SCION™

ELEVATING SECURE COMMUNICATION

OVERCOMING DEPLOYMENT AND APPLICATION CHALLENGES: INTRODUCING THE SCION EDUCATION NETWORK

Prof. Dr.
Adrian Perrig
ETH Zurich
Switzerland

Prof. Dr.
David Hausheer
Universität Magdeburg
Germany

SCION ASSOCIATION ETH zürich ANAPAYA eraneos satw technology for society

SCION
SCALABILITY, CONTROL, AND ISOLATION
ON NEXT-GENERATION NETWORKS

Overcoming Deployment and Application Challenges: Introducing the SCION Education Network

Adrian Perrig, ETH Zürich
David Hausheer, OVGU Magdeburg

Benefits of a SCION Connection

Security: Authenticated control plane and resilience against path hijacks

Stability: Native multipath capability at the network level with rapid path failover ensures high stability despite link failures at the physical layer

Control: Path-awareness for end hosts enables application-specific path control and optimization

E.g., possibility for traffic geofencing determined by the sender

Protection: Hidden paths and sender-based path selection increase protection against DDoS attacks.

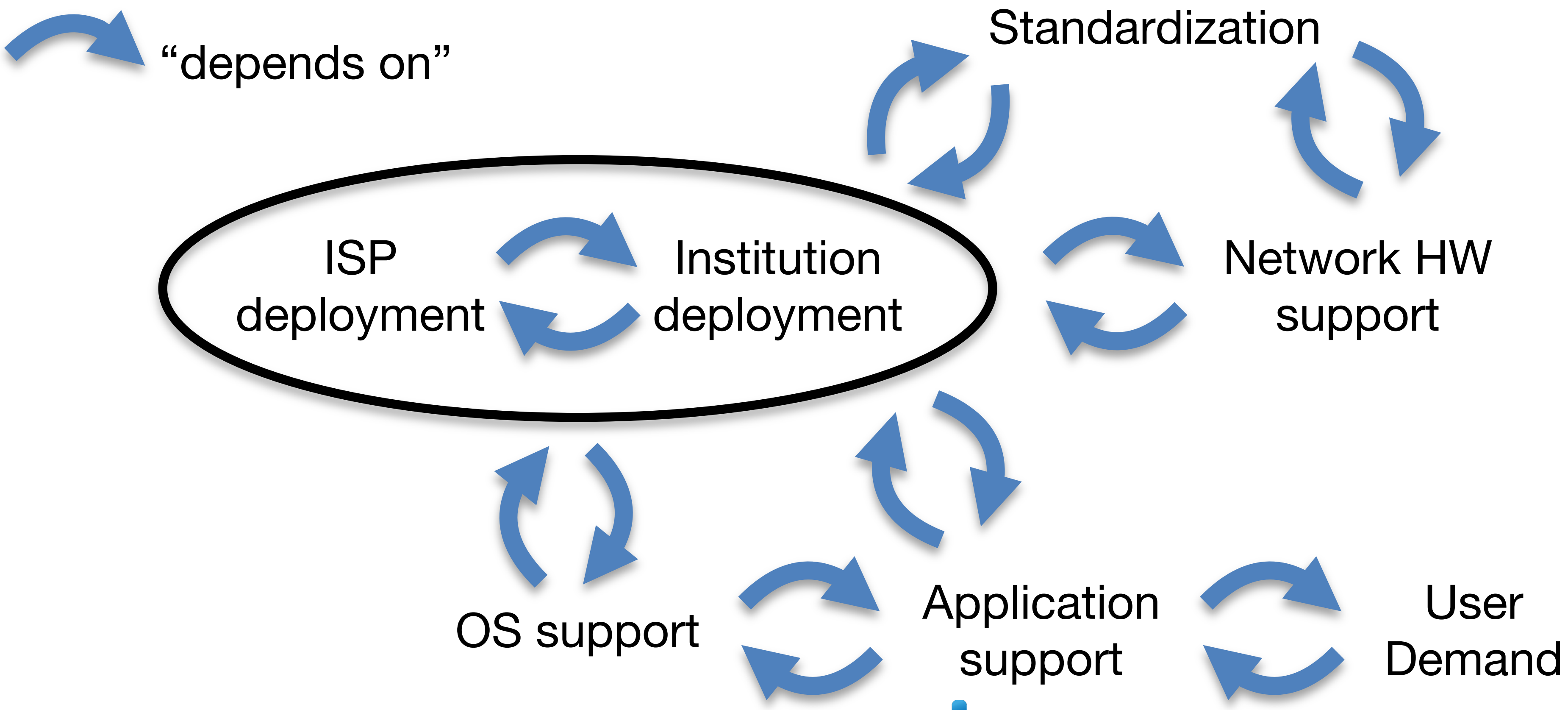
Performance: SCION applications can select the best paths based on latency, bandwidth, loss, or jitter

Exciting Development

- If the local network supports SCION, then any application on any device can use native SCION connectivity
- So everyone here in this room is one application update away from using SCION on their device!
- Goal: by next SCION Day, many participants' devices will have applications that can natively use SCION

Deployment Challenges

- Disruptive technologies often face adoption challenges
- Several circular dependencies complicate deployment



"depends on"

