SCION ASSOCIATION

# SCION: Secure Path-Aware Internet Routing for Critical Infrastructures

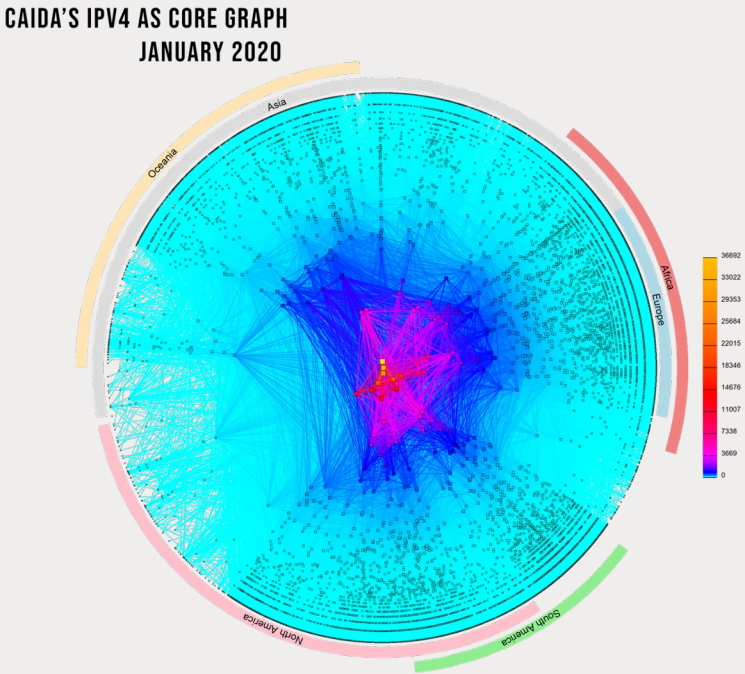
Kevin Meynell, SCION Association kme@scion.org

NetUK 3, 7 July 2026

# THE ROUTING PROBLEM

## Border Gateway Protocol (BGP): the Internet routing protocol

- The current Internet routing system is inherently based on unverified trust between networks and does not have predictable route propagation.
- No built-in validation that route advertisements are legitimate – in the absence of RPKI and ROV, any network can announce any ASN or IP prefix and thereby cause traffic to be re-routed. Problem = route leaks and hijacks
- Sending and receiving networks typically cannot decide the path that intermediate routers direct their traffic across the Internet. Data sovereignty breaches
- BGP can send traffic through different jurisdictions thereby creating opportunities for surveillance, compromising security and making regulatory compliance complex Problem - data sovereignty breaches
- BGP failover is relatively slow with convergence times of up to 3 minutes



# HOW IS THIS BEING ADDRESSED?

Some info @ a glance

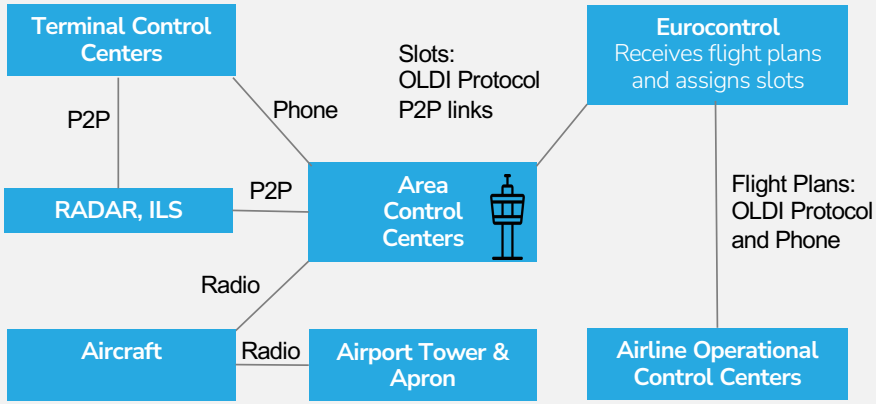
| EVENT | EXPLANATION | LIMITATIONS |
|---|---|---|
| **RPKI & ROV**<br>Resource Public Key Infrastructure & Route Origin Validation | ROAs (Route Origin Authorisations) provide cryptographic assertions of IP prefix ownership and which ASNs are allowed to originate them. Routers can validate ROAs and generate appropriate route filters. | Requires widespread deployment to be effective (62% of IP prefixes are signed in mid-2026)<br>Few network operators currently use ROV (8%).<br>Only does origin validation and does not validate paths through the Internet. |
| **BGPSEC**<br>BGP Security | Builds on RPKI to provide cryptographic assertions that every router (hop) en-route to a destination has authorized the advertisement of that route. Prevents unauthorised insertion of ASNs into a path to circumvent RPKI. | Needs to be explicitly supported by all routers along a path to achieve full benefits.<br>Computationally intensive and introduces significant delays in route convergence.<br>Explicit path selection is not possible.<br>Almost no deployment. |
| **ASPA**<br>Autonomous System Provider Authorization | ASPA objects are similar to ROAs, but allow ASNs to authorize other ASNs to carry their traffic through the Internet. Works out-of-band so doesn't need to be deployed on all routers. | Developmental technology and not yet an Internet standard.<br>Does not provide assurances that traffic will actually follow validated paths. |
| **SCION** | Inter-domain routing architecture offering secure path awareness and selection. | Needs to be supported by border routers. |

