SCION ASSOCIATION

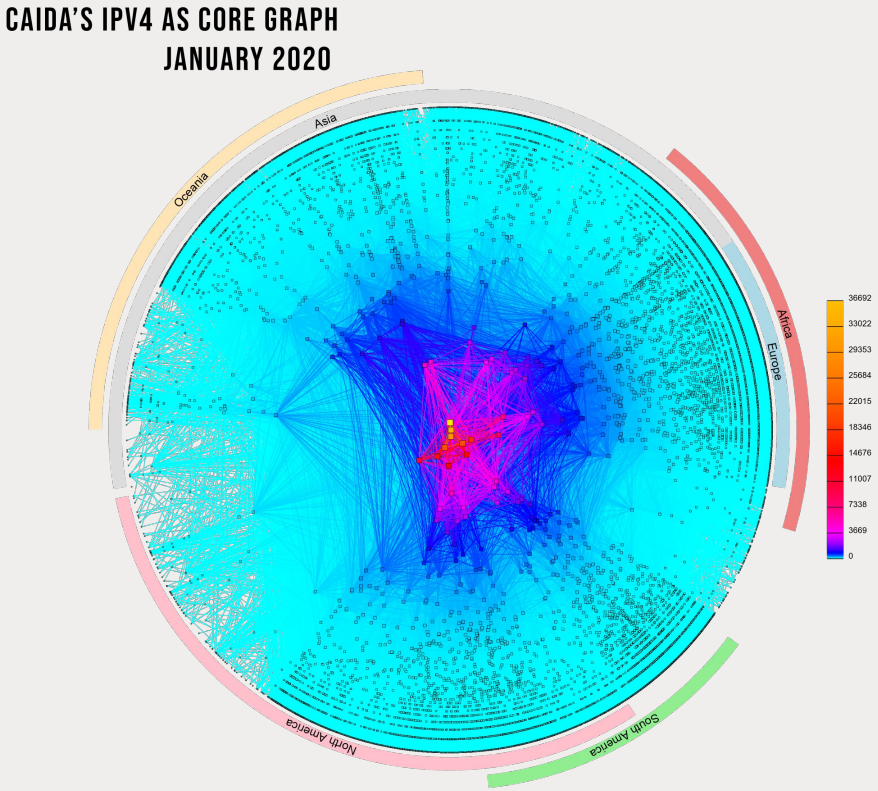
SCION: Secure Path-Aware Internet Routing for Critical Infrastructures

Kevin Meynell, SCION Association <kme@scion.org>

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 (route leaks and hijacks)
- Sending and receiving networks typically cannot decide the path that intermediate routers direct their traffic across the Internet
- BGP can send traffic through different jurisdictions thereby creating opportunities for surveillance, compromising security and making regulatory compliance complex
- BGP failover is relatively slow with convergence times of up to 3 minutes



INTERNET ROUTING: WHAT ARE THE PROBLEMS?

Some info @ a glance

EVENT	EXPLANATION	REPERCUSSIONS	EXAMPLE
ROUTE LEAK	Usually accidental but sometimes malicious redirection of traffic through an unintended path. A network operator with multiple links announces to an upstream provider that it has a route to a destination through another link.	Traffic is delayed or never delivered, with the intermediate network(s) carries unintended traffic. Can be used for MITM including traffic inspection and/or modification.	In Jun 2019, Verizon accepted incorrect routes from DQE Communications that diverted traffic destined for Cloudflare, Facebook & Amazon through small ISP.
ROUTE OR PREFIX HIJACKING	A network operator or attacker impersonates another network operator by falsely announcing ownership of IP prefixes and/or ASNs. Re-routes traffic by offering a shorter or more specific path for malicious or censorship reasons.	Traffic is forwarded to the wrong destination. Can be used for Denial-of-Service attacks, traffic interception or network masquerading.	Feb 2022 – KLAYswap Cryptocurrency hijack Apr 2018 - Amazon Route 53 hijack Feb 2008 - YouTube hijack
DATA SOVEREIGNTY BREACHES	BGP routing can, and often does, send traffic across geopolitical boundaries.	Can breach national and supra-national (e.g. GDPR) data protection legislation.	May 2023 – Australian healthcare data transferred through another country.

HOW IS THIS BEING ADDRESSED?

