

The SCION Inter-Domain Routing Architecture

A journey from research to deployments, IETF, and more

12-FEB-2024

SCION™

Adrian Perrig, Network Security Group, ETH Zürich

- Professor @ Carnegie Mellon University 2002-2012
- Technical director CyLab 2007-2012
- Professor @ ETH Zurich 2013—
- Founder and board member Anapaya Systems
- Head of advisory board of SCION Association
- Advisor to Mysten Labs
- Fellow of ACM and IEEE

- Main project since 2009: SCION secure Internet architecture
 - Secure control and data plane
 - PKIs: control-plane and TLS
 - Built-in DDoS defense mechanisms
 - Multipath communication system
 - Secure time synchronization system
 - ...



A new era for Internet technologies?

- AR / VR with haptic feedback
- IoT for critical infrastructure
- Interactive telepresence
- 3D hologram imaging
- Immersive games
- ...

The unpredictability of the future is the only certainty we can have



Image source: Siemens, A new era for the Internet of Things

Internet Routing Challenges: Availability

This SLA and any applicable Service Levels do not apply to any performance or availability issues:

- 1. Due to factors outside our reasonable control (for example, **natural disaster, war, acts of terrorism, riots, government action**, or a **network** or device **failure** external to our data centers, including at your site or **between your site and our data center**);...*

Microsoft Azure SLA

Difficulties in Deployment

New technologies lacking early adopters' incentives ...