# CRITICAL INFRASTRUCTURE

## Legacy infrastructure needs replacing

- Many critical infrastructures in power, transport, emergency services etc.. run on legacy infrastructures
- Many important legacy infrastructures are still not fully networked and/or are not IP based
- It is expensive, inefficient and becoming harder to support these legacy infrastructures
- The Internet is now able to provide sufficiently reliable and resilient connectivity, like the power grid
- Critical infrastructure operators want to take advantage of commodity Internet services as they offer cost and resilience advantages, but higher trust and data sovereignty assurances are required
- True inter-domain and multi-ISP support is highly desirable or required

**Example: Air Traffic Control**




Star centered around Area Control Centers

Radar & ILS physically connected to control towers

No connectivity between Control Centers beyond phone

Aircraft can only be managed within radio range of Control Center (so cannot be slowed/speed-up by destination)

OLDI protocol is based on data layer similar to RS232

Aircraft transponders can be spoofed and jammed

Limited coordination means inefficient management of slots

System heavily reliant on closed loop and implicit trust

# WHAT IS SCION?

SCION is a resilient multi-domain path-aware architecture

## ENHANCED TRUST

- Establishes trust domains with self-governance model that are not reliant on third-party Certificate Authorities (such as RPKI)
- ASes are admitted and verified with X.509 certificates

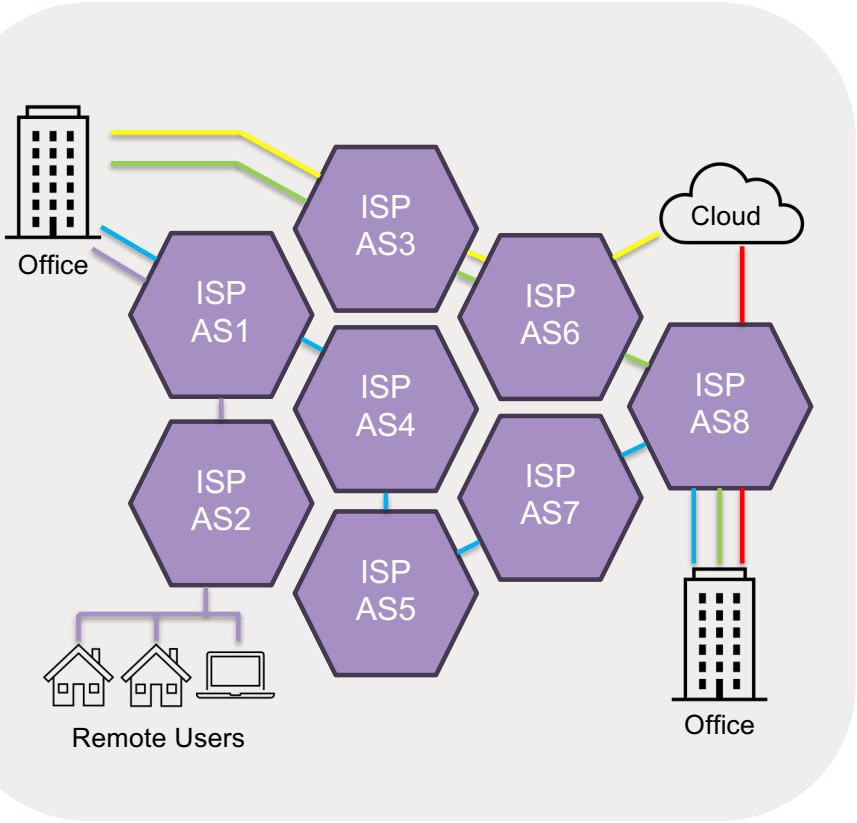
## PATH CONTROL

- Source endpoints select paths across SCION-enabled ASes
- Paths can be selected based on requirements (e.g. latency)
- Geofencing & Hijacking prevention

## MULTI-PATH DISCOVERY & FAILOVER

- Fast path switching when connections fail (in ~RTT, 1-2 secs)
- Multiple paths can be used concurrently

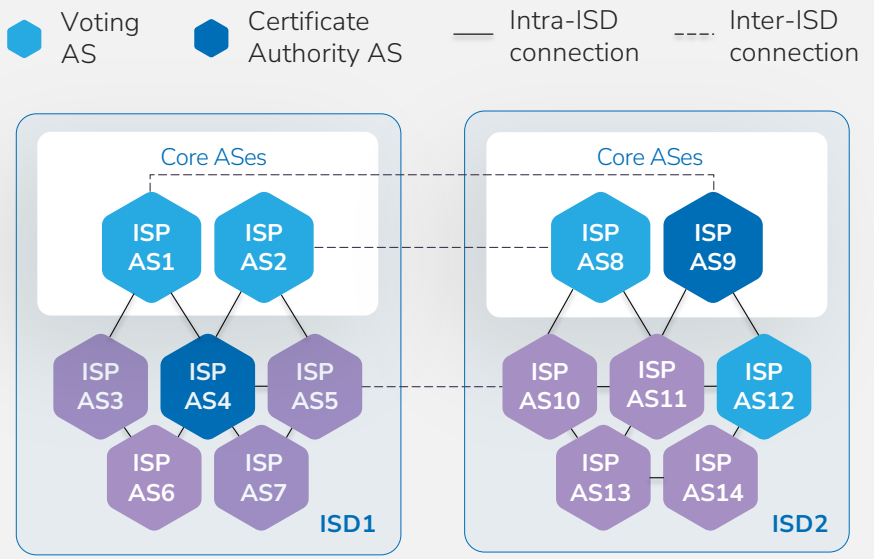
SCION runs over IPv4 and IPv6 and provides benefits similar to leased lines, but in a resilient multi-operator and multipath environment.



