



SIX

External Connectivity Guide

For Secure Swiss Finance Network (SSFN)



Contents

1	Introduction	3
2	Customer Deployment Models	4
3	Verified Deployment Topologies	5
4	SSFN Onboarding	7
5	SIX Service Access	9
6	Support	12
7	Appendix	13

1 Introduction

SSFN is a network environment based on SCION technology. It consists of multiple carriers, service providers and customers forming a unified network with a distributed governance model. Even though SIX plays a major role in this environment, SSFN is not in place to provide SIX services only, but allows all participants to exchange data and offer services among each other as they please.

This Guideline describes the policy of how customers and partners can access SIX services via SSFN and provides some guidance for the design and implementation process.

1.1 Security

The SSFN and the SCION technology in general has multiple security attributes that let it stand out against traditional networks. As such, it offers transparent path information and path selection to the participants via cryptographically validated path segments. Further, it incorporates DDoS protection mechanisms by design and introduces a shared governance that is enforced by TRC including the right to exclude non-compliant participants from the network. Last but not least, the SSFN specifically is isolated from other traditional networks (e.g. Internet), as well as from other ISDs within the SCION world.

However, it is important to mention here that the network connections are **NOT encrypted** out of the box. Encryption can be added by using encrypted protocols for service access or via traditional VPN tunnels on top of the network infrastructure (on request).

2 Customer Deployment Models

Each customer is free to choose on how the access to SSFN in their local premises is realized. This also involves the decision on bandwidth needs. Due to the distributed governance model, SIX or any other participant is not able to take on any end to end bandwidth or services guarantees. However, SIX is monitoring its own bandwidth consumption to be always prepared to meet bandwidth requirements.

Two main deployment models are to be differentiated:

Managed Service

Multiple providers offer SCION as a managed service, where the carrier is responsible for configuration and maintenance of the SSFN Gateways. The redundancy patterns and configuration details need to be clarified with the respective provider based on their offerings.

Unmanaged Access

This model only includes a SCION enabled network uplink from the carrier(s) of choice. The sourcing and provisioning of the SSFN gateway(s) is up to the customer in this case. This includes the network design for the required redundancy needs as well as the registration at SIX for the initial SSFN certificate that is required for the access. However, the sourcing partner (typically Anapaya) will support the process.

2.1 Carriers

The ISD-Core services providers in SSFN are Swisscom, Sunrise and SWITCH, but there is a growing list of connected carriers that provide customer services as well. Please visit the [SSFN web page](#) and check the "SSFN Service Providers" section to find the up to date list of partners and carriers.

International connectivity within the SSFN is provided by providers on request. Please get in contact with the provider of choice to check the individual availability.

3 Verified Deployment Topologies

All existing topologies shown below assume that the deployment is based on a central SCION-IP Gateway (EDGE), connecting the traditional IP network with the SCION world. Native SCION deployments are not expected in this stage of the technology.

Further, please note that the described topologies provide examples and are not binding or exclusive at all.

3.1 Dynamic Site-Redundant Setup

This setup relies on a pre-existing, dynamically routed access platform that interconnects the two datacenter locations. Each EDGE must connect one or multiple carrier uplinks.

The EDGE is connected to the access platform with dynamic routing – BGP in this case. The gateways share the same AS to avoid routing loops.

IP filtering is applied on the BGP peerings, allowing only SSFN-prefixes to be advertised from the access platform environment to the EDGES as well as in the reverse direction.

As a consequence, it is expected that only traffic with valid SSFN IP addresses communicates via the EDGES. In case a NAT translation is applied, this must happen on the access platform or on firewalls connecting the access platform.

