Next-Generation Network Security with SCION

Building a secure communication network for the financial community

Fritz Steinmann, SIX
08. September 2021

AGENDA

What is SCION?

Security Aspects

Use case – SSFN

Cyber Security – Today's Communication Networks are Expensive, Inflexible or Unreliable

Leased provider connections (e.g. MPLS-Networks, "Finance IPNet")
for large companies, banks and financial market infrastructures (e.g. Swiss Interbank Clearing):

- secure, but expensive and lack flexibility
- limited to the telecom provider in question
- do not allow for open, community-based communication between FMI participants

Using the Internet
for data transmission between participants in the Swiss financial center:

- flexible, but no protection against cyber-risks

Cyber Security – Three Risks Prevail When Using the Internet for Communication

DoS and DDoS Attacks

- Expensive and difficult to protect against DoS und DDoS attacks
- Despite large investments, attacks continue to be successful

Communication Path Hijacking

- Sender und receiver have limited control over routing
- Attacks can hijack and relay paths

Kill Switch ruptures Sovereignty

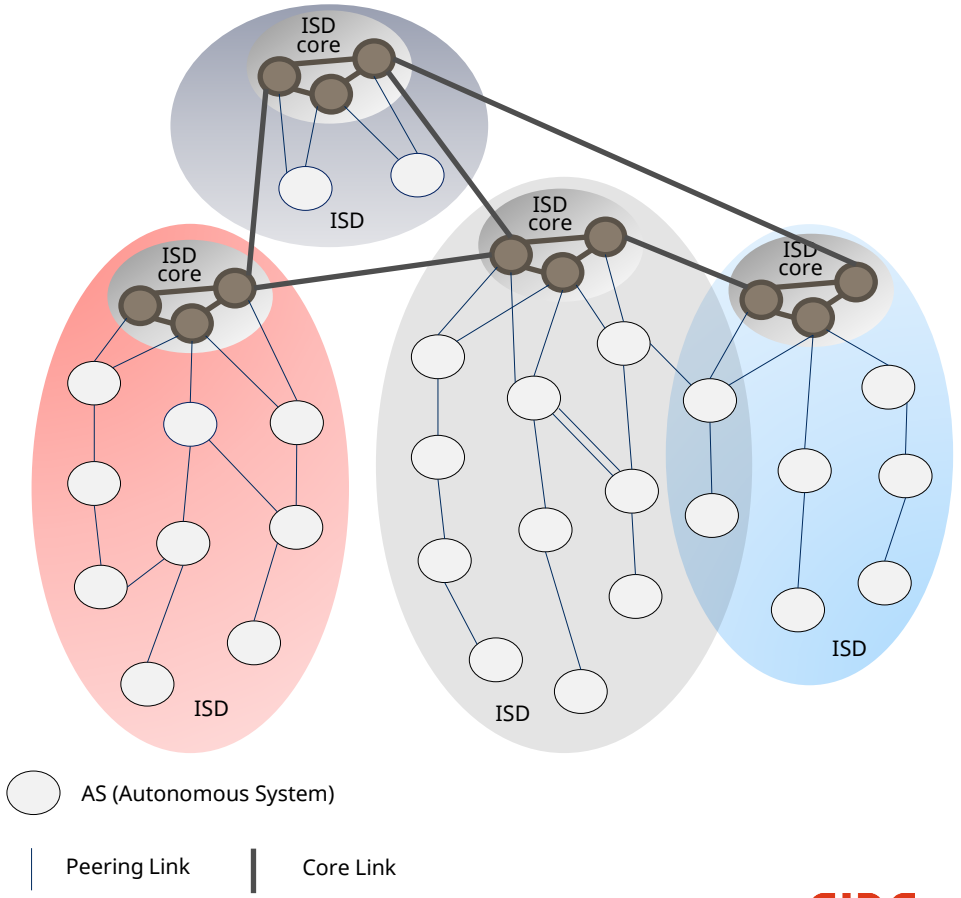
- Current Internet suffers from several "Kill Switches", which can halt communication within a geographical area
- Several attack avenues exist
- Revocation of certificates is also possible