# TRUST-ENHANCED NETWORKING

Trust model is based on Isolation Domains (ISDs)

- An ISD is a logical grouping of ASes sharing a uniform trust environment (e.g. a common jurisdiction)
- Each ISD is administered by one or more ***Voting ASes***
- Every ISD has its own trust root specified in the ***Trust Root Configuration*** - a collection of X.509 certificates with ISD information
- TRC is negotiated by the Voting ASes according to its own trust policy
- Not reliant on third-party CAs
- The CAs in an ISD can only create certificates for ASes in their respective ISD
- Each ISD must have at least one Core AS to initiate path discovery and construction (which may also be Voting ASes)




ISDs are the building blocks of SCION

# HOW IT WORKS

SCION core components in a nutshell

## CONTROL PLANE - BEACONING

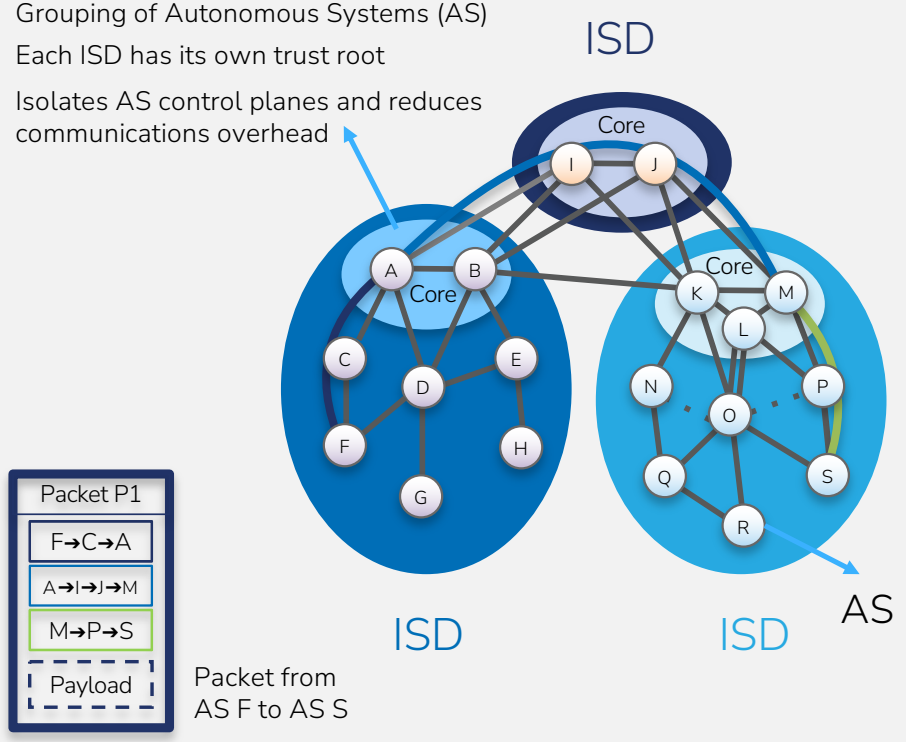
- Establishes paths based on AS rather than prefixes
- Beacon server uses path segment construction beacons (PCBs) to build path segments and routing paths
- Path server stores paths to AS discovered during beaconing
- PKI authenticates path information

## DATA PLANE – PACKET FORWARDING

- Runs over IPv4 and/or IPv6
- Endpoints combine path segments into end-to-end paths, supporting multiple paths and fast failover
- SCION packets contain end-to-end ISD-AS path
- Border routers forward SCION packets to next SCION router or end destination based on end-to-end path

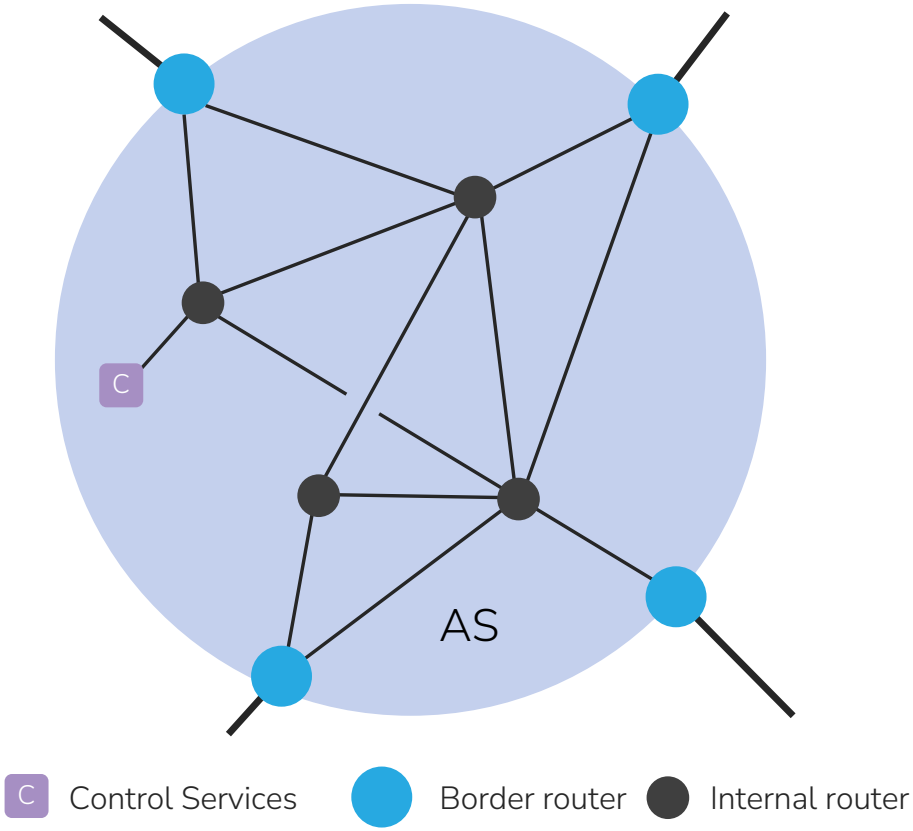
**Isolation Domain (ISD)**

- Grouping of Autonomous Systems (AS)
- Each ISD has its own trust root
- Isolates AS control planes and reduces communications overhead