Some info @ a glance

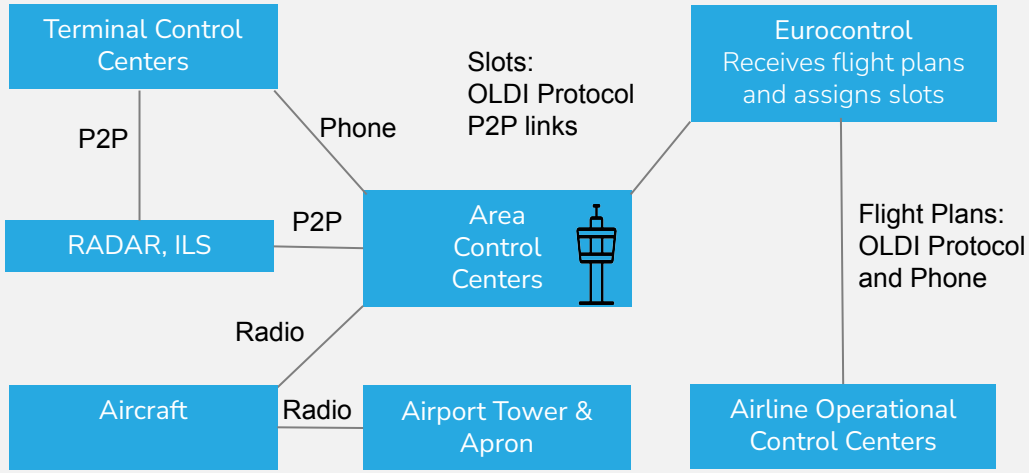
EVENT	EXPLANATION	LIMITATIONS
RPKI & ROV Resource Public Key Infrastructure & Route Origin Validation	ROAs (Route Origin Authorisations) provide cryptographic assertions of IP prefix ownership and which ASNs are allowed to originate them. Routers can validate ROAs and generate appropriate route filters.	Requires widespread deployment to be effective (less than 50% of IP prefixes are signed in 2024) Few network operators currently use ROV (5%). Only does origin validation and does not validate paths through the Internet.
BGPSEC 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. Computationally intensive and introduces significant delays in route convergence. Explicit path selection is not possible. Almost no deployment.
ASPA 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 stop-gap technology and not yet an Internet standard. 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

FACTS ABOUT SCION

Dispelling the Myths

Is SCION trying to replace the Internet?

- SCION works with the existing Internet, but aims to address some of the shortcomings of BGP for particular users.
- SCION introduces the concept of trusted ASes and provides greater assurances about inter-domain path security, whilst offering interoperability with the wider Internet as required.

Is SCION just an experimental technology for researchers?

- SCION is already deployed and actively used in production networks including SSFN, SSHN & SCIERA (which is used by research and education networks).
- SCION has commercial and open source implementations.
- The SCION specification is being documented at the IETF.

What are the main use cases for SCION?

- SCION is actively being evaluated by the financial, healthcare, power utility, government, defence, aviation and rail sectors, and is also being considered for time distribution networks.
- Several ISPs and IXPs are considering deployment.

