inhaltlichen Abweichungen kommen, ist die deutsche Fassung massgebend.

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

Inhaltsverzeichnis

Revisionsnachweis **2**
Allgemeine Hinweise **3**
Inhaltsverzeichnis **4**
Tabellenverzeichnis **6**
Abbildungsverzeichnis **7**
1 Grundlagen SSFN **8**
1.1 SSFN und Teilnehmer 8
1.2 Zweck des SSFN Reglements 9
1.3 Adressaten SSFN Reglement 9
1.4 Referenzdokumente 9
2 Gesamtsystem SSFN **10**
2.1 SCION-Technologie 10
2.2 SCION Netzwerkverbund 11
2.3 Einordnung SSFN 13
2.4 SSFN ISD 13
2.5 Spezifikationen von SSFN 17
2.6 Funktion als Netzwerk 19
3 Governance **20**
3.1 Formale Struktur 20
3.2 Product Owner 20
3.3 SSFN Voting Members 21
3.4 Governance Regeln 21
3.5 Gremien 23
3.6 SSFN Dienste / Dienstleistungen 23
4 Zugangsvoraussetzungen **24**
4.1 Erfüllung Zulassungskriterien 24
4.1.1 SSFN Nutzer 24
4.1.2 SSFN Dienstleister 24
4.1.3 SIX als Primary Certificate Issuer 25
4.2 SSFN-Zertifikat 25
5 Aufgaben der SSFN Teilnehmer **26**
5.1 SSFN Dienstleister 26
5.1.1 SSFN Certificate Issuers 26
5.1.2 SSFN Core Members 27
5.1.3 SSFN Carrier 27
5.1.4 SSFN Endpunktanbieter 28
5.1.5 SSFN Anbieter SCION-Lösung 28
5.2 SSFN Nutzer 29
5.3 Informationsaustausch zur Störungsbehebung 29
6 Verantwortlichkeiten **30**
7 Onboarding-Prozess für SSFN Dienstleister **31**
8 Mängelbehebung, Suspendierung bzw. Ausschluss eines SSFN Teilnehmers **33**
9 Änderungsmanagement des SSFN Reglements **36**

10 Verträge 37
Anhang A: Zulassungskriterien für SSFN Dienstleister 38
Anhang B: Änderungshistorie 42
Anhang C: Glossar 44

Tabellenverzeichnis

Tabelle 1: Revisionsnachweis 2
Tabelle 2: Referenzdokumente 9
Tabelle 3: Links zu entsprechenden Internetseiten 9
Tabelle 4: Regelung der Governance 22
Tabelle 5: Onboarding-Prozess für SSFN Dienstleister 32
Tabelle 6: Prozess für Mängelbehebung, Suspendierung bzw. Ausschluss eines SSFN Teilnehmers 35
Tabelle 7: Übersicht Verträge im SSFN 37
Tabelle 8: Anforderungen an SSFN Dienstleister 41

Abbildungsverzeichnis

Abbildung 1: Elemente eines ISD 11
Abbildung 2: SCION Verbund und Vertragsbeziehungen 12
Abbildung 3: Schematische Darstellung eines ISD, inkl. Rollen in einem ISD 13
Abbildung 4: Governance Struktur SSFN 20

1 Grundlagen SSFN

1.1 SSFN und Teilnehmer

Das Secure Swiss Finance Network («**SSFN**») ist ein für den Finanzplatz Schweiz bereitgestelltes, eigenständiges SCION-basiertes Kommunikationsnetzwerk, welches allen Akteuren, primär den dort zugelassenen Nutzern des Finanzplatzes Schweiz («**SSFN Nutzer**») erlaubt, unter Reduktion der Cyberrisiken des Public Internets in einem in sich geschlossenen System geschützt untereinander zu kommunizieren, ohne dass diese bei demselben Telekommunikationsanbieter angeschlossen sein müssen.

Das SSFN basiert auf einem SCION Netzwerkverbund und stellt aus technischer Sicht eine eigene Isolation Domain («**ISD**») dar. Somit wird zwischen einem SCION Netzwerkverbund der Infrastruktur-Provider (hier «SSFN Dienstleister») sowie dem SSFN als spezifischer SCION-Isolation-Domain unterschieden.

Die SSFN Dienstleister können folgende Rollen haben:

1. SSFN Certificate Issuer
2. SSFN Carrier mit Core Services («Core Members»)
3. SSFN Carrier
4. SSFN Endpunkt-Anbieter
5. SSFN Anbieter SCION-Lösungen.

SSFN Dienstleister können vergleichbare Dienstleistungen - unabhängig vom SSFN - auch für Teilnehmer anderer SCION Isolation Domains anbieten.

Teilnehmer am SSFN sind entweder reine SSFN Nutzer, können aber gleichzeitig auch SSFN Dienstleister sein. Sie werden gesamthaft als «**SSFN Teilnehmer**» bezeichnet.

SIX BBS AG («**SIX**») ist «Product Owner» des SSFN. Die Kontroll- und Steuerungsstruktur (Governance) von SSFN wird gemeinsam von der Schweizerischen Nationalbank (SNB), Switch und SIX wahrgenommen («**SSFN Voting Members**»). SIX hat das vorliegende Reglement für das ISD SSFN in Abstimmung mit den SSFN Voting Members definiert («**SSFN Reglement**»). SIX agiert zusätzlich als Certificate Issuer für das SSFN («**SSFN Certificate Issuer**»). In dieser Funktion nimmt SIX die initiale Ausstellung und Erneuerung des für den Zugang zum SSFN notwendigen AS-Zertifikats («**SSFN-Zertifikat**») für alle SSFN Teilnehmer vor.

1.2 Zweck des SSFN Reglements

Das SSFN Reglement beschreibt:

1. was das Gesamtsystem SSFN beinhaltet (z. B. anhand der Spezifikationen),
2. definiert die Governance von SSFN,
3. legt fest, welche Kriterien ein SSFN Teilnehmer als SSFN Dienstleister oder als SSFN Nutzer erfüllen muss, um zum SSFN zugelassen zu werden,
4. listet Aufgaben und Verantwortlichkeiten aller SSFN Teilnehmer auf,
5. definiert den Prozess bei Verfehlungen gegen das SSFN Reglement,
6. erläutert den Prozess zur Anpassung des SSFN Reglements und
7. bietet eine Übersicht relevanter Verträge im Rahmen des SSFN.

1.3 Adressaten SSFN Reglement

Das SSFN Reglement richtet sich an SSFN Teilnehmer, die entweder als SSFN-Dienstleister und/oder SSFN Nutzer Zugang zum SSFN erhalten.

1.4 Referenzdokumente

Ref	Dokument/Schema	Titel	Quelle
[1]	Vereinbarung SSFN Dienstleister	Vereinbarung für SSFN-Dienstleister	SIX
[2]	Best practice Dokument (allg. Teil)	Best Practices for SCION ISD Operations for ISPs	Anapaya
[3]	Best practice Dokument (SSFN spezifischer Teil)	ISD Operations Manual for SSFN Core ISPs	Anapaya, SIX
[4]	SSFN Zertifikatsvertrag	Vereinbarung betreffend SSFN-Zertifikat	SIX

Tabelle 2: Referenzdokumente

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

Tabelle 3: Links zu entsprechenden Internetseiten

2 Gesamtsystem SSFN

2.1 SCION-Technologie

SCION ist eine Technologie, die an der ETH Zürich entwickelt wurde.

SCION organisiert bestehende autonome Systeme[1] («**AS**») in Gruppen unabhängiger Routing-Ebenen, die Isolation Domains («**ISD**») genannt werden, und ermöglicht so eine vertrauenswürdige Kommunikation zwischen den Mitgliedern in dieser Gruppe, unabhängig, bei welchem teilnehmenden Netzwerkanbieter diese angeschlossen sind.

Um eine ISD aufzusetzen, wird eine durch die Voting Members ausgestellte und gültige Trust Root Configuration («**TRC**») benötigt. Darin werden die Governance Prinzipien und wesentliche zugelassene Dienstleister in diesem ISD (Core Members [für Routing] und Certificate Issuers [für AS-Zertifikate]) hinterlegt. Die Vergabe eines AS-Zertifikats (siehe unten) durch im TRC bezeichnete Certificate Issuers basiert auf den in den Governance Prinzipien definierten Zulassungskriterien. Das TRC bildet somit den «Root of Trust» für die entsprechende ISD. Der «Trust», also das TRC, wird deshalb auch jährlich erneuert.

Kernelement eines SCION-basierten Netzwerks ist die Kontrolle über den Pfad, den Daten vom Sender zum Empfänger nutzen (Routing). Hierbei werden dem Sender jederzeit die möglichen Pfade zum Empfänger in Echtzeit aufgezeigt. Der Pfad beinhaltet hierbei die Zwischenschritte, d. h. die SCION-Gateway, welche auf dem Weg zwischen Sender und Empfänger verwendet werden können.

Die Kontrolle, dass die Datenpakete tatsächlich dem vom Sender ausgewählten Pfad zum Empfänger folgen, wird auf Basis kryptographischer Prozesse mittels Zertifikaten sichergestellt. Die SCION-Gateways leiten dabei die Datenpakete gemäss der im jeweiligen Paket hinterlegten Anweisung des Senders an den nächsten SCION-Gateway weiter, ohne Möglichkeit, einen anderen Weg zu wählen. Dank der Echtzeitinformation kann bei Nicht-Erreichbarkeit / Ausfall eines SCION-Gateways nahezu unterbruchsfrei ein neuer Pfad bestimmt und genutzt werden. Der Sender kann hierzu Prioritäten für die Pfadwahl in seinen SCION-Gateways hinterlegen.

Jedes AS hinterlegt auf seinen SCION-Gateways ein Zertifikat, welches das jeweilige AS als Teil einer ISD ausweist («**AS-Zertifikat**»). Ein AS-Zertifikat hat gemäss SCION-Spezifikation aus Sicherheitsüberlegungen eine kurze Gültigkeit (in der Regel 72h). Es muss daher periodisch mittels Antrag an den Certificate Issuer erneuert werden. Diese Antrags- und Erneuerungs-Prozesse erfolgen vollständig automatisiert und bedingen keine manuellen Eingriffe der Teilnehmer. Die Gültigkeitsdauer des aktuellen sowie diejenige des neuen AS-Zertifikates überschneiden sich, sodass jederzeit ein gültiges AS-Zertifikat vorhanden ist.

AS-Zertifikate können ausschliesslich von jenen Certificate Issuern ausgestellt und erneuert werden, welche im TRC von den Voting Members bezeichnet und somit autorisiert wurden. Die Ermittlung der Echtzeitinformation über den Zustand möglicher Pfade erfolgt ebenfalls von im TRC bezeichneten Core Members.

Jeder SCION-Gateway benötigt für das Funktionieren eine spezielle SCION-Software. Diese muss innerhalb der ISD untereinander kompatibel sein. Die SCION-Software ist als Open Source ausgestaltet (siehe github.com/scionproto/scion).

Insbesondere die ETH Zürich sowie Anapaya Systems, ein Spin-off der ETH Zürich und kommerzieller Anbieter von SCION-Lösungen, tragen wesentlich zur Weiterentwicklung der

[1] Unter einem Autonomen System (AS) versteht man ein in der Aussensicht als eigenständig wahrnehmbares und adressierbares Netzwerk. In der Regel unterhält z.B. eine Unternehmung (bzw. eine Unternehmensgruppe) ein solches Netzwerk, um es mit einer gemeinsamen Routing-Richtlinie verwalten zu können.

SCION-Software bei. Zudem wurde 2023 die SCION Association gegründet, die sich u.a. auch bei IETF für eine Standardisierung von SCION einsetzt sowie eine Zertifizierung von SCION-Anbietern anstrebt.

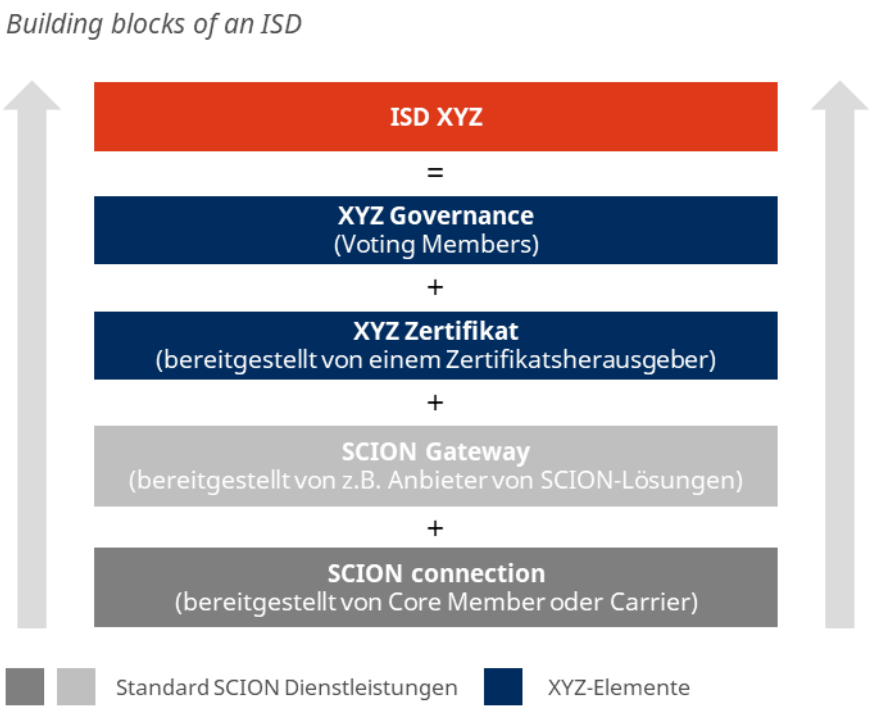


Abbildung 1: Elemente eines ISD

Die SCION-Technologie ist so aufgebaut, dass eingesetzte Hardware-Komponenten wie z.B. SCION-Gateway, gleichzeitig in unterschiedlichen ISDs eingesetzt werden können. Hierzu müssen die entsprechenden Zertifikate für die jeweiligen ISDs auf den Gateways abgespeichert werden.