# DEPLOYMENT MODEL

SCION Service Provider




## SCION ROUTERS

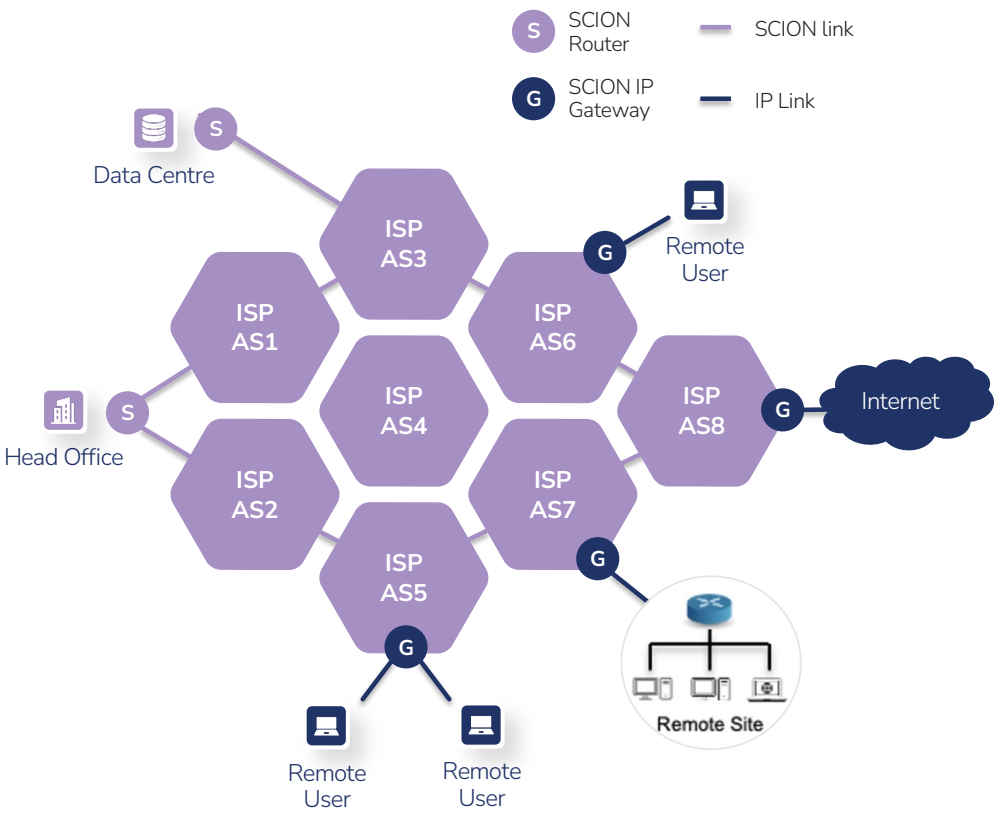
- SCION routers are set up at the borders of an AS
- Border routers peer with other SCION-enabled networks and collect customer traffic
- Control services discover, map and validate network paths
- No change to the internal network infrastructure needed
- Endpoints run a SCION stack
- Legacy endpoints can use SCION gateways

## CONTROL SERVICES (PER AS)

- **Beacon server** – propagates and receives PCBs to construct path segments and routing paths
- **Path server** – store mappings of AS to path discovered during beaconing
- **Certificate server** – caches copies of TRCs and AS certificates and key management for inter-AS comms

