SCION™
ASSOCIATION

SCION: SECURE PATH-AWARE INTERNET DEPLOYMENT UPDATE

Nicola Rustignoli, SCION Association , nic@scion.org
RIPE 87, November 2023

ABOUT SCION

SCION is a path-aware *inter-domain* architecture providing:

Inter-domain multipath:

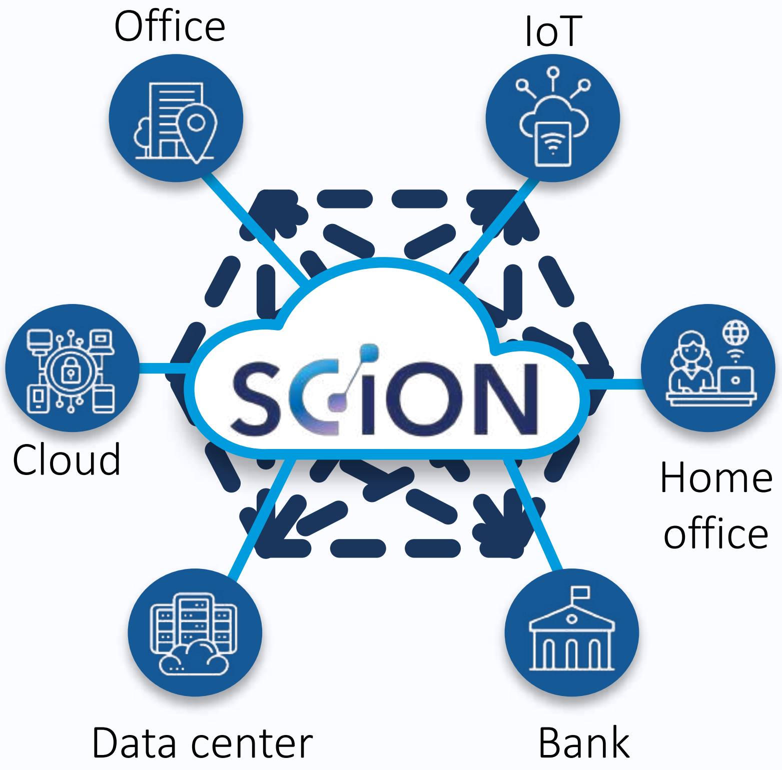
- Performance-based routing
- Fast path failover (can switch to backup path in ~RTT)
- Multi operator (not an SD-WAN)

Endpoint path control:

- source endpoints have choice of AS path (included in packet header)

Paths are authenticated at discovery and **verified at forwarding**

- Hijacking prevention
- Geofencing



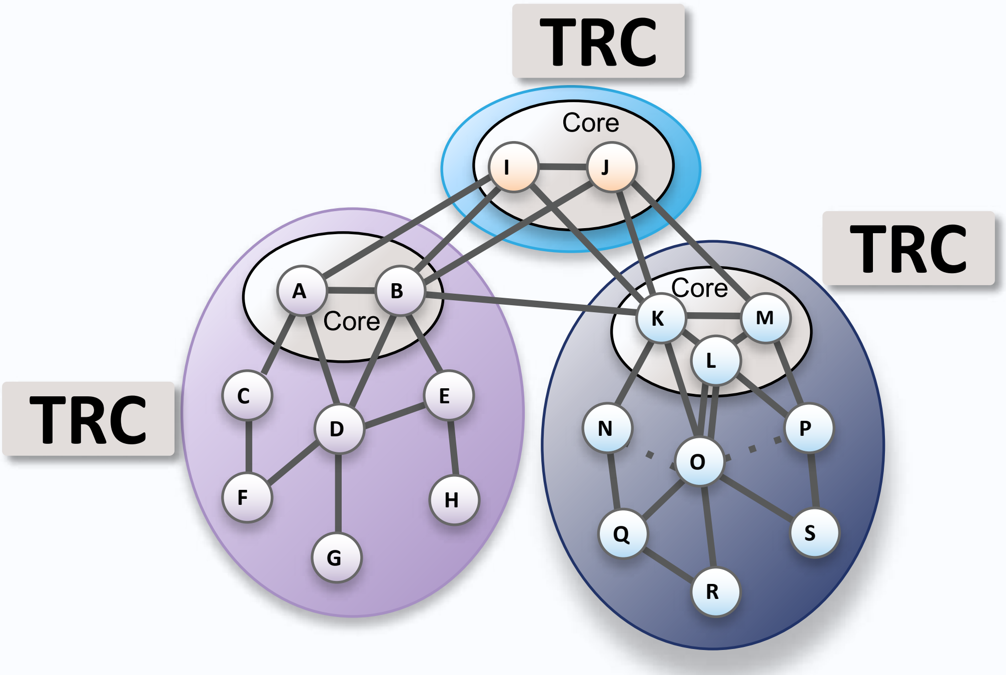
Main use case: Internet-based secure and reliable communication for critical infrastructure ecosystems (e.g. finance, power, blue lights, government, …)

TRUST MODEL

Isolation Domains (ISD)