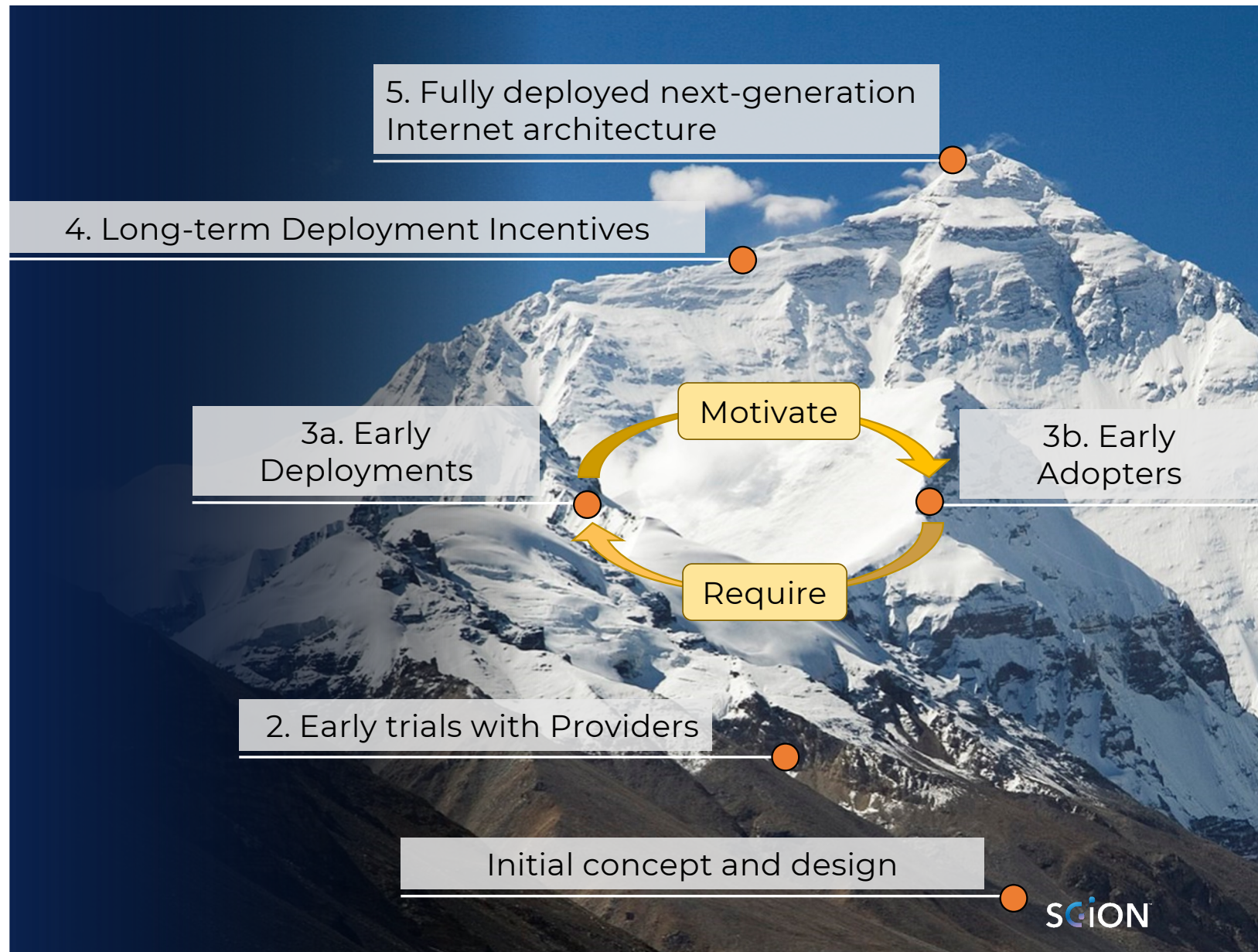
Egress filtering
BGPsec
DNSsec



... experience deployment challenges in the real-world

In this presentation...

We explore a path towards a next-generation Internet



What is SCION?

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

Inter-domain multipath routing:

- Rapid failover (switch to backup path in ~RTT)
- Multi-operator (not an SD-WAN)

Path control:

- Source endpoints can select AS path (included in packet header)

Paths are authenticated at discovery and verified during forwarding

- High assurance that packets follow path
- Hijacking prevention
- Geofencing

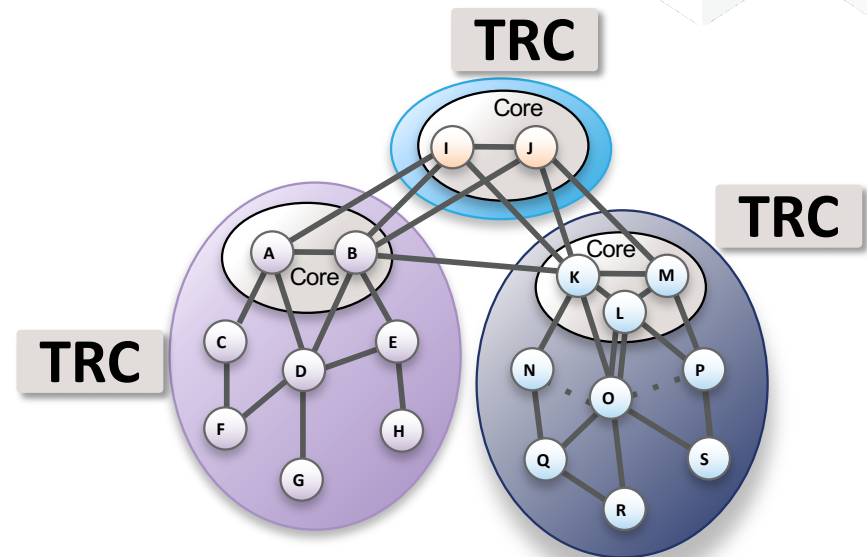


Internet-based secure and reliable communication for critical infrastructure ecosystems
(in production use for financial services, education, healthcare, government, ...)

Trust-enhanced networking

Trust model based on fault 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 ASes via a voting mechanism. These are known as **core ASes** and form the **ISD core**
- Every ISD has its own trust root specified in the Trust Root Configuration (a collection of X.509 certificates with ISD information) - negotiated by the ISD core 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