In der Konsequenz bedeutet dies, dass insbesondere Core Members, Carrier oder Anbieter von SCION-Lösungen, ihre Dienstleistungen weitgehend unabhängig von einzelnen ISDs definieren und daher standardisierte SCION Dienstleistungen anbieten können.

Für jedes ISD muss bestimmt sein, wer Voting Member ist und welche Regeln in Bezug auf Teilnahme in diesem ISD gelten sollen. Die Einhaltung dieser Regeln zur Teilnahme wird durch die Voting Members und den jeweiligen Certificate Issuer einer ISD sichergestellt.

Speziell Core Members können in verschiedenen ISDs Verbundleistungen zur Bereitstellung eines SCION-basierten Netzwerks und für die darauf basierenden ISDs erbringen (SCION Netzwerkverbund). Um die notwendigen Leistungen der jeweiligen Core Members im Rahmen der Verbundleistung sicherzustellen, haben sie erhöhte Anforderungen zu erfüllen.

Die SCION-Technologie definiert keine fixe Anzahl an Voting Members, Certificate Issuers oder Core Members. Jedoch bedingt jede Änderung bei diesen drei Rollen eine Aktualisierung des TRC. Mit zunehmender Anzahl steigt zudem die Komplexität, ohne dass in gleichem Ausmass die Verfügbarkeit verbessert wird.

2.2 SCION Netzwerkverbund

Der SCION Netzwerkverbund bildet die Basis-Netzwerkinfrastruktur, auf der verschiedene ISDs betrieben werden. Der SCION Netzwerkverbund ist der Zusammenschluss der Core Members, die

die SCION Spezifikation einhalten und somit die Kommunikation für beliebige ISDs ermöglichen (siehe *Abbildung 2*).

Anapaya definiert in Zusammenarbeit mit Telekommunikationsunternehmen und CAs («**SCION Community**») in einem «**Best practice-Dokument (allg. Teil)**» [2] - basierend auf Erfahrungswerten - Vorgaben für Aktivitäten und Prozesse in einem SCION Netzwerkverbund. Die dort enthaltenen Regeln definieren die «Best practices» für das sichere, technisch korrekte und resiliente Betreiben eines SCION Netzwerkverbunds und regeln Verhaltenspflichten, namentlich:

1. Die redundante Anbindung zwischen den Carriers, um eine hohe Netzwerk-Verfügbarkeit zu garantieren (redundantes Peering).
2. Die redundante Anbindung zwischen den Carriers an die entsprechenden CA-Dienstleister (Certificate Issuer), um eine hohe Verfügbarkeit zu garantieren (redundante CA-Anbindung).
3. Verbundweite betriebliche Regelungen, wie bspw. ein betrieblich übergreifendes Management von Sicherheits-Vorfällen (Incident Management) zu erfolgen hat.

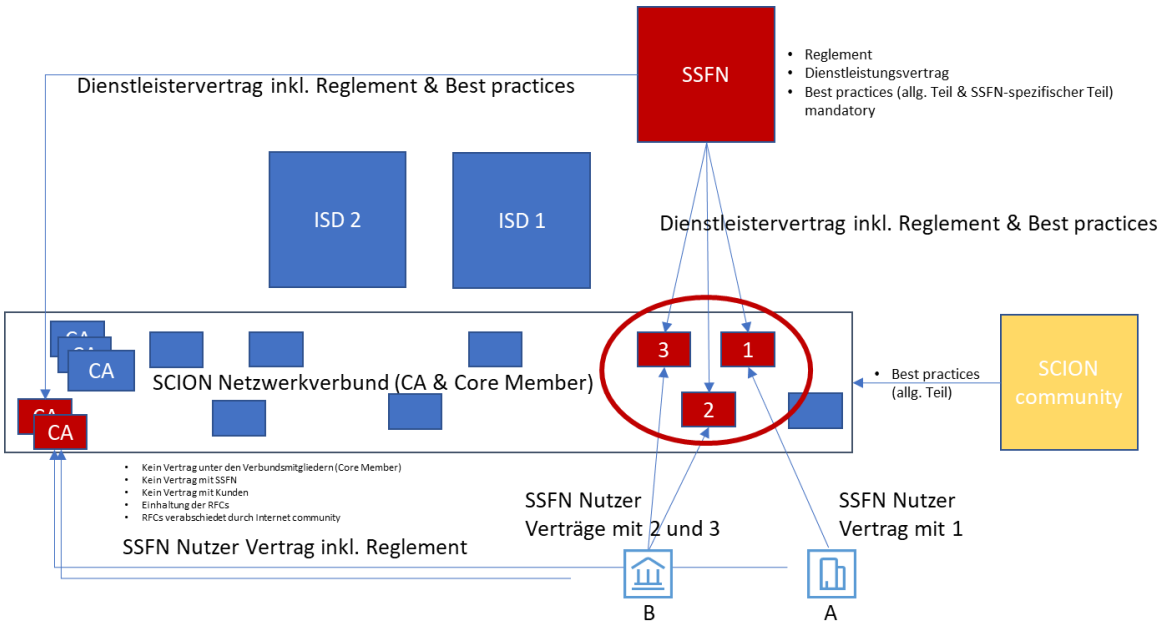


Abbildung 2: SCION Verbund und Vertragsbeziehungen

Für SCION-Verbundsmitglieder, die das SSFN anbieten, müssen das Best Practice-Dokument (allg. Teil) [2] sowie die Präzisierungen für SSFN (Best practice Dokument (SSFN spezifischer Teil) [3]) eingehalten werden. In SSFN hat das Best Practice Dokument (SSFN spezifischer Teil) [3] Vorrang vor dem Best Practice Dokument (allg. Teil) [2].

2.3 Einordnung SSFN

Das SSFN ist ein für den Finanzplatz Schweiz bereitgestelltes, auf der SCION Technologie basierendes eigenständiges Kommunikationsnetzwerk. Es erlaubt den zugelassenen SSFN Nutzern, unter Reduktion der Cyberrisiken des Public Internets, in einem in sich geschlossenen Netzwerk geschützt untereinander zu kommunizieren, ohne dass diese bei demselben SSFN Carrier angeschlossen sein müssen.

Die funktionale Beschreibung des SSFN verzichtet bewusst auf technologische Aspekte. Das SSFN hat seine Fundierung in der Kooperation von Infrastruktur-Providern, die ihrerseits die SCION-Technologie als Routing-Architektur nutzen (siehe Kapitel 2.2).

Die Trennung zwischen dem SCION-basierten Netzwerkverbund und dem SSFN als ISD erfolgt beim sogenannten Service Access Point. Diese Trennung erlaubt, die Spezifikation und Verantwortlichkeit jeweils klar entweder dem SCION-basierten Netzwerkverbund oder dem SSFN zuzuordnen.

Entsprechend regeln und definieren die SSFN Dienstleister ihre technischen und betrieblichen Aspekte sowie Prozesse untereinander.

2.4 SSFN ISD

SSFN ist ein Kommunikationsnetzwerk auf Basis eines SCION-basierten Netzwerkverbundes und stellt als solches eine eigenständige ISD mit eigenem TRC dar. Ein AS-Zertifikat im SSFN wird als SSFN-Zertifikat bezeichnet («**SSFN Zertifikat**»).

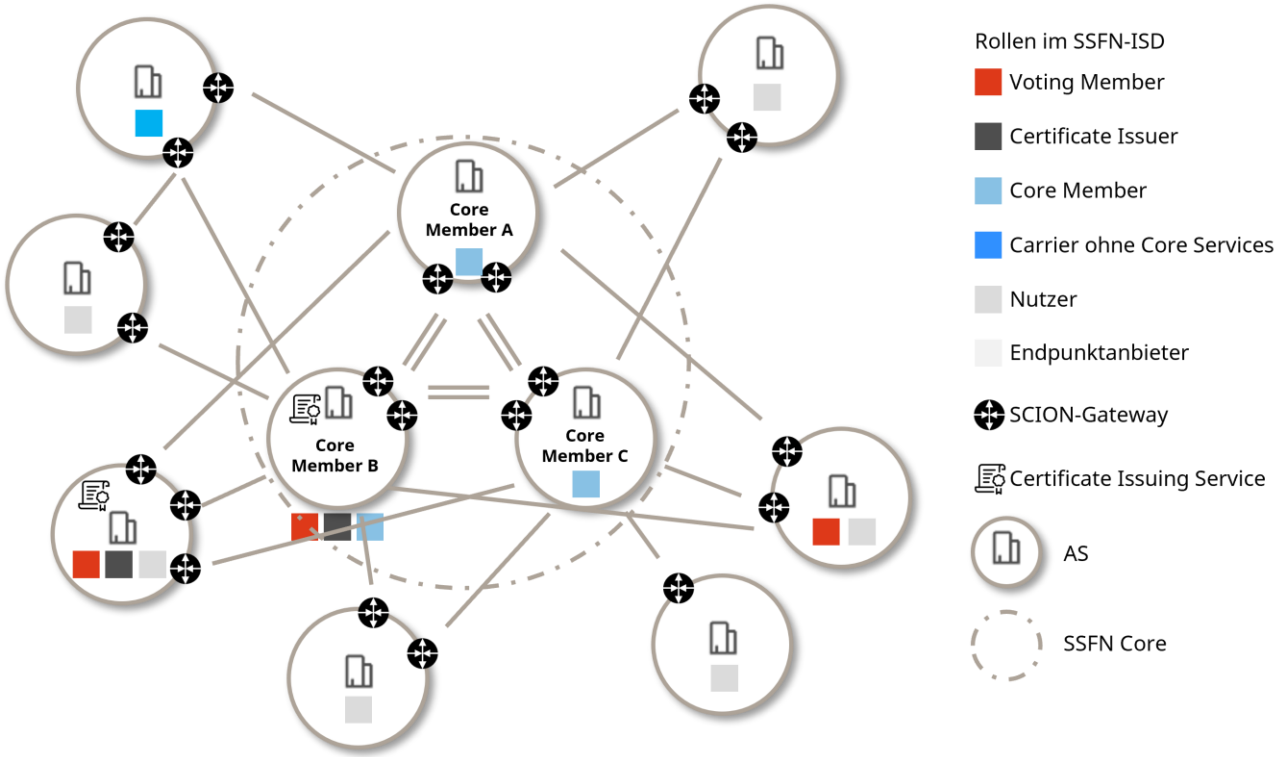


Abbildung 3: Schematische Darstellung eines ISD, inkl. Rollen in einem ISD

In einem ISD, in Abbildung 3 am Beispiel SSFN dargestellt, sind durch die zugehörigen AS folgende Rollen wahrzunehmen (vgl. dazu Kapitel 4 «Zugangsvoraussetzungen»):

ISD Rolle	Beschreibung	Parteien im SSFN
Voting Members	Erstellung und Aktualisierung des TRC, ebenfalls verbunden mit dem Aufsetzen einer Governance für die ISD sowie der Abnahme von Anpassungen (z.B. Reglementsanpassungen, Zulassungskriterien u.ä.).	SIX, Schweizerische Nationalbank (SNB), Switch (siehe Kapitel 3)
Certificate Issuer	Erstellung und Erneuerung aller im ISD notwendigen AS-Zertifikate (auf Basis der Governance des ISD), mit Ausnahme jener für das TRC.	SIX, (siehe Kapitel 5.1.1) als Backup für die Zertifikatserneuerung ist es Switch
Core Member (Carrier mit Core Services)	Erbringen von Core Services (z.B. Path Finding / Beaconing für Ermittlung in Echtzeit des Zustands jedes möglichen Pfads, TRC dissemination) für den ISD, Bereitstellen von Konnektivität (auf Basis der Governance des ISD). Beim Core Member handelt es sich in der Regel um einen Telekommunikationsanbieter mit signifikanter eigener Netzwerkinfrastruktur (z.B. Internet Service Provider).	Sunrise, Swisscom, Switch (siehe Kapitel 5.1.2)
Carrier	Bereitstellung von Konnektivität (auf Basis der Governance des ISD). Hinweis: diese Rolle ist nicht zwingend notwendig für das Funktionieren einer ISD. Beim Carrier handelt es sich in der Regel ebenfalls um einen Internet Service Provider oder Telekommunikationsanbieter, jedoch ohne signifikante eigene Netzwerkinfrastruktur oder der Anbieter ist im Ausland domiziliert.	weitere Carriers (siehe Kapitel 5.1.3)
Nutzer	Nutzer eines SCION ISDs.	zugelassener (nach Kapitel 4.1.1) Akteur des Finanzplatzes Schweiz (z.B. Teilnehmer am SIC)
Anbieter von SCION-Lösungen (In Abbildung 3 nicht dargestellt, jedoch ebenfalls wesentlich für das Funktionieren eines ISD)	Erstellung, Bereitstellung/Vertrieb und Wartung von kommerzieller SCION-basierter Software (allenfalls inkl. Hardware).	Anapaya Systems AG (derzeit einziger Anbieter; siehe hierzu Kapitel 5.1.5)
SCION Endpunktanbieter (in Abbildung 3 nicht dargestellt)	«Dienstleister», welche Nutzern, die NICHT am ISD direkt angeschlossen sind, den Zugang zu Diensten via dem ISD ermöglichen oder diesen Nutzern sonstige Services via dem ISD (z.B. Managed Services für den SCION Anschluss) anbieten. Im Gegensatz zu «Carrier» sind diese Dienstleister nicht Telekommunikationsanbieter, sondern z.B. Outsourcing-Anbieter (wie Service Büros).	Dienstleister für SIX Kunden (z.B. Service Büro für SIC-Teilnehmer), welche einen SSFN Anschluss benötigen, um damit indirekt zugelassenen SSFN-Nutzern den Zugang zum SSFN zu ermöglichen oder

ISD Rolle	Beschreibung	Parteien im SSFN
		diesen sonstige Services via SSFN (z.B. Managed Services für den SSFN Anschluss) anbieten. Siehe hierzu auch Kapitel 5.1.4

SSFN als eigenständige ISD hat eine eigene, von anderen ISDs unabhängige Governance definiert (siehe hierzu Kapitel 3). Diese regelt die Aufgaben und Verantwortlichkeiten innerhalb der ISD SSFN.