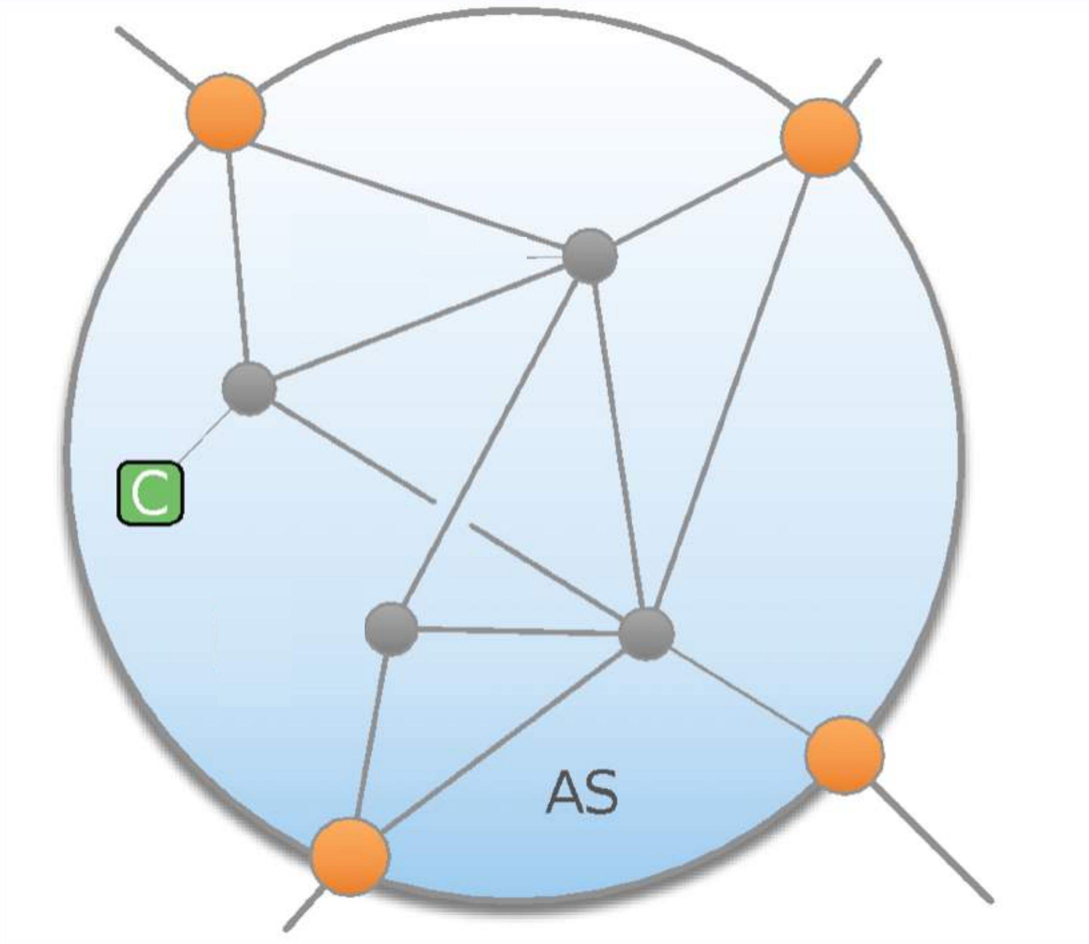
SCION's trust model is based on Isolation Domains (ISD):

- Logical grouping of ASes that share a **uniform trust environment** (for example, a common jurisdiction)
- Each ISD is administered by several core ASes, the ISD core via a voting mechanism
- The ISD core negotiates its own trust policy/contract called Trust Root Configuration (TRC) → No omnipotent CA
- The CAs in an ISD can only create certificates for ASes in this respective ISD



DEPLOYMENT MODEL

A SCION AS



SCION routers are set up at the borders of an ISP

to peer with other SCION-enabled networks

to collect customer accesses

No change to the internal network infrastructure of an ISP needed

Endpoints run a SCION stack, legacy endpoints can leverage gateways.

More deployment scenarios: vendor technical documentation: https://docs.anapaya.net/