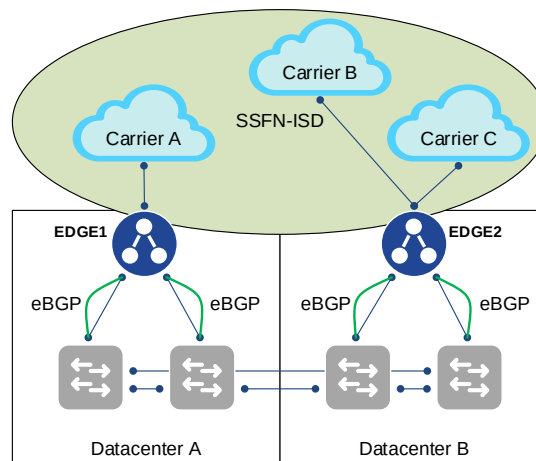


Figure 1: Dynamic Site-Redundant Setup

Dynamic SGRP IP advertisement is used from EDGE to other SSFN participants. As soon as a gateway is isolated (no connection to BGP anymore), the prefixes via this gateway will be withdrawn in SSFN. The same happens in reverse direction if no valid SCION path is available anymore.

The SCION path policy on the gateways must exclude paths from the remote EDGE to avoid inefficient routing.

For the IP overlay to work, each participant where communication is desired to and from, must be added separately and can be covered either by a specific or a generic SGRP filter policy.

3.2 Static Cluster Setup

This setup relies on local failover within a datacenter. It doesn't require any dynamic inter-connection between the datacenters. Each EDGE must connect one or multiple carrier uplinks.

The local EDGEs within a datacenter are clustered and require a shared layer 2 segment to advertise a virtual IP address from the primary cluster member (VRRP).

The downstream devices (routers or firewalls) use static routing to point to the virtual IP of the EDGE cluster. Likewise, static routes are added to the EDGEs to point to the downstream next hop(s).

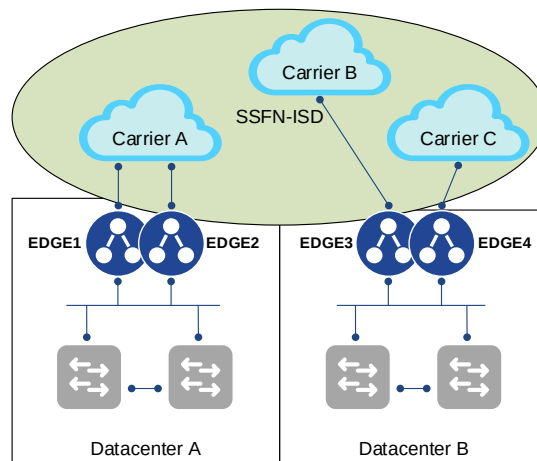


Figure 2: Static Cluster Setup

The public IP addresses in use are datacenter local. Each of the two EDGE-clusters statically advertises independent IP addresses to the SSFN. Accordingly, a datacenter failover will happen on an application level and always require an applicational reconnect.

Dynamic SGRP IP advertisement is used from EDGE to other SSFN participants. The prefixes of a cluster are never withdrawn in SSFN and only disappear in case both gateways are gone. In the reverse direction, the virtual IP is monitored to discover a complete failure of a gateway cluster and act accordingly.

For the IP overlay to work, each participant where communication is desired to and from, must be added separately and can be covered either by a specific or a generic SGRP filter policy.

4 SSFN Onboarding

There are specific aspects to SCION networks and SSFN in particular, which must be considered when building up a SCION access for your company. This is a short wrap-up on the most important ones.

4.1 Certificate handling

One of the major differentiations of SCION against traditional routing technologies is the built-in integrity check for path validation using certificates. Accordingly, a valid certificate from one of the SSFN issuing instances (SIX or SWITCH) is the pre-condition to be able to establish any connection within SSFN.

The initial certificate is manually issued by SIX and has an extended validity of 30 days. The certificate should be ordered shortly before the environment is ready to connect SSFN (e.g. gateways installed and able to create a CSR and carrier lines ready). Once the initial connection is completed, the certificates are automatically renewed and have a validity of three days going forward.

The process to order an initial certificate is described on the following public web page in detail including the contact to place the order: <https://www.six-group.com/ssfn>

4.2 AS Numbering

SCION AS numbers are 48 bits and typically formatted in a Hex notion as (0:0:0 to ffff:ffff:ffff), but decimal format is supported as well, especially for readable numbers up to 65535. The AS number must only be unique in conjunction with a SCION ISD. If multiple ISDs are connected, the same AS can be used to connect each of them. For more details on the SCION numbering scheme, please visit the [online documentation](#).