Zur Wahrung einer hohen Verfügbarkeit, bei gleichzeitiger Minimierung der Auswirkungen auf die technische Komplexität, erscheint in der ISD SSFN bezüglich Anzahl SSFN Certificate Issuers und SSFN Core Members, ein Verhältnis von zwei SSFN Certificate Issuers gegenüber drei SSFN Core Members als optimal.

SIX als Product Owner definiert gemeinsam mit den weiteren SSFN Voting Members die Governance des SSFN (Kapitel 3).

2.5 Spezifikationen von SSFN

SSFN stellt eine ISD auf Basis des bestehenden SCION Netzwerkverbunds dar. Als solches sind gewisse Spezifikationen des Kommunikationsnetzwerks durch das SCION-Protokoll vorgegeben, andere werden durch die SSFN Voting Members spezifiziert.

Nachfolgend werden die Spezifikationen ausserhalb des generellen SCION-Protokolls aufgeführt.

Betriebliche Anforderungen an die SSFN Teilnehmer: Aufgaben und Verantwortlichkeiten jedes SSFN Teilnehmers werden entsprechend seiner Rolle definiert. Dies beinhaltet insbesondere auch Anforderungen an die Sicherheit. Die Verletzung der Anforderungen kann zu einem Ausschluss im SSFN führen oder es werden andere geeignete Massnahmen getroffen (z.B. Pfadeinschränkungen, Firewall-Rules). Die betrieblichen Anforderungen an die SSFN Dienstleister werden im Rahmen der Zulassungskriterien für SSFN Dienstleister (gemäss Anhang A) sichergestellt.

Verfügbarkeit / Zuverlässigkeit: Die Verfügbarkeit bzw. Zuverlässigkeit des SSFN wird im Wesentlichen durch die involvierten SSFN Dienstleister bestimmt. Diese definieren in ihren Kundenverträgen entsprechende Service-Aspekte (z.B. Verfügbarkeit, Reaktionszeit bei Incidents, Betriebszeiten). Die Zuverlässigkeit der relevanten SCION-Komponenten (z.B. Core Services, Verbindung zwischen den SSFN Core Members, SSFN Certificate Issuers) wird durch eine hohe Redundanz unter den SSFN Dienstleistern erreicht und im Rahmen der *Zulassungskriterien für SSFN Dienstleister* (gemäss Anhang A) sichergestellt.

Leistung / Kapazität: Die Leistung und Kapazität des SSFN ergibt sich durch das Zusammenspiel der involvierten SSFN Dienstleister. Diese definieren in ihren Kundenverträgen entsprechende Aspekte (z.B. Bandbreite, Latenz, Verfügbarkeit) und stellen darauf basierend eine entsprechende Qualität und Leistung im eigenen Netzwerk zur Verfügung. Die Qualität und Leistung im eigenen Netzwerk werden im Rahmen der *Zulassungskriterien für SSFN Dienstleister* (gemäss Anhang A) sichergestellt.

Fehlerbehandlung, BCM, BCP und DR: Diese Aspekte des SSFN ergeben sich durch das Zusammenspiel der involvierten SSFN Dienstleister. Alle SSFN Dienstleister haben im Rahmen der *Zulassungskriterien für SSFN Dienstleister* gemäss Anhang A sicherzustellen, dass geeignete Prozesse, Systeme und Ressourcen zur Erkennung und Behandlung von Fehlern bzw. Ausfällen vorhanden sind. Ebenso sind einzelne Regeln dazu in den Best Practice-Dokumenten (allg. & SSFN-spezifischer Teil) vorgegeben.

«Best Practice-Dokument» zu Aktivitäten im SCION-Verbund: Unter der Leitung von Anapaya und unter Mithilfe der SSFN Core Members und SIX sind, basierend auf Erfahrungswerten, Vorgaben für Aktivitäten und Vorgehen in einem SCION Netzwerkverbund (z.B. Incident- / Problemmanagement) erarbeitet worden. Alle SSFN Dienstleister bestätigen im Rahmen der *Zulassungskriterien für SSFN Dienstleister* (gemäss Anhang A), dass sie die Bestimmungen in ([2] und [3]) einhalten oder gleichwertige Massnahmen umgesetzt haben.

Monitoring. Jeder SSFN Teilnehmer hat den Zustand aller seiner sichtbaren Pfade sowie seiner SSFN-spezifischen Dienste zu überwachen, um im Bedarfsfall geeignete Massnahmen ergreifen zu können. Es existiert kein zentrales Monitoring für das SSFN.

Geofencing: Es werden keine spezifischen Vorgaben bzgl. Geofencing gemacht. SSFN Dienstleister geben den SSFN Voting Members auf Anfrage bekannt, wo deren für SSFN relevante SCION-Gateways lokalisiert sind. Auch müssen SSFN Dienstleister unaufgefordert ihren Kunden bekannt geben, falls ausländische «Hops» verwendet werden. Innerhalb des Netzwerks eines SSFN Dienstleisters kann nicht geregelt werden, dass ausschliesslich Datenleitungen in der Schweiz für den Transport von SSFN-Daten verwendet werden. SSFN Nutzer können bei ihrem

jeweiligen Vertragspartner und SSFN Dienstleister jedoch jederzeit anfragen, wo die für SSFN relevanten SCION-Gateways lokalisiert sind. Es besteht eine diesbezügliche Auskunftspflicht der SSFN Dienstleister.

Zugelassene Teilnehmer: SSFN stellt hohe Anforderungen an die Zulassung und damit den Erhalt eines SSFN-Zertifikats. Ausschliesslich Parteien, welche die im SSFN Reglement festgelegten Kriterien erfüllen, können bei SIX ein SSFN-Zertifikat beantragen und erhalten (Kapitel 4.2).

Verwendung des SSFN-Zertifikats: Das SSFN-Zertifikat darf ausschliesslich im Kontext von SSFN verwendet werden.

Schutz vor Cyberrisiken / (D)DoS: SSFN ist logisch getrennt von allen anderen Netzwerken (inkl. dem Public Internet). Innerhalb des SSFN könnte jedoch ein zugelassener SSFN Teilnehmer andere zugelassene SSFN Teilnehmer absichtlich oder unabsichtlich mit Traffic überlasten. Hierfür existieren auf Basis des SCION-Protokolls Schutzmechanismen. Betroffene SSFN Teilnehmer können selbst Massnahmen ergreifen (z.B. Informieren des Senders durch den Empfänger, Blockieren von Pfaden vom Sender zum Empfänger durch den Empfänger, Anpassen von eigenen Firewall-Rules). Im Übrigen kann dem Sender bei Verfehlungen gegen das SSFN Reglement die Erneuerung des SSFN-Zertifikats durch den SSFN Certificate Issuer verweigert werden (siehe hierzu Kapitel 8).

Verwendete Netzwerkprotokolle beim SSFN Dienstleister: Es wird erwartet, dass SSFN Dienstleister native SCION-Verbindungen anbieten. Es besteht jedoch die Möglichkeit, den SCION-Traffic auch als Overlay (z.B. auf dem eigenen IP-Backbone) auszugestalten. Unabhängig davon, muss der SSFN Dienstleister nachweislich sicherstellen, dass zu keiner Zeit ein unautorisierter Übergang zu einer anderen ISD oder zum Public Internet existiert. Dies wird im Rahmen der *Zulassungskriterien für SSFN Dienstleister* (gemäss Anhang A) sichergestellt.

Ausschliessliche Nutzung öffentlich registrierter IP Adressen. Alle SSFN Teilnehmer verwenden ausschliesslich registrierte öffentliche IP Adressen. Die SSFN Teilnehmer sorgen dafür, dass die Adressen aus dem Internet (oder anderen öffentlichen Netzen) nicht erreichbar sind.

Segregierung vom Public Internet: *Für SCION-Verbindungen zur SSFN-ISD gilt zudem, dass die durch den SCION-Provider bereitgestellten SSFN-Access Links zwischen dem CPE (Customer Premises Equipment) und dem Core des Providers nicht aus dem Public Internet des Providers sowie dem Public Internet adressier- und erreichbar sein dürfen.*

SCION-Lösungen, inkl. zugehöriges Software-Deployment:

Die SSFN Teilnehmer haben SCION-Lösungen wie folgt umzusetzen:

1. Die im Einsatz stehende SCION-Lösung eines SSFN Teilnehmers muss den aktuell gültigen SCION-Spezifikationen entsprechen. Massgebend ist die Kompatibilität der verwendeten SCION-Lösung zur Referenzimplementation des Technologie-Anbieters, z. Zt. einzig Anapaya Systems AG. Dies ist von jedem SSFN Teilnehmer eigenständig sicherzustellen.
2. Die Anschlussarchitektur und der Software-Deployment Prozess müssen den geschäfts-üblichen Sicherheitsanforderungen genügen sowie die Integrität und Autorisierung jederzeit gewährleisten.

Schutz des Schlüsselmaterials. Es gelten je nach verwendetem kryptographischem Schlüssel-material nachfolgende Anforderungen:

1. SSFN-Zertifikate: SSFN-Zertifikate und die zugehörigen Schlüssel (Public und Private Keys), werden gemäss SCION-Protokoll auf den SCION-Gateways gespeichert (keine HSM). Die SCION-Gateway müssen gehärtet und der Zugriff - insbesondere auf Schlüsselmaterial - mittels definierter Regeln eingeschränkt sein.

2. Zertifikate der SSFN Certificate Issuers: Standardmässig sollen SSFN Certificate Issuers ihr geheimes Schlüsselmaterial (Private Keys) in HSMs mit den geschäftsüblichen Schutzmassnahmen speichern. Dies ist zwingend für die «Root Certificate Private Keys». Auf eine Speicherung in einem HSM kann verzichtet werden, falls stattdessen kurze Zertifikatslaufzeiten (<10 Tage für Intermediär-Zertifikate) verwendet werden. In einem solchen Fall muss das verwendete Gerät (z.B. Server) gehärtet und der Zugriff mittels definierter Regeln eingeschränkt sein.
3. Trust Root Configuration (TRC): Hier muss das geheime Schlüsselmaterial (Private Keys) zwingend in HSM mit den hierzu geschäftsüblichen Schutzmassnahmen gespeichert werden.

2.6 Funktion als Netzwerk

SSFN-Teilnehmer kann werden, wer entweder als SSFN-Nutzer oder als SSFN-Dienstleister die entsprechend definierten Zulassungskriterien im Vorfeld erfüllt (siehe Kapitel 4 «Zugangsvoraussetzungen»).

Über das SSFN ISD ist es den SSFN Teilnehmern erlaubt, miteinander Daten auszutauschen. Dabei definieren die SSFN Teilnehmer unilateral, bilateral oder multilateral, welche Daten über welche Pfade ausgetauscht werden können.

- SSFN in seiner Funktion als Netzwerk macht keine Vorgabe zur Datennutzung. SSFN darf indessen ausschliesslich für den Austausch des von den jeweilig involvierten SSFN Teilnehmern legitimierten Datenaustausches verwendet werden: Jeder Teilnehmer ist in seinem Bereich für die Einhaltung des geltenden Rechts verantwortlich.
- Haben Parteien ihre Pfadpräferenzen jeweils so gewählt, dass sich diese widersprechen und damit ein Datenaustausch nicht erfolgen kann, müssen die betroffenen Parteien diesen Widerspruch bilateral lösen

Um als SSFN Teilnehmer die ISD SSFN nutzen zu können, ist die nachfolgende Infrastruktur von jedem SSFN Teilnehmer bereitzustellen:

a) eine (oder mehrere) Datenverbindung zum SSFN (i.d.R. ein SCION-Anschluss zu einem SSFN Core Member oder einem SSFN Carrier). Empfohlen wird eine redundante Anbindung über verschiedene Carriers (SSFN Core Member oder SSFN Carrier).

b) das Vorhandensein mindestens eines SCION-Gateways.

c) SSFN Teilnehmer müssen zudem über ein gültiges SSFN-Zertifikat verfügen (siehe hierzu Kapitel 4.2) und sind verpflichtet, keine Handlungen vorzunehmen, die negativen Einfluss auf andere SSFN Teilnehmer oder die ISD SSFN haben.

d) SSFN Teilnehmer müssen in ihren Rollen als SENDER und EMPFÄNGER die notwendigen Arbeiten pro Service vornehmen (z.B. Einrichten / Erfassen IP-Adresse des Services für SSFN, DNS-Einstellungen, Firewall-Regeln).

3 Governance

3.1 Formale Struktur

Im SSFN bilden die SSFN Voting Members SIX, SNB und Switch die Governance. SIX agiert gleichzeitig auch als Product Owner sowie als SSFN Certificate Issuer.

Die Anforderung einer ungeraden Anzahl von SSFN Voting Members stellt eine Beschlussfähigkeit sicher (Mehrheitsbeschluss). Die Anzahl von drei Voting Members reduziert die Komplexität und garantiert, dass, bei einem Ausfall eines Voting Members die beiden verbleibenden SSFN Voting Members die TRC weiterhin verwalten und aktuell halten können (zu Änderungen an der TRC werden mindestens zwei Parteien benötigt).