SCION

Scalability, Control and Isolation on Next-Generation Networks

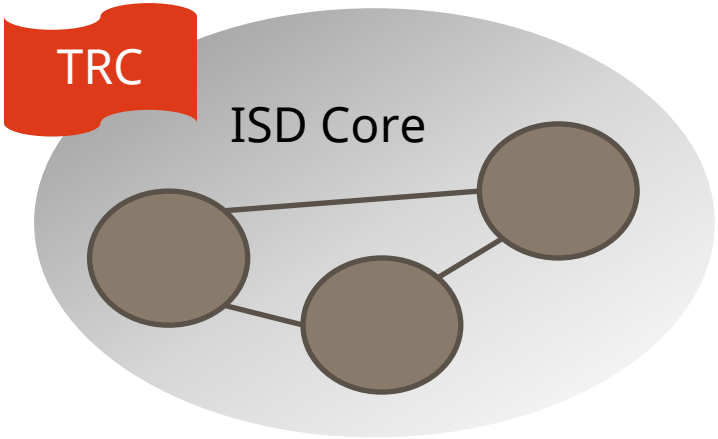
Control and Isolation

- In SCION, the Internet is segmented into smaller areas, so-called “Isolation domains” (ISD’s)
- Think of it as a logical grouping of nodes with similar interests or boundaries



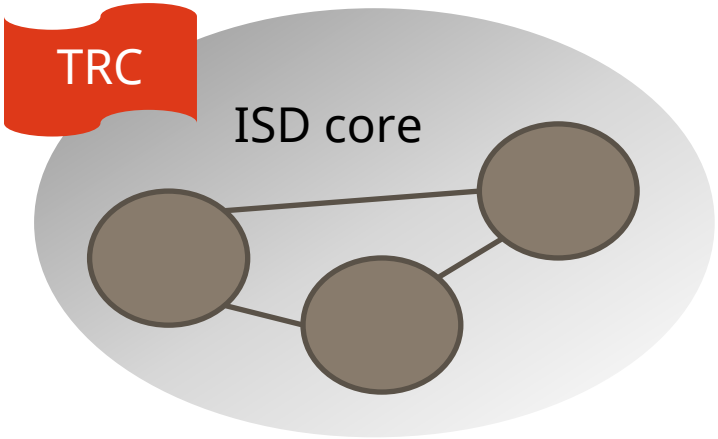
Control and Isolation

- Some entities (typically ISP's) form the Core of each ISD
- They are governed by a digitally signed policy called "Trust Root Configuration" (TRC)
- They provide common services to the members of the ISD
- They also serve as interconnection to other ISD's



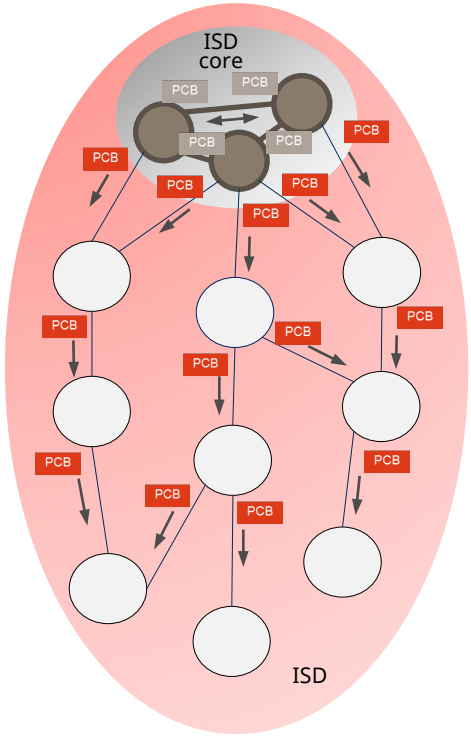
Control and Isolation

- ISD core services are comprised of:
  - Certificate management (all AS'es need certificates)
  - HA services for ISD path servers, name resolution, time servers etc.
  - Inter-ISD trust
  - Inter-ISD connectivity
  - Inter-ISD path services