SCION Next-Generation Internet

Path-based Network Architecture Overview

Control Plane - Routing

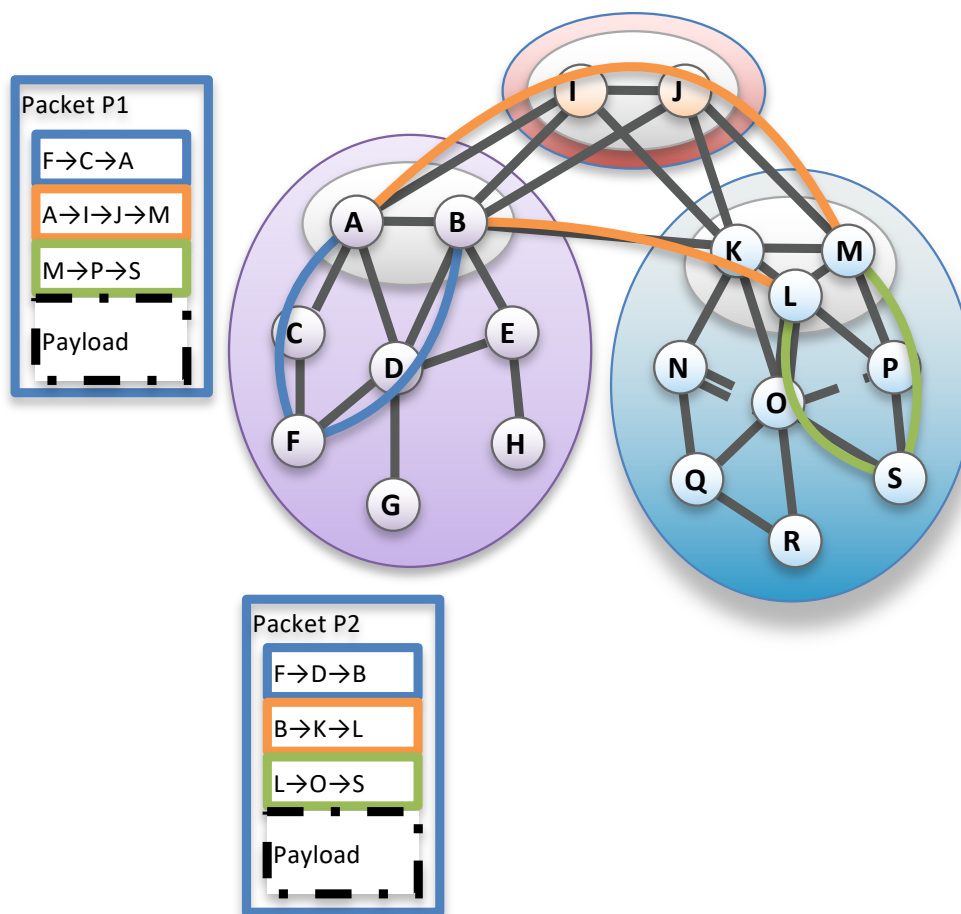
- **Constructs** and **Disseminates** Path Segments

Data Plane - Packet forwarding

- **Combine** Path Segments to Path
 - Packets contain AS-level path
 - Routers forward packets based on path
- Simple routers, stateless operation