Standardization

ISP deployment

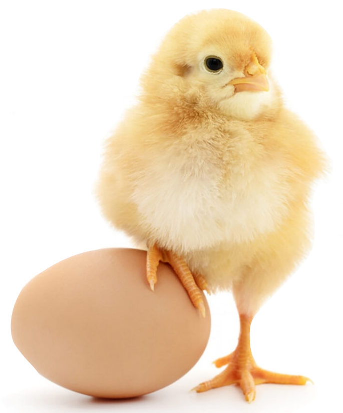
Institution deployment

Network HW support

OS support

Application support

User Demand

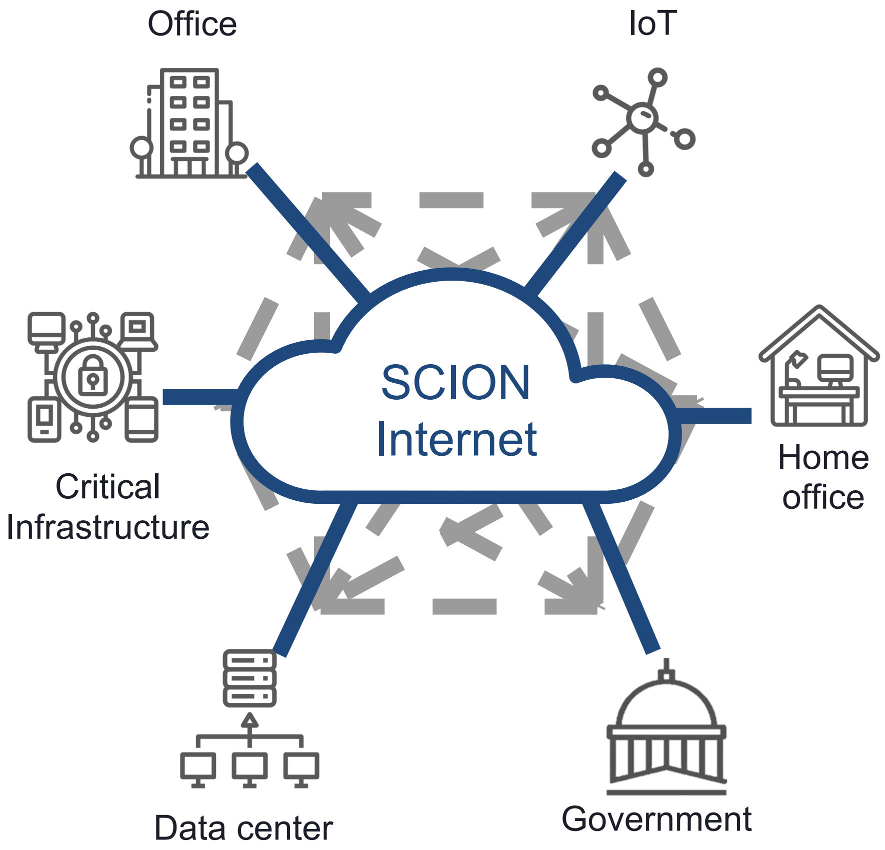


Main Use Case: Communication among Community

Single SCION connection offers secure communication to any other entity on SCION network

- ⊕ High availability, secure against DDoS and routing attacks
- ⊕ Geofencing
- ⊕ High efficiency through path optimization
- ⊕ Fast failover
- ⊕ Easy to extend to new use cases
- ⊕ Low cost
- ⊖ Initial setup requires effort
- ⊖ Training required for network admins

Takeaway:
Single SCION connection approximates
a leased line to all SCION destinations



ETH zürich

SCION™

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

SCION Production Network

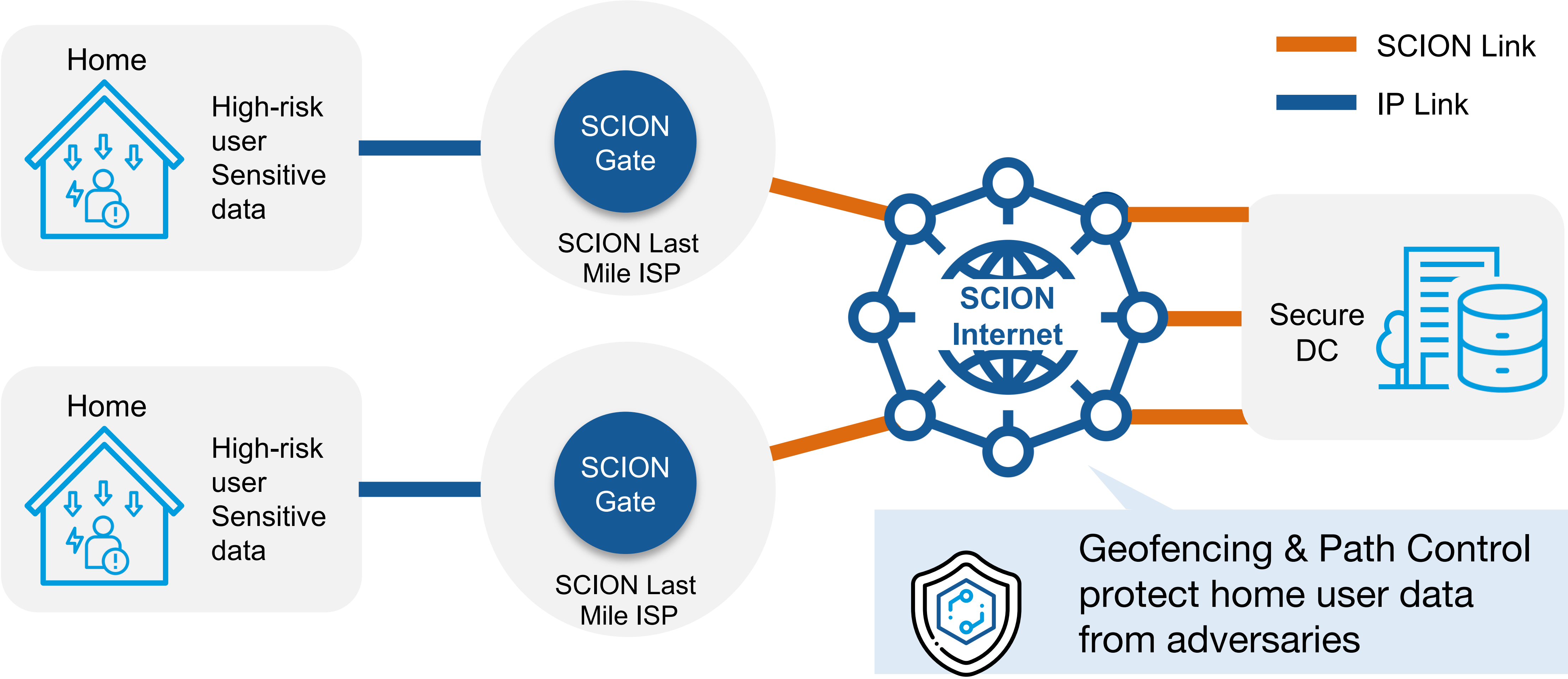
- **Not an overlay!**
  BGP-free global communication
  - Fault independent from BGP protocol
- Deployment with international ISPs
  - First **global public secure** communication network
- Construction of SCION network backbone at select locations to bootstrap adoption