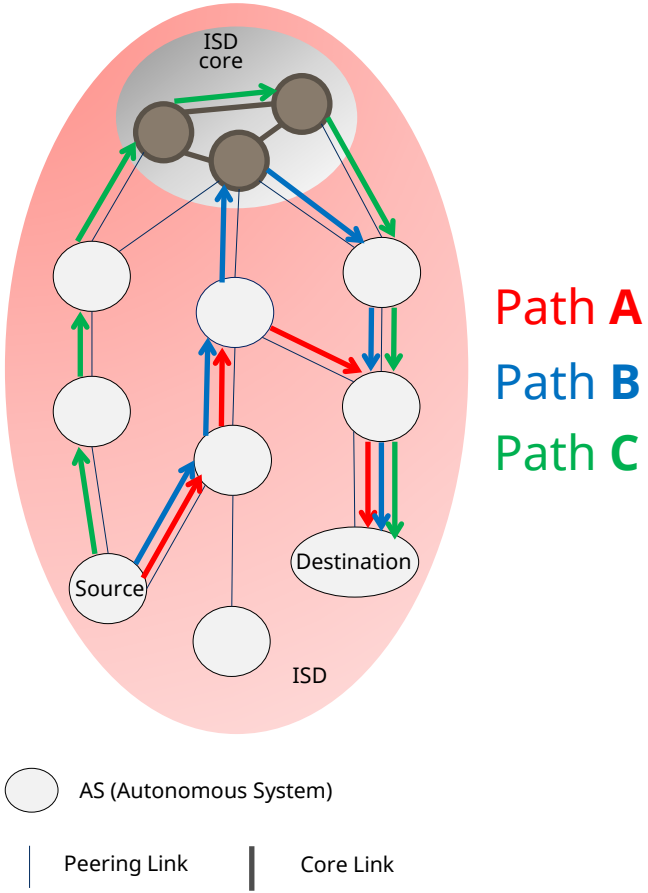
Path Discovery

- ISD core sends Path-segment Construction Beacons (PCBs)
- PCBs accumulate cryptographically protected AS-level path information as they traverse the network
- This information is chained together by sources to create a communication path
- This path is stored in path servers within the AS’es



SCION Communication

- All paths are visible to the source
- Attributes are mapped to the paths (latency, loss rate, throughput, availability)
- Source will decide on full path based on the attributes (e.g. lowest latency)
- Multi-path supported
- Failover path predefined (No learning necessary)