# SCION IP GATEWAYS

## Integrating IP networks and hosts with SCION



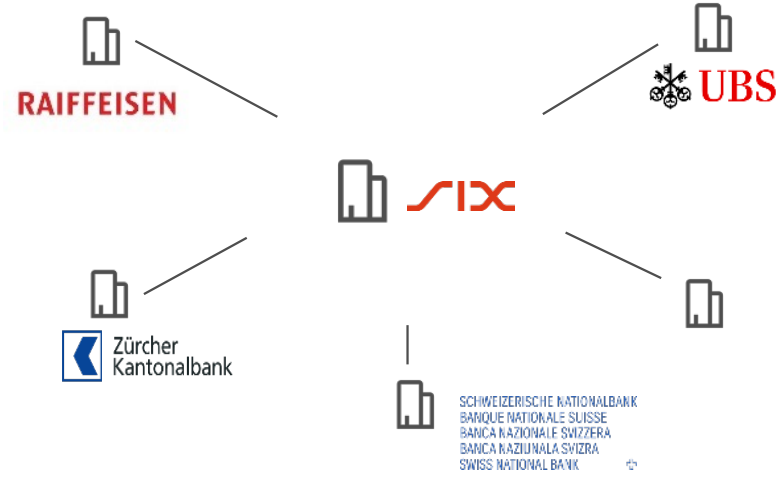

Example SCION IP Gateway Deployment

### ENTERPRISE DEPLOYMENT

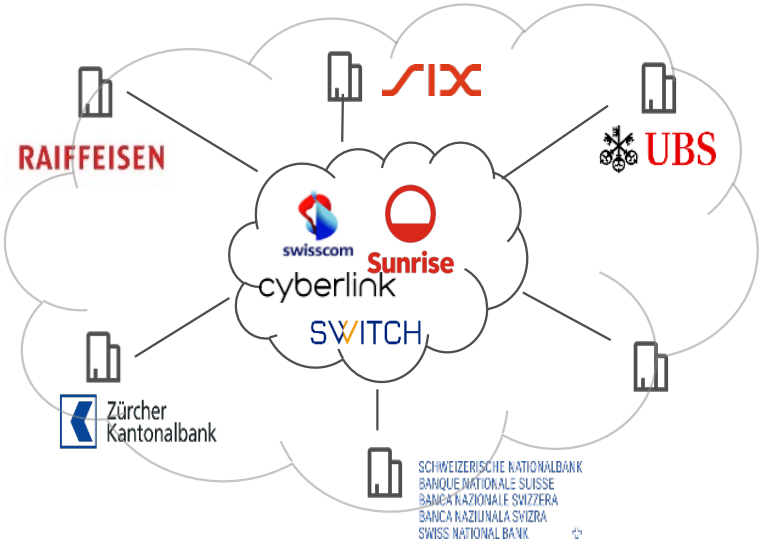
- SIGs support communication between IP-based hosts that are not running SCION
- SIGs tunnel IP over SCION networks and allow existing networks to be integrated with SCION
- SIGs can protect against DDoS attacks and malicious traffic by only allowing traffic to/from authorized Ases
- SIGs can render networks invisible to anyone outside of the trusted ASes within a SCION network, therefore reducing potential attack surfaces
- SIGs can be configured with path selection and failover policies
- No changes to internal networks required

# REAL-WORLD DEPLOYMENT: SECURE SWISS FINANCE NETWORK (SSFN)

- Swiss inter-banking network for **300+ finance institutions**, handling **~200 billion CHF/day** worth of transactions between banks and other critical real-time financial services
- From 2019 to 2021, SIX and Swiss National Bank built SSFN to replace older MPLS-based FinanceIP Net

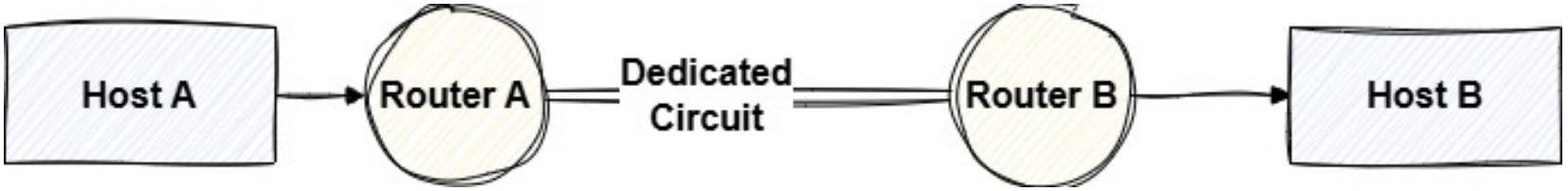



Centralized “Hub and Spoke” architecture



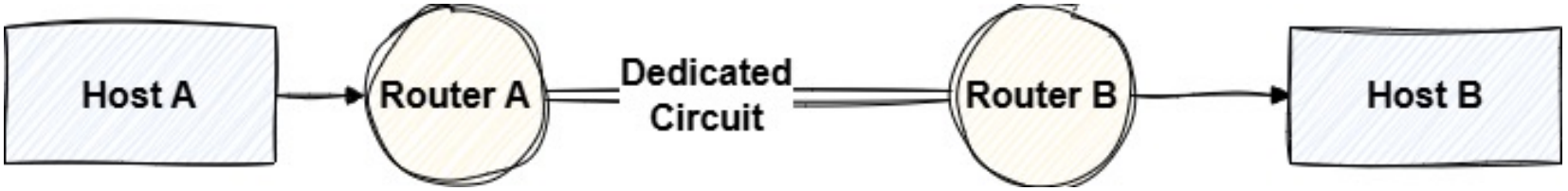

Internet ecosystem “any-to-any” architecture

# LEGACY NETWORK: POINT-TO-POINT PRIVATE CIRCUITS




- Great control & predictability, but costly and inflexible as ecosystems grew (many sites, many partners)
- Reliability is designed by over-building: lots of links, long procurement cycles, complex contracts
- The more parties you connect, the complex the topology and more difficult to manage

# LEGACY NETWORK: MPLS




- MPLS provides simpler connectivity model than many P2P lines, but typically single operator at the network layer, or operator-provided NNIs required
- Routing choices sit mostly with the operator or a central coordination entity
- Requires dedicated infrastructure so unsuitable for many edge locations and remote users.
- Third-party and supply chain risk management is increasingly good practice and mandated by NIS2, whilst optionality/sovereignty matter as much as raw uptime

