ANAPAYA

Built on SCION: The Secure Swiss Finance Network

Secure. Resilient. Sovereign.

Management summary

The Secure Swiss Finance Network (SSFN) is a SCION-based, closed communication infrastructure for the Swiss financial sector. Launched by the Swiss National Bank and SIX, it replaced the outdated Finance IPNet in 2024.

SSFN enables secure, resilient communication for over 300 financial institutions, supporting critical services like the Swiss Interbank Clearing (SIC) system, handling CHF 200B+ daily.

Key benefits include sub-second failover, strong governance, and data sovereignty, all the while preventing cyberattacks and ensuring operational continuity.

SSFN is now the standard for secure communication in the Swiss financial sector.

About the Secure Swiss Finance Network (SSFN)

Initiators: SCHWEIZERISCHE NATIONALBANK
BANQUE NATIONALE SUISSE
BANCA NAZIONALE SVIZZERA
BANCA NAZIUNALA SVIZRA
SWISS NATIONAL BANK
SIX

Timeline:

2020	2022	2024
SSFN pilot	SSFN go-live	SSFN replaces FinanceIPNet, the legacy network

Geography: Switzerland

Network participants:

- Banks
- Insurance companies
- Securities firms

Core services on the SSFN: SIC and euroSIC

About SIC:

200B+	2.6M+	300+
CHF daily	payments	financial institutions

SCION software provider: Anapaya

SSFN certificate provider: SIX

Connectivity providers:

BT cyberlink EveryWare InfoGuard SWISS CYBER SECURITY
Sunrise BUSINESS Switch swisscom

How the SSFN began

The SSFN (Secure Swiss Finance Network) emerged from a shared need identified by the Swiss National Bank (SNB) and SIX, Switzerland's financial IT infrastructure provider.

The Swiss National Bank's mandate

The SNB's core mandate is to maintain trust in money. Central to this is the Swiss Interbank Clearing (SIC) system, which uses central bank money to settle interbank and retail payments in a final and irrevocable way. Given its importance, the SIC requires a highly secure, reliable, and resilient data communication network.

> "The SSFN protects against major Internet risks such as distributed denial of service, or DDoS, attacks, thereby strengthening the cybersecurity of the Swiss financial center ("Finanzplatz Schweiz") as a whole."

Andrea Maechler, Deputy General Manager at the Bank for International Settlements and former Member of the Swiss National Bank, says "The SSFN protects against major Internet risks such as distributed denial of service, or DDoS, attacks, thereby strengthening the cybersecurity of the Swiss financial center ("Finanzplatz Schweiz") as a whole. Since communications within this network do not depend on a single provider, the SSFN offers a high level of reliability and resilience.

Both reliability and resilience are essential, as they help establish trust of both financial system participants and the general public in the safety and security of the payments system and other financial infrastructure organizations in Switzerland."

The role of SIX

As the operator of Switzerland's financial infrastructure, SIX delivers essential services to the financial sector, including managing the SIC. To help the SNB fulfil its mandate, SIX must ensure the uninterrupted, secure, and efficient flow of information and money between market participants.

Finance IPNet, the predecessor to SSFN, was aging and increasingly vulnerable to cyber risks. Recognizing this, the SNB and SIX began looking for new, more secure solutions for data exchange via the SIC system.

Financial sector challenges

The Swiss finance sector is one of Switzerland's core industries, with both macroeconomic dynamics and technical considerations prompting a review of the digital infrastructure for SIC, one of the SNB's key areas of operation.