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

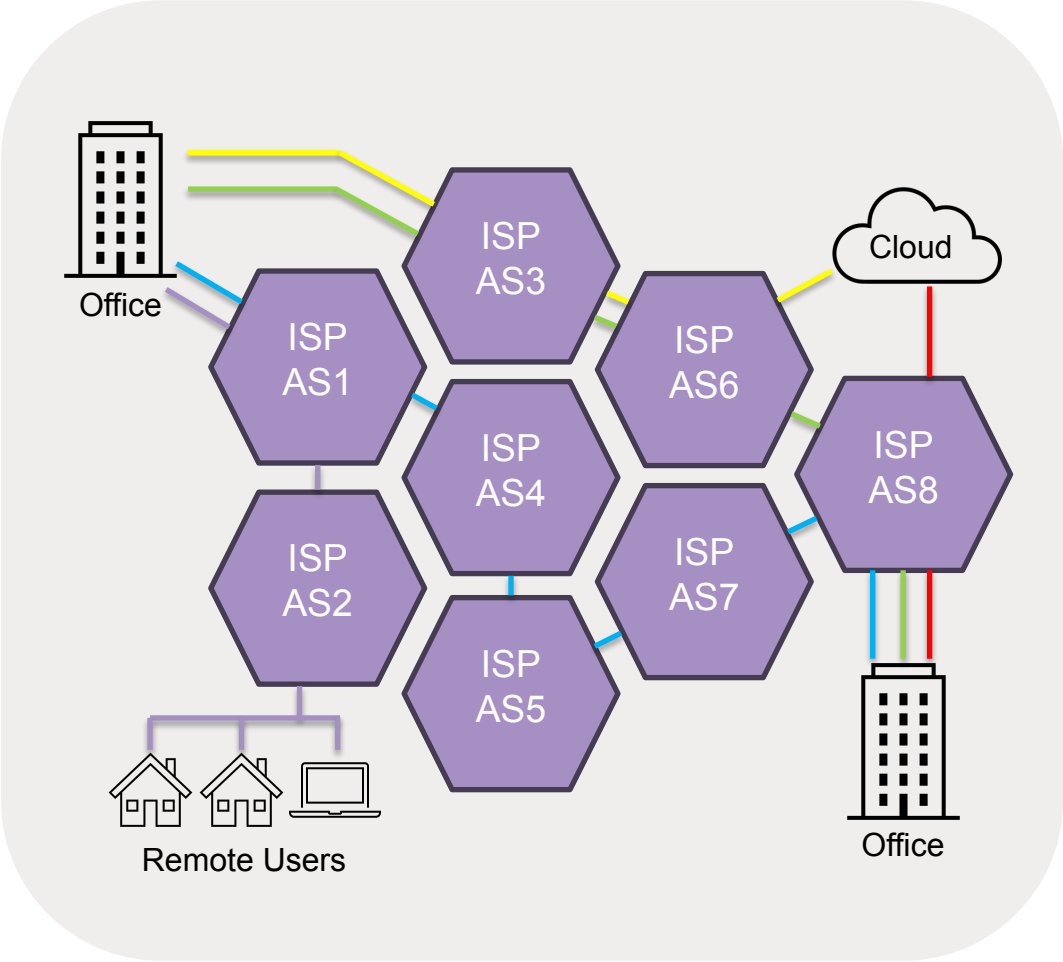
PATH CONTROL

- 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)
- Multiple paths can be used simultaneously

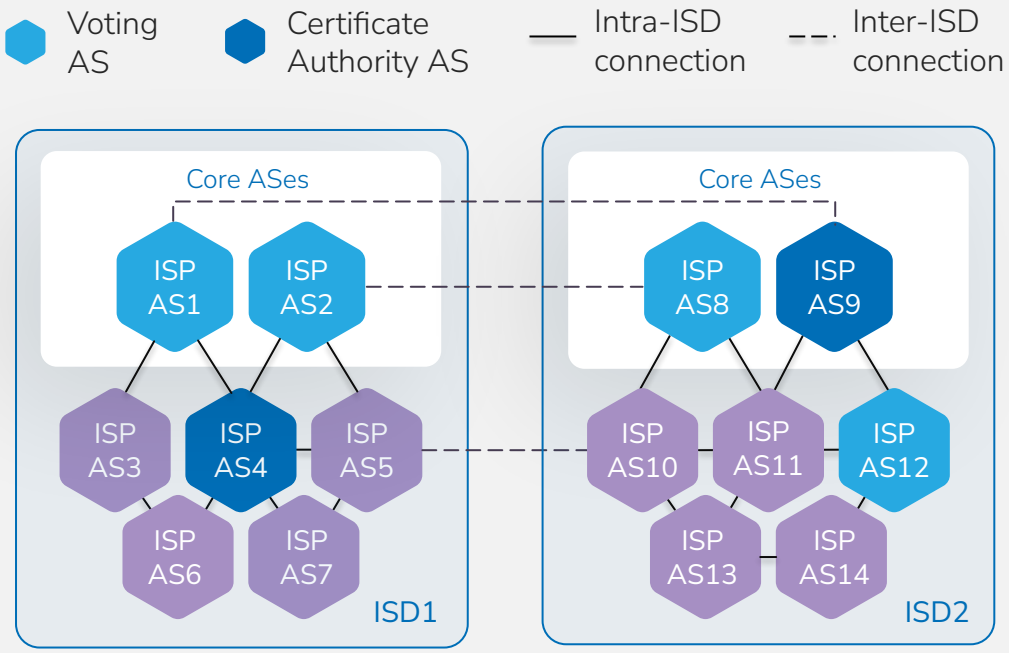
SCION provides benefits similar to leased lines, but in a resilient multi-operator and multipath environment.