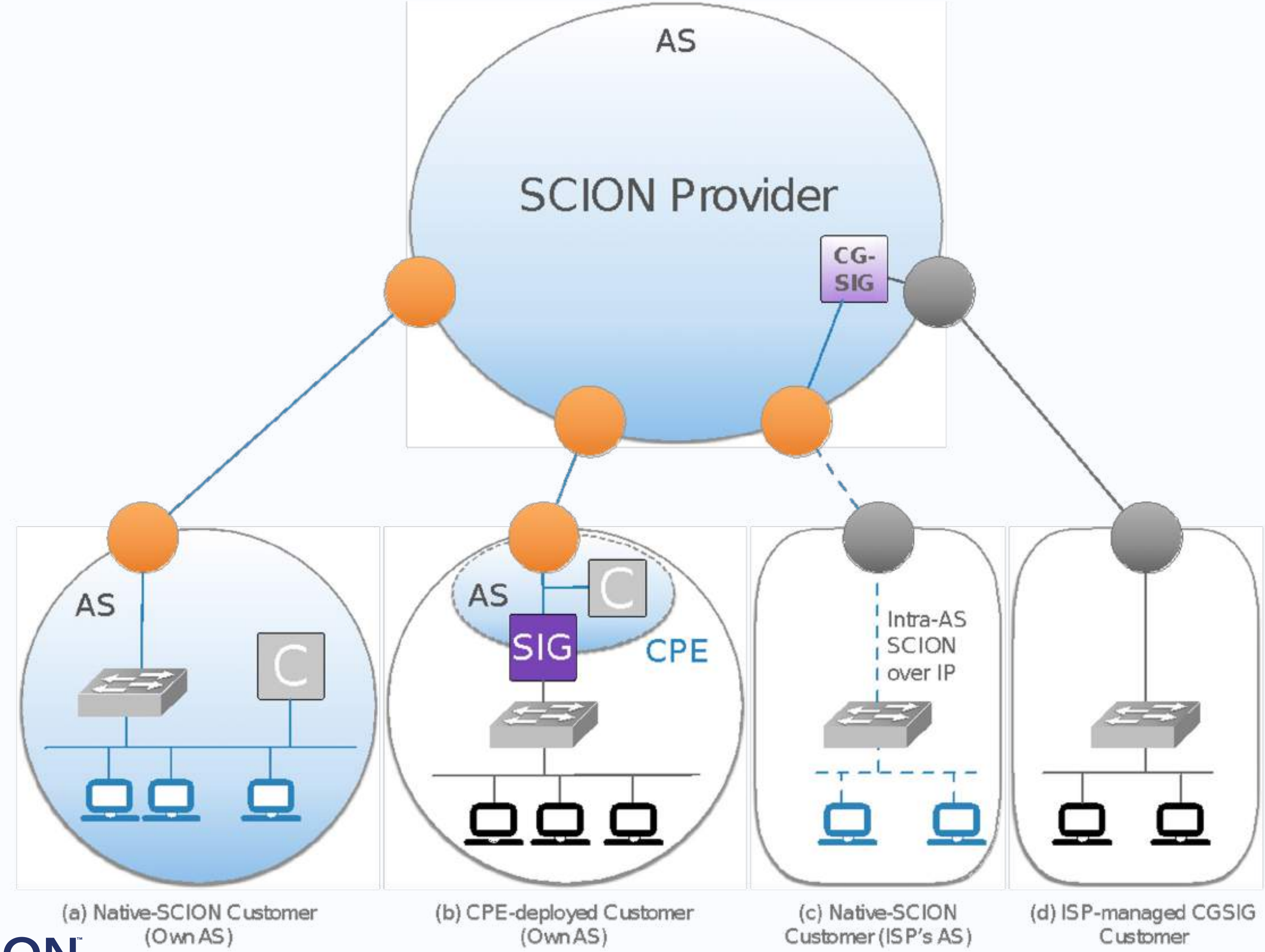
🟩 Control Services

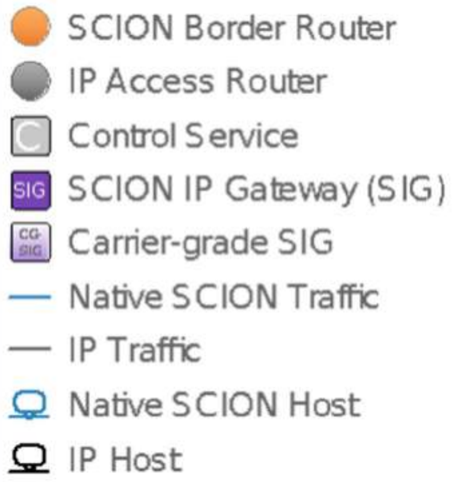
● Border router

● Internal router

DEPLOYMENT MODEL

Customer connection


AS
SCION Provider
CG-SIG
AS
C
AS
C
SIG
CPE
Intra-AS SCION over IP
(a) Native-SCION Customer (Own AS)
(b) CPE-deployed Customer (Own AS)
(c) Native-SCION Customer (ISP's AS)
(d) ISP-managed CGSIG Customer



SCION ASSOCIATION

DEPLOYMENT – THE SECURE SWISS FINANCE NETWORK

Lighthouse use case

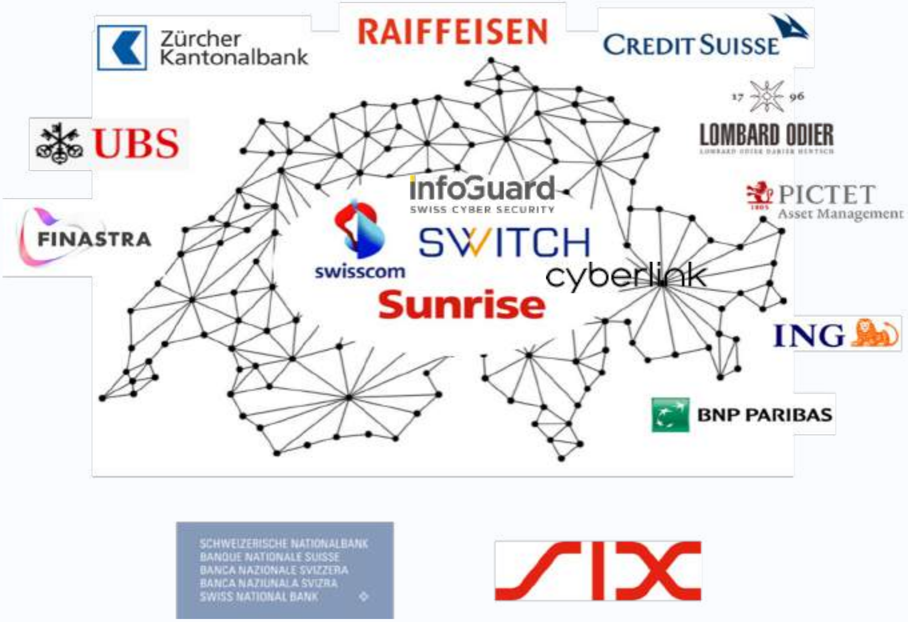
Swiss inter-banking network, handling money transfers between banks and other critical real-time financial services