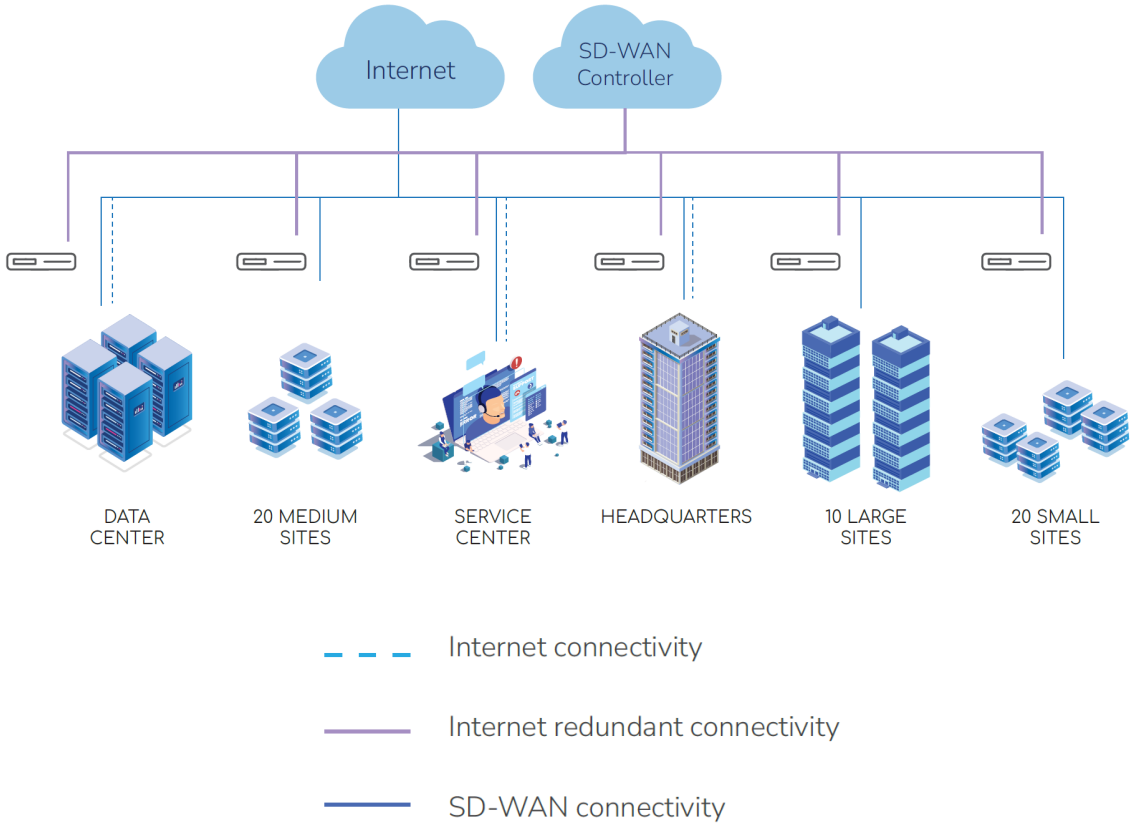
# THE SD-WAN OPTION

**Pros**

- Allows secure private networks to be built using commercially available Internet access provided by different ISPs
- Offers some resilience, traffic prioritization and QoS capabilities

**Cons**

- Connectivity is dependent on the underlying Internet connections and thus vulnerable to shared attack surfaces and DoS attacks
- Each vendor has its own proprietary standards which limit interoperability and encourage vendor lock-in
- Limited path control capability



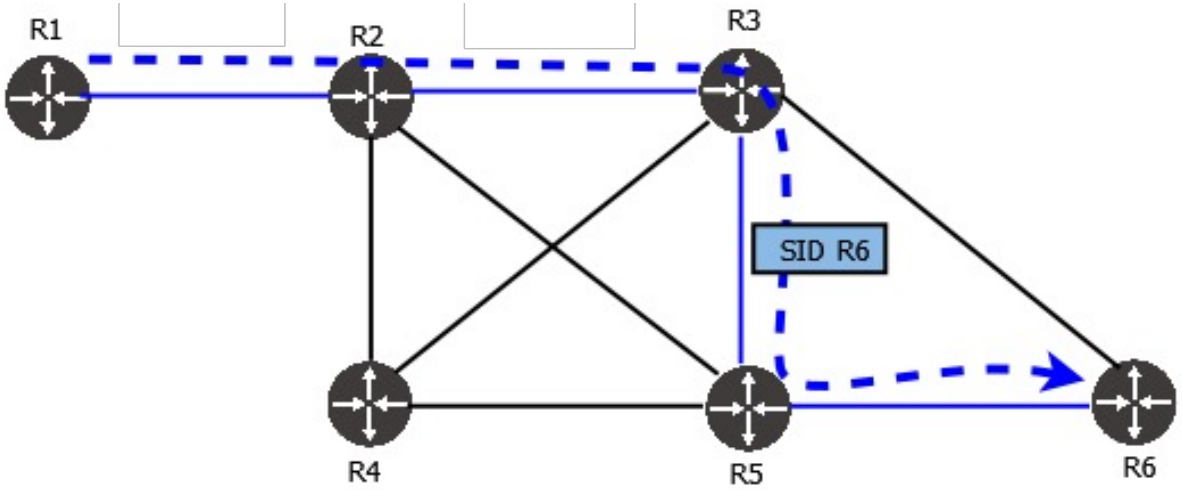
# WHY NOT SEGMENT ROUTING?

**Pros**

- Works over multiple ISPs and does not need to be supported by all routers on a path.
- Offers path control capability, faster path convergence, and traffic prioritization.