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

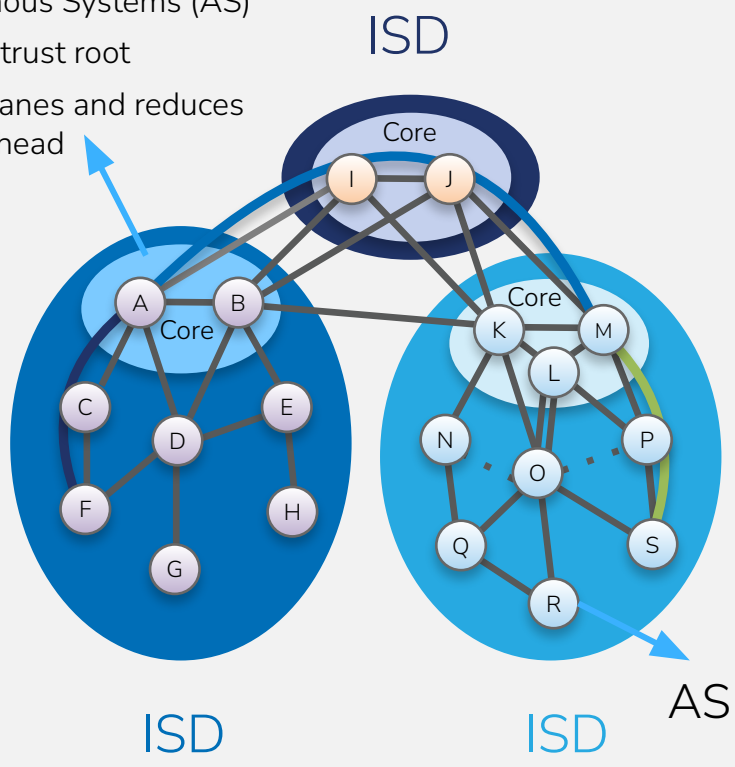
- Establishes paths based on AS rather than prefixes
- Beacon server uses path segment construction beacons (PCBs) to build path segments and routing paths
- Path server stores paths to AS discovered during beaconing
- Endpoints combine path segments to form end-to-end paths
- PKI authenticates path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

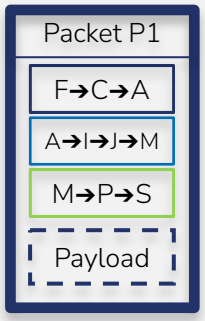
DATA PLANE – PACKET FORWARDING

- Combine path segments into end-to-end path (ISD-AS level)
- 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