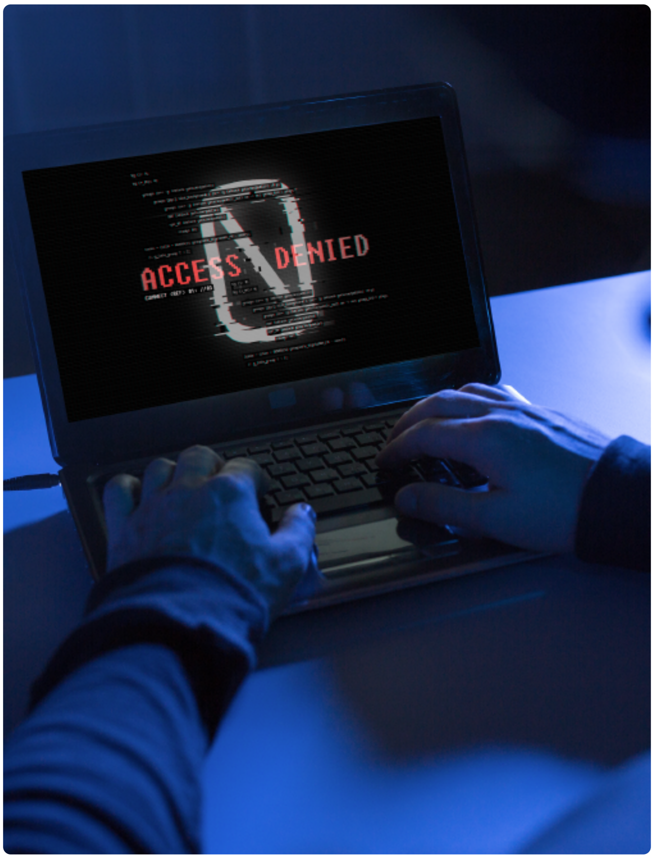
Macro-dynamics

Financial networks are vulnerable to outages.

Interruptions can result from malfunctions, cyberattacks, or external factors.

Expectations for availability, security, and resilience continue to rise, but existing technologies fall short.

The introduction of instant payments demands greater resilience in connections between banks and SIX, the IT infrastructure provider.



Technical factors

As the industry shifted from private networks to more flexible, Internet-based solutions, the 20-year-old Finance IPNet was put under review. Despite a long track record of strong security and capacity, it faced several challenges: inflexibility, high costs, and growing cyber risks. This was especially critical given that the network supports real-time systems like SIC, which demand the highest levels of protection and availability.

The key limitations of the legacy network were as follows:

- **Inflexible and costly architecture:** Built on leased lines and MPLS connections, it only supported limited point-to-point links, falling short of the flexible any-to-any communication required by modern financial participants.
- **Insufficient resilience:** Challenges included hidden "kill switches," slow response times during failures, and no control over routing paths.
- **Single point of failure (SPOF):** The network wasn't multi-provider, making it vulnerable to SPOFs.
- **Limited security for critical payment data:** Sensitive payment information requires robust in-transit protection to ensure it stays within a trusted environment, shielded from network-based attacks – not just encryption and authentication at the payment message layer.
- **Lack of governance:** The network lacked clear, enforceable rules and boundaries needed to ensure security and maintain trust among participants.

Technology evaluation of the new solution

During the evaluation phase, different technology options were carefully reviewed.

The digital communication platform replacing Finance IPNet had to fulfill the following requirements set by the SNB and SIX:

Security about the identity of the participants with clear governance

Unaltered transmission of messages

A stable and resilient communication system

SCION offers the best of both worlds: the security of private lines and the flexibility of the Internet.

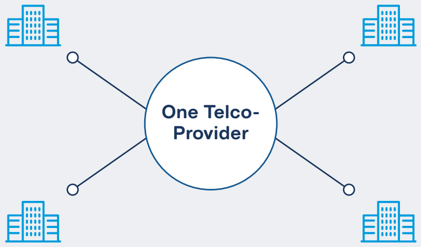
MPLS/Private lines

Pros

- Reliable
- Secure

Cons

- Vendor lock-in
- High costs
- Inflexible



One provider to which all involved connect

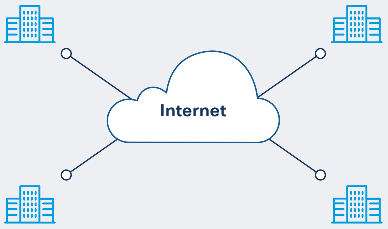
Internet

Pros

- Flexible
- Cheap

Cons

- Unreliable
- Insecure
- Very limited control
- No geo-fencing
- Hidden “kill switches”
- No Quality of Service (QoS) or Bandwidth (BW) management