BGP FREE

ANAPAYA
cyberlink
interCloud
proximus
telindus
SWITCH
swisscom
axpo
swissix SWISS INTERNET EXCHANGE
LG U+
vtx
Sunrise
GÉANT

GATE Approach for Secure Small-Site Communication

Seamless secure SCION for remote users



Geofencing & Path Control protect home user data from adversaries

ETH zürich

SCION

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

Ecosystem nurtured by SCION Association

PRINCETON UNIVERSITY

SIDN

ETH zürich

고려대학교 KOREA UNIVERSITY

NUS National University of Singapore

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

CYBEXER TECHNOLOGIES

CSCS Centro Svizzero di Calcolo Scientifico Swiss National Supercomputing Centre

KAIST

UNIVERSITY of VIRGINIA

ΔΗΜΟΚΡΙΤΟΣ DEMOKRITOS

cyberlink

proximus telindus

interCloud

SWITCH

swisscom

axpo

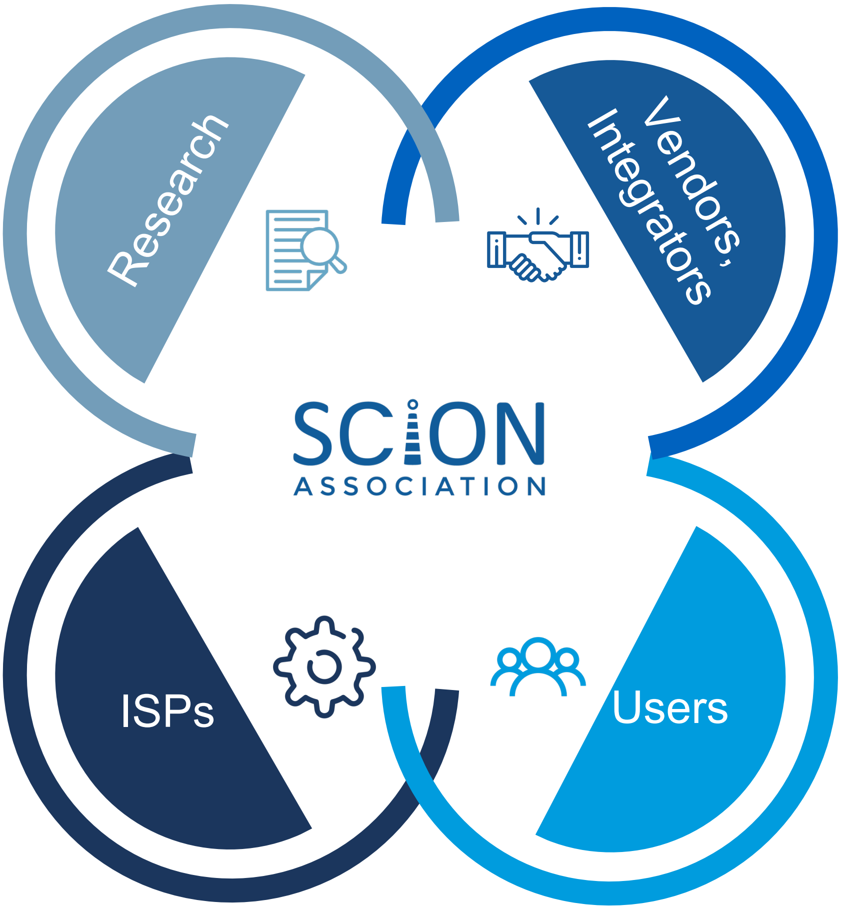
swissix SWISS INTERNET EXCHANGE

LG U+

vtx

Sunrise

GÉANT



SCION™

ANAPAYA

bnc business network communications

Extreme™

infoGuard SWISS CYBER SECURITY

INFOSEC GLOBAL