- Operated by SIX, the Swiss Financial Infrastructure operator

Using SCION because of:

- enforceable governance thanks to SCION’s trust concept
- performance-based routing & fast failover
- Geofencing
- Multi-ISP

Info: https://www.six-group.com/en/products-services/banking-services/ssfn.html



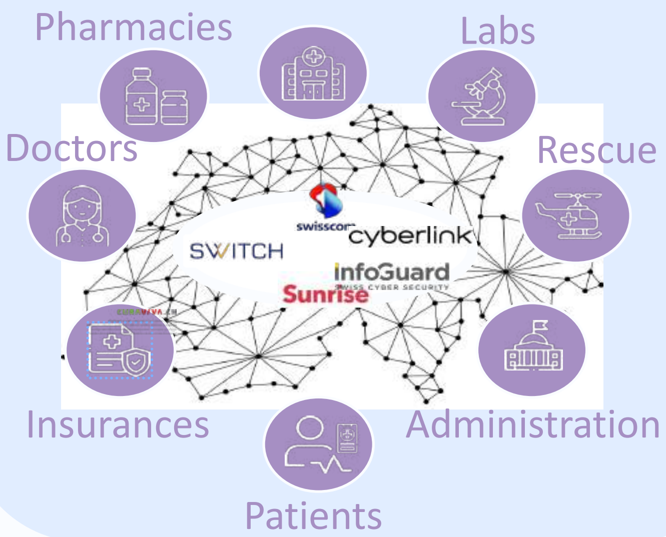
Some facts:

- 300+ finance institutions
- Network handling ~200 B CHF/day
- Migration to SCION-based SSFN ongoing until September 2024

BEYOND FINANCE

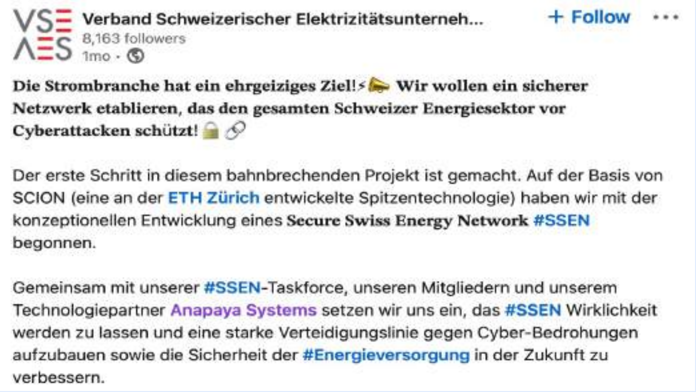
Healthcare

The HIN Trust Circle adopts SCION to interconnect hundreds of hospitals and thousands of doctors



Power

In 2023 the Association of Swiss Electricity Companies explores SCION to connect electricity market players.



Verband Schweizerischer Elektrizitätsunterneh...
8,163 followers
1mo ·

Die Strombranche hat ein ehrgeiziges Ziel!⚡📣 Wir wollen ein sicherer Netzwerk etablieren, das den gesamten Schweizer Energiesektor vor Cyberattacken schützt!🔒🔗

Der erste Schritt in diesem bahnbrechenden Projekt ist gemacht. Auf der Basis von SCION (eine an der ETH Zürich entwickelte Spitzentechnologie) haben wir mit der konzeptionellen Entwicklung eines **Secure Swiss Energy Network** #SSEN begonnen.

Gemeinsam mit unserer #SSEN-Taskforce, unseren Mitgliedern und unserem Technologiepartner Anapaya Systems setzen wir uns ein, das #SSEN Wirklichkeit werden zu lassen und eine starke Verteidigungslinie gegen Cyber-Bedrohungen aufzubauen sowie die Sicherheit der #Energieversorgung in der Zukunft zu verbessern.