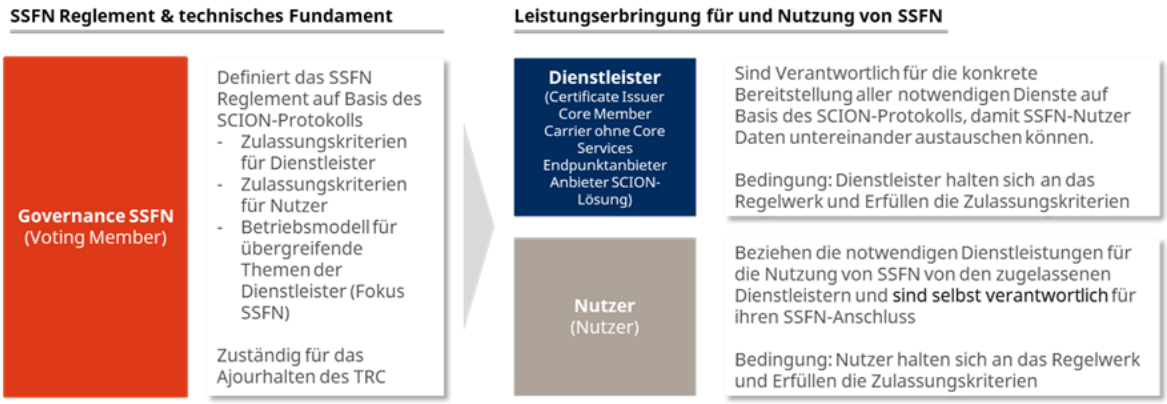


Abbildung 4: Governance Struktur SSFN

3.2 Product Owner

SIX als Product Owner koordiniert die Abstimmung mit den zwei weiteren SSFN Voting Members die Regeln des SSFN Reglements sowie des Best practice Dokuments (SSFN spezifischer Teil) [3] und kann an die SCION Community Empfehlungen zur Anpassung des Best practice Dokuments (allg. Teil) [2] aussprechen.

Der Product Owner erbringt alle delegierbaren Aufgaben der SSFN Voting Members (Ausgenommen sind jene Aufgaben, die zwingend den Einbezug der übrigen SSFN Voting Members bedingen (z.B. Entscheidungen, Aktualisierung TRC)).

Die Aufgaben des Product Owners sind insbesondere:

- Tritt in dieser Rolle gegen aussen für das SSFN auf und vertritt zugleich die anderen SSFN Voting Members
- Koordiniert und prüft die Resultate von Assessments durch externe Prüfer bei Anträgen um Zulassung zum SSFN als Dienstleister oder Service Büro. Vom Product Owner als im SSFN zulässig befundene Antragssteller werden den Voting Members zur Abstimmung vorgelegt.
- Koordiniert die Prüfung zur Erfüllung der Zulassungskriterien der SSFN Teilnehmer (Kapitel 4.1.1 und 4.1.2). inkl. zugehöriger vertraglicher Regelung
- Koordiniert das zentrale Risikomanagement für SSFN im Auftrag und unter Teilnahme der Voting Members
- Führt Verfahren bei Verfehlungen gegen das SSFN Reglement von SSFN Teilnehmern (Kapitel 8) in Abstimmung mit den weiteren SSFN Voting Members durch

- Stellt Änderungsbegehren an die weiteren SSFN Voting Members zu; Aktualisiert das SSFN Reglement in Abstimmung mit den weiteren SSFN Voting Members und stellt die Informationsweitergabe gegenüber den SSFN Teilnehmern (Kapitel 9) sicher
- Unterstützt die SSFN Teilnehmer bei Fragestellungen im Rahmen des SSFN Reglements oder der Teilnahme am SSFN im Allgemeinen
- Koordiniert Aktivitäten rund um die TRC Aktualisierung
- Koordiniert die SSFN Gremien (Kapitel 3.5)

3.3 SSFN Voting Members

Die drei SSFN Voting Members haben die Kernaufgabe, das SSFN Reglement zu definieren und damit die Regeln für ein ordentliches Funktionieren des SSFN festzulegen oder diese Regelungen anzupassen (Kapitel 9). Dazu gehört ebenfalls die aktive Mitwirkung am SSFN Risikomanagement unter der Leitung des Product Owners.

Sie unterstützen den Product Owner in Fragestellungen zum SSFN Reglement seitens der SSFN Dienstleister und SSFN Nutzer. Auf Antrag unterstützen die SSFN Voting Members den Product Owner bei der Erbringung seiner Aufgaben; die SSFN Voting Members können nach Absprache auch Spezialaufgaben übernehmen.

Des Weiteren regeln sie die Aspekte rund um den TRC (Kapitel 2.1). und stellen die Aktualität des TRC sicher. Sie befinden final über die Weiterentwicklung der SSFN ISD (Kapitel 2.5). Hierzu gehört insbesondere den TRC initial zu erstellen, ihn regelkonform inkl. ausreichender Vorlaufzeiten zu erneuern und bei Bedarf anzupassen (inkl. der Zulassung von SSFN Core Members und SSFN Certificate Issuer).

Die SSFN Voting Members befinden gemeinsam über die Zulassung (oder auch den Ausschluss) von Dienstleistern im SSFN und deren Rolle.

3.4 Governance Regeln

Die Governance ist wie folgt geregelt:

Element	Konkrete Regelung
Anzahl	SSFN wird durch drei SSFN Voting Members etabliert und definiert. Die Anzahl darf kurzfristig unter drei fallen (z.B. aufgrund eines Austrittes), jedoch ist schnellstmöglich ein neues SSFN Voting Member für das Gremium zu gewinnen. Als Voting Member gelten Institutionen (nicht Personen); jedoch muss eine für das Voting Member agierende Person von der jeweiligen Institution definiert werden.
Kriterien für die Aufnahme	SSFN Voting Member darf nur sein, wer die Ziele von SSFN aktiv unterstützt, bereit ist, die im SSFN Reglement definierten Aufgaben und Verantwortlichkeiten wahrzunehmen, einen Mehrwert für SSFN bringt und von den bestehenden SSFN Voting Members bestätigt wird. Es besteht kein Anspruch auf Aufnahme.
Austritt	Austretende SSFN Voting Members haben bei der Suche nach einem Ersatz aktiv zu unterstützen. Es wird erwartet, dass das austretende SSFN Voting Member erst nach erfolgreicher Wahl eines neuen SSFN Voting Members seine Aufgaben niederlegt. Die Kündigungsfrist beträgt 12 Monate und erfolgt auf ein Quartalsende. In dieser Frist sind die Aufgaben und Verantwortlichkeiten weiterhin wahrzunehmen.

Product Owner	Die SSFN Voting Members bestimmen den Product Owner. Der Product Owner ist SIX, welche zugleich auch SSFN Voting Member, wie auch Zertifikatsstelle ist. Tritt der Product Owner von seiner Aufgabe zurück, hat er gleich wie beim Austritt als Voting Member, eine Kündigungsfrist von 12 Monaten auf Quartalsende einzuhalten und in dieser Frist seine Aufgaben weiterhin vollumfänglich zu erfüllen. Bei einer Übergabe sind alle notwendigen Informationen/Daten an den neuen Product Owner unaufgefordert und vollständig zu übergeben. Die SSFN Voting Members sind für einen Ersatz innert dieser Frist besorgt.
Beschluss-fassung	Beschlüsse werden grundsätzlich durch die SSFN Voting Members und i.d.R. einstimmig (i.S. eines Konsensbeschlusses) gefällt. Kann keine gemeinsame Position gefunden werden, so gilt ein einfaches Mehr. Die SSFN Voting Members sind grundsätzlich gleichberechtigt, bei Stimmengleichheit (z.B. Stimmenthaltung) hat SIX in ihrer Rolle als Product Owner den Stichentscheid. ***Vorbehalte bei Beschlüssen zum Ausschlussverfahren (siehe Kapitel 8)***: 1. Ist ein potenziell auszuschliessender SSFN Teilnehmer zugleich einer systemisch bedeutsamen Finanzmarktinfrastruktur gemäss Finanzmarktinfrastrukturgesetz («FinfraG») angeschlossen, so entscheidet ausschliesslich die Betreiberin der systemisch bedeutsamen Infrastruktur über die weitere Teilnahme eines solchen Teilnehmers im Rahmen eines Verfahrens gemäss Kapitel 8. Der Product Owner hat diesen Entscheid einzuholen und das Verfahren demgemäss weiterzuführen bzw. zu beenden. 2. Ist ein potenziell auszuschliessender SSFN Teilnehmer zugleich am SIC-System - als systemisch bedeutsame Infrastruktur - angeschlossen, entscheidet ausschliesslich die SNB über die weitere Teilnahme eines solchen Teilnehmers im Rahmen eines Verfahrens gemäss Kapitel 8. Der Entscheid der SNB betreffend Teilnahme am SIC-System hat Vorrang ggü. dem Entscheid des Finanzmarktinfrastruktur-Betreibers. Die Entscheide im Rahmen des SSFN gelten als final, d.h. es existieren keine Anfechtungsmöglichkeiten innerhalb der SSFN Governance. Betroffene Parteien haben zudem keinerlei rechtliche oder finanzielle Ansprüche gegenüber der Entscheid fällenden Instanz noch gegenüber sonst einer Partei innerhalb des SSFN für allfällige Schäden als Folge eines Verfahrensentscheids gemäss Kapitel 8.
Entschädigung	Die SSFN Voting Members erhalten für ihre Funktion als SSFN Voting Members keine finanzielle Entschädigung. Von dieser Regelung ausgenommen ist SIX in ihrer Rolle als Product Owner. Die aus dieser Rolle resultierenden Aufwendungen werden via Gebühreneinnahmen gemäss «Vereinbarung betreffend SSFN-Zertifikat» entschädigt.

Tabelle 4: Regelung der Governance

3.5 Gremien

Es existieren nachfolgende drei Gremien im SSFN:

- **SSFN Governance Board**: SSFN Voting Members treffen sich ad-hoc nach Bedarf.
  Funktion: Austausch unter den SSFN Voting Members und Treffen von grundlegenden Entscheidungen (z.B. Weiterentwicklung von SSFN, Abnahme von Systemtests, Anpassungen des SSFN Reglements, Erneuerung des TRC, Änderungen technischer Natur, Behandlung von Anträgen aus anderen Gremien u. ä.).

- **SSFN Provider Meeting**: Trifft sich periodisch, mindestens jedoch zwei Mal jährlich unter dem Vorsitz des Product Owners. Teilnehmer sind die SSFN Dienstleister in den Rollen als SSFN Certificate Issuer, SSFN Core Members, SSFN Carriers und optional die SSFN Voting Members. Weitere SSFN Dienstleister wie SSFN Endpunkt-Anbieter oder SSFN Anbieter von SCION-Lösungen können bei Bedarf zu einzelnen Sitzungen eingeladen werden.
  Funktion: Austausch unter den Betreibern der SCION Core Infrastruktur über betriebliche Aspekte des Netzwerkes, insbesondere dessen Stabilität, Verfügbarkeit und ausserordentlichen Vorkommnisse. Anforderungen an Verbesserungen und Weiterentwicklungen des SCION Netzwerkverbundes sollen ebenfalls diskutiert werden. Anpassungen, die zu Änderungen innerhalb der ISD SSFN führen, müssen bei den SSFN Voting Members beantragt werden.

- **SSFN Risk-Management:** Die Risk Delegierten der Voting Members treffen sich halbjährlich und bewirtschaften die SSFN Risiken aus dem Risiko-Inventar und nehmen wenn notwendig neue Risiken zur Bearbeitung auf.

3.6 SSFN Dienste / Dienstleistungen

- Zugelassene SSFN Dienstleistungen (**«SSFN Dienstleistungen»**)

  SSFN Dienstleistungen sind grundsätzlich die Dienstleistungen der SIX-Group, die Schweizer Finanzmarkt-Regulationen oder Schweizer Finanzmarkt-Standards erfüllen. Zudem muss eine Dienstleistung im Rahmen ihrer vertraglichen Vereinbarung mit den Kunden einen formellen Identifizierungsnachweis beinhalten (z.B. SIC). Über die Zulassung einer Dienstleistung am SSFN entscheiden abschliessend die SSFN Voting Members. Zur Zeit gelten folgende Dienste als „SSFN Dienstleistungen“: SIC, euroSIC und SECOM.

- Via SSFN erreichbare Dienste (**«erreichbare Dienste»**)

  Jeder Dienst, der von einem SSFN Nutzer oder einem SSFN Endpunktanbieter via SSFN erreichbar ist.

  Hinweis: Ein SSFN Nutzer darf SSFN nebst der Verwendung für erreichbare Dienste grundsätzlich auch verwenden, um eigene Standorte (z.B. Filialen und eigene Rechenzentren), welche nicht im gleichen Netzwerkverbund (= gleiches AS) sind, via SSFN zu vernetzen (ausgeschlossen zum heutigen Zeitpunkt sind hierbei IoT-Devices, insbesondere auch Kartenterminals und einzelne Bancomaten). Jeder Standort, der nicht im gleichen Netzwerkverbund eines SSFN Teilnehmers steht, wird technisch als eigenständiger SSFN Nutzer betrachtet; entsprechend ist für jeden solchen Standort mit einer eigenen AS-Nummer ein eigenes SSFN-Zertifikat notwendig. Dieses SSFN-Zertifikat wird auf die gleiche juristische Person ausgestellt wie das initial erteilte SSFN-Zertifikat. Kunden von SSFN Nutzern dürfen nicht über die SSFN ISD angeschlossen werden, können aber mittels einer anderer ISD (z.B. der SwissISD) über das SCION-Protokoll mit ihrem Dienstleister, dem SSFN Nutzer, kommunizieren. Diese Kommunikation findet jedoch ausserhalb des SSFN statt.