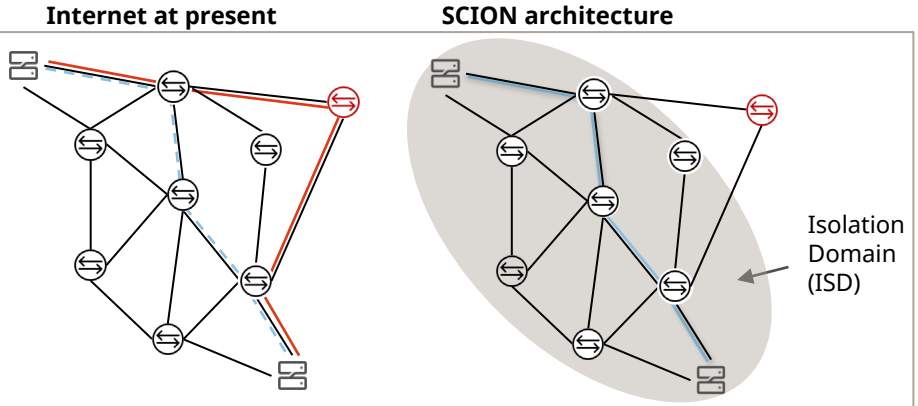


Security Aspects

SCION – a Network Architecture for Safe and Reliable Data Communication

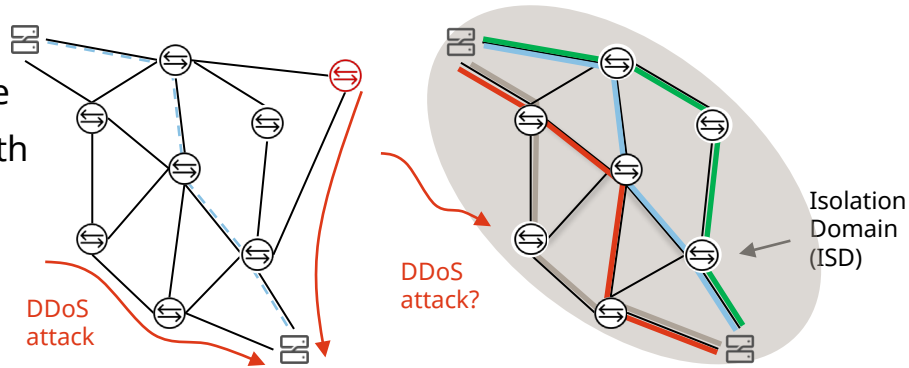
Avoiding undesired network paths

- Internet at present: Impossibility to avoid certain networks or geographic regions due to lack of route controls
- SCION architecture: Path defined by end-users; cryptographic path protection prevents re-routing



Preventing DDoS with isolation domains (ISDs)

- Internet at present: End points are vulnerable
- SCION architecture: Addresses are shared with selected communications partners only; a DDOS attack from the internet can thus no longer penetrate through to these addresses



Other Security Benefits

- Fast failover
  - While BGP can be tuned to detect dead neighbors fast, it still takes seconds to minutes to failover
  - Due to known health states on each path segment failover in SCION is milliseconds
- Participation criteria
  - Core members can enforce TRC policy

Use Case – SSFN

Secure Swiss Finance Network

Together with its partners, SIX launched the project to introduce SSFN as the new communication network

Under the leadership of SIX the project brought together a dedicated team of **partners**

- **SIX** (project lead)
- **SNB** (Manager SIC)
- **Anapaya** (commercial SCION technology)
- **Sunrise, Swisscom & SWITCH** (Partners for **connectivity**)

Three banks actively participated in the **pilot**

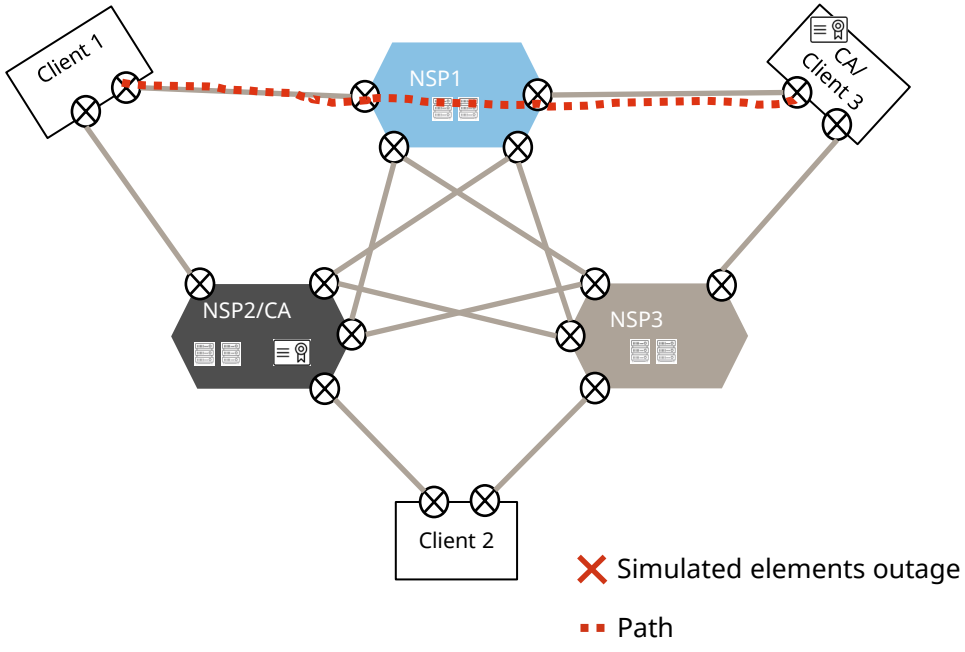
Active **collaboration** in the project

- Set-up a pilot network and performed testing using test traffic
- Defined governance principles
- Identified and partially tested use cases for SSFN or SCION-based networks beyond SIC / euroSIC
  - SSFN: Most SIX services
  - SSFN: “Secure” connection between banks
  - SCION: Working from home or eBanking

SSFN shall go live in November 2021 and replace Finance IPNet in the medium term due to its superior flexibility, resilience and functionality.