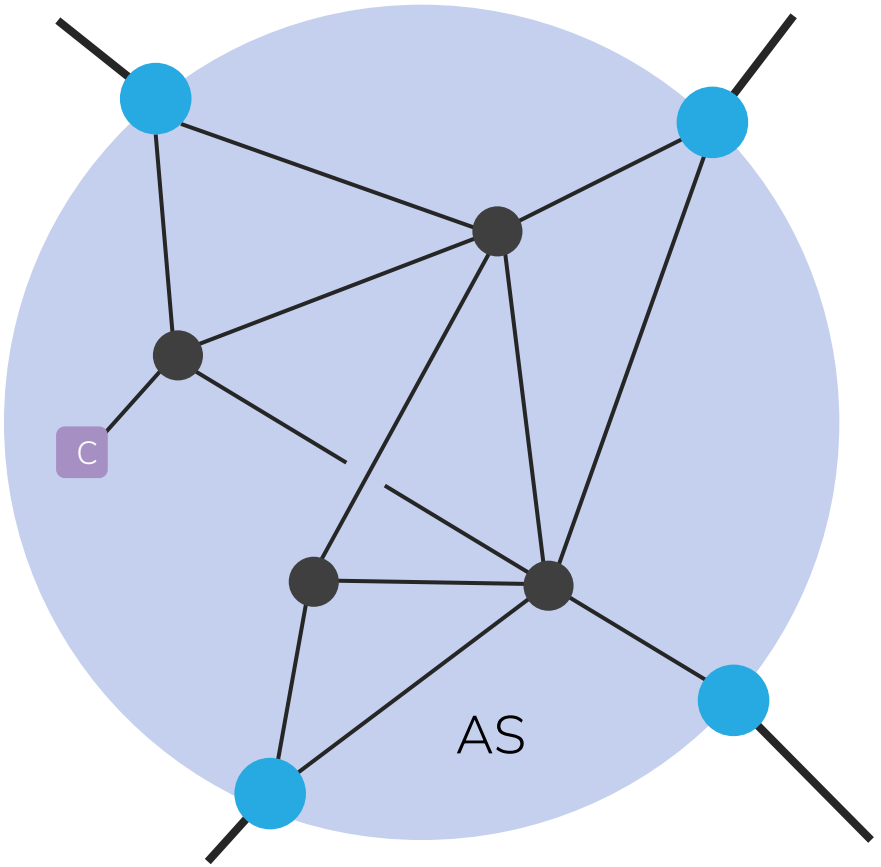




Packet from AS F to AS S

DEPLOYMENT MODEL

SCION Service Provider



C Control Services Border router Internal router

SCION ROUTERS

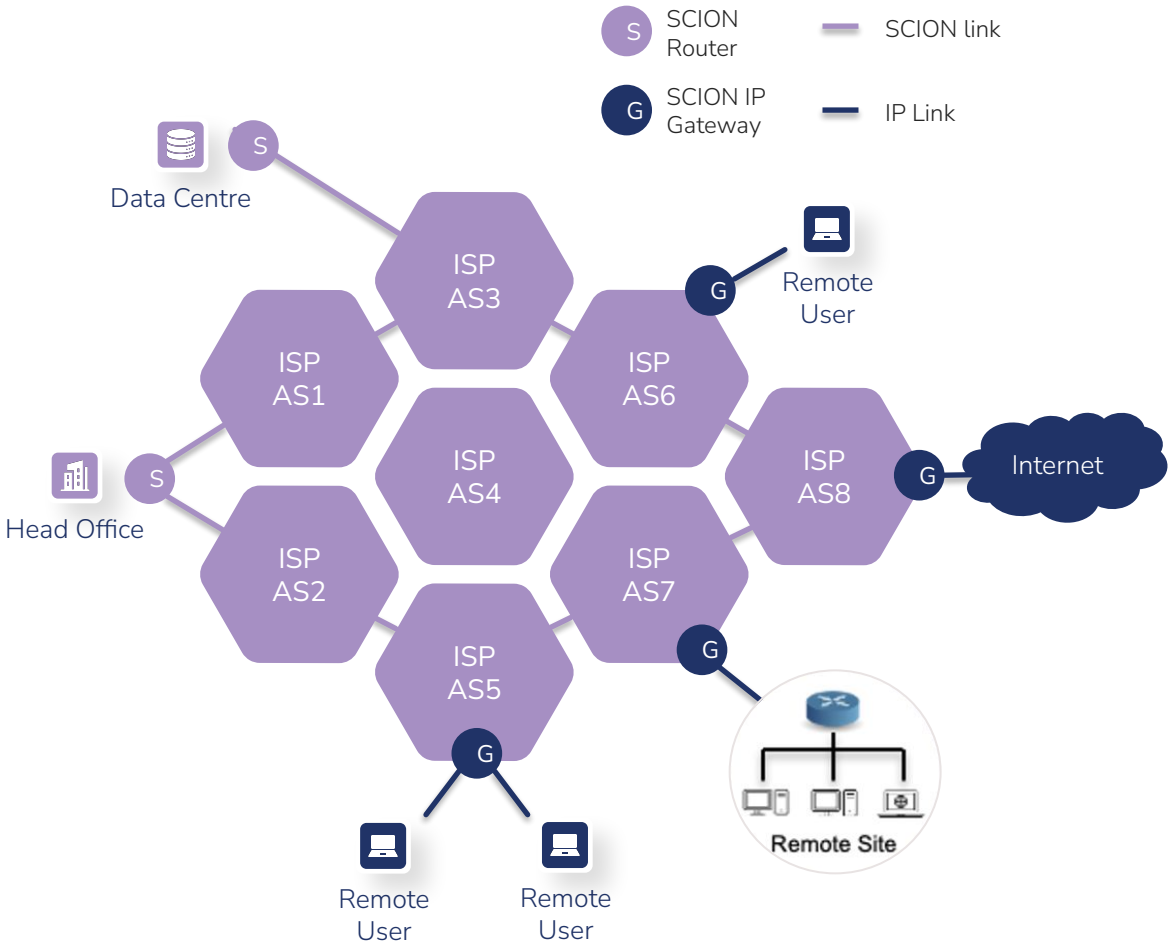
- SCION routers are set up at the borders of an AS
- Border routers peer with other SCION-enabled networks and collect customer traffic
- Control services discover, map and validate network paths
- No change to the internal network infrastructure needed
- Endpoints run a SCION stack
- Legacy endpoints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