Startups

eraneos

HIN

ICRC

libC TECHNOLOGIES

securosys

RAIFFEISEN

SIX

UBS

armasuisse

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA

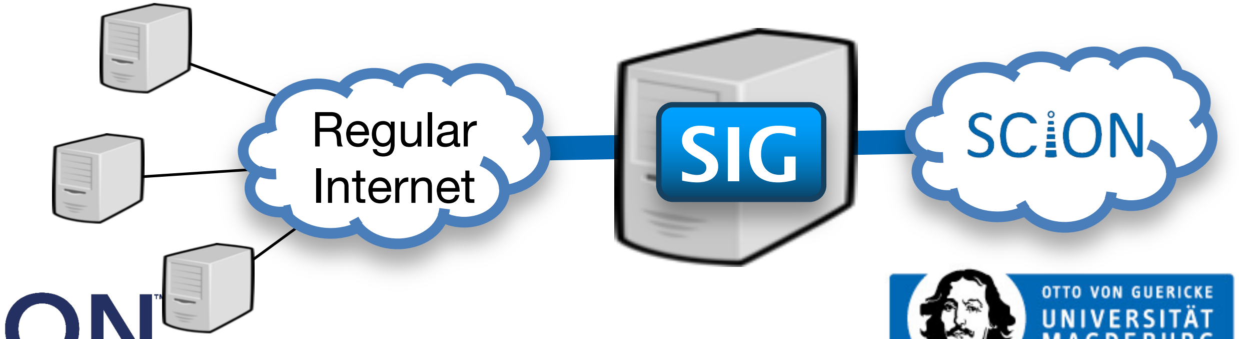
SCHWEIZERISCHE NATIONALBANK
BANQUE NATIONALE SUISSE
BANCA NAZIONALE SVIZZERA
BANCA NAZIUNALA SVIZRA
SWISS NATIONAL BANK

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

SCION Access for Universities and Research Institutes

- Connect universities and research institutes with SCION
- Participate in research on emerging topics of path-aware networking and multipath communication
  - True inter-domain multipath
  - Software packages and setup instructions are provided for different platforms to enable use of SCION native application

- SCION IP Gateway (SIG) enables use of regular IP applications
  - Using SCION for users not involved in network research is no harder than using regular Internet services

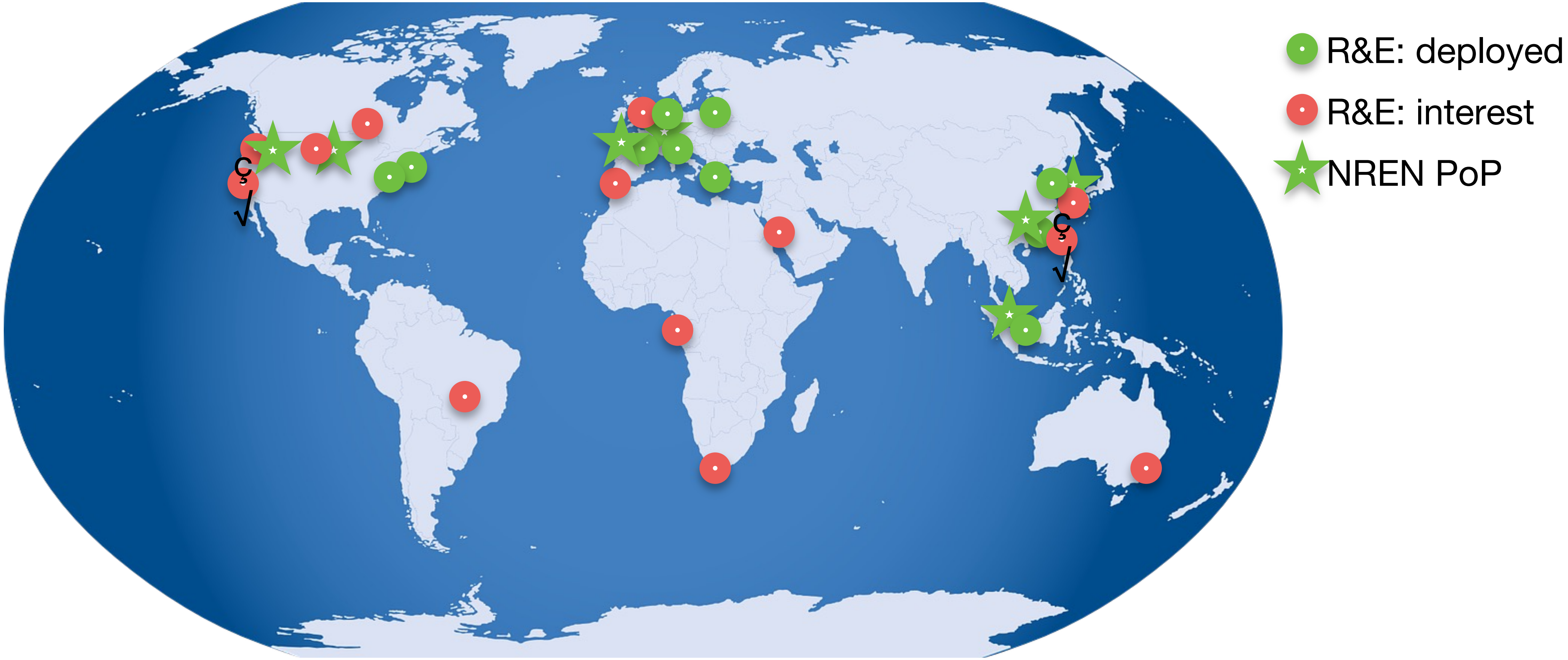


Academia as Early Adopters Build Critical Mass!