4 Zugangsvoraussetzungen

4.1 Erfüllung Zulassungskriterien

4.1.1 SSFN Nutzer

Akteure des Finanzplatzes Schweiz, welche eines der folgenden Kriterien erfüllen, sind grundsätzlich zum SSFN als SSFN Nutzer zugelassen:

a) Teilnehmer ist SSFN Voting Member oder

b) Teilnehmer ist Vertragspartner der SIX Group AG oder einer Gruppengesellschaft der SIX Group AG und bezieht eine SSFN Dienstleistung (siehe Kapitel 3.6).

Der Product Owner hat das Recht, das Zulassungskriterium lit. b) zum SSFN Nutzer als Vertragspartner jederzeit zu überprüfen.

Der SSFN Nutzer hat des Weiteren im Rahmen der «Vereinbarung betreffend SSFN-Zertifikat» gegenüber dem SSFN Certificate Issuer die Anerkennung und Befolgung des SSFN Reglements zu bestätigen (Kapitel 4.2).

4.1.2 SSFN Dienstleister

Um als SSFN Dienstleister zur Teilnahme am SSFN zugelassen zu werden, muss der SSFN Dienstleister im Rahmen der separaten Vereinbarung «Teilnahme am SSFN als SSFN Dienstleister» gegenüber dem Product Owner bestätigen, dass er das SSFN Reglement einhält und die Zulassungskriterien gemäss Anhang A dieses Reglements dauerhaft erfüllen wird («***Anerkennung des SSFN Reglements***», Kapitel 7). Anhang A dieses Reglements ist im Übrigen identisch zu Anhang 2 der erwähnten Vereinbarung. Anhang A bestimmt die jeweils gültige Version von Anhang 2 der Vereinbarung «Teilnahme am SSFN als SSFN Dienstleister»[2].

Die zu erfüllenden Zulassungskriterien sind der jeweiligen Rolle des SSFN Dienstleisters im SSFN zugeordnet. Beispiele möglicher Nachweise zur Dokumentation der Erfüllung der Zulassungskriterien sind in Anhang A (bzw. Anhang 2 der Vereinbarung «Teilnahme am SSFN als SSFN Dienstleister») aufgeführt.

Agiert der SSFN Dienstleister in mehreren Rollen (z.B. SSFN Core Member und SSFN Certificate Issuer), so muss er die Anforderungen gemäss Anhang A für alle auf ihn zutreffenden Rollen einhalten und hat dies im Rahmen der *Anerkennung des SSFN Reglements* in Anhang 2 der Vereinbarung «Teilnahme am SSFN als SSFN Dienstleister» entsprechend zu vermerken.

Der Product Owner hat gemäss Vereinbarung «Teilnahme am SSFN als SSFN Dienstleister» das Recht, die Erfüllung der Zulassungskriterien beim SSFN Dienstleister jederzeit zu überprüfen bzw. durch einen entsprechend beauftragten Dritten überprüfen zu lassen. Die elektronischen Nachweise müssen hinsichtlich Erfüllung der Zulassungskriterien gemäss Anhang A vom SSFN Dienstleister stets vollständig und aktuell bereitgehalten werden.

Erfüllt ein SSFN Teilnehmer die Kriterien als SSFN Nutzer (z. B. als SIC-Teilnehmer), agiert aber gleichzeitig auch als SSFN Dienstleister (z.B. Service Büro für andere SIC-Teilnehmer), so ist die Vereinbarung «Teilnahme am SSFN als SSFN Dienstleister» ebenfalls zu unterzeichnen. Technisch kann der gleiche SCION-Anschluss für beide Rollen verwendet werden.

[2] Unterschiede können aus der Weiterentwicklung des Anhangs A im Gegensatz zum Wording in Anhang 2 zur Zeit der Vertragsunterzeichnung entstehen. Anpassungen in Anhang A werden immer mit den Anpassungen des SSFN Reglements bekannt gegeben und somit ab dessen Gültigkeit automatisch anerkannt.

SSFN Dienstleister können zur Erbringung ihrer Services Subunternehmer einsetzen. Dabei bleibt der SSFN Dienstleister verantwortlich für die Einhaltung aller für die durch den Dienstleister eingenommene Rolle geltenden Zulassungskriterien und muss, falls anwendbar, dies gegenüber dem/der Subunternehmer durchsetzen.

4.1.3 SIX als Primary Certificate Issuer

Ausschliesslich SIX ist als Primary Certificate Issuer am SSFN zugelassen und nimmt damit nebst der Rolle als Product Owner und SSFN Voting Member auch jene des SSFN Dienstleisters wahr (siehe Kapitel 5.1.1).

Die initiale Ausstellung eines gültigen SSFN-Zertifikats gilt als Spezialaufgabe innerhalb des SSFN. Die Bereitstellung eines gültigen SSFN-Zertifikats ist Bestandteil der Governance und deshalb durch ein SSFN Voting Member sicherzustellen. SIX in ihrer Rolle als Primary Certificate Issuer und gleichzeitig Voting Member ist deshalb von der Unterzeichnung der Vereinbarung «Teilnahme am SSFN als SSFN Dienstleister» ausgenommen. Ungeachtet dessen ist auch SIX als Primary Certificate Issuer an die Regeln des SSFN Reglements (inkl. Einhaltung der relevanten Vorgaben in Anhang A) gebunden und hat spezifisch definierte Aufgaben und Verantwortlichkeiten wahrzunehmen (Kapitel 5.1.1 und Kapitel 6).

4.2 SSFN-Zertifikat

Für die Teilnahme am SSFN benötigt jeder SSFN Teilnehmer ein SSFN-Zertifikat, (Kapitel 2.6), welches ihm im Rahmen der «Vereinbarung betreffend SSFN-Zertifikat» [4] und bei Erfüllung der Zulassungskriterien gemäss Kapitel 4.1.1 und/oder Kapitel 4.1.2 vom SSFN Certificate Issuer initial ausgestellt wird.

Zur Wahrung der Sicherheit ist die Gültigkeit des SSFN-Zertifikats durch den SSFN Certificate Issuer kontinuierlich zu erneuern (Kapitel 5.1.1). Die jeweilige Erneuerung setzt voraus, dass der SSFN Teilnehmer die Zulassungskriterien gemäss Kapitel 4.1.1 und/oder Kapitel 4.1.2 dauerhaft erfüllt.

Der Prozess der Erneuerung des SSFN-Zertifikats gestaltet sich wie folgt:

SSFN-Zertifikate haben grundsätzlich eine Gültigkeitsdauer von 72 Stunden, davon ausgenommen ist das initiale SSFN-Zertifikat mit einer Gültigkeit von 30 Tagen. Vor Ablauf der Gültigkeit eines «normalen» SSFN-Zertifikats muss die Erneuerung desselben durch den SSFN Teilnehmer jeweils 18 Stunden nach Einsatz des aktuell gültigen SSFN-Zertifikats (im Rahmen eines vollautomatischen Prozesses) wieder initiiert werden. Damit erfolgt eine zeitliche Überschneidung des aktiven mit dem bereits erneuerten SSFN-Zertifikat, sodass der SSFN Teilnehmer auch bei technischen Problemen über ein gültiges SSFN-Zertifikat verfügt.

5 Aufgaben der SSFN Teilnehmer

Es existieren nachfolgend aufgeführte Kategorien von SSFN Teilnehmern mit spezifischen Aufgaben:

- **SSFN Dienstleister**: SSFN Certificate Issuers, SSFN Core Members, SSFN Carriers, SSFN Endpunkt-Anbieter, SSFN Anbieter SCION-Lösungen; siehe hierzu Kapitel 5.1
- **SSFN Nutzer**, siehe hierzu Kapitel 5.2

Ein SSFN Teilnehmer kann mehrere Rollen einnehmen. Die Aufgaben und Anforderungen die erfüllt werden müssen, kumulieren sich hierbei.

Alle SSFN Teilnehmer sind verantwortlich für ihren SSFN-Anschluss und damit verbunden für den ordnungsgemässen Betrieb ihres SSFN-Anschlusses. Dazu gehört u.a. auch die Wahrnehmung geeigneter Schutzmassnahmen.

5.1 SSFN Dienstleister

SSFN Dienstleister erbringen im SCION Netzwerkverbund Dienstleistungen für die ISD SSFN. Sie verpflichten sich mittels Vereinbarung «Teilnahme am SSFN als SSFN Dienstleister» gegenüber dem Product Owner, die Zulassungskriterien gemäss Anhang A dauerhaft zu erfüllen.

Die SSFN Dienstleister stellen sicher, dass ihre SW-Deployment-Prozesse (siehe Zulassungskriterien, Anhang A) vorgängig ein adäquates Testing beinhalten.

SSFN Dienstleister haben vor Austritt aus dem ISD SSFN die Kündigungsfrist gemäss Vereinbarung «Teilnahme am SSFN als SSFN Dienstleister» einzuhalten, damit rechtzeitig ein allfälliger Ersatz gefunden werden kann.

Ein SSFN Nutzer hat im Übrigen keinen Anspruch, dass ein SSFN Dienstleister mit ihm eine vertragliche Beziehung eingeht.

5.1.1 SSFN Certificate Issuers

SIX fungiert als “**Primary Certificate Issuer”** und Switch als “**Secondary Certificate Issuer”.** Switch erfüllt damit die wichtige Backup-Funktion für SIX im Rahmen der Kontinuität bei der Erneuerung von SSFN Zertifikaten.

SIX als “**Primary Certificate Issuer”** (Kapitel 4.1.3) hat die ausschliessliche Berechtigung, *initiale* SSFN-Zertifikate für SSFN Teilnehmer im Rahmen der separaten «Vereinbarung betreffend SSFN Zertifikat» auszustellen. SIX stellt den dafür notwendigen Prozess sicher bzw. kann diesen an einen Dritten auslagern.

Sowohl SIX als auch Switch unterhalten als derzeitige SSFN Certificate Issuers die für die Erneuerung der SSFN-Zertifikate notwendige Infrastruktur, inkl. zugehöriger Ressourcen.

Die Zertifikatserneuerung erfolgt in der Regel durch SIX, es sei denn, ihre Infrastruktur funktioniert nicht ordnungsgemäss. Für diesen Fall erfolgt die Zertifikatserneuerung automatisch durch Switch als Backup. Die für Switch entstehenden Aufwendungen für die Leistung als Secondary Certificate Issuer werden durch SIX als Primary Certificate Issuer. basierend auf einer separaten Vereinbarung zwischen SIX und dem Secondary Certificate Issuer, entschädigt.

Die SSFN Certificate Issuers haben im Übrigen die nachfolgenden Aufgaben wahrzunehmen:

- SIX: Prüfung der Berechtigung des SSFN Teilnehmers für die initiale Ausstellung eines SSFN-Zertifikats gemäss «Vereinbarung betreffend SSFN-Zertifikat».
- SIX & Switch: Prüfung der Berechtigung des SSFN Teilnehmers für die Erneuerung von SSFN-Zertifikaten.
- SIX & Switch: Pflicht zur zeitgerechten Ausstellung eines integren Zertifikats, sofern der SSFN Teilnehmer nicht suspendiert ist.
- SIX & Switch: Suspendierung von SSFN-Zertifikaten (temporär oder final) auf Basis des Entscheids der SSFN Voting Member (Kapitel 8) inkl. Informationsabgleich hierzu.
- SIX & Switch: Information der anderen SSFN Voting Members über operationelle Probleme.

5.1.2 SSFN Core Members

Die SSFN Core Members bilden zusammen einen SCION Netzwerkverbund, bestehend aus ihren autonomen Netzwerken inkl. Erbringung zugehöriger Core Services (siehe auch Kapitel 2).

Zusätzlich zum Core Service bieten diese ihren Kunden (SSFN Teilnehmer) auch Carrier-Dienste an.

Der SSFN Core Member hat im Übrigen die nachfolgenden Aufgaben wahrzunehmen:

- Bereitstellen von SCION-Dienstleistungen im SSFN für SSFN Nutzer und SSFN Endpunkt-anbieter. Sie akzeptieren und erfüllen dafür zusätzlich das «ISD operations manual for SSFN core ISPs» sowie die «Best practices for SCION ISD operations for ISPs».
- Diskriminierungsfreie Bereitstellung von Anbindungen für SSFN Carriers.
- Kooperation mit SSFN Voting Members, dem Product Owner, anderen SSFN Core Members sowie SSFN Certificate Issuers und deren zeitgerechte Information bei technischen Problemen.
- Unterstützung seiner SSFN-Kunden bei technischen Problemen.

5.1.3 SSFN Carrier

Beim SSFN Carrier handelt es sich um einen Carrier ohne eigene Erbringung von Core Services im SCION-Verbund.

Er bietet seinen Kunden SCION Konnektivität an, um sich mit der ISD SSFN verbinden zu können, allenfalls ergänzt um «Managed Services». Es kann sich beispielsweise um einen Carrier handeln, der hauptsächlich als «Connector» zum SSFN für ausländische Nutzer agiert.

Der SSFN Carrier hat im Übrigen die nachfolgenden Aufgaben wahrzunehmen:

- Bereitstellen von SCION-Dienstleistungen im SSFN für SSFN Nutzer und SSFN Endpunktanbieter.
- Kooperation mit SSFN Voting Members, dem Product Owner, anderen SSFN Core Members sowie SSFN Certificate Issuers und deren zeitgerechte Information bei technischen Problemen.
- Unterstützung seiner SSFN-Kunden bei technischen Problemen.