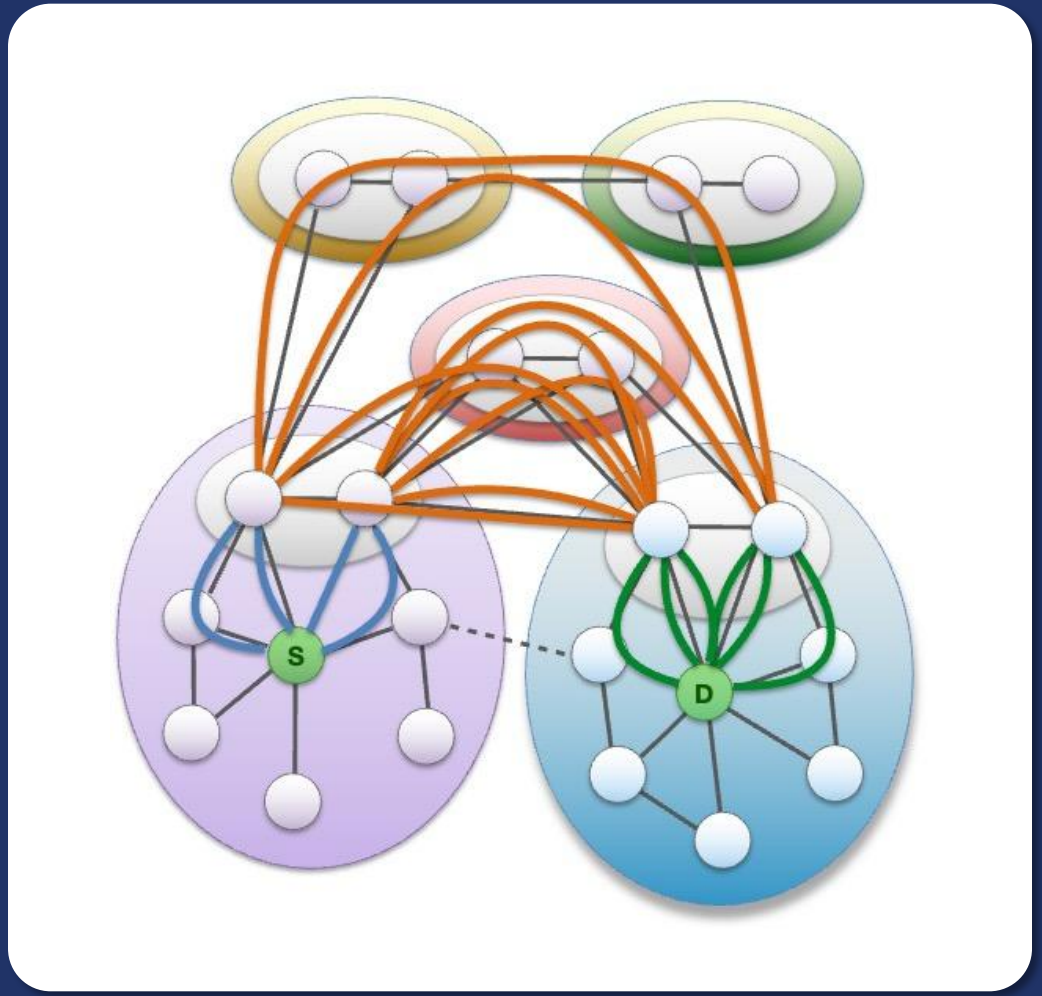
ENTERPRISE DEPLOYMENT

- 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

SCION BENEFITS: FAST MULTI-PATH DISCOVERY & FAILOVER

Advantages over regular Internet

- BGP generally selects routes based on ‘lowest cost’ regardless of whether these are in practice the most optimal or they meet particular requirements.
- With SCION, Leaf ASes only receive and do not forward any beacons. Only core ASes initiate beacons.
- Beaconing does not rely on iterative convergence nor forwarding table updates, allowing rapid path exploration within ISDs.
- The control services discover path segments and assemble these into available paths.
- Tests show path failover to be within 1-2 seconds.
- Applications can choose paths based on optimal characteristics or other parameters, and can also use multiple paths simultaneously.



SCION PERFORMANCE

Comparisons of tested platforms, using AES operations

PLATFORM	CONFIGURATION	PERFORMANCE
Lanner Used by Anapaya devices	L-1515B-4C-8E-64M-EU L-1515B-4C-8E-128M-EU	Edge device up to 1 Gb/s
SuperMicro Used by Anapaya devices	SYS 110D-8C-FRAN8TP-OTO-32 Intel Xeon D-2733NT, 32 GB memory, 6 x SFP28	Core, Edge or Gateway device up to 25 Gb/s
SuperMicro Used by Anapaya devices	SYS 11OD-16C-FRAN8TP-OTO-47 Intel Xeon D-2755TE, 32 GB memory, 2 x SFP28, 6 x QSFP28	Core, Edge or Gateway device up to 100 Gb/s
SuperMicro Tested by Anapaya	SYS-1019D-14CN-RAN13TP+ Intel Xeon D-2177NT, 32 GB memory	Core, Edge or Gateway device up to 10 Gb/s
HPE Proliant Tested by Anapaya	HPE ProLiant DL380 Gen11 Intel Xeon Gold 5418Y, 128 GB memory	Core, Edge or Gateway device up to 25 Gb/s
AMD-based H/W Tested with open-source implementation	AMD Jaguar GX-412TC	Edge device up to 10 Mb/s
Lenovo Tested with open-source implementation	Intel i9-13900, 32 GB memory, 2 x 10 GE (Intel X550T/PCIe x 4)	Core, Edge or Gateway device up to 5 Gb/s

COMPARING SCION WITH OTHER SOLUTIONS

Why not use MPLS, SD-WAN or Segment Routing?