Education

The SCION education network connects campuses with path-aware high performance SCION connectivity

KAIST
한국과학기술원
OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
PRINCETON UNIVERSITY
UNIVERSITY of VIRGINIA
ETH zürich
SWITCH
GÉANT
Networks · Services · People
KOREA UNIVERSITY
NUS

SCION TODAY

A growing ecosystem

PRINCETON UNIVERSITY

SIDN

ETH zürich

고려대학교 KOREA UNIVERSITY

NUS National University of Singapore

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

UNIVERSITY of VIRGINIA

CSCS Centro Svizzero di Calcolo Scientifico Swiss National Supercomputing Centre

KISTI www.kisti.re.kr

cyberlink

proximus

interCloud

SWITCH

swisscom

axpo

swissix SWISS INTERNET EXCHANGE

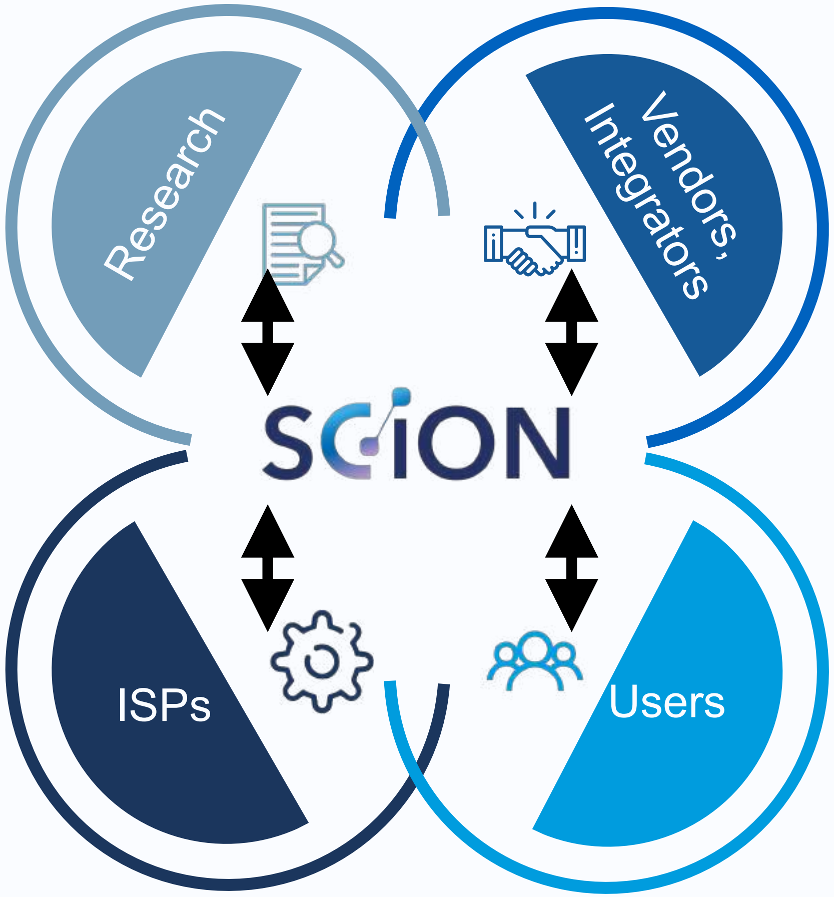
LG U+

vtx

Sunrise

GÉANT

telindus



ANAPAYA

bnc business network communications

Extreme

infoGuard SWISS CYBER SECURITY

Startups

INFOSEC GLOBAL

HIN

eraneos

libC TECHNOLOGIES

zühlke empowering ideas

securosys

RAIFFEISEN

SIX

UBS

armasuisse

ICRC

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA

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

COMMUNITY, IETF & OPEN SOURCE

- Implementations available:

ANAPAYA

Commercial

scionproto/scion

SCION Internet Architecture

80 Contributors · 53 Used by · 3 Discussions · 324 Stars · 140 Forks

Open Source

- SCION ASSOCIATION created by some of the deployers and early adopters
  - Open source
  - Specification
  - Community

- SCION can get even better and more interoperable with community feedback. We are active at the IETF/IRTF. Feedback welcome ☺

SCION @ IETF 118 Prague Hackathon

Current Internet Drafts
draft-dekater-scion-pki
draft-dekater-scion-controlplane
draft-dekater-scion-dataplane
draft-dekater-panrg-scion-overview
draft-rustignoli-panrg-scion-components

NEXT STEPS

And some open questions

- Advance work at IRTF/IETF
- Open source implementation (2024 roadmap)
- Getting more productive deployments outside of Switzerland 🧀
- Explore additional use cases
- More interoperability
- Getting large vendors onboard
- Assign SCION numbers (one day)

QUESTIONS?