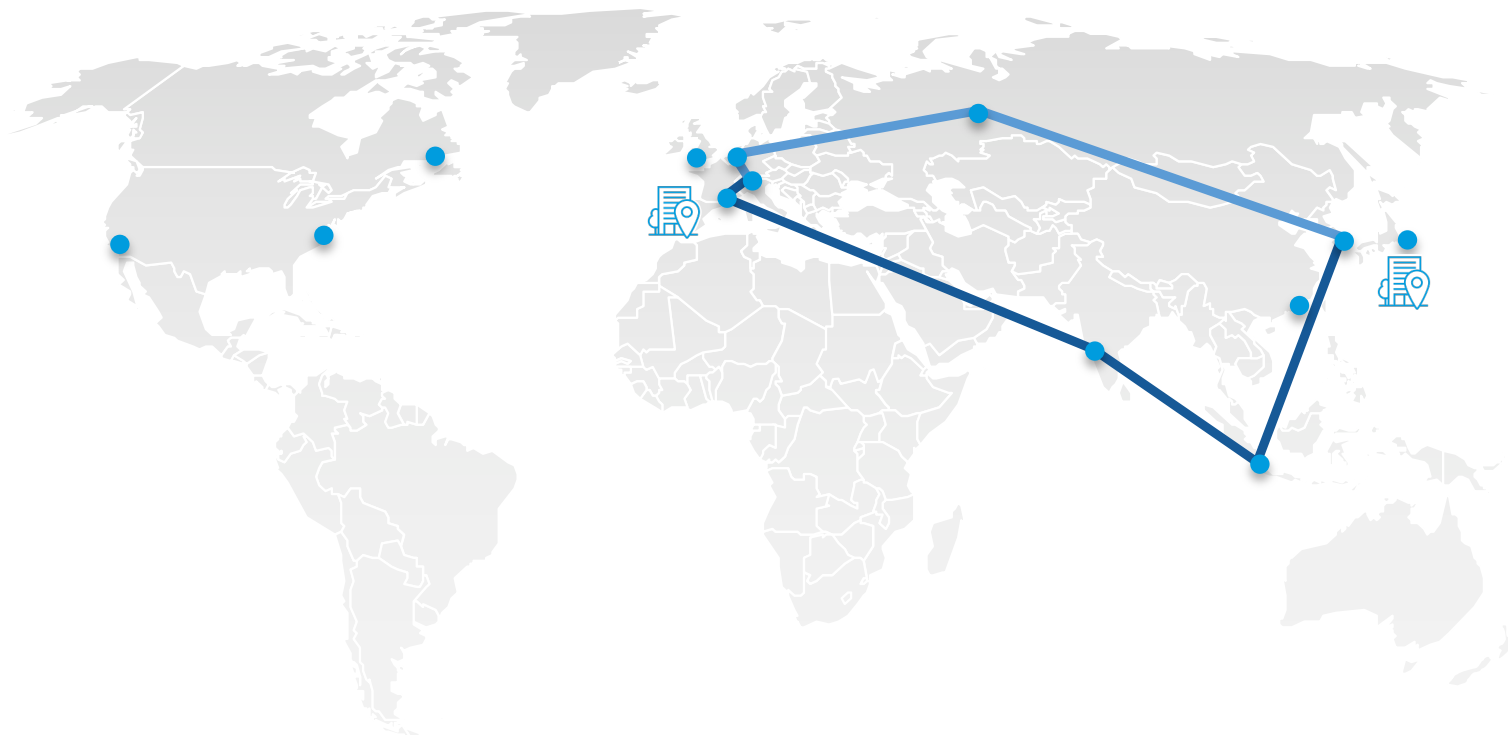
Control Plane PKI - Authentication

- **Authenticate** path information
- Basis for unique ISD trust model



Use case: Enterprise Traffic Management

Performance-based routing & path control

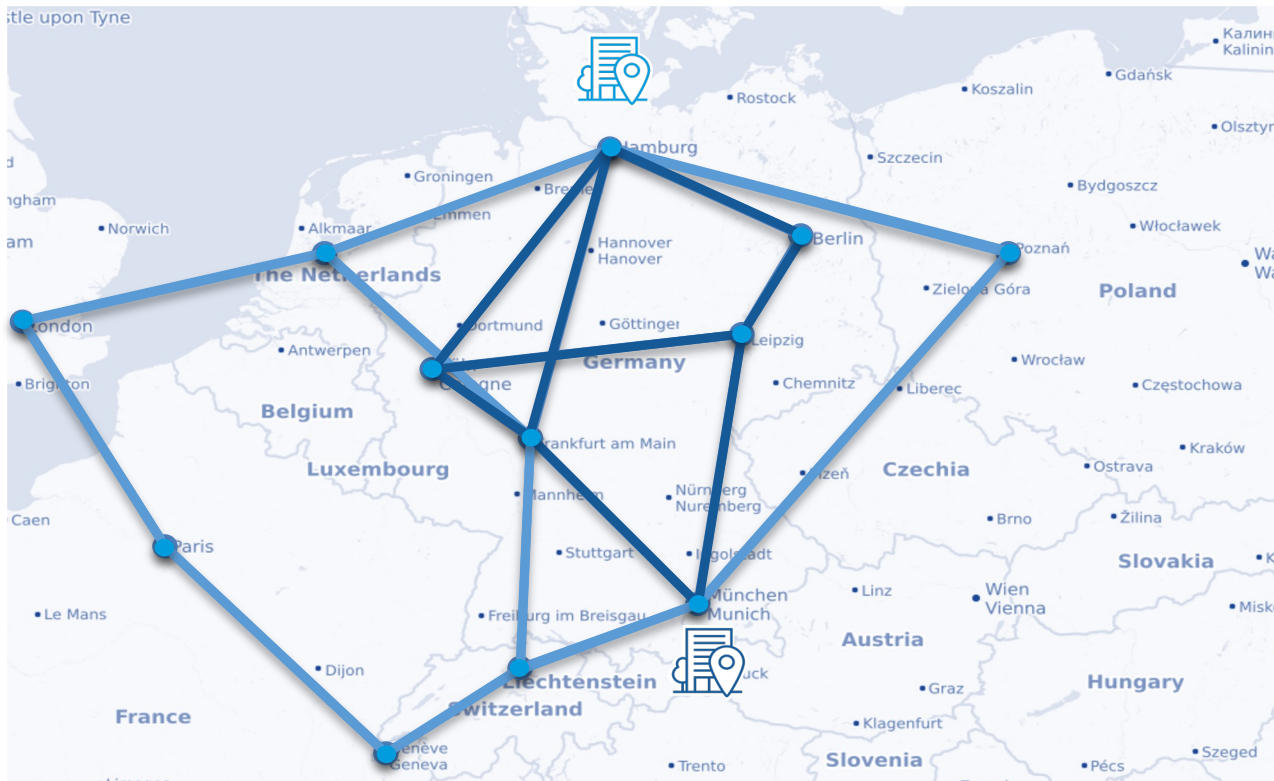



Optimization criteria


- Latency
- Bandwidth
- Jurisdiction
- CO₂

Use case: Geofencing

Keeping traffic within jurisdiction



 Non-compliant paths

 Compliant (sovereign) paths

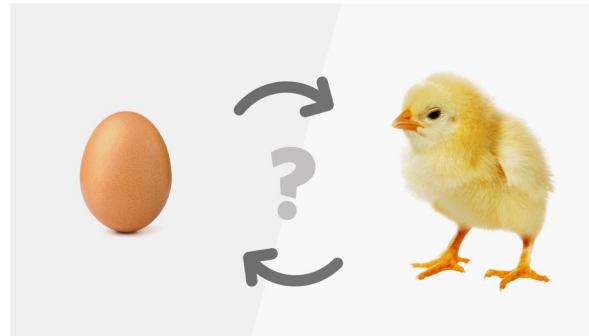
Use Case: Path Validation

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)

This seems impossible to deploy!

Need early adopters
deploying the
architecture



Need initial deployment to
convince early adopters



Need long-term incentives for providers

New opportunities to generate revenue

Reduce operational network cost

From the Lab to ISPs Selling Products

SWITCH
Services ▾ Stories ▾ About us ▾
EN ▾
SWITCHlan SCION Access
SWITCHlan SCION Access
More security, reliability and control: SWITCHlan SCION access provides the best conditions for ensuring that your data is only transferred to the parts of the internet that you want it to reach.

swisscom Offer Insights and Success Stories
Business customers > Enterprise Customers > Offer > Network, Internet & Landline
SCION – transporting sensitive data securely
The secure, high-speed Internet under your control
Contact an expert

Sunrise Medium & Large Business
EN ▾
SCION - the innovative solution for secure multi-site connectivity.

telindus
Home SCION
A New Architecture that Overcomes the Limitations of the Internet