EVENT	EXPLANATION	LIMITATIONS
MPLS Multi-Protocol Label Switching	Provides high reliability and low latency routing with path selection, traffic prioritization, QoS and VPN capabilities. Has isolated control planes and infrastructure that offer DoS protection.	Connectivity is only possible over a single ISP. Designed for point-to-point connectivity so less suited to cloud environments. Requires dedicated infrastructure so unsuitable for many edge locations and remote users. MPLS deployment is declining.
SD-WAN Software-Defined Wide Area Networking	Allows secure private networks to be built using commercially available Internet access provided by different ISPs. Offers some resilience, traffic prioritization and QoS capabilities.	Connectivity is dependent on the underlying Internet connections and thus vulnerable to DoS attacks Each vendor has its own proprietary standards which limit interoperability and encourage vendor lock-in. Limited path control capability.
Segment Routing	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.	Requires MPLS or IPv6 networks. Connectivity is only possible over limited domains. Limited vendor support and interoperability. Lack of cryptographic verification of paths. Configuration and management is complex and requires understanding of underlying networks.

FAQs

Answering the questions about SCION

How does SCION know when a specific route is vulnerable, unsafe, or congested?

- SCION routes traffic on ‘trust domains’ (known as Isolation Domains) formed from groups of trusted ISPs (e.g. SSFN).
- Traffic policies can be configured so that traffic never leaves this trusted domain, with cryptographic authentication ensuring that the intended paths are actually followed.

How does the dynamic routing work? Are multiple paths continuously being assessed for integrity, availability and performance?

- SCION endpoints can use multiple paths across multiple ISPs
- Available paths are always calculated so an alternative path is usually immediately available when a link fails.
- Endpoints continuously assess path performance and may switch paths to meet certain requirements.

What is the response time in the case of a network router failure, or DDoS attack, etc?

- Failover can be as fast as the round-trip time
- Link failures can be detected by endpoints or signaled by the network. Failover parameters are configurable by policies.

FAQs

Answering the questions about SCION

Will SCION help against a DDoS attack?

- Some SCION networks are isolated from the Internet, reducing attack surface.
- On public SCION networks, If an Internet path is unavailable due to a DoS attack, SCION can quickly switch to alternative paths.

Is it compatible with both IPv4 and IPv6, and/or does it put constraints on protocol stacks and application services to be used?

- SCION works with both IPv4 and IPv6
- SCION Gateways are normally deployed at the edge of SCION networks to translate packets from IP-to-SCION and vice-versa. This is also where the ‘magic’ happens in terms of traffic policies, monitoring and switching paths.

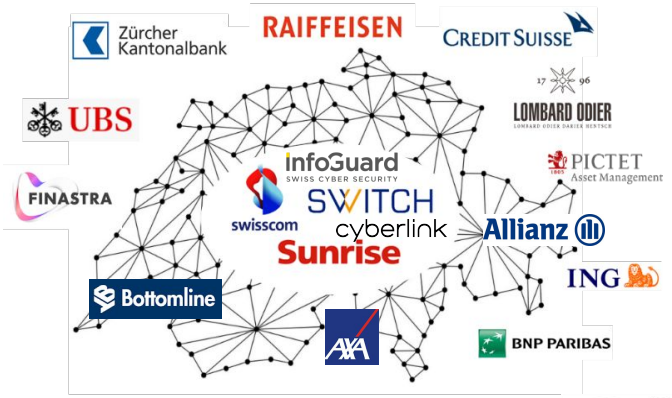
Is SCION compatible with (New)PENS?

- IP-based applications or VPNs run over a SCION network.
- SCION offers the advantage of supporting a multi-ISP and inter-domain environment, with end-to-end capabilities.

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

- Swiss inter-banking network among 300+ finance institutions, handling ~200 billion CHF/day worth of transactions between banks and other critical real-time financial services

  Governed by the Swiss National Bank and SIX



Andrea M Maechler · 1st
Member of the Governing Board...
1mo ·

A great initiative, which will allow us to build a secure, more cost efficient and resilient «any-to-any» communication network for the Swiss RTGS and other critical financial markets infrastructures in Switzerland. We look forward to finalizing the pilot project with Anapaya Systems and SIX.