5.1.4 SSFN Endpunktanbieter

Ein SSFN Endpunktanbieter ermöglicht einem SSFN Nutzer im Rahmen eines Vertrags entweder

a) den Zugang zu SSFN-Dienstleistungen über SSFN (z.B. Service Büro für SIC-Teilnehmer) oder

b) erbringt Managed Services für den SSFN Anschluss eines SSFN Teilnehmers.

Damit ein Dienstleister SSFN Endpunktanbieter werden kann, bedarf es eines vorbestehenden Vertrags seitens Dienstleister mit mindestens einem SSFN Nutzer.

Im Falle a) gilt:

- Der vorbestehende Vertrag muss einen wesentlichen Zusammenhang mit einer SSFN Dienstleistung seitens SSFN Nutzer aufweisen (z.B. Service Büro für SIC-Teilnehmer, Service Provider für SECOM-Kunden).
- Ist noch kein Kunde des Dienstleisters ein SSFN Nutzer, kann der Dienstleister trotzdem als SSFN Endpunktanbieter während einer Frist von sechs Monaten (mit möglicher Verlängerung auf begründetem schriftlichem Antrag) am SSFN teilnehmen. Diese Zeitspanne dient dazu, einen SSFN Nutzer als Kunden zu gewinnen und damit die Anforderung a) zu erfüllen.

Im Falle b) gilt:

- Der vorbestehende Vertrag ist explizit und ausschliesslich für Wartungs- und Monitoring Dienstleistungen zu einem SSFN Anschluss des SSFN Teilnehmers aufgesetzt.

Ein SSFN Endpunktanbieter hat im Übrigen die nachfolgenden Aufgaben wahrzunehmen:

- Kooperation mit SSFN Voting Members, dem Product Owner, anderen SSFN Core Members sowie SSFN Certificate Issuers und deren zeitnahe Information bei technischen Problemen.

Im Falle a) gilt:

- Kundenanbindung und Sicherstellung der Kommunikation seiner Kunden via SSFN.
- Bereitstellung des sicheren Zugangs zu seiner Infrastruktur für seine Kunden, welche SSFN Nutzer sind, via dem Kommunikationsnetzwerk SSFN.

5.1.5 SSFN Anbieter SCION-Lösung

Der SSFN Anbieter SCION-Lösung erstellt und wartet SCION-basierte Software für den Einsatz in einem SCION-basierten Netzwerk. Er bietet skalierbare SCION-Lösungen an, die in SCION-Netzwerken einsetzbar sind.

Bemerkung: SSFN Anbieter SCION-Lösung erhalten kein SSFN Zertifikat.

Der SSFN Anbieter SCION-Lösung hat im Übrigen die nachfolgenden Aufgaben wahrzunehmen:

- Weiterentwicklung und Wartung seiner SCION-Software und Appliances unter Einhaltung des SCION-Protokolls und Verwendung der SCION-Open Source.
- Vertrieb von SCION-Lösungen (z.B. Software, Support, Management, Hardware, Lizenzen) an SSFN-Teilnehmer.
- Zeitgerechte und vollständige Information des Product Owners betreffend wesentliche Änderungen (z.B. Releasewechsel, Hot-Fixes).
- Unterstützung seiner SSFN-Kunden bei Problemen.
- Kooperation mit SSFN Voting Members, dem Product Owner, anderen SSFN Core Members sowie SSFN Certificate Issuers und deren zeitnahe Information bei Problemen.

5.2 SSFN Nutzer

Ein SSFN Nutzer verwendet SSFN, um sich mit Dienstleistungen der SIX Group zu verbinden und bei Bedarf mit anderen SSFN Teilnehmern (SSFN Dienstleister oder SSFN Nutzer) Daten auszutauschen.

Zu diesem Zweck bezieht ein SSFN Nutzer bei SSFN Dienstleistern (vgl. anfangs Kapitel 5) die für seine Bedürfnisse notwendigen Dienstleistungen.

Der SSFN Nutzer hat im Übrigen die nachfolgenden Aufgaben wahrzunehmen:

- Beschaffung der SCION-Anbindung(en) und entsprechender SCION-Gateway gemäss eigenen Bedürfnissen (Redundanz, Bandbreite, BCM, Verfügbarkeit u. ä.) sowie unter Berücksichtigung allfälliger dienstleistungsspezifischer Regeln (z.B. SIC).
- Sicherer Betrieb seines SSFN-Anschlusses (z.B. Überwachung, Konfiguration, Zugriffsschutz, Zertifikate, Pfadredundanz, Firewalls, aktuelle SCION-Software, Knowhow) Nebst dem Betrieb von aktueller SCION-Software ist der SSFN-Nutzer verpflichtet, die Anweisungen in den Releasenotes des Herstellers zeitnah zu berücksichtigen.
- Entscheidet selbst, mit welchen anderen SSFN-Nutzern er Daten via SSFN austauschen will.
- Wird der SSFN Anschluss (ganz oder teilweise) durch einen Dritten betrieben, behält der SSFN Nutzer dennoch immer die Verantwortlichkeit und muss stets seine Pflichten daraus erfüllen. Dazu kann auch eine wiederkehrende adäquate Risikobeurteilung des beauftragten Dritten im Sinne der Prüfung einer Outsourcing-relevanten Dienstleistung gemäss FINMA gehören.

5.3 Informationsaustausch zur Störungsbehebung

SSFN Dienstleister und SSFN Nutzer unterstützen sich gegenseitig bei der Behebung von Vorfällen und Störungen. SSFN Dienstleister und SSFN Nutzer sind sich deshalb bewusst, dass die für die Störungsbehebung notwendigen Informationen (z.B. Software-Version des Gateways, Port-Einstellungen, IP-Adresse, Mitschnitt von Netzwerkverkehr) mit anderen SSFN Teilnehmern geteilt werden können. Jeder SSFN Nutzer ist selbst für die Informationen, die von ihm geteilt werden, verantwortlich.

Die im genannten Zusammenhang mit Störungen ausgetauschten Informationen sind nach dem Need-to-Know Prinzip zu behandeln und einzig im Kontext der Störungsbehebung zu verwenden.

6 Verantwortlichkeiten

Der Product Owner, die SSFN Voting Members – einzeln und als Gremium – sowie die anderen Entscheid fällenden Instanzen und Gremien im SSFN übernehmen aufgrund der als Verbundsleistung erbrachten Bereitstellung von SSFN (Kapitel 1.1) keinerlei Gewährleistungen oder Zusicherungen gegenüber den SSFN Teilnehmern. Jegliche Forderungsansprüche der SSFN Teilnehmer gegenüber diesen Parteien im Zusammenhang mit deren Teilnahme am SSFN sind im gesetzlich zulässigen Rahmen wegbedungen.

Verstösst ein SSFN Teilnehmer gegen das SSFN Reglement, gilt das Verfahren gemäss Kapitel 8.

Im Übrigen ist jeder SSFN Teilnehmer – sei es als SSFN Dienstleister oder als SSFN Nutzer – für die Leistungen gegenüber seinem Vertragspartner verantwortlich. Allfällige Gewährleistungen oder Zusicherungen sind in den bilateralen Vertragsbeziehungen zwischen den SSFN Teilnehmern zu regeln. Werden vertragliche Leistungen zwischen den SSFN Teilnehmern nicht oder mangelhaft erbracht, so ist dies ausschliesslich im Rahmen der jeweiligen vertraglichen Beziehung untereinander zu klären.

Für die SSFN Certificate Issuers gelten die spezifischen Regelungen gemäss «Vereinbarung betreffend SSFN-Zertifikat».

Der Product Owner kann bei Streitigkeiten zum SSFN unter SSFN Teilnehmern einzig im Sinne einer Vermittlung angefragt werden. Der Product Owner entscheidet (z. B. aufgrund seines Knowhows) nach freiem Ermessen, ob es zweckmässig erscheint, in der angefragten Streitigkeit zu vermitteln. Der Product Owner wird indessen keinesfalls Parteistellung beziehen oder eine juristische Beurteilung hinsichtlich Streitigkeit abgeben, sondern einzig einen Konsens zwischen den betroffenen SSFN Teilnehmern anstreben.

7 Onboarding-Prozess für SSFN Dienstleister

Die Aufnahme neuer SSFN Dienstleister erfolgt gemäss nachfolgendem Prozess:

#	Schritt	Beschreibung
1	Interesse als SSFN Dienstleister	Ein Dienstleister bekundet beim Product Owner Interesse als potenzieller SSFN Dienstleister.
2	Product Owner: Vorprüfung	Anhand nachfolgender Kriterien erfolgt eine objektive Vorprüfung der Eignung des Dienstleisters durch den Product Owner mit anschliessender Abstimmung mit den SSFN Voting Members. Prüfungsrelevante Kriterien sind: – Grad der Unterstützung bei der Anwendung von SCION Technologie – Komplexität in der Einbindung in SSFN – Auswirkung auf den Betrieb – technische Kompetenz – Reputation im Markt. Das Resultat der Vorprüfung hat eine Gültigkeit von maximal 12 Monaten.
3	Product Owner: Entscheid Vorprüfung; Information Zulassungskriterien	Das Ergebnis der Vorprüfung wird dem Dienstleister durch den Product Owner schriftlich kommuniziert. Gegen diesen Entscheid existieren keine Anfechtungs-möglichkeiten seitens des betroffenen Dienstleisters (Kapitel 1.1). Bei positivem Ergebnis wird der Dienstleister durch den Product Owner über die zu erfüllenden Zulassungs-kriterien und die entsprechend nötigen Nachweise (Anhang A) als Zugangsvoraussetzung zum SSFN informiert.
4	Dienstleister: Bereitstellung Nachweise und Anerkennung des SSFN Reglements	Nach Bereitstellung entsprechender Nachweise durch den Dienstleister, bestätigt dieser mit Unterzeichnung der Vereinbarung «Teilnahme am SSFN als SSFN Dienstleister» gegenüber dem Product Owner, dass er das SSFN Reglement einhält und die Zulassungskriterien gemäss Anhang A dieses Reglements dauerhaft erfüllen wird (siehe Kapitel 4.1.2).
5	Product Owner: Prüfung Erfüllung Zulassungskriterien	Der Product Owner bzw. ein von ihm beauftragter Dritter prüft die Erfüllung der Zulassungskriterien gemäss Anhang A (siehe Kapitel 4.1.2). Der künftige SSFN Dienstleister bereitet sich für diese Prüfung wie folgt vor: – Bereitstellen aller vorhandener Evidenzen (Dokumente, Prozessbeschreibungen, Testergebnisse u.ä.) gemäss den Zulassungskriterien – Nennung von Ansprechperson(en) im Falle von Fragen während der Prüfung, so dass eine effiziente Prüfung sichergestellt ist.

6	Product Owner: Empfehlung an SSFN Voting Members SSFN Voting Members: Finaler Entscheid	Der Product Owner erstellt zuhanden der übrigen SSFN Voting Members eine Empfehlung zur Zulassung bzw. zur Ablehnung der Teilnahme am SSFN (inkl. Begründung, z. B. Nichterfüllung einzelner Zulassungskriterien). Die SSFN Voting Members entscheiden final hinsichtlich Zugang SSFN (siehe Kapitel 3.4). Gegen diesen Entscheid existieren keine Anfechtungsmöglichkeiten seitens des Dienstleisters.
7	Product Owner: Kommunikation Entscheid	Das Ergebnis des finalen Entscheids wird dem betroffenen Dienstleister durch den Product Owner schriftlich kommuniziert.
8	Zulassung zur Teilnahme am SSFN	Bei positivem Zulassungsentscheid werden die notwendigen Massnahmen für den Zugang des SSFN Dienstleisters zum SSFN umgesetzt.

Tabelle 5: Onboarding-Prozess für SSFN Dienstleister

8 Mängelbehebung, Suspendierung bzw. Ausschluss eines SSFN Teilnehmers

Bei Verfehlungen eines SSFN Teilnehmers gegen das SSFN Reglement kann - nach Absprache des Product Owners mit den übrigen SSFN Voting Members - das nachfolgende Verfahren eröffnet werden.

#	Schritt	Beschreibung
1	Vorwurf des Verstosses gegen das SSFN Reglement. Product Owner: Prüfung des Vorwurfs	Der Product Owner erhält Kenntnis vom Vorwurf (z.B. durch einen SSFN Teilnehmer), dass ein anderer SSFN Teilnehmer die Vorgaben des SSFN Reglements nicht einhält und daraus ein Risiko- oder Schadenspotential entsteht. Der Product Owner überprüft den Vorwurf einer möglichen Verfehlung gegen das SSFN Reglement.
2	Product Owner: Möglichkeit zur Stellungnahme; Eröffnung Mängelbehebungsverfahren Dienstleister: Erstellung Vorgehensplan mit definierten Massnahmen zur Behebung der mangelhaften Situation Product Owner Bestätigung Vorgehensplan und Massnahmen unter Frist-ansetzung.	Bei einem plausibel erscheinenden Vorwurf kontaktiert der Product Owner den betroffenen SSFN Teilnehmer und gibt ihm Gelegenheit, sich zur vorgeworfenen Verfehlung schriftlich zu äussern. Je nachdem eröffnet der Product Owner das Mängelbehebungsverfahren oder passt den Verfahrensprozess in Abstimmung mit den SSFN Voting Members an (z.B. Verzicht auf Verfahrenseröffnung oder Verzicht auf Mängelbehebungsverfahren oder Entscheid zur Suspendierung oder dem Verfahrensausstand eines SSFN Voting Members wegen Befangenheit etc.). Sofern eine Verfehlung durch den SSFN Teilnehmer angenommen werden muss und/oder durch den Product Owner als begründet erachtet wird, erhält der betroffene SSFN Teilnehmer die Möglichkeit, einen Vorgehensplan mit definierten und terminierten Massnahmen zwecks Behebung des mangelhaften Zustands zu erstellen. Der Product Owner hat die Möglichkeit, diesen Plan in Absprache anzupassen. Der Vorgehensplan wird anschliessend vom Product Owner gegenüber dem Teilnehmer mit Fristansetzung zur vollständigen Umsetzung bestätigt. Ist ein SSFN Teilnehmer zugleich einer systemisch bedeutsamen Finanzmarktinfrastruktur gemäss Finanz-marktinfrastrukturgesetz («FinfraG») angeschlossen, so informiert der Product Owner die Betreiberin dieser FMI über den Stand des laufenden Verfahrens gegenüber eines SSFN Teilnehmers. Ist ein SSFN Teilnehmer zugleich am SIC-System - als systemisch bedeutsame Infrastruktur - angeschlossen, so informiert der Product Owner die SNB über den Stand des laufenden Verfahrens gegenüber eines SSFN Teilnehmers.