In November last year, Telindus announced having joined its forces with Anapaya, an ETH Zurich spin-off, thereby becoming the first player to offer the SCION architecture in Luxembourg. SCION is an innovative connectivity solution that combines the openness and flexibility of the Internet with the security and resilience of a private network, eliminating the risks of network cyber-attacks towards its users. We met Adrian Perrig, creator of SCION, and asked him a few questions.
What is SCION?

SIX
Banking Services Billing and Payments Debit & Mobile Services
SIC System euroSIC System Info Center Online Services
Governance SIC euroSIC SIC/euroSIC Providers Security Systems
• With the SCION technology developed by ETH Zurich, new level of security, performance and functionality – information at: [SCION ↗](#).

swissix
SWISS INTERNET EXCHANGE
Home Association Participation Infrastructure Partners/Sponsors About
Participants
Participants SCION
Get connected
Connection Agreement
Peering Policy
Equipment Configuration BCP
Home / Participation / Participants SCION
More about the SwissIX SCION peering mesh [here](#).
Participants SCION

How did we get there?

Commercial connectivity offering 2021

Finance Network announced 2019

- Commercial implementation
- First production traffic

2017

- First field trials
- SCIONLab R&D network

2016

Initial concept and design 2009

Deployment: Secure Swiss Finance Network (SSFN)

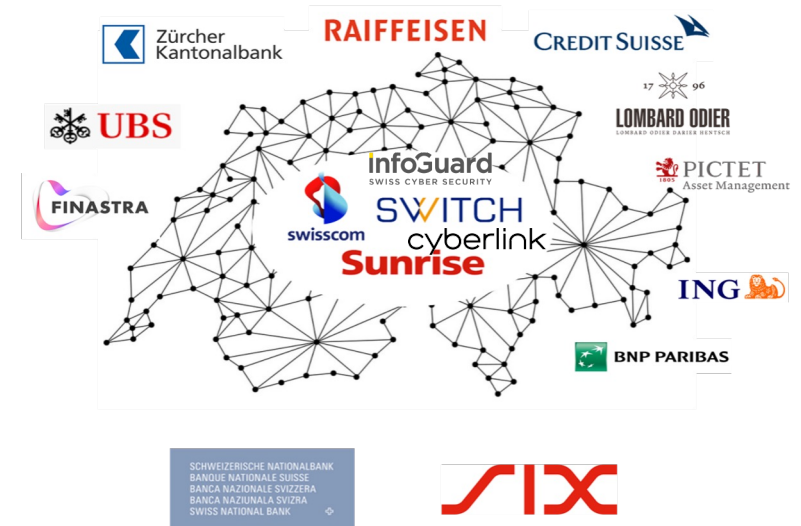
Swiss inter-banking network, handling money transfers between banks and other critical real-time financial services