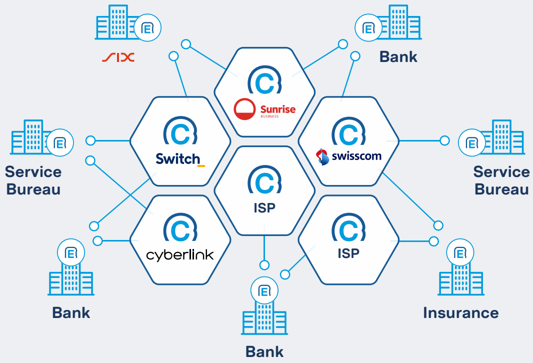


The Internet as a cost-efficient network

SCION

Pros

- Any-to-any architecture
- Higher level of reliability and security
- Protection against attack from the Internet
- Multi-provider and multi-path for cyber resilience
- Data sovereignty
- Control and governance for higher trust
- Ecosystem cost-efficiencies



ANAPAYA

SSFN: Designing a closed, trusted network

The SSFN is a closed network (known as an Isolation Domain or ISD) where participants are granted access only after obtaining the appropriate certificate based on established governance rules.

Building such a network required careful planning across several key elements, as listed here:

- Defining governance roles, responsibilities, admission criteria and legal groundwork
- Designing the network architecture and pilot operations (such as certificate issuance, IP addressing, and DNS structure)
- Developing an SSFN ecosystem with a broad SCION community
- Creating a comprehensive process catalog for members, IT, and business continuity management
- Carrying out extensive external security checks and testing cycles

Governance structure

The SSFN ISD focuses on a user-centric, enforceable, and shared governance model. Authentication in the network does not rely on external parties and is fully governed by a set of voting members, including the Swiss National Bank, SIX, and SWITCH, who collaboratively define rules. Thanks to SCION's cryptographic features, no single entity retains full control over the network, enhancing trust.

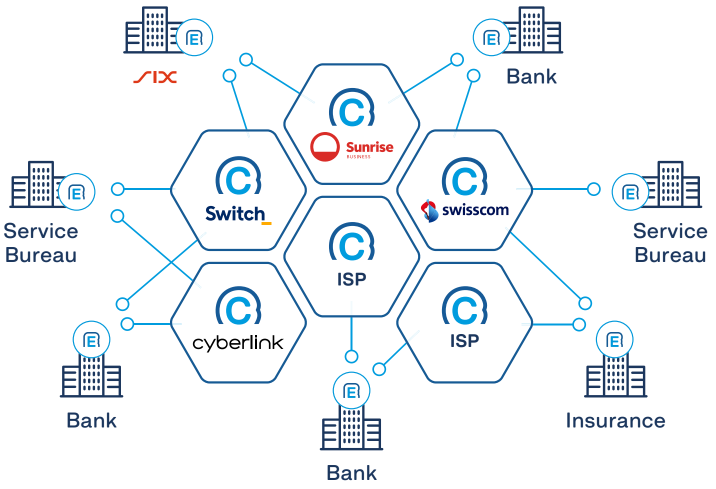
SCHWEIZERISCHE NATIONALBANK
BANQUE NATIONALE SUISSE
BANCA NAZIONALE SVIZZERA
BANCA NAZIUNALA SVIZRA
SWISS NATIONAL BANK

SIX

Switch

Technical configuration

SCION network providers form a federation by deploying Anapaya's SCION routers (also known as Anapaya CORE) at the borders of their networks. These routers are interconnected to create a redundant, highly available core network.



Users of this network, such as financial institutions, connect to the core through one or more network providers using Anapaya EDGE gateways. EDGE gateways act as entry points to the SSFN network and to the SIC system.

SSFN the de facto system in Swiss finance

With over 300 banks and financial institutions exchanging payment transactions over the SIC – amounting to 200 billion CHF daily – the SSFN has repeatedly proven its security, reliability, and sovereignty since its go live in 2022. It is now the de facto technology on which the Swiss finance sector relies for its operations.

300
banks and financial institutions

200
billion CHF daily

"With the SSFN, our customers in Switzerland can feel confident that data exchanges are facilitated with the highest level of security, performance, and functionality."

As **Andreas Helbling**, Country Head of Switzerland at Finastra, one of the largest global services bureaus and SSFN participant, says: "As cyber threats become more prevalent, strengthening security is a major focus for all institutions. With the SSFN, our customers in Switzerland can feel confident that data exchanges are facilitated with the highest level of security, performance, and functionality. Anapaya's robust technology enables us to continue delivering our mission-critical services with added protection."