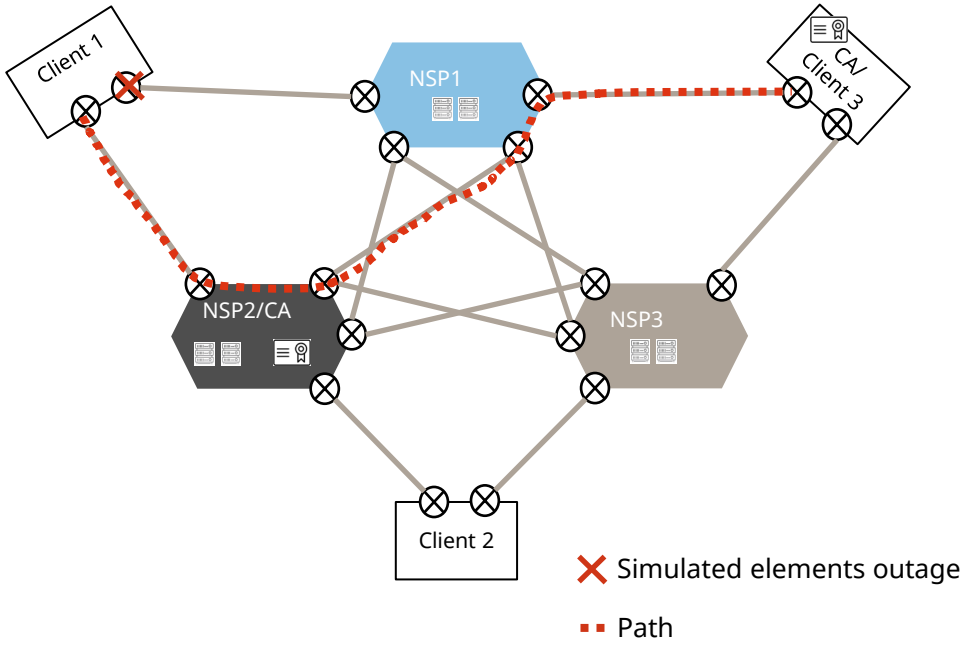
The Higher Resilience and Functionality of SSFN Was Demonstrated in the Pilot

(Still) functioning SSFN after multiple outages. Goal: client 1 talks to client 3 over shortest available path



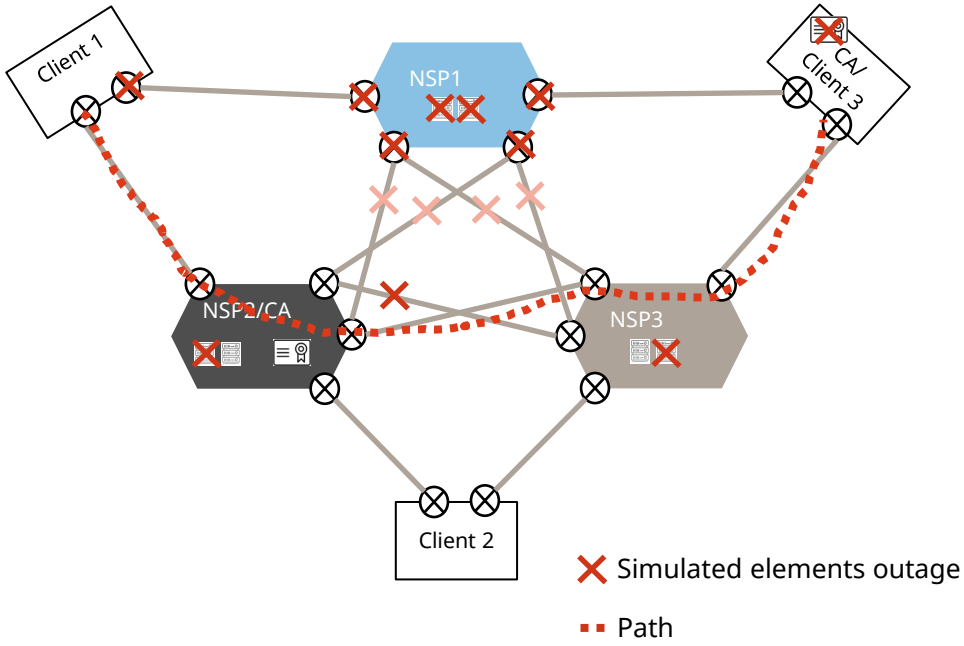
The Higher Resilience and Functionality of SSFN Was Demonstrated in the Pilot