**Cons**

- Requires MPLS or IPv6 networks
- Connectivity is only possible over limited domain
- Limited vendor support and interoperability
- Lack of cryptographic verification of paths
- Configuration and management is complex and requires understanding of underlying networks

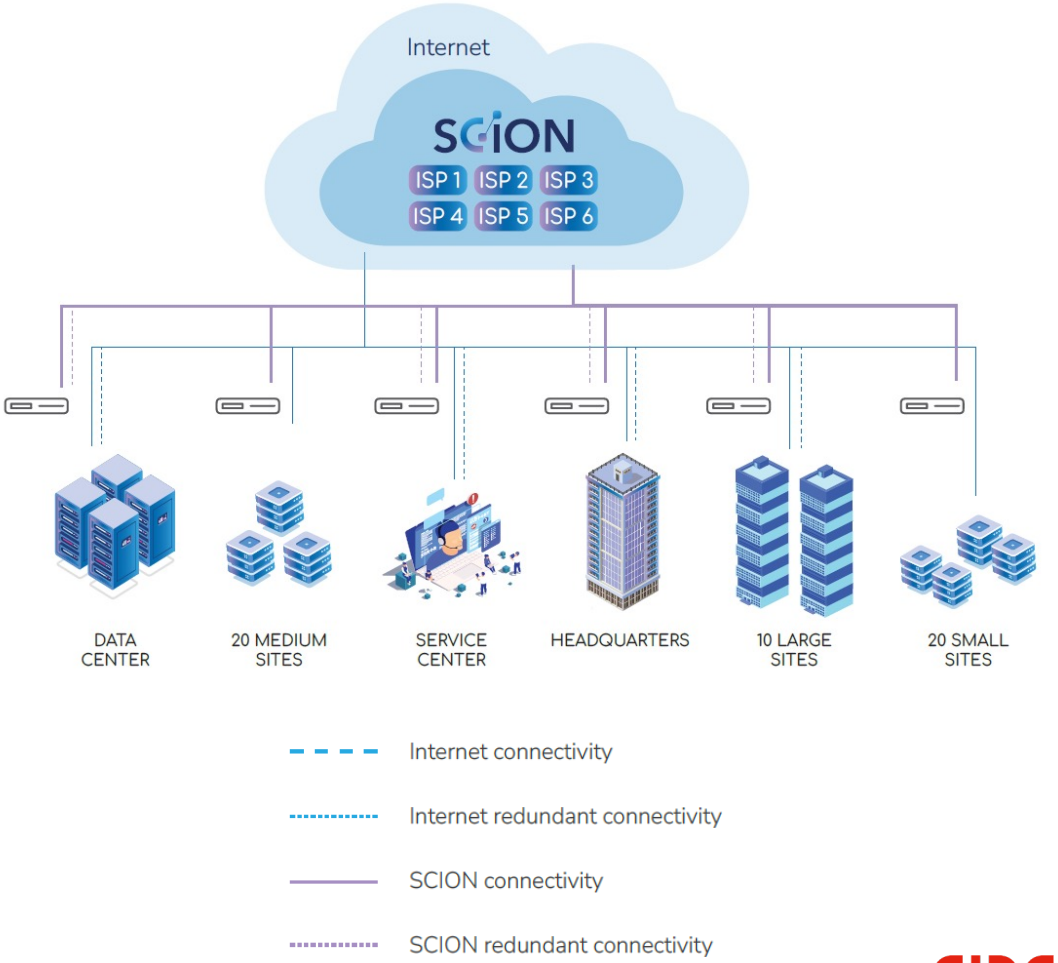



Credit: APNIC

# THE SCION OPTION

SCION provides the security and control of private connections whilst being able to utilize commodity Internet connections

- Open protocol that works with different vendors and ISPs
- Allows establishment of trust domains with governance, control over participation, and cryptographic verification (i.e .who can acces or transit a network)
- Provides path control to direct traffic across SCION-enabled networks, with multi-path and fast failover capabilities
- Offers data optionality and aligns with regulatory requirements



# SSFN DEPLOYMENT EXPERIENCES

## LESSONS LEARNED

- Establishment of an ISD requires the creation of admission criteria, process documentation, and legal agreements
- Initial establishment of ISDs requires key-signing ceremony involving voting ASes
- Manual checks are needed when onboarding candidate ASes to ensure they meet admission criteria
- Building the PKI and management integration of the services was challenging (although SSFN offers managed service)
- Certificate revocation not possible, although they expire within 72 hours
- SCION products are still relatively new and not all features are implemented yet
- Inter-ISD path control is currently limited
- The community and sources of expertise are currently limited
- Practical experience has been that path failover and fallback occurs within a few seconds.

# REAL-WORLD DEPLOYMENT: FINANCE, HEALTHCARE, POWER & EDUCATION

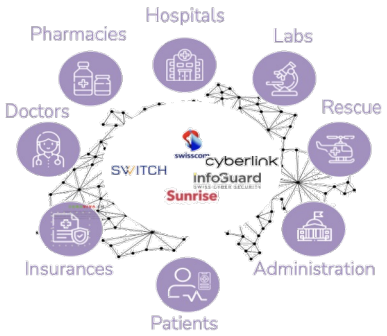
## PAYMENTS

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

epc VEZ Verband Elektronischer Zahlungsverkehr Association les Paiements Electroniques SWISS PAYMENT ASSOCIATION SPA

## HEALTHCARE

HIN adopts SCION to interconnect Swiss hospitals and thousands of doctors.




## POWER

The Association of Swiss Electricity Companies has completed the concept for the Secure Swiss Utility Network (SSUN).

This is a community network, designed to integrate validated ecosystem and industry platforms, cloud applications, BPO providers, IoT, technicians, remote workers, security operation centers, and more...