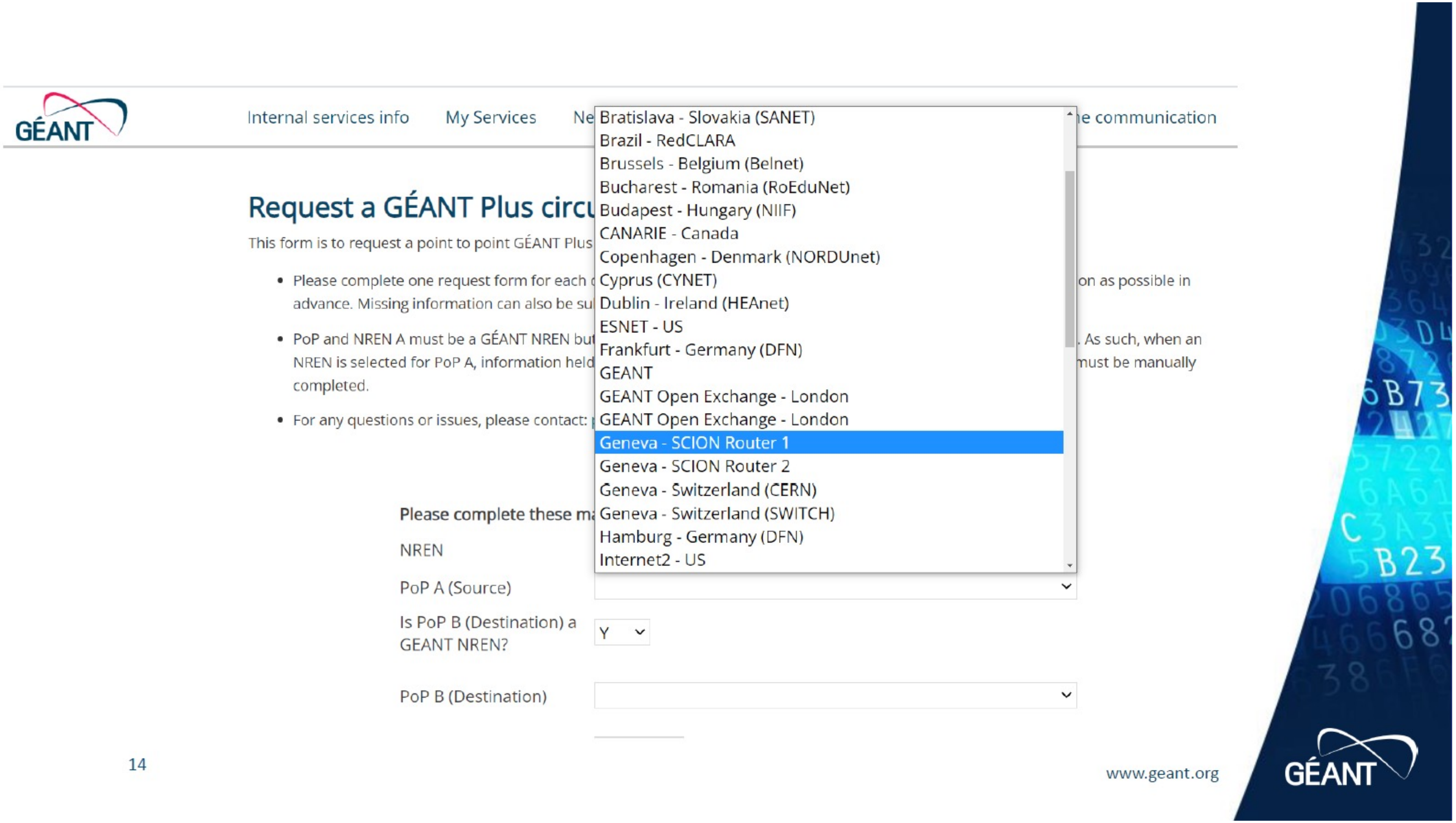
- Many large Universities with 10’000+ hosts: possibility to get to a 1 million hosts with access to native SCION connectivity
- National Research and Education Networks (NREN) and Universities embrace innovation
- Compelling use cases
  - Next-generation Internet research infrastructure
  - DDoS defense
  - Security-sensitive data transmission
  - Next-generation web browsing
  - High-speed Hercules file transfer and LightningFilter firewall

Global SCION Education Network

Main networks providing connectivity: GÉANT, Kreonet, SWITCH



SCION @ GEANT



GÉANT

Internal services info | My Services | Ne | ...e communication

Request a GÉANT Plus circu

This form is to request a point to point GÉANT Plus

- Please complete one request form for each ... advance. Missing information can also be su ... on as possible in
- PoP and NREN A must be a GÉANT NREN but ... NREN is selected for PoP A, information held ... . As such, when an ... must be manually completed.
- For any questions or issues, please contact:

Bratislava - Slovakia (SANET)
Brazil - RedCLARA
Brussels - Belgium (Belnet)
Bucharest - Romania (RoEduNet)
Budapest - Hungary (NIIF)
CANARIE - Canada
Copenhagen - Denmark (NORDUnet)
Cyprus (CYNET)
Dublin - Ireland (HEAnet)
ESNET - US
Frankfurt - Germany (DFN)
GEANT
GEANT Open Exchange - London
GEANT Open Exchange - London
Geneva - SCION Router 1
Geneva - SCION Router 2
Geneva - Switzerland (CERN)
Geneva - Switzerland (SWITCH)
Hamburg - Germany (DFN)
Internet2 - US

