SCION ASSOCIATION

FACT SHEET

SCION FOR CRITICAL INFRASTRUCTURE

Connecting over the standard Internet hides intrinsic vulnerabilities that can put your data and business continuity at risk. To overcome these challenges, many critical infrastructures still rely on costly and inflexible private lines, often depending on a single connectivity provider. And yet, cyberattacks and outages continue to rise.

CYBERSECURITY CHALLENGES

SECURITY: VULNERABILITY TO ROUTE LEAKS AND HIJACKING

This type of cyberattacks can result in service disruptions, traffic interception or alteration, and potential large-scale DDoS attacks.

RESILIENCE: LACK OF REDUNDANCY AND LONG FAILOVER TIMES

Internet routing has a failure reaction time that is too long for critical infrastructure. On the other hand, private lines are often provided by a single ISP, creating single points of failure.

NO CONTROL OVER DATA SOVEREIGNTY

Traffic can be routed through different countries, disrupted, intercepted, or monitored by bad actors, potentially breaching data protection laws like GDPR by routing data outside designated jurisdictions.

SINGLE CONNECTIVITY PROVIDER

Relying only on a single provider for connectivity is a risk due to potential service outages, lack of redundancy, and increased vulnerability to cyberattacks.

WHY SCION?

Today’s Internet can no longer meet the security and reliability needs of critical infrastructure ecosystems, particularly those in the finance, healthcare, utilities, and public sectors.

Many critical infrastructures in finance, power, transport, and emergency services run on legacy infrastructures that lack sufficient reliability and resilience.

True inter-domain and multi-ISP support is highly desirable or required for uninterrupted operations and connectivity.

Many important legacy infrastructures are still not fully networked due to Internet threats.

Supporting legacy infrastructures is becoming increasingly costly, inefficient, and challenging due to rising complexity.

SCION BENEFITS

TRUSTED NETWORKS FOR REDUCED ATTACK SURFACE

Clear network governance with common trust domains with enforceable, multilateral controls for admission to the network.

SECURITY AGAINST HIJACKINGS

Paths are cryptographically secured at each hop. Networks can choose how they advertise their network topologies and how they send and receive traffic from other SCION networks.

DATA SOVEREIGNTY AND COMPLIANCE

Users can select the path(s) by which to send their data across the Internet, based on optimal characteristics or other parameters (e.g., geofencing, latency).

MULTI-OPERATOR FOR CYBER RESILIENCE & PERFORMANCE

SCION uses multiple paths and operators simultaneously, switching paths in less than a second, increasing resilience and performance by selecting the fastest path.

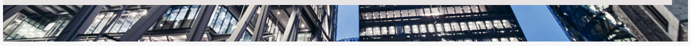
SCION-ENABLED CRITICAL SYSTEMS TODAY

The SCION infrastructure is constantly expanding, with established Swiss ISPs as well as new SCION ISPs in Benelux, enabling critical infrastructure operators everywhere to easily build SCION networks.

FINANCE

The Secure Swiss Finance Network (SSFN) is an inter-banking network that handles up to ~200B CHF/day transfers between 300+ banks.

READ THE CASE STUDY



HEALTHCARE

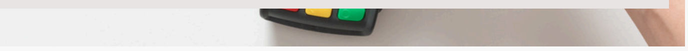
Health InfoNet (HIN), a company that protects patient digital data, adopts SCION to interconnect Swiss hospitals and 50k+ doctors over the Secure Swiss Healthcare Network (SSHN).

ENERGY & UTILITIES

The Secure Swiss Utility Network (SSUN) is a community network connecting ecosystems and industry platforms, cloud applications, IoT, technicians, remote workers, and security operation centers.

PAYMENTS

The Secure EFTPOS Network (SEPN) leverages SCION technology to deliver unmatched resilience, security, and flexibility in cashless payments.



CONTACT US TO TALK ABOUT YOUR NEEDS