## EDUCATION

The SCION Education, Research & Academic Network (SCIERA) connects campuses with path-aware high performance SCION connectivity

KAIST 한국과학기술원 · Otto von Guericke Universität Magdeburg · Princeton University · SWITCH · ETH zürich · Korea University · University of Virginia · GÉANT Networks · Services · People · NUS

# RETURN ON INVESTMENT

## ENTERPRISE WAN CONNECTIVITY

### HIGH AVAILABILITY WAN

#### SCION VS LEASED LINES

**91%** reduction of yearly costs

**1.34M** annual savings

**2389%** ROI

**<1 MONTH** payback time

#### SCION VS MPLS

**81%** reduction of yearly costs

**600K** annual savings

**1110%** ROI

**<1 MONTH** payback time

### BRANCH NETWORKING

#### SCION VS SD-WAN

**33%** reduction of yearly costs

**315K** annual savings

**228%** ROI

**<4 MONTH** payback time

## REMOTE ACCESS

### WEB SERVICES & APPS

#### SCION GATE BY ANAPAYA + CURRENT SOLUTION

**142K** average annual savings across 3 years

**71.6%** ROI (using 3-year amortized cost basis)

**9 MONTHS** payback time

SCION ASSOCIATION

# INTERNET ENGINEERING TASK FORCE

- Open specifications are important for interoperability and to encourage other implementations
- SCION core components and functionality are documented in 3 Internet Drafts
- Currently in RFC publication queue in IETF Independent Submission Stream

Internet Drafts:

| | |
|---|---|
| • SCION PKI | draft-dekater-scion-pki |
| • SCION Control Plane | draft-dekater-scion-controlplane |
| • SCION Data Plane | draft-dekater-scion-dataplane |



Workgroup: Network Working Group
Internet-Draft: draft-dekater-scion-controlplane-latest
Published: 30 April 2026
Intended Status: Informational
Expires: 1 November 2026
Authors: C. de Kater, SCION Association
N. Rustignoli, SCION Association
S. Hitz, Anapaya Systems

## SCION Control Plane

**Abstract**

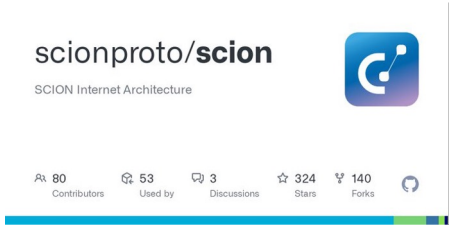
This document describes the Control Plane of the path-aware, inter-domain network architecture SCION (Scalability, Control, and Isolation On Next-generation networks). A fundamental characteristic of SCION is that it gives path control to SCION-capable endpoints that can choose between multiple path options, thereby enabling the optimization of network paths. The SCION Control Plane is responsible for discovering these paths and making them available to the endpoints.

# COMMERCIAL & OPEN-SOURCE IMPLEMENTATIONS

If you're interested in deploying SCION, there are currently two options:

ANAPAYA

Commercial




Open Source

Other implementations under development: P4, Rust, OpenWRT

SCION Association formed by deployers and early adopters to support open source development, standardization, and community involvement.

# THE SCION ASSOCIATION

- Promoting openness and collaboration to unlock the full potential of SCION
- Non-profit association established in 2022
- Open for membership to all entities interested in SCION

https://www.scion.org

ETH zürich
Dr. Uli Sigg
Private individual
SCHWEIZERISCHE NATIONALBANK
BANQUE NATIONALE SUISSE
BANCA NAZIONALE SVIZZERA
BANCA NAZIUNALA SVIZRA
SWISS NATIONAL BANK
SIX
ANAPAYA
axpo
cyberlink
DIDAS
eraneos
ETH Foundation
libC TECHNOLOGIES
OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
MystenLabs
Sunrise BUSINESS
swisscom
Swiss Finance + Technology Association
Switch

## COMMUNITY

Raising awareness of SCION, promoting the benefits and encouraging adoption, developing its community, and providing marketing support to implementors and deployers

## STANDARDIZATION

Developing the specifications to implement SCION, with the goal of making it an interoperable Internet standard

## OPEN SOURCE

Maintaining and coordinating the SCION implementation for research, development, and experimental deployments

# SCION TODAY

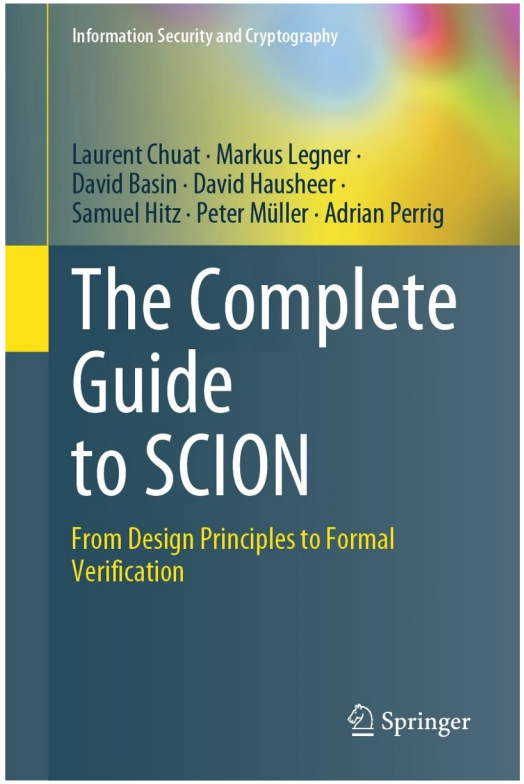
A growing ecosystem

## SERVICE PROVIDERS


## USERS


## RESEARCHERS


SCION ASSOCIATION




The Complete Guide to SCION
Springer Verlag, 2022

# THANK YOU!

More information:

- SCION Association: https://www.scion.org
- Reference & Developer Docs: https://docs.scion.org/
- Research: https://scion-architecture.net
- Vendor: https://www.anapaya.net/resources
- Latest Release: https://github.com/scionproto/scion/releases/