Operated by SIX, the Swiss Financial Infrastructure operator

Reasons for using SCION:

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

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

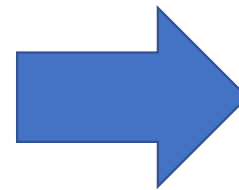


Some facts:

- 300+ finance institutions
- Network handling ~200 Billion CHF/day
- Migration to SCION-based SSFN by September 2024

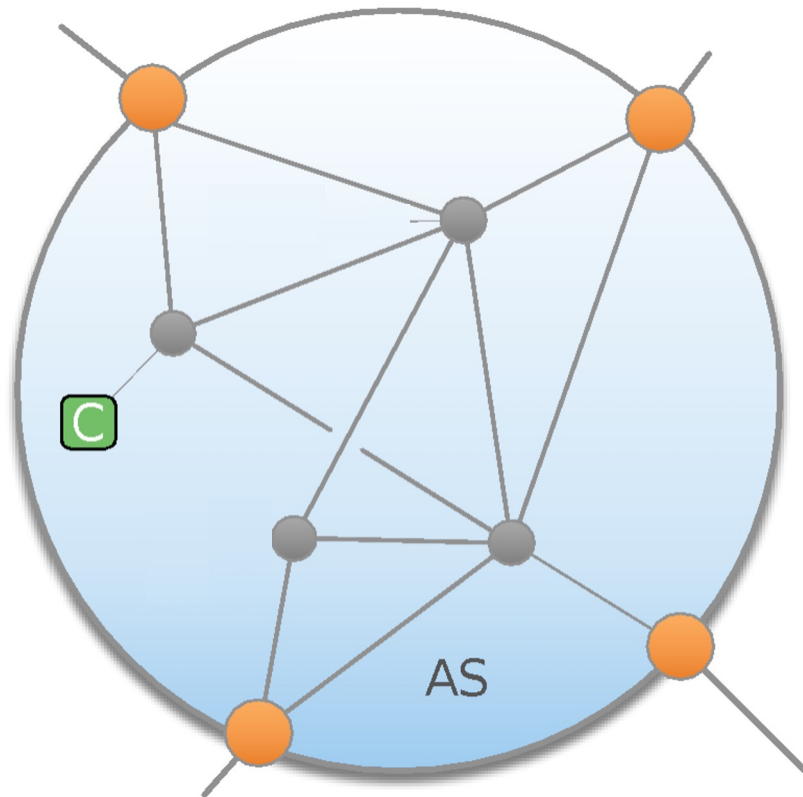
SCION is federated

SCION is federated and offered as a product deployed by several ISPs



Any ISP can connect to the SCION Internet and provide new connectivity offerings

AS Deployment Model



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 and map network paths

No change to the internal network infrastructure of a network operator needed

Endpoints run a SCION stack; legacy endpoints can leverage gateways

 Control Services

 Border router

 Internal router

Getting broader adoption

- IETF draft specification
- Education network

2023

- Healthcare network announced
- SCION Association founded
- New SCION book

2022

Commercial connectivity offering

2021

Finance Network announced

2019

- Commercial implementation
- First production traffic

2017

- First field trials
- SCIONLab R&D network

2016

Initial concept and design

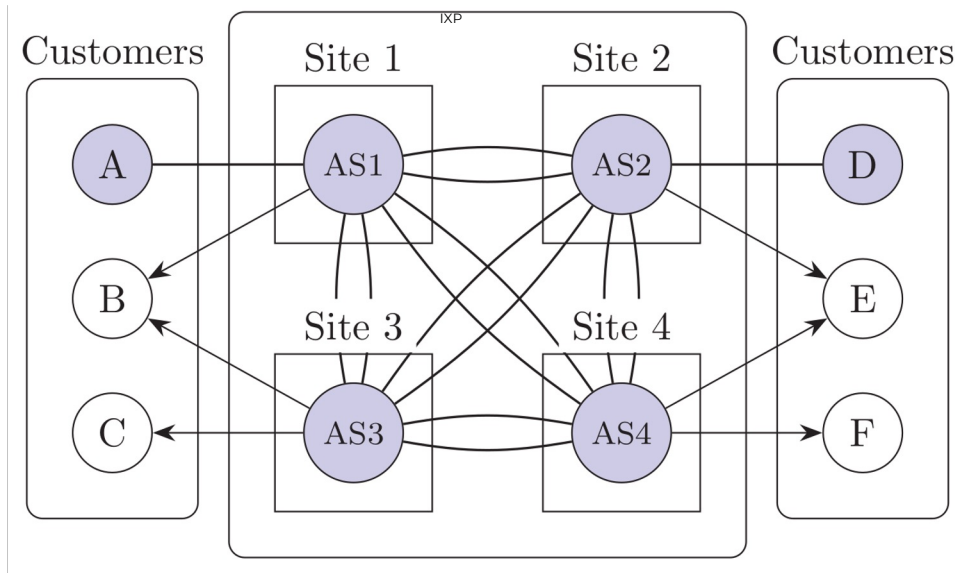
2009