With this use of SCION technology that translated into a closed network, SNB and SIX can benefit from:

Security:
Data remains within a closed user group on defined paths, isolated from the rest of the Internet, thus preventing cyberattacks.

Resilience:
A multi-provider setup and SCION's multipath capabilities prevent session interruptions and ensure business continuity.

Sovereignty:
Financial data stays within chosen countries and avoids routing through jurisdictions at risk of surveillance or tampering.

Control:
Only certified participants, enabled by certificates issued by SIX, can access the network for higher trust and reduced attack surface.

Governance:
Clear governance and enforceable eligibility criteria create a trusted environment.

Flexibility:
Supports any-to-any communication between certified participants and financial service providers.

Ecosystem cost efficiencies:
The switch from point-to-point connections, especially for aggregators such as Bottomline or Finastra, but also banks, bring significant cost savings.

SSFN: Tested and proven

Test framework

This table shows the results of various test scenarios carried out during the evaluation phase of the technology. It compares the SCION-based SSFN against Finance IPNet across various dimensions.

> “The SSFN offers the same level of security and reliability as before, as well as enabling us to develop new business opportunities faster with more flexibility.”

Patrick Bamert
Head of Network and Security Engineering,
Zürcher Kantonalbank (ZKB)

> “With SCION, we have archieved the desired resilience against cyber-attacks.”

William Boye
Head of Network Services
Swiss National Bank

	SSFN		Legacy solution	
Scenario	**Failover time**	**Session upheld?**	**Failover time**	**Session upheld?**
Link failure-access	>1s	yes	>3 min	no
Link failure-core	>1s	yes	n/a	no
Core Router failure	>1s	yes	n/a	no
EDGE Gateway failure	>5s	yes	>3 min	no
Provider failure	>1s	yes	n/a	no

Key takeways

- Uninterrupted information flow
- Sub-second failover
- No application session interruptions

“Extensive testing under extreme conditions has proven the reliability and resilience of the infrastructure - made possible by the path control and inherent multipathing properties of a SCION-based network architecture. This level of reliability and resilience is a vast improvement to ensure business continuity for current and future system-relevant use cases and applications not only in the financial sector but also for other critical infrastructures.” **Fritz Steinmann**, SIX, Senior Network and Network Security Architect

> “Extensive testing under extreme conditions has proven the reliability and resilience of the infrastructure.”

Beyond SIC use cases for SSFN

SIX will continue expanding the range of services available over the SSFN – not just SIC – establishing it as the standard communication network for the entire Swiss financial center in the future. SSFN users, such as banks, can also leverage their existing SSFN connection and expertise for additional use cases, including secure remote work.

Private Client Bank and Frankfurter Bankgesellschaft are already using the SSFN network to upgrade the security and resiliency of business-critical services accessed by their remote workers by leveraging the Anapaya GATE solution.

> **“This air-gapped setup remains isolated from internal networks and the public Internet while leveraging SCION’s inherent security and resilience. ”**

Steve Erzberger, Head IT at Frankfurter Bankgesellschaft reports: “Building on our existing SCION infrastructure, we have enabled secure remote access to our out-of-band management network for IT administrators– ensuring controlled access to critical data center devices for maintenance work and disaster recovery. This air-gapped setup remains isolated from internal networks and the public Internet while leveraging SCION’s inherent security and resilience. By doing so, we have expanded our administrators’ flexibility and reach without compromising security, compliance, or operational integrity.”

Trusted by over 300 global banks and financial institutions – meet some of them

BIS
BNP PARIBAS
Cembra
Deutsche Bank
HSBC
J.P.Morgan
Julius Bär
RAIFFEISEN
Santander
SIX
SCHWEIZERISCHE NATIONALBANK
BANQUE NATIONALE SUISSE
BANCA NAZIONALE SVIZZERA
BANCA NAZIUNALA SVIZRA
SWISS NATIONAL BANK
UBS
vaudoise
Zürcher Kantonalbank

Download the case study "SCION vs. the Internet"

Have questions? Contact us at **team@anapaya.net**