Resources

- Dev: docs.scion.org
- Vendor: anapaya.net
- Research: scion-architecture.net

Contact

Nicola Rustignoli
SCION Association
nic@scion.org
http://scion.org

BACKUP

HOW IT WORKS

SCION core components in a nutshell

Data Plane - *Packet Forwarding*

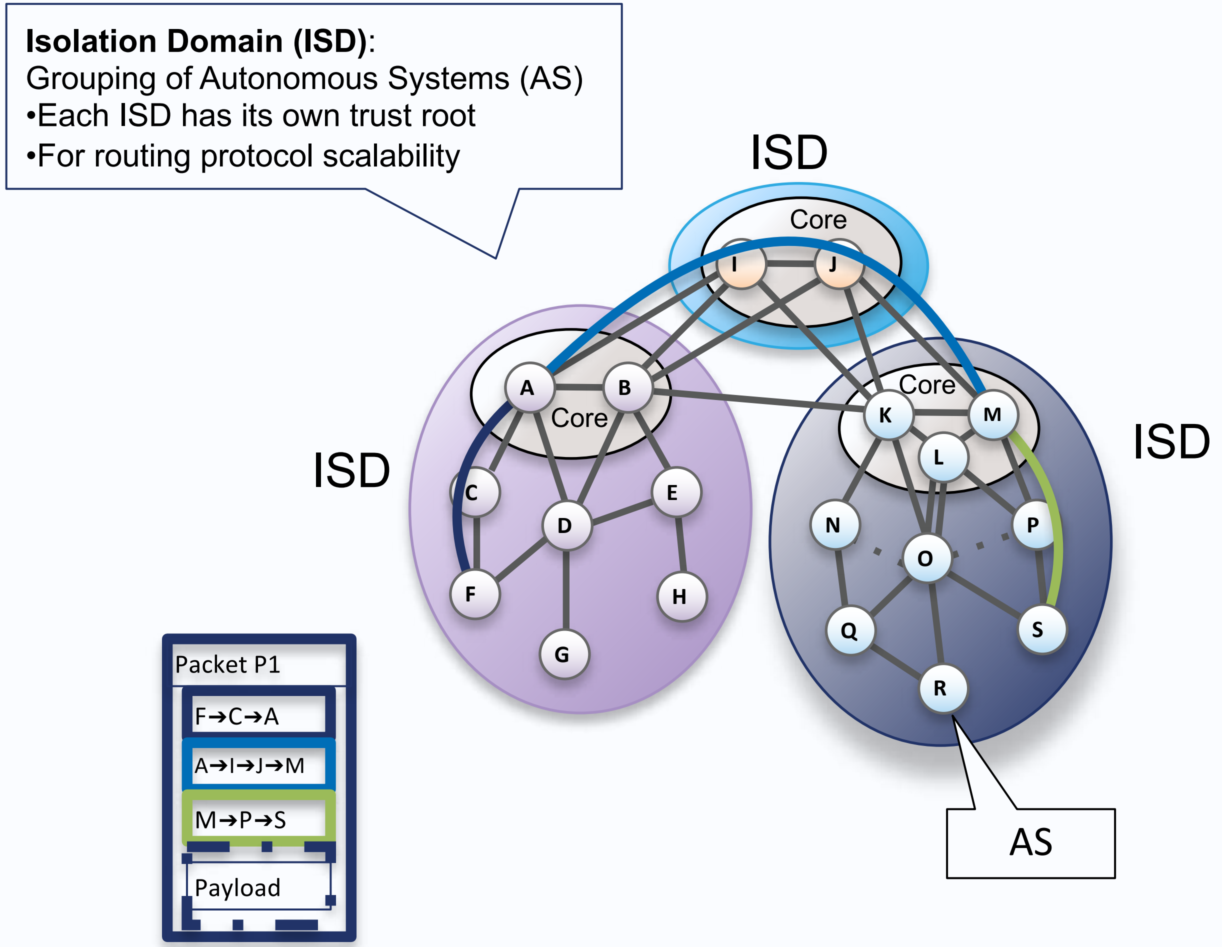
- Combine path segments into end-to-end path (ISD-AS level)
- Packets contain end-to-end ISD-AS path
- Forward packet based on e2e path, agnostic of end-host address

Control Plane – *Inter-Domain Routing*

- Discover valid inter-domain paths
- Construct and disseminate path segments
- Routing is based on <ISD>-<AS> tuple as “locator”
- Intra-AS communication reuses existing data plane and routing (e.g., IPv6/IPv4)

Control Plane PKI (CP-PKI) - *Authentication*

- Authenticate path information
- Used by control plane
- Basis for unique ISD trust model



Isolation Domain (ISD):
Grouping of Autonomous Systems (AS)
•Each ISD has its own trust root
•For routing protocol scalability

Packet from AS F to AS S

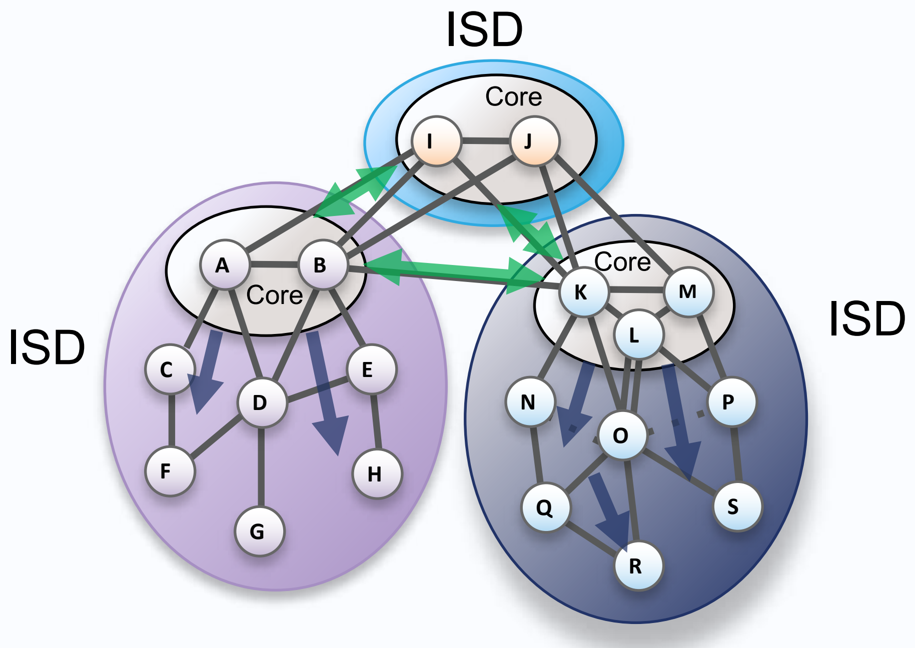
SCALABILITY

Control plane:

- Grouping ASes into ISDs (each being an isolated control plane)
- Hierarchical beaconing (**core** / **intra-ISD**)
- AS-level routing
- No control-plane operations on routers

Data plane:

- Push-based connectivity establishment with pull based path lookup
- No inter-domain forwarding tables on routers
- One AES operation per packet for Message Authentication Code verification

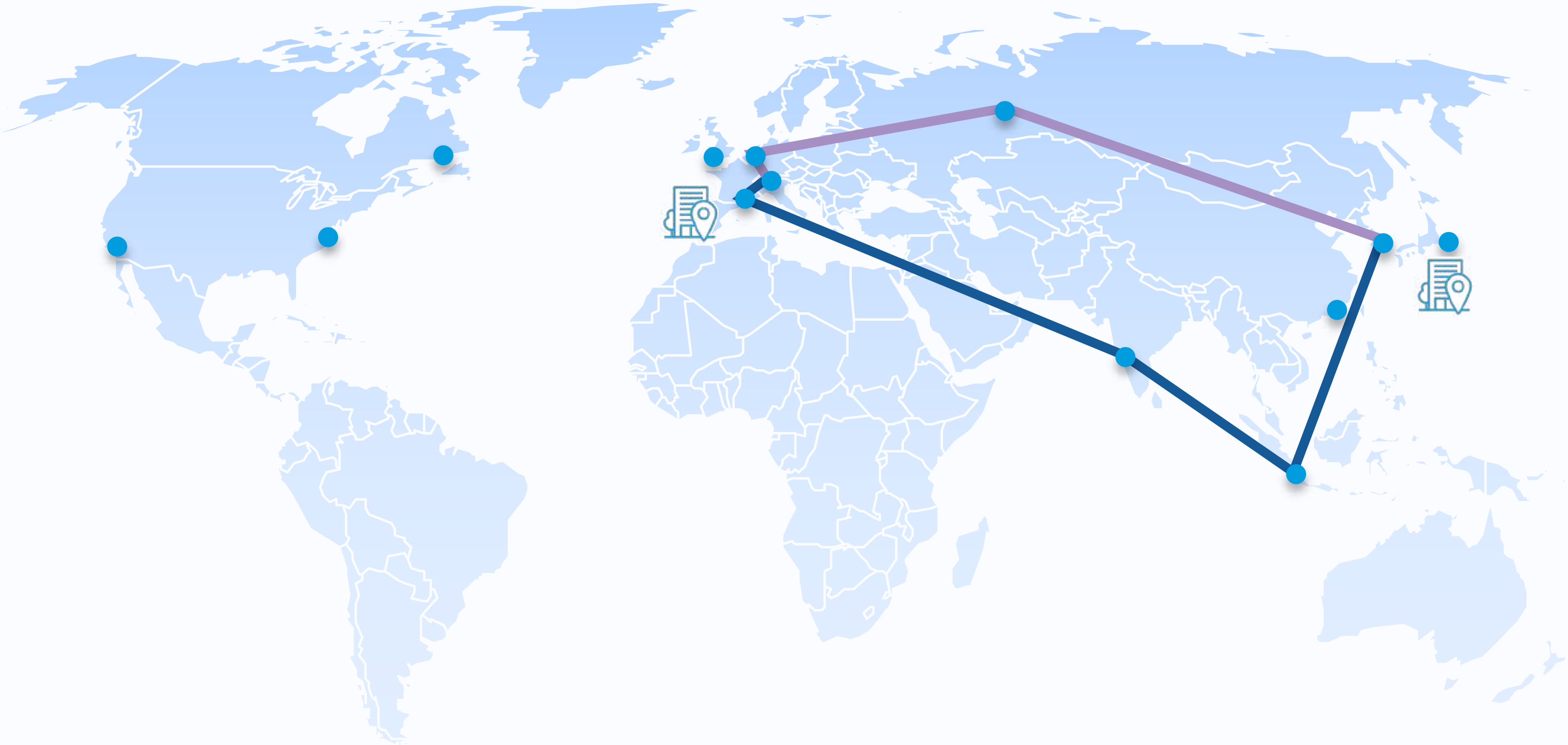


For more:

- Krähenbühl, Cyrill, et al. "Deployment and scalability of an inter-domain multi-path routing infrastructure.", CoNEXT 2021
- de Ruiter, Joeri, and Caspar Schutijser. "Next-generation internet at terabit speed: SCION in P4." CoNEXT 2021.