Please complete these m

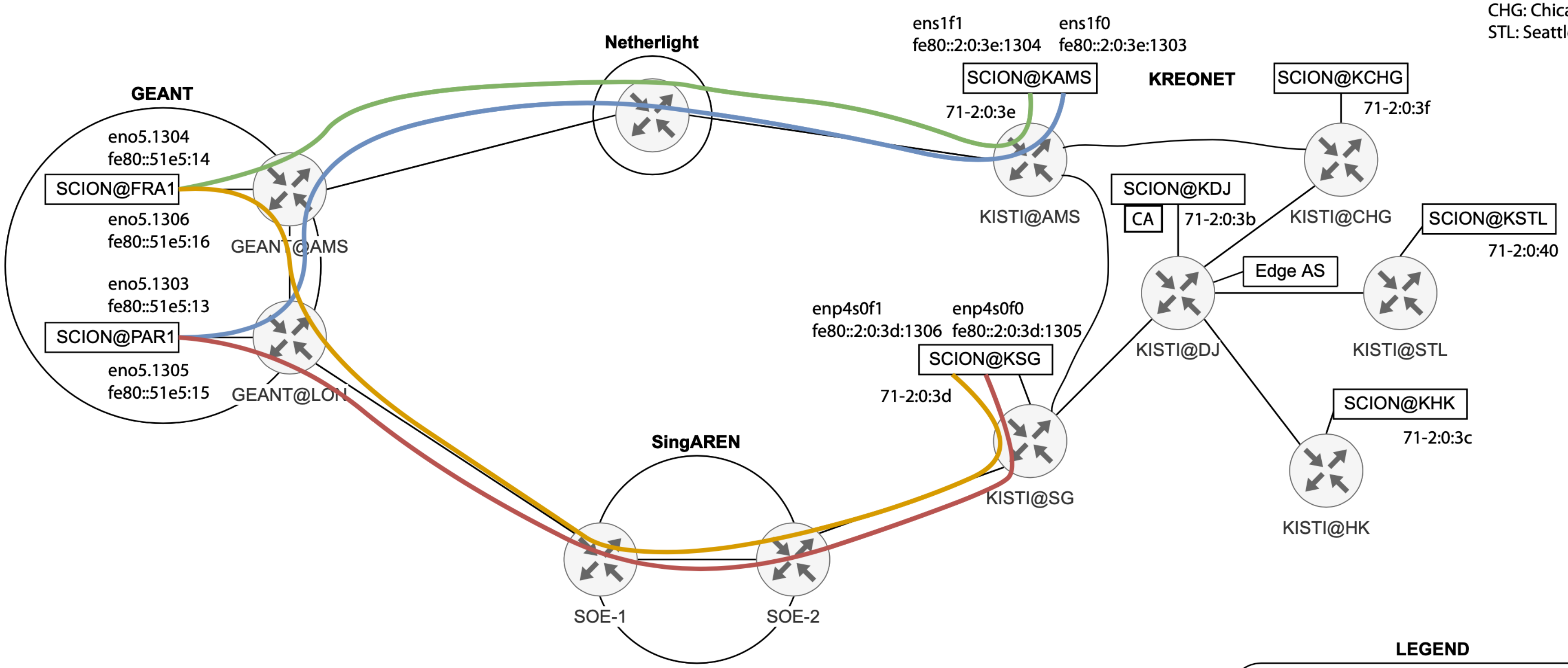
NREN	
PoP A (Source)	
Is PoP B (Destination) a GEANT NREN?	Y
PoP B (Destination)	

14

www.geant.org

SCION @ Kreonet

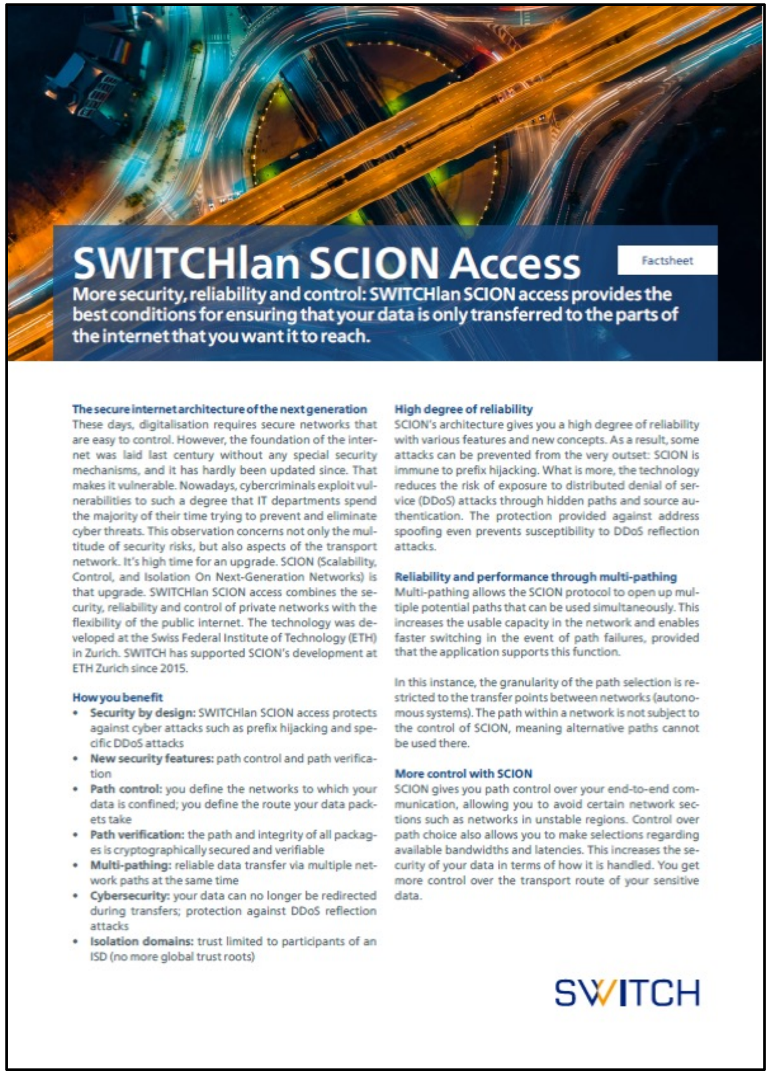
DJ: Daejeon / Seoul
HK: Hong Kong
SG: Singapore
AMS: Amsterdam
CHG: Chicago
STL: Seattle