IXP Deployment: model

SCION supports peering links.

Two IXP Deployment Models:

- **Traditional:** An IXP is treated as a large layer 2 switch between its customer ASes
- **Multipath:** an IXP exposes its internal structure by modelling each site as an individual AS



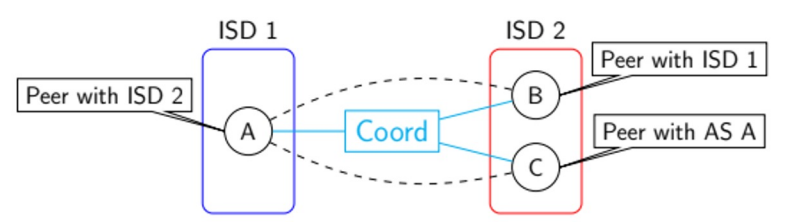
IXP Deployment: Considerations

SwissIX productive SCION Peering Mesh:

- Add-on to regular peering
- www.swissix.ch/participation/participants-scion
- 8/8 sites, with 1/10/100G ports.
- L2 peering mesh, independent from BGP

No multilateral peering in SCION

- experimental peering coordinator available, automating configuration of peering links, like a “SCION route server”.
(In collaboration with DE-CIX, Germany)

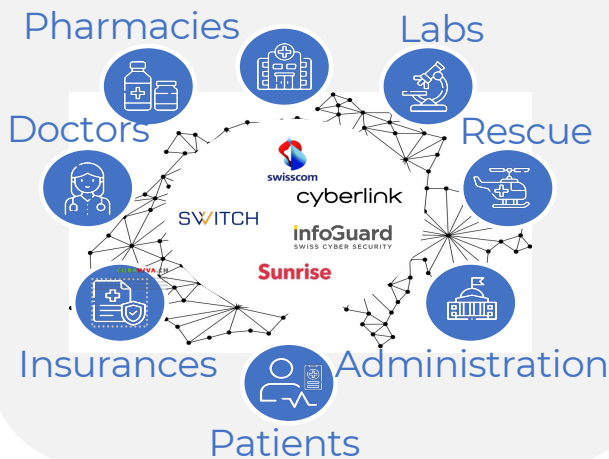


Further research collaborations with SIDN Labs/AMS-IX

Deployment Beyond Finance

Healthcare

The [HIN Trust Circle](#) adopts SCION to interconnect hundreds of hospitals and thousands of doctors



Education

The [SCION education network](#) connects campuses with path-aware high performance SCION connectivity



Energy

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

VSE Verband Schweizerischer Elektrizitätsunternehm... + Follow
AES 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 **#Energieversorgun**g in der Zukunft zu verbessern.