REASONS FOR USING SCION:

- Enforceable governance with SCION's trust concept
- Multi-ISP
- Geofencing
- Performance-based routing & fast failover

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

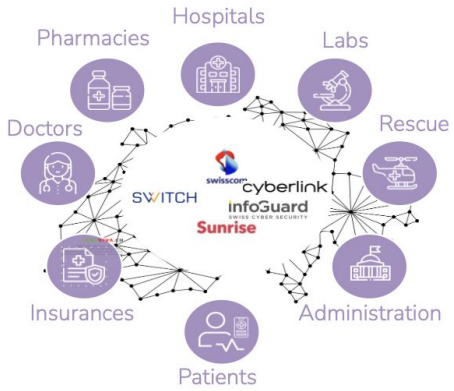
PAYMENTS

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 National University of Singapore

SSFN DEPLOYMENT EXPERIENCES

WHY WAS SCION ADOPTED?

- SIX clients previously used Finance IPNet or point-to-point connections. Finance IPNet was reaching end-of-life.
- IPNet did not limit connections to the rest of the Internet (e.g. no route controls) and offered limited protection against cyber risks.
- Point-to-point connections lacked flexibility and had single points of failure.
- Lacked strong governance and geofencing.

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.

IXP DEPLOYMENT: SwissIX

SwissIX is first IXP to offer native SCION interconnection

Why should IXPs support SCION?

- SSFN has already deployed SCION and other European financial networks are considering deployment
- Many legacy critical infrastructures are due for replacement in coming years
- Trusted domains and path security is important in many sectors
- National critical infrastructures require secure inter-operation
- IXPs are key components in the critical infrastructure landscape
- Supporting SCION will encourage deployment

https://www.swissix.ch/services/scion-peering-mesh/

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 under review in the IETF Independent Submission Stream

Specification 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-06
Published: 19 October 2024
Intended Status: Informational
Expires: 22 April 2025
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). One of the basic characteristics of SCION is that it gives path control to SCION-capable endpoints that can choose between multiple path options, enabling the optimization of network paths. The Control Plane is responsible for discovering these paths and making them available to the endpoints.

The main goal of the SCION Control Plane is to create and manage path segments which can then be combined into forwarding paths to transmit packets in the data plane. This document discusses how path exploration is realized through beaconing and how path segments are created and registered. Each SCION Autonomous System (AS) can

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

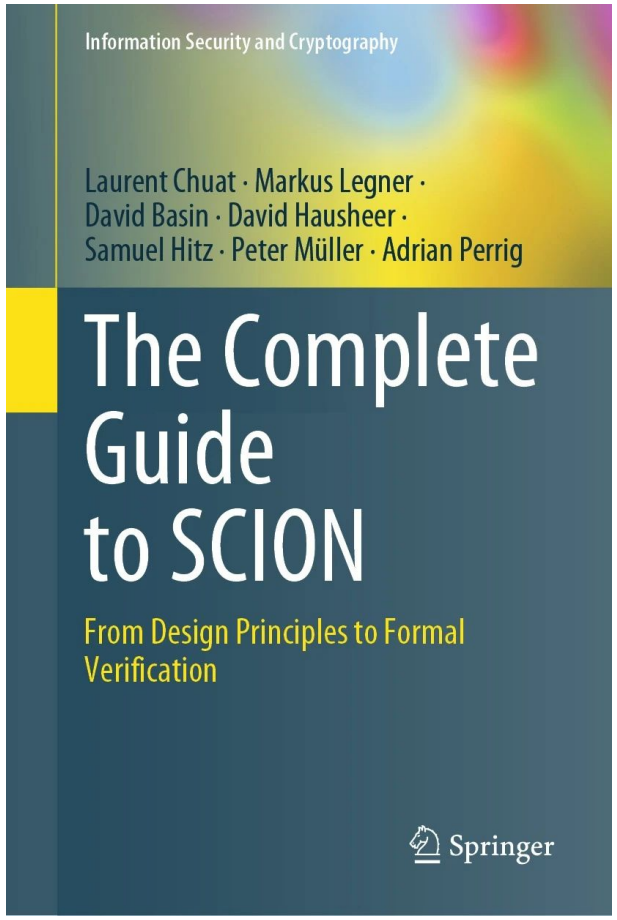
Developing the specifications to implement SCION, with the goal of making it an interoperable Internet standard

OPEN SOURCE

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

SCION TODAY

A growing ecosystem



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/