LEGEND

- 🟦 Circuit 1: VLAN 1303 PAR to KISTI@AMS
- 🟩 Circuit 2: VLAN 1304 FRA to KISTI@AMS
- 🟥 Circuit 3: VLAN 1305 PAR to KISTI@SG
- 🟨 Circuit 4: VLAN 1306 FRA to KISTI@SG

SCION @ SWITCH



SWITCHlan SCION Access

Factsheet

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.

The secure internet architecture of the next generation

These days, digitalisation requires secure networks that are easy to control. However, the foundation of the internet was laid last century without any special security mechanisms, and it has hardly been updated since. That makes it vulnerable. Nowadays, cybercriminals exploit vulnerabilities to such a degree that IT departments spend the majority of their time trying to prevent and eliminate cyber threats. This observation concerns not only the multitude of security risks, but also aspects of the transport network. It's high time for an upgrade. SCION (Scalability, Control, and Isolation On Next-Generation Networks) is that upgrade. SWITCHlan SCION access combines the security, reliability and control of private networks with the flexibility of the public internet. The technology was developed at the Swiss Federal Institute of Technology (ETH) in Zurich. SWITCH has supported SCION's development at ETH Zurich since 2015.

How you benefit

- **Security by design:** SWITCHlan SCION access protects against cyber attacks such as prefix hijacking and specific DDoS attacks
- **New security features:** path control and path verification
- **Path control:** you define the networks to which your data is confined; you define the route your data packets take
- **Path verification:** the path and integrity of all packages is cryptographically secured and verifiable
- **Multi-pathing:** reliable data transfer via multiple network paths at the same time
- **Cybersecurity:** your data can no longer be redirected during transfers; protection against DDoS reflection attacks
- **Isolation domains:** trust limited to participants of an ISD (no more global trust roots)

High degree of reliability

SCION's architecture gives you a high degree of reliability with various features and new concepts. As a result, some attacks can be prevented from the very outset: SCION is immune to prefix hijacking. What is more, the technology reduces the risk of exposure to distributed denial of service (DDoS) attacks through hidden paths and source authentication. The protection provided against address spoofing even prevents susceptibility to DDoS reflection attacks.

Reliability and performance through multi-pathing

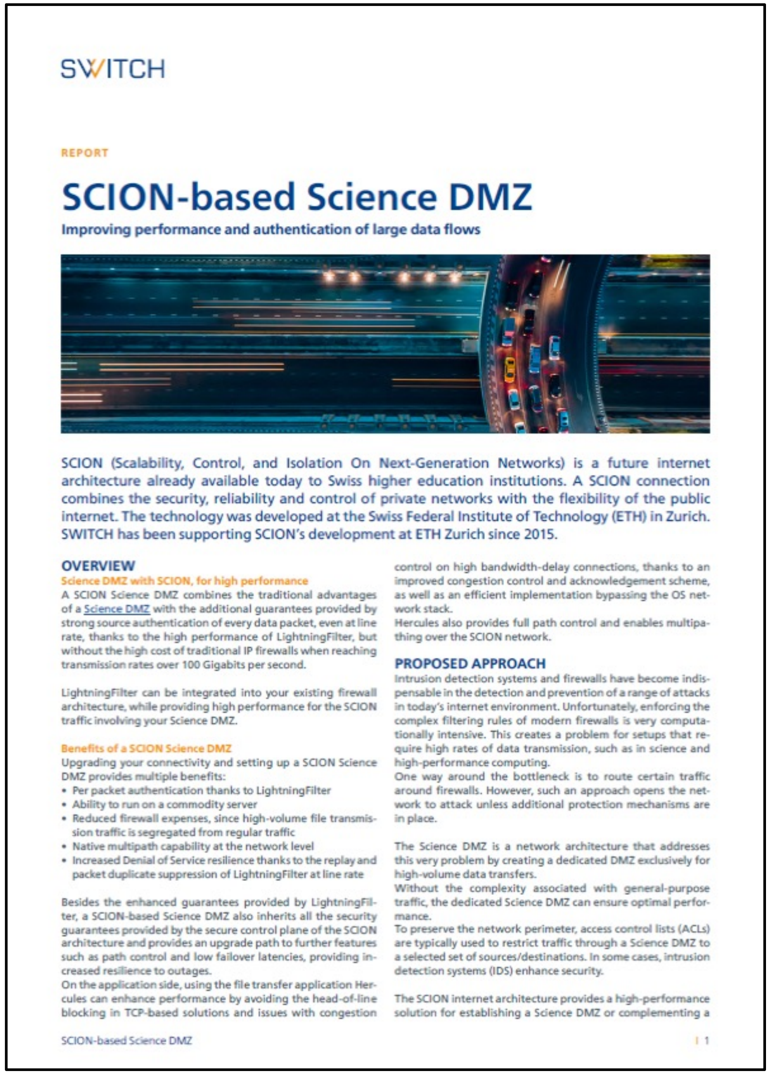
Multi-pathing allows the SCION protocol to open up multiple potential paths that can be used simultaneously. This increases the usable capacity in the network and enables faster switching in the event of path failures, provided that the application supports this function.