Growing the community

In 2022 some of the SCION early adopters and deployers joined forces to establish the SCION Association



Ecosystem

Accelerate adoption, nurture an ecosystem with partners across verticals



Standardization

Establish SCION as an internet standard



Certification

Ensure compliance and global interoperability



Development

Maintain and coordinate open source implementation



<https://scion.org>

IETF

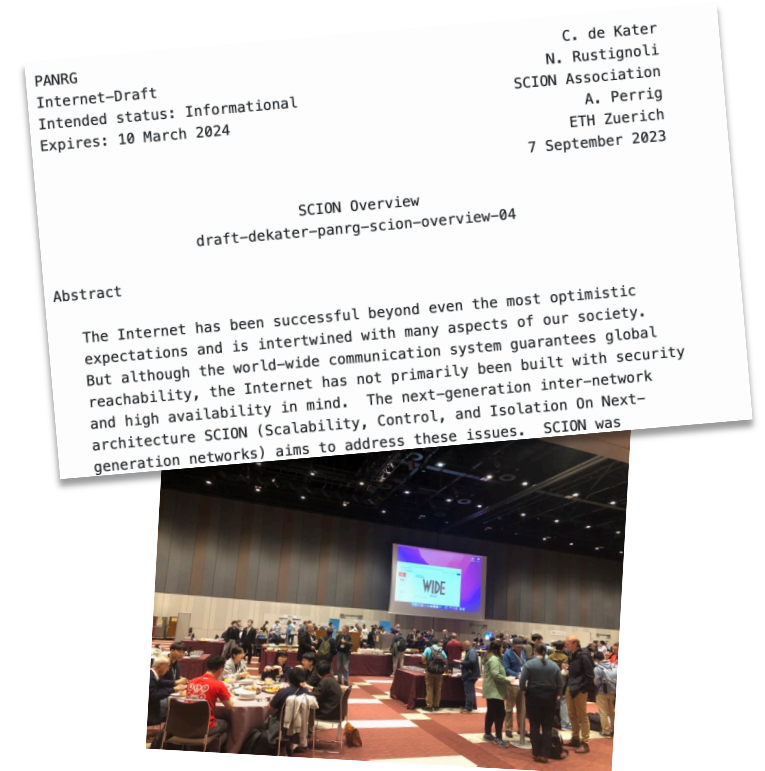
Ongoing work

Proposing a new Internet Architecture at the IETF can be a challenge. Yet, there is interest into the problems SCION addresses, and we have been discussing next steps for SCION at PANRG.

Community feedback is welcome 😊. Read some of our drafts:

- Overview [draft-dekater-panrg-scion-overview](#)
- Components analysis [draft-rustignoli-panrg-scion-components](#)
- Control Plane PKI [draft-dekater-scion-pki](#)
- Control Plane [draft-dekater-scion-controlplane](#)
- Data Plane [draft-dekater-scion-dataplane](#)

Other activity (TAPS): [PANAPI](#): a path-aware transport API



Commercial & Open-Source Implementations

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



Commercial

scionproto/scion
SCION Internet Architecture




80 Contributors 53 Used by 3 Discussions 324 Stars 140 Forks

Open Source



SCION @ IETF 118 Prague Hackathon

- Other implementations under development: P4, OpenWRT, APIs (Java, C/C++, Go, Rust, Python)
- SCION Association formed by deployers and early adopters to support open-source development, standardization, and community involvement
- Offered on Extreme Networks commercial routers 



Looking ahead

Open challenges

- Long term protocol evolution
 - Interoperability (e.g., with IPv6)?
 - Full standardization
- Handing out SCION numbers (ISDs, SCION ASes)
 - Could RIRs take a role for numbering in the SCION Internet?

More deployment beyond “ecosystem” industries

- Further developing interfaces for path-aware networking towards applications (e.g., ongoing collaboration with Brave browser)
- Getting large vendors onboard

Conclusion

- SCION is an inter-domain multi-path Internet architecture, born in research and today in use to protect critical infrastructure communication
- Innovation in inter-domain routing is possible
- Lots of work left, to continue the journey at IETF, and growing community & deployment

Thank you!

- <http://scion.org/>
- SCION Association
- <https://www.scionlab.org>
- SCIONLab testbed
- <https://github.com/scionproto/scion>
- Open-source code
- <https://www.anapaya.net>
- ETH-Spin-off offering SCION-based products

We thank the following people for a few inputs for this presentation:

Cyrill Krähenbühl*, Seyedali Tabaeiaghdaei*, Christelle Gloor*, Jonghoon Kwon*, Adrian Perrig*‡, David Hausheer**, Dominik Roos‡

*ETH Zürich, ** OVGU Magdeburg, ‡Anapaya Systems

And for their work: “**Deployment and Scalability of an Inter-Domain Multi-Path Routing Infrastructure.**” (CoNEXT '21)



Book: The Complete Guide to SCION, 2022, Springer Verlag

For more information:

Adrian Perrig <aperrig@inf.ethz.ch>

Nicola Rustignoli <nic@scion.org>