(Still) functioning SSFN after multiple outages. Goal: client 1 talks to client 3 over shortest available path



The Higher Resilience and Functionality of SSFN Was Demonstrated in the Pilot

(Still) functioning SSFN after multiple outages. Goal: client 1 talks to client 3 over shortest available path

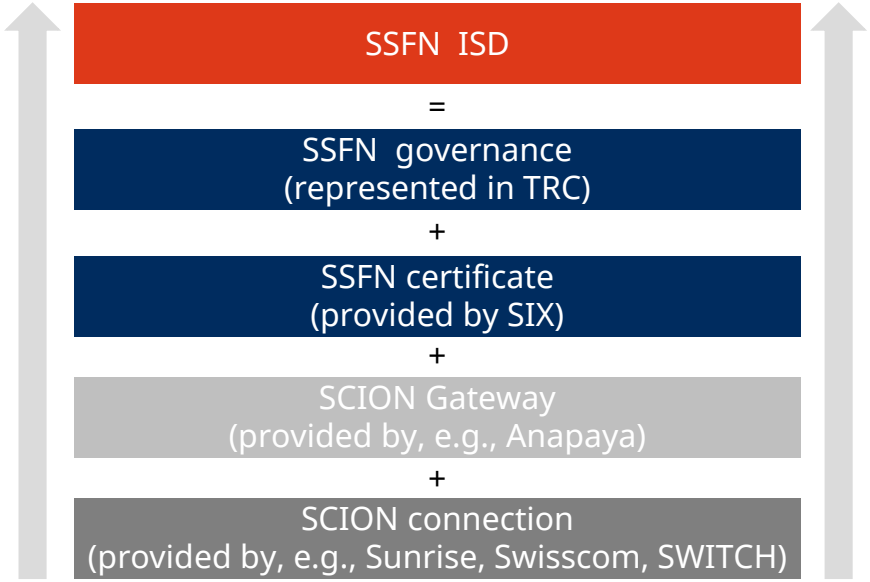


Demonstrated resilience and functionality properties in the pilot with various services

- Steady application session even when changing carriers, entry points or outage of multiple elements
- In comparison, an outage of an element with Finance IPNet results in a session interruption of roughly four minutes
- No impact on application – reachability of service performed at network level

SSFN is an ISD based on the SCION technology

Building blocks of SSFN



- SSFN is based on “standard” SCION services provided by service providers
- Access to SSFN is enabled and controlled through the SSFN certificate, just as the access to any other ISD is enabled and controlled by its certificate
- Access criteria for issuing SSFN certificates are the key definitions in the SSFN governance. The SSFN governance also defines key parties of the SSFN ISD

Resources

SIX
Hardturmstrasse 201
CH-8021 Zürich

www.six-group.com

SCION:
www.scion-architecture.net
www.scionlab.org
www.github.com/netsec-ethz

SSFN:
www.six-group.com/ssfn
www.six-group.com/en/newsroom/magazines/pay.html

Disclaimer

This material has been prepared by SIX Group Ltd, its subsidiaries, affiliates and/or their branches (together, "SIX") for the exclusive use of the persons to whom SIX delivers this material. This material or any of its content is not to be construed as a binding agreement, recommendation, investment advice, solicitation, invitation or offer to buy or sell financial information, products, solutions or services. It is solely for information purposes and is subject to change without notice at any time. SIX is under no obligation to update, revise or keep current the content of this material. No representation, warranty, guarantee or undertaking – express or implied – is or will be given by SIX as to the accuracy, completeness, sufficiency, suitability or reliability of the content of this material. Neither SIX nor any of its directors, officers, employees, representatives or agents accept any liability for any loss, damage or injury arising out of or in relation to this material. This material is property of SIX and may not be printed, copied, reproduced, published, passed on, disclosed or distributed in any form without the express prior written consent of SIX.