3	Product Owner: Prüfung umgesetzter Massnahmen und allfällige Einstellung des Mängelbehebungsverfahren bzw. Gewährung Fristverlängerung	Der Product Owner prüft und dokumentiert, spätestens nach Ablauf der angesetzten Frist, die Umsetzung der definierten Massnahmen. Er kann auch einen Dritten mit der Prüfung beauftragen. Sind die Massnahmen aus Sicht des Product Owners vollständig umgesetzt, und ist der mangelhafte Zustand behoben, wird das angesetzte Mängelbehebungsverfahren eingestellt. Sind die Massnahmen aus Sicht des Product Owners nicht bzw. nur unvollständig umgesetzt oder ist der mangelhafte Zustand weiterhin vorhanden, kann vom Product Owner eine Fristverlängerung mit allfällig neu definierten Massnahmen gewährt werden.
4	Product Owner: Einstellung des Mängelbehebungsverfahrens oder Empfehlung an SSFN Voting Members für temporären oder endgültigen Ausschluss vom SSFN **Vorbehalt**: Einholung separater Entscheid, wenn systemisch bedeutsame Infrastruktur betroffen (gemäss FinfraG)	Sind nach angesetzter Nachfrist aus Sicht des Product Owners die definierten Massnahmen – jene aus dem Vorgehensplan oder allenfalls mit Nachfristansetzung neu definierte – umgesetzt und der mangelhafte Zustand behoben, wird das Mängelbehebungsverfahren eingestellt. Sind die definierten Massnahmen nicht bzw. nur unvollständig umgesetzt oder der mangelhafte Zustand weiterhin vorhanden und erscheint – eine weitere Nachfristansetzung aus Sicht des Product Owners als nicht zielführend und/oder – ein weiterer Verbleib des SSFN Teilnehmers im SSFN aus Sicht des Netzwerkverbundes SSFN unzumutbar, erstellt der Product Owner zuhanden der SSFN Voting Members eine Empfehlung zum weiteren Vorgehen wie folgt: -> temporäre oder endgültige Aberkennung der Zulassung des betroffenen SSFN Teilnehmers zum SSFN mittels Suspendierung der Erneuerung des SSFN-Zertifikats (Kapitel 5.1.2). **Vorbehalt:** Ist ein SSFN Teilnehmer zugleich einer systemisch bedeutsamen Finanzmarktinfrastruktur gemäss Finanzmarktinfrastrukturgesetz («FinfraG») angeschlossen, so entscheidet ausschliesslich die Betreiberin der systemisch bedeutsamen Infrastruktur über die weitere Teilnahme eines solchen Teilnehmers. Der Product Owner hat diesen Entscheid einzuholen und das Verfahren demgemäss weiterzuführen bzw. zu beenden. Ist ein SSFN Teilnehmer zugleich am SIC-System - als systemisch bedeutsame Infrastruktur - angeschlossen, entscheidet ausschliesslich die SNB über die weitere Teilnahme eines solchen Teilnehmers. Der Entscheid der SNB betreffend Teilnahme am SIC-System hat Vorrang ggü. dem Entscheid des Finanzmarktinfrastruktur-Betreibers.

5	Finaler Entscheid	Die SSFN Voting Members entscheiden in der Regel einstimmig (Kapitel 3.4). Das Ergebnis des Entscheids der SSFN Voting Members wird dem SSFN Teilnehmer schriftlich kommuniziert. Der Entscheid gilt als final und der SSFN Teilnehmer hat gegen diesen Entscheid keine Anfechtungsmöglichkeit innerhalb der SSFN Governance. Der gefällte Entscheid im Rahmen des «Vorbehalt» gemäss Punkt 4 gilt als final innerhalb der SSFN Governance.
6	SSFN Certificate Issuers: Suspendierung des SSFN-Zertifikats	Basierend auf dem Entscheid der SSFN Voting Members bzw. basierend auf einem - Entscheid im Rahmen des «Vorbehalt» gemäss Punkt 4 suspendiert der SSFN Certificate Issuers temporär oder endgültig die Erneuerung des SSFN-Zertifikats des fehlbaren SSFN Teilnehmers und informiert allfällig betroffene SSFN Dienstleister.
7	Folgen der Suspendierung	Der von der Suspendierung betroffene SSFN Teilnehmer hat keinerlei rechtliche oder finanzielle Ansprüche gegenüber der Entscheid fällenden Instanz noch gegenüber sonst einer Partei innerhalb des SSFN für allfällige Schäden als Folge der Suspendierung des SSFN Zertifikats.

Tabelle 6: Prozess für Mängelbehebung, Suspendierung bzw. Ausschluss eines SSFN Teilnehmers

9 Änderungsmanagement des SSFN Reglements

Wesentliche Änderungen am SSFN Reglement, das heisst solche, die Auswirkungen auf die SSFN Teilnehmer haben, erfolgen wie folgt:

1. Einreichen von Änderungsvorschlägen durch die SSFN Voting Members oder durch die SSFN Teilnehmer beim Product Owner.
2. Zusammenstellung und Erstbeurteilung der Vorschläge (z.B. in Bezug auf Sinnhaftigkeit, Nutzen, Kosten, Auswirkungen) durch den Product Owner.
3. Konsultation der vorgeschlagenen Anpassungen mit dem SSFN Risiko-Management
4. Eröffnung der Konsultation der vorgeschlagenen wesentlichen Änderungen bei allen SSFN Teilnehmern durch den Product Owner (Review).
5. Beurteilung der eingegangenen Stellungnahmen durch die SSFN Voting Members (Koordination / Vorbereitung durch Product Owner) und gemeinsamer Entscheid der SSFN Voting Members, welche der vorgeschlagenen Änderungen final umgesetzt werden sollen.
6. In der Regel, mindestens jedoch drei Monate vor Inkraftsetzung, sind die SSFN Teilnehmer über die neue Version des SSFN Reglements durch den Product Owner in geeigneter Weise zu informieren.
7. Der Zeitpunkt der Inkraftsetzung des angepassten SSFN Reglements liegt im Ermessen der SSFN Voting Members, in der Regel erfolgt dies auf Jahresmitte. Bei dringlichen Anpassungen für das SSFN – gemäss Beurteilung der SSFN Voting Members – ist eine Inkraftsetzung nach angemessener Frist ab Information der SSFN Teilnehmer möglich.

Formale Anpassungen am SSFN Reglement können durch die SSFN Voting Members jederzeit über den Product Owner vorgenommen werden und bedürfen keiner Konsultation bei den SSFN Teilnehmern. Die SSFN Teilnehmer sind indessen vor deren Inkraftsetzung angemessen zu informieren.

10 Verträge

Nachfolgende Übersicht zeigt die wesentlichen Vertragsverhältnisse im Zusammenhang mit der Teilnahme am SSFN auf:

#	Partei 1	Partei 2	Vertragsinhalt
1	Telekommunikations-anbieter (SSFN Core Members, SSFN Carrier)	SSFN Teilnehmer (Ausnahme: SSFN Core Members)	SCION-Anschluss
2	SSFN Anbieter SCION-Lösung oder SSFN Core Members bzw. SSFN	SSFN Teilnehmer (Ausnahme: SSFN Core Members)	SCION-Lösung (Software und/oder Hardware) → für eigene Zwecke oder zum Weitervertrieb an eigene Kunden
3	SSFN Certificate Issuer (SIX)	SSFN Teilnehmer	«Vereinbarung betreffend SSFN-Zertifikat» SSFN-Zertifikat
4	Product Owner	SSFN Dienstleister	«Vereinbarung SSFN Dienstleister» [1] Anerkennung und Befolgung des SSFN Reglements, insbesondere die Erfüllung der Zulassungskriterien gemäss Vereinbarung
5	SIX	Switch	Switch als secondary certificate issuer
6	SNB	Anapaya	Massnahmen zur Sicherung des Betriebs des SSFN, inkl. Governance
7	SIX	Anapaya	Leistungserbringung für SSFN sowie Verhaltensregeln

Tabelle 7: Übersicht Verträge im SSFN

Anhang A: Zulassungskriterien für SSFN Dienstleister

Dieser Anhang A listet die Zulassungskriterien auf, welche SSFN Dienstleister gemäss Kapitel 4.1.2 des SSFN Reglements nachweislich zu erfüllen haben. Je nach Rolle sind unterschiedliche Kriterien zu erfüllen. Ein SSFN Dienstleister kann mehrere Rollen einnehmen, die zu erfüllenden Kriterien kumulieren sich hierbei. Er kann zur Erbringung seiner Services Subunternehmer einsetzen. Dabei bleibt er immer verantwortlich für die Einhaltung gemäss seiner Rolle geltenden Zulassungskriterien und muss dies gegenüber dem/der Subunternehmer jederzeit durchsetzen

#	Relevant für:					Zulassungskriterien	Empfehlungen bzgl. möglicher Nachweise
	SSFN Core Member	SSFN Carrier	SSFN Certificate Issuer	SSFN Endpunkt-anbieter	SSFN Anbieter für SCION-Lösungen		
1	x	x				Partei ist im BAKOM-Register als Fernmeldedienstanbieter mit einem Eintrag in der Kategorie 5.1 oder 5.2 aufgeführt bzw. in einem entsprechendem Register der nationalen Zulassungsbehörde im IT- und Fernmeldewesen (falls im Ausland domiziliert) ODER die Partei kann eine dauerhafte Tätigkeit im Rahmen von IT-Netzwerk-/Telekommunikationsdienstleistung (analog den BAKOM Kategorien 5.1 oder 5.2) für Dritte vorweisen (z.B. mittels «Firmenzweck» in aktuellem Handelsregisterauszug).	SSFN Core Member: Printscreen BAKOM-Register-Auszug mit Zeitstempel SSFN Carrier: Printscreen BAKOM-Register-Auszug oder adäquate Bestätigung (wenn im Ausland domiziliert), mit Zeitstempel
2	x	x	x	x	x	Rechnungsprüfung der Partei erfolgt durch einen RAB-zugelassenen Wirtschaftsprüfer (https://www.rab-asr.ch/#/publicregister), oder adäquat, falls im Ausland domiziliert.	- Kopie letztjähriger Bericht der Revisionsstelle (z.B. aus Geschäftsbericht) - Printscreen RAB-Register-Auszug mit Zeitstempel - oder adäquat, falls im Ausland domiziliert
3	x	x	x	x		Zugriff auf das eigene AS-Zertifikat und zugehöriger Schlüssel wird adäquat geschützt (at rest, at processing)	- Prozessdokumentation mit Rollen, ggf. RACI-Matrix, ggf. Segregation of Duty nach Industry best practices (e.g. ITIL), Zugriff basierend auf dem least privilege Prinzip und Zugriffsrechte werden in regelmässigen Abständen überprüft - Audit-Trail / Log auf Zugriffe
4			x			Zugriff auf und Verwahrung des CP Root Key und CP CA Key wird mit einem HSM und adäquaten Prozessen geschützt (at rest, at processing)	- Prozessdokumentation mit Rollen, ggf. RACI-Matrix, ggf. Segregation of Duty nach Industry best practices (e.g. ITIL), Zugriff basierend auf dem least privilege Prinzip und Zugriffsrechte werden in regelmässigen Abständen überprüft - Audit-Trail / Log auf Zugriffe
5	x	x	x	x	x	Erteilung der Zugriffsrechte auf Zertifikate und Schlüssel sind geregelt	- Prozessdokumentation mit Rollen, ggf. RACI-Matrix, ggf. Segregation of Duty nach Industry best practices (e.g. ITIL), Zugriff basierend auf dem least privilege Prinzip - Audit-Trail / Log auf Zugriffe
6	x	x	x	x	x	Bei Datenhaltung der Partei oder Zugriff seitens autorisierter Personen der Partei von ausserhalb des Landes ihres Standortes (z. B. der Schweiz), sind deren Kunden klar und verständlich dazu informiert und die entsprechende Zustimmung ist nachweislich vorhanden	- Einhaltung der Datenschutzbestimmungen als Vertragsbestandteil (z.B. AGB)