There is no dependency on the public BGP AS number used in the open Internet, but for readability and tracability reasons, it is strongly recommended for customers to use their publicly registered Internet AS numbers if available. SIX uses the AS number 9025 for SSFN connectivity accordingly.

For customers that don't possess a public Internet AS or don't want to use it in SSFN, there is an option to register a dedicated number for SSFN from the public SCION AS space (2:1:0/32).

If required, SIX as SSFN primary certificate issuer will assign an AS number for usage in SSFN. For more information, please refer to the [Guidelines to Apply for an SSFN Certificate](#).

4.3 SCION Gateway Routing Protocol

It is assumed that most customers will exclusively work with SCION-IP-Gateways for the time being. Doing so implements a SCION encapsulation on the gateway, but it also requires mapping of IP addresses to SCION ASes. On the Anapaya EDGE, this is implemented using SGRP (SCION Gateway Routing Protocol), which creates dedicated control plane tunnels between participants to exchange IP routing information.

This allows individual filters for announced and accepted IP routes per peer (whereas there can also be a default policy, which applies to all neighbors).

For the IP overlay to work, each participant where communication is desired to and from, must be added separately and can be covered either by a specific or a generic SGRP filter policy.

4.4 Traffic Policies

The SCION technologies offers a multitude of traffic control features, but not all of them are implemented yet. However, there's one setting that is particularly recommended, which is the limitation of accepted paths to the SSFN-ISD (+ 70-0) and the denial of all other paths (- 0-0).

5 SIX Service Access

As the SSFN is based on public IP addressing and allows customer IPs, there is no synchronized IP space within the network and no need for any NAT translations per SCION gateway (EDGE) to cater for redundancy scenarios. As such, there is a high session resilience in case of failover within the SSFN network, making failover more seamless for applications running on top of it.

However, NAT is still required in most cases to present SSFN specific public IPs on the network. Where the termination takes place (firewall, router, loadbalancer, other) may vary for each participant and service, but the following principle is generally valid:

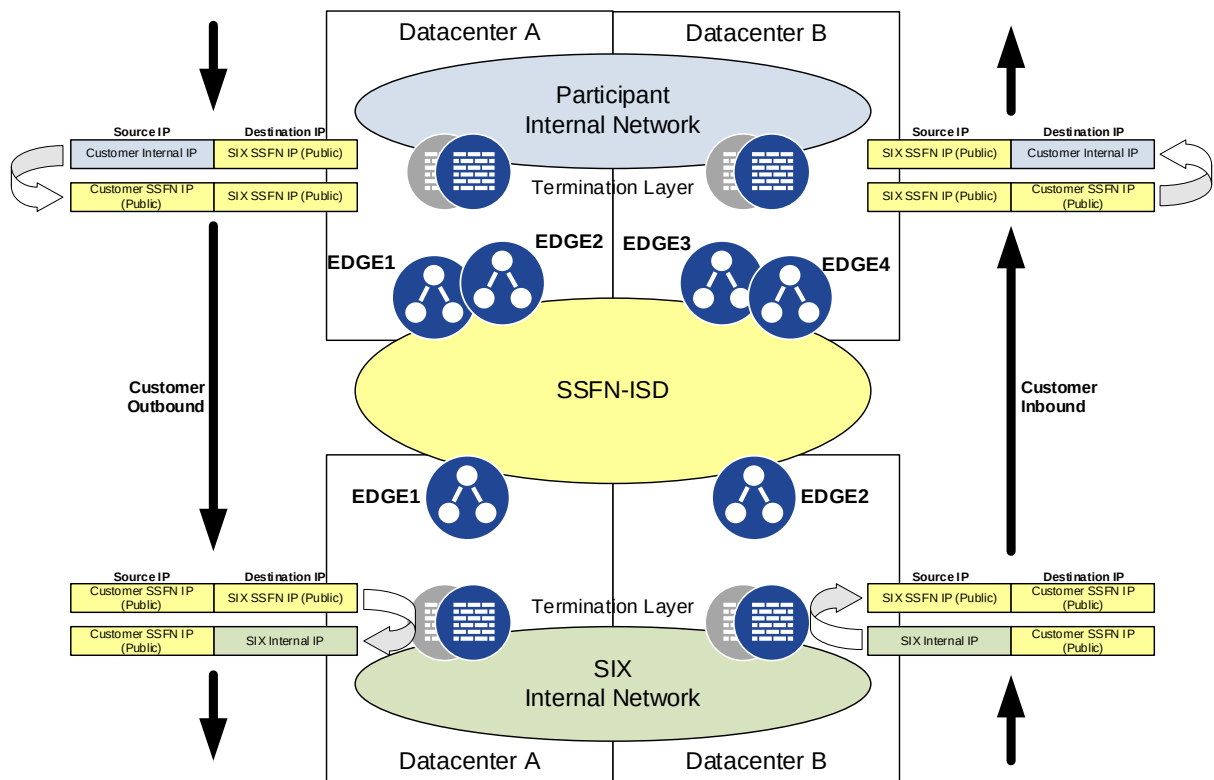


Figure 3: Service Access Principle

For more information on the specific service access you require (Availability on SSFN, URLs, Permissions and Accounts), please get in contact with your respective service representative at SIX.

5.1 IP Addressing

SIX enforces the policy to route only registered public IP addresses via SSFN. To avoid any future conflicts, it is strongly recommended by SIX, but in the responsibility of customers to use only IPs from a range which is not part of a routed summary in the Internet space or any other SCION ISD.

Likewise, SIX will also work exclusively with public IPs on the SSFN network. Moreover, these public IPs are exclusively used in the SSFN network to avoid any routing overlaps with other access technologies (Internet / P2P / MPLS).

The following IP summaries are advertised by SIX via SSFN:

- 153.46.40.0/21
- 153.46.168.0/21

5.2 Name resolution / Domain Name System (DNS)

To support name based services access and ensure usability, there is a dedicated SSFN DNS naming service. Since SSFN is a completely isolated network, reliance on Internet for name resolution is against isolation principles and therefore not foreseen.

To provide a consistent and separate namespace, all services in SSFN are provided within `ssfn.ch`¹, whereas different subdomain will be used to segregate different service providers (e.g. `six.ssfn.ch`). Service names will be provided by the respective service owner. To resolve SSFN service names, a resolution forwarder to the resolver provided by SIX must be established.

The forwarder IP address for `ssfn.ch` resolution at SIX is as follows:

- 153.46.41.132

Even though the services is presented as a single virtual IP address, there are redundant worker nodes in the background.

In addition to SIX, ZKB is acting as a secondary authoritative DNS provider to increase resiliency of the name resolution service in SSFN using the following IPs:

- 62.240.216.7
- 62.240.216.8

Please note that a SCION peering to ZKB is required by the customer to make use of the backup DNS service. SCION peerings have to be configured on both ends, please contact firewall@zkb.ch (+41 44 292 89 89) for further coordination with ZKB.

To set up a forwarder, the following directive must be set up in the client's DNS configuration (example for `bind9` name server):

```
zone "ssfn.ch" {
    type forward;
    forward only;
    forwarders { 153.46.41.132; 62.240.216.7; 62.240.216.8; };
};
```

Customers can host their own DNS (sub-) domain in `ssfn.ch`. To enable public TLS certificate issuing for `ssfn` hosted services, the empty (sub-) domains can be made available and delegated to the customer in the Internet as well for the customer to create the required `txt`-records. The implementation will be done by SIX using delegations for the (sub-) domains to the customers name servers in SSFN as well as in Internet (if required). If there are no dedicated DNS servers on customer side, SIX can take over the hosting for a limited amount of entries.

Independent of the preferred DNS hosting solution, please contact SIX network team for the initial setup of dedicated DNS (sub-) domains and include the name server IPs (Internet and SSFN) in case they are already defined.

5.3 Connectivity Check

Once the SSFN setup is completed, the connectivity can be verified by accessing the following destination via ICMP. Once successful, services may be migrated to the SSFN connections:

- 153.46.40.40 (`health.six.ssfn.ch`)

¹ `ssfn.com` and `ssfn.net` are in preparation

5.4 Service Onboarding

SIX hosts most of their services on SSFN (excluding Stock Exchange trading). Please refer to the service documentation for the SSFN IP addresses of each service. To facilitate things, SSFN Product Management has created a service inventory which can be requested by email and is also available in the download section of the SSFN landing page (www.six-group.com/ssfn).