USE CASE: ENTERPRISE TRAFFIC MANAGEMENT

Performance-based routing & path control



VoIP
(latency optimised)

Generic traffic
(cost optimised)

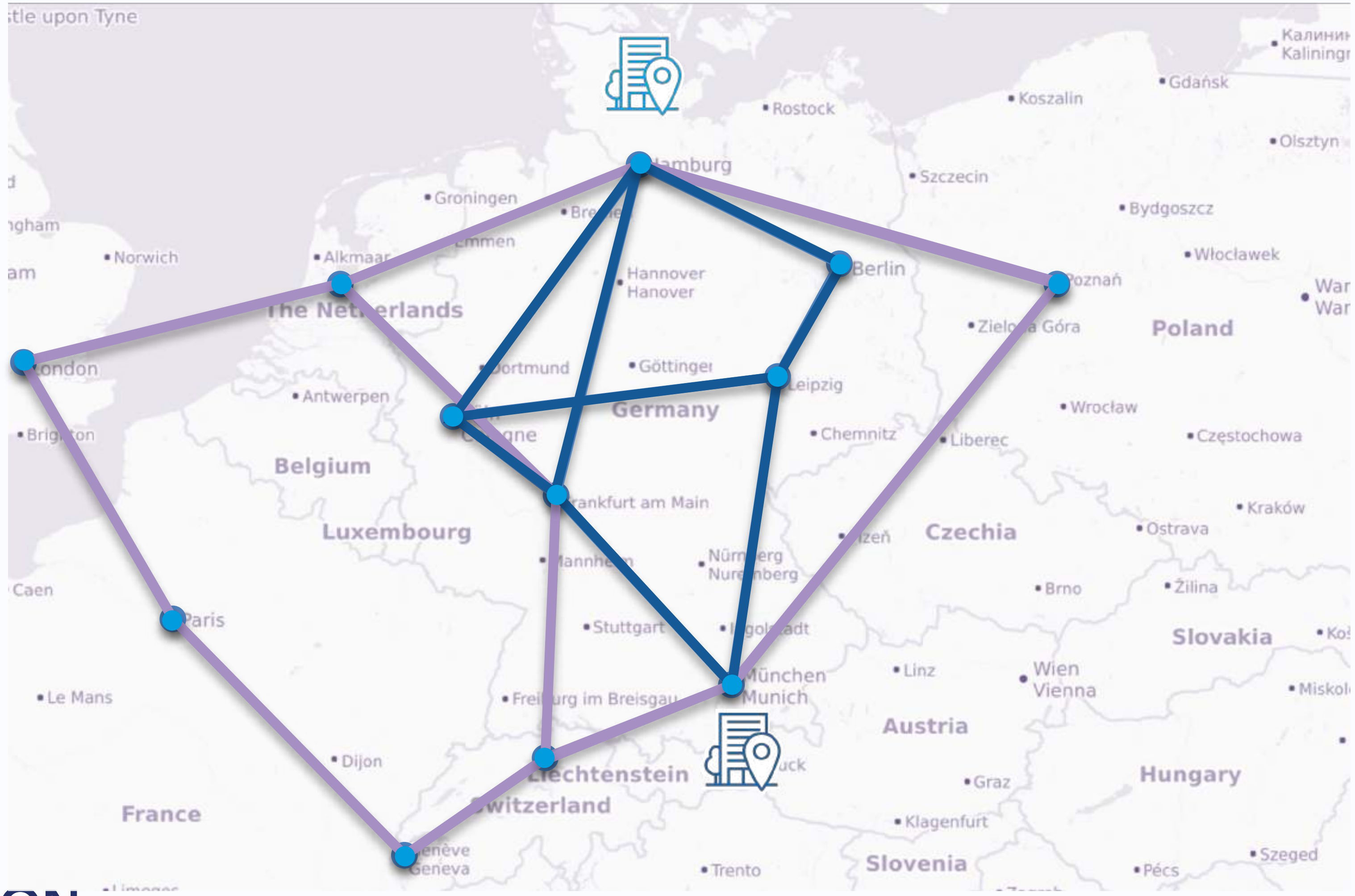
Optimization criteria

- Latency
- Bandwidth
- Jurisdiction
- CO_2 (experimental)

SCION
ASSOCIATION

USE CASE: GEOFENCING

Keeping traffic within jurisdiction



✕ Non-compliant paths

✓ Compliant (sovereign) paths

SCION ASSOCIATION

USE CASE: PATH VALIDATION

Experimental extensions

Property	Approach	Component
Path authorization (hop by hop)	Information at **each hop is authenticated with a MAC** (Message Authentication Code), checked by border routers at forwarding. Each AS only forwards traffic on paths that are explicitly authorized by the AS.	Standard SCION
Proof of Forwarding	EPIC adds **short *per-packet* MACs at each SCION hop**. Source authentication and path validation are enabled by the additional use of efficiently derivable symmetric keys.	EPIC extension, L3 [1]
Trust-enhanced networking	Packet headers are extended with policies **telling border routers which intra-AS path to forward the packet**, so that endpoints can select routers/ASes with specific path policies. Inter-domain paths are this way mapped to policy-compliant intra-domains paths. Per-AS attestation done by a third part.	FABIRD extension [2]

1. Legner, Markus, et al. "EPIC: every packet is checked in the data plane of a Path-Aware Internet." 29th USENIX Security Symposium (USENIX Security 2020).
2. Krähenbühl, C., Wyss, M., Basin, D., Lenders, V., Perrig, A. and Strohmeier, M., 2023. FABRID: Flexible Attestation-Based Routing for Inter-Domain Networks. (USENIX Security ‘23)