#	Relevant für: SSFN Core Member	SSFN Carrier	SSFN Certificate Issuer	SSFN Endpunkt-anbieter	SSFN Anbieter für SCION-Lösungen	Zulassungskriterien	Empfehlungen bzgl. möglicher Nachweise
7	x	x	x	x		Die Liste der Standorte der SSFN-Gateway (Strasse, Hausnummer, PLZ, Ort, Land) ist vollständig und korrekt	- Liste mit Standorten (Adresse) inkl. Bezeichnung des Datacenters (z.B. Auszug CMDB inkl. Zeitstempel)
8	x	x				Die SSFN-ISD wird ausschliesslich für SSFN-Verkehr (Data und Control Plane) genutzt, der SSFN-Verkehr (Data und Control Plane) fliesst ausschliesslich innerhalb der SSFN-ISD. Es erfolgt eine transparente Offenlegung von Geofencing und ausländischen Hops (sofern anwendbar) gegenüber den eigenen Kunden.	- Netzwerkplan mit allen SSFN-Elementen, bei welchen ein Übergang zu einem anderen Netzwerk möglich ist (inkl. Zeitstempel) - Pentest - (Screenshot Offenlegung Geofencing/ausländische Hops inkl. Zeitstempel)
9	x	x	x	x	x	Keine nicht-autorisierte (durch SSFN Voting Members) Interkonnektion mit Fremdnetzen (inkl. anderer SCION-Netzwerken und dem globalen Internet) (zu/weg von SSFN) existiert oder wird gebaut.	- Pentest - Prozessdokumentation mit Rollen, ggf. RACI-Matrix, ggf. Segregation of Duty nach Industry best practices (e.g. ITIL)
10			x			Ein Audit-Log über Zugriffe auf Zertifikate wird geführt.	- Prozessdokumentation mit Rollen, ggf. RACI-Matrix, ggf. Segregation of Duty nach Industry best practices (e.g. ITIL), Zugriff basierend auf dem least privilege Prinzip - Audit-Trail / Log auf Zugriffe
11	x	x	x	x		Ein "Security Operations Center" wird betrieben, inkl. zugehöriger Prozesse zur Bearbeitung von sicherheitsrelevanten Vorfällen.	- Prozessdokumentation mit Rollen, ggf. RACI-Matrix, ggf. Segregation of Duty nach Industry best practices (e.g. ITIL)
12	x	x	x			Sicherheitsrelevante Netzwerkdienste (insbesondere Netzwerkzeit) werden geschützt, inkl. zugehöriger Detektion und Behebung von Abweichungen.	- Prozessdokumentation mit Rollen, ggf. RACI-Matrix, ggf. Segregation of Duty nach Industry best practices (e.g. ITIL) - Pentest
13	x					SCION Core Services (insbesondere SCION Control Services) werden redundant angeboten.	- Liste mit Hostnamen und Standorten der Server mit Control Services (z.B. Auszug CMDB inkl. Zeitstempel) - Netzwerkzeichnung
14			x			Issuing-Services werden redundant angeboten (gilt nicht für Initial Zertifikat)	- Liste mit Hostnamen und Standorten der Server mit Issuing Services (z.B. Auszug CMDB inkl. Zeitstempel) - Netzwerkzeichnung
15	x	x	x	x		Geeignetes Business Continuity Planning bzw. Management (BCP bzw. BCM) Massnahmen wurden getroffen, um bei Ausfall eines RZs operativ verfügbar zu bleiben.	- Prozessdokumentation mit Rollen, ggf. RACI-Matrix, ggf. Segregation of Duty nach Industry best practices (e.g. ITIL) - BCP-Pläne, Test-Drehbücher und Testberichte

#	Relevant für: SSFN Core Member	SSFN Carrier	SSFN Certificate Issuer	SSFN Endpunkt-anbieter	SSFN Anbieter für SCION-Lösungen	Zulassungskriterien	Empfehlungen bzgl. möglicher Nachweise
16	x	x	x			"Monitoring and Capacity Management Processes" existieren, um gegenüber Kunden und allenfalls anderen Core-Service-Anbietern vereinbarte Bandbreiten, Verfügbarkeiten und Latenzzeiten einzuhalten	- Prozessdokumentation mit Rollen, ggf. RACI-Matrix, ggf. Segregation of Duty nach Industry best practices (e.g. ITIL) - Screenshot Monitoring / Capacity Management SSFN, inkl. Zeitstempel
17	x	x	x			Ein Monitoring existiert, um die garantierten (gemäss Punkt 16) Verfügbarkeiten einzuhalten.	- Prozessdokumentation mit Rollen, ggf. RACI-Matrix, ggf. Segregation of Duty nach Industry best practices (e.g. ITIL) - Screenshot Monitoring SSFN, inkl. Zeitstempel - Service-Level-Report
18	x	x	x	x	x	Alle Dienste und Appliances decken die aktuell gültigen technischen Kern-Spezifikationen (SCION-Protokoll) vollständig ab.	- Bestätigung Anapaya (Kern-Spezifikationen) bzw. der SCION Foundation (künftige Zertifizierungsstelle SCION)
19	x					Redundante Peerings mit anderen SSFN Core Members existieren, werden überwacht und bei Ausfall in angemessener Zeit wiederhergestellt.	- Prozessdokumentation mit Rollen, ggf. RACI-Matrix, ggf. Segregation of Duty nach Industry best practices (e.g. ITIL) - Netzwerkzeichnung (oder Peering-Inventory)
20		x	x			Redundante SCION-Anschlüsse (an zwei SSFN Carrier mit Core Services) existieren, werden überwacht und bei Ausfall in angemessener Zeit wiederhergestellt.	- Prozessdokumentation mit Rollen, ggf. RACI-Matrix, ggf. Segregation of Duty nach Industry best practices (e.g. ITIL) - Netzwerkzeichnung
21	x	x	x			Ein "Incident Management Process" ist vorhanden, Stör- und Sicherheitsvorfälle werden verwaltet und Sicherheitsvorfälle kommuniziert.	- Prozessdokumentation mit Rollen, ggf. RACI-Matrix, ggf. Segregation of Duty nach Industry best practices (e.g. ITIL)
22	x	x	x	x	x	Ein "Change Management Process" ist vorhanden und umgesetzt, inkl. 4-Augen-Prinzip für konfigurative Änderungen in der SSFN-ISD.	- Prozessdokumentation mit Rollen, ggf. RACI-Matrix, ggf. Segregation of Duty nach Industry best practices (e.g. ITIL)
23	x	x	x	x	x	SCION/SSFN Netzwerk-Devices und weitere für SCION angebotene Devices/Services sind physisch angemessen geschützt.	- Schutzkonzept - Prozessdokumentation mit Rollen, ggf. RACI-Matrix, ggf. Segregation of Duty nach Industry best practices (e.g. ITIL) - Audit-Berichte
24	x	x	x	x	x	Integrität und Autorisierung der SW-Deployment-Prozesse sind gewährleistet und stellen sichere Prozesse, Testing und Verfahren für die Kunden dar..	- Prozessdokumentation mit Rollen, ggf. RACI-Matrix, ggf. Segregation of Duty nach Industry best practices (e.g. ITIL). Ebenso muss ein Testverfahren bei SW-Deployments in Place sein.

#	Relevant für:					Zulassungskriterien	Empfehlungen bzgl. möglicher Nachweise
	SSFN Core Member	**SSFN Carrier**	**SSFN Certificate Issuer**	**SSFN Endpunkt-anbieter**	**SSFN Anbieter für SCION-Lösungen**		
25	x	x	x	x	x	Die Bestimmungen der «Best practices im SCION-Verbund» (Referenzdokumente [2] und [3]) werden eingehalten oder sind mit gleichwertigen Massnahmen umgesetzt	- Prozessdokumentation mit Rollen, ggf. RACI-Matrix, ggf. Segregation of Duty nach Industry best practices (e.g. ITIL)
26	x	x				SSFN Voting Members, resp. stellvertretend der Product Owner, werden über den Verkauf eines SCION-Anschlusses für SSFN informiert	- Auszug Customer Database SSFN inkl. Zeitstempel
27				x		Ein Vertrag mit mindestens einem SSFN Nutzer bzw. bei Managed Services für den SSFN-Anschluss mit mindestens einem SSFN Teilnehmers besteht (siehe Kapitel 5.1.4)	- gültiger Vertrag (siehe Kapitel 5.1.4)

Tabelle 8: Anforderungen an SSFN Dienstleister

Anhang B: Änderungshistorie

Version 1.3
Neben der Korrektur allfälliger Rechtschreibefehler und Formulieren wurden folgende wesentliche Änderungen vorgenommen

Kapitel	Was
Allgemeine Hinweise	Anpassung der Lizenz von streng restriktiv auf CC BY 4.0
1.4	Link zur ETH entfernt, da Informationen direkt bei der SCiON Association zu finden sind
2.1	Rollenbeschreibung in einer ISD wurde in Kapitel 2.4 verschoben und dort mit der Nennung der spezifischen Parteien im SSFN zusammengeführt. Dies erhöht Lesbarkeit in Kapitel 2.1 (Da Fokus auf SCION) und stärkt das Verständnis von den Ausprägungen in SSFN in Kapitel 2.4 Abbildung zu Rollen in ISD wurde aktualisiert
3.5	Anpassung der Gremien auf aktuelle Repräsentation
3.6	«SSFN Dienstleistungen» grundsätzlich als Dienstleistungen der SIX beschrieben, für «erreichbare Services» Einschränkung auf SIX entfernt
4.1.1	Aufzählung «b)»: keine Einschränkung mehr auf «zahlungspflichtige» SSFN Dienstleistungen
4.1.2	Detaillierung für Subunternehmer aufgenommen
5.1/5.2	Verpflichtung der Dienstleister und Nutzer aufgenommen, entsprechende Sorgfalt bei der Einspielung von Software und Überwachung der Dienstleister walten zu lassen
5.1.2	Dienste der Core Members verweist neu auch auf Carrier-Dienste
5.1.4	Für den “Fall a)” das Beispiel “Service Provider für SECOM-Kunden" aufgenommen, um Kopplung zu SIC zu lockern.
5.2	Ergänzung um Empfehlung für eine Risikobeurteilung für Drittbeauftragte
Anhang A	Erweiterung zur Berücksichtigung von Delegation an Subunternehmer Detaillierung Kriterium 9 Detaillierung Kriterium 24, Erweiterung Geltungsbereich auf SSFN CA und Endpunktanbieter
Anhang C	Überarbeitung Formulierung von «cross-connect» zu «Interkonnektion…»

Version 1.2
Neben der Korrektur allfälliger Rechtschreibefehler und Formulieren wurden folgende wesentliche Änderungen vorgenommen

Kapitel	Was
2.5	Präzisierung: Einhaltung „Best Practice-Dokument“ Diese sind einzuhalten oder **müssen durch gleichwertige Massnahmen umgesetzt werden**.

2.5	Präzisierung/Neu: **Ausschliessliche Nutzung öffentlich registrierter IP Adressen**
2.5	Neu: **Segregierung des SSFN vom Public Internet**
2.6	Neu: Bilaterale Abstimmungen bei widersprechenden Pfadpräferenzen zweier Teilnehmer
3.2	Neu: Koordination des erforderlichen externen Assessments durch den Product Owner SIX
3.2	Neu: Koordination des zentralen Risikomanagements der SSFN Voting Member durch den Product Owner SIX
3.3	Neu: Voting Member entscheiden gemeinsam über die Zulassung etc. von SSNF Dienstleistern und deren Rolle
3.6	Präzisierung: Hinweis, dass SIX eine aktuelle Liste der zugelassene SSFN Dienstleistungen führt (und publiziert)
5	Neu: Alle SSFN Teilnehmer sind für ihren Anschluss etc. verantwortlich
7	Neu: Resultate einer Vorprüfung eines SSFN Dienstleisters haben Gültigkeit von maximal 12 Monaten
7	Neu: künftige SSFN Dienstleister bereiten alle erforderlichen Unterlagen für das Assessment im Vorfeld vor
8	Präzisierung: Wenn aus Nichteinhaltung des Reglements z.B. Risiko- oder Schadenspotenzial entstanden ist., Schriftform; Beauftragung Dritter; finaler Entscheid liegt bei SSNB
9	Neu: Konsultation des Risikomanagements der SSFN Voting Member
Anhang A	Präzisierung: # 25 Einhaltung „Best Practice-Dokument“ Diese sind einzuhalten oder **müssen durch gleichwertige Massnahmen umgesetzt werden**

Anhang C: Glossar

AS	Autonome Systeme
AS Nr.	Eindeutige Zahl, die ein AS kennzeichnen
AS-Zertifikat	Zugangszertifikat für jedes AS in einem spezifischen ISD
BCM, BCP und DR	Business Continuity Management, Business Continuity Plan, Disaster Recovery
CA	Certificate Authority
CI	Certificate Issuer
Interkonnektion mit Fremdnetzen (inkl. anderer SCION-Netzwerken)	Im SSFN-Zusammenhang ein Zusammenschluss von SSFN-fremden Netzwerken mit SSFN. Dies umfasst sowohl Internet als auch Intercompany-Netzwerke, nicht aber Intracompany-Verbindungen.
(D)DoS	(Distributed) Denial of Service Attack
HSM	Hardware Security Module
ISD	Isolation Domain
ISP	Internet Service Provider
ITIL	Information Technology Infrastructure Library
Managed Services	Verantwortung für bestimmte IT- oder Netzwerkfunktionen werden an einen externen Dienstleister (Managed Service Provider, MSP) übertragen (vollständig oder teilweise)
Pfad	Route eines Datenpakets vom Sender zum Empfänger
Peering	Eine Netzwerkverbindung eingehen
RACI	Responsible, Accountable, Consulted, Informed
SCION	SCALABILITY, CONTROL, AND ISOLATION ON NEXT-GENERATION NETWORKS
SIC	Swiss Interbank Clearing - Das SIC-System ist eine systemisch bedeutsame Infrastruktur gemäss Finanzmarktinfrastrukturgesetz («FinfraG») ist das RTGS-System für die Währung CHF. Es wird von der SIC AG (eine Tochtergesellschaft der SIX) im Auftrag der SNB betrieben.
SLA	Service Level Agreement (Dienstleistungsvereinbarung)
SNB	Schweizerische Nationalbank
SCION Gateway	Gateway und Router werden synonym verwendet
SSFN	Secure Swiss Finance Network
TRC	Trust Root Configuration
Voting Member	Entscheidungsgremium für SSFN; SNB, SIX, Switch