For Services where the customer establishes the session **to SIX**, the following points need to be considered on customer side:

- The SSFN Public IPs of SIX (153.46.40.0/21 and 153.46.168.0/21) must be accessible from the source system
- The source system is either directly addressed by or its source is translated to the customers SSFN IP address space as advertised to SIX
- The destination address and port for the SIX service intended to use is opened in the respective firewall rule set
- In case the accessed service is based on name resolution, the DNS connection for ssfn.ch is established by pointing to the SIX and ZKB DNS servers as described in chapter 5.2.
- As soon as the general connectivity is verified as by chapter 5.3, customer can verify service accessibility either with a test connection or by telnet to <service-IP>:<service-port>.
- It is advisable to contact the service management of each SIX service before migrating its connection to SSFN, as certain services may require additional settings.

For Services where SIX is required to establish the session **to the customer**, the following points need to be considered on customer side:

- The SSFN Public IPs of SIX (153.46.40.0/21 and 153.46.168.0/21) must be accessible from the destination system
- The destination system/service is either directly addressed by or its destination is translated from the customers SSFN IP address space as advertised to SIX
- The destination address and port for the service intended to use is opened for the SIX sources in the respective firewall rule set
- The SSFN IP address of the entry point at the customer side must be defined, setup and communicated to SIX service operator
- Test and migration must be scheduled with the SIX service operator, starting with connectivity verification (e.g. telnet to <service-IP>:<service-port> or test connection)

6 Support

The chapters above provide a brief overview of the supported connectivity options and their properties.

If customers need support to choose the right option or to configure customer CPE devices for a selected option, the SIX network team will be happy to support the customer in all matters.

Once you have decided on an option, SIX network team will assist you with the definition of the implementation details.

For initial contact, administrative questions and certificate issuing, please reach out to the SSFN product management within SIX:

E-mail: pm-ssfn@six-group.com

Office hours: Monday – Friday, 08:00 – 17:00

The SIX network team can be reached by E-mail or phone during office hours:

Phone: +41 58 399 26 26

E-mail: 2626@six-group.com

Office hours: Monday – Friday, 08:00 – 17:00

For emergencies or carrier issues, the carrier info desk can be reached by E-mail or phone 7x24:

Phone: +41 58 399 40 20

E-mail: carrierinfo@six-group.com

7 Appendix

7.1 Abbreviations

Following abbreviations are used within the document.

Abbreviation	Description
SCION	Scalability, Control, and Isolation on Next-Generation Network <i>Underlying SSFN technology developed by ETH</i>
SSFN	Secure Swiss Financial Network <i>SCION implementation for a shared network among the financial sector</i>
ISD	Isolation Domain <i>independent Governance entity in SCION. SSFN is an ISD</i>
TRC	Trust Root Configuration <i>The trust anchor in an ISD</i>
EDGE	SCION IP Gateway is called EDGE in Anapaya Terminology <i>The component to encapsulate/decapsulate SCION traffic in IP</i>
SGRP	SCION Gateway Routing Protocol <i>Protocol to advertise IPs in SCION tunnels across participant</i>
NAT	Network Address Translation
VRRP	Virtual Router Redundancy Protocol <i>Protocol to manage a shared virtual IP among two router in a subnet</i>
CSR	Certificate Signing Request <i>Based on a CSR, a certificate authority generates a certificate</i>

7.2 List of Figures

Figure 1: Dynamic Site-Redundant Setup.....	5
Figure 2: Static Cluster Setup	6
Figure 3: Service Access Principle	9

7.3 Revision Log

Date	Changed	Revision	Who
06. Apr 2022	Initial version	0.9	tk574
28. Apr 2022	Final Markup	1.0	tk574
14. Oct 2022	Name Resolution added	1.1	tk57f
09. May 2023	Minor corrections	1.2	tk57f
29. Feb 2024	Service Onboarding added	1.3	tk574
21. Mar 2024	SSFN Onboarding extended	1.4	tk574
17. Feb 2025	Clarifications added about name resolution	1.5	tk574