In this instance, the granularity of the path selection is restricted to the transfer points between networks (autonomous systems). The path within a network is not subject to the control of SCION, meaning alternative paths cannot be used there.

More control with SCION

SCION gives you path control over your end-to-end communication, allowing you to avoid certain network sections such as networks in unstable regions. Control over path choice also allows you to make selections regarding available bandwidths and latencies. This increases the security of your data in terms of how it is handled. You get more control over the transport route of your sensitive data.

SWITCH



SWITCH

REPORT

SCION-based Science DMZ

Improving performance and authentication of large data flows

SCION (Scalability, Control, and Isolation On Next-Generation Networks) is a future internet architecture already available today to Swiss higher education institutions. A SCION connection combines the security, reliability and control of private networks with the flexibility of the public internet. The technology was developed at the Swiss Federal Institute of Technology (ETH) in Zurich. SWITCH has been supporting SCION's development at ETH Zurich since 2015.

OVERVIEW

Science DMZ with SCION, for high performance

A SCION Science DMZ combines the traditional advantages of a Science DMZ with the additional guarantees provided by strong source authentication of every data packet, even at line rate, thanks to the high performance of LightningFilter, but without the high cost of traditional IP firewalls when reaching transmission rates over 100 Gigabits per second.

LightningFilter can be integrated into your existing firewall architecture, while providing high performance for the SCION traffic involving your Science DMZ.

Benefits of a SCION Science DMZ

Upgrading your connectivity and setting up a SCION Science DMZ provides multiple benefits:

- Per packet authentication thanks to LightningFilter
- Ability to run on a commodity server
- Reduced firewall expenses, since high-volume file transmission traffic is segregated from regular traffic
- Native multipath capability at the network level
- Increased Denial of Service resilience thanks to the replay and packet duplicate suppression of LightningFilter at line rate

Besides the enhanced guarantees provided by LightningFilter, a SCION-based Science DMZ also inherits all the security guarantees provided by the secure control plane of the SCION architecture and provides an upgrade path to further features such as path control and low failover latencies, providing increased resilience to outages.

On the application side, using the file transfer application Hercules can enhance performance by avoiding the head-of-line blocking in TCP-based solutions and issues with congestion control on high bandwidth-delay connections, thanks to an improved congestion control and acknowledgement scheme, as well as an efficient implementation bypassing the OS network stack.

Hercules also provides full path control and enables multipathing over the SCION network.

PROPOSED APPROACH

Intrusion detection systems and firewalls have become indispensable in the detection and prevention of a range of attacks in today's internet environment. Unfortunately, enforcing the complex filtering rules of modern firewalls is very computationally intensive. This creates a problem for setups that require high rates of data transmission, such as in science and high-performance computing.

One way around the bottleneck is to route certain traffic around firewalls. However, such an approach opens the network to attack unless additional protection mechanisms are in place.

The Science DMZ is a network architecture that addresses this very problem by creating a dedicated DMZ exclusively for high-volume data transfers.

Without the complexity associated with general-purpose traffic, the dedicated Science DMZ can ensure optimal performance.

To preserve the network perimeter, access control lists (ACLs) are typically used to restrict traffic through a Science DMZ to a selected set of sources/destinations. In some cases, intrusion detection systems (IDS) enhance security.

The SCION internet architecture provides a high-performance solution for establishing a Science DMZ or complementing a

SCION-based Science DMZ

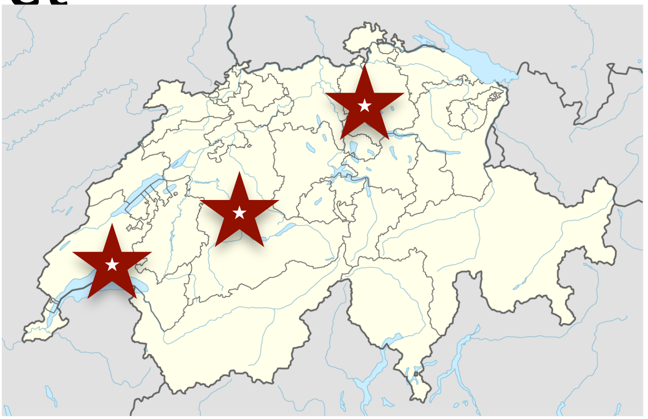
| 1

https://www.switch.ch/scion/

Cyber-Defence Campus Connections

- Armasuisse has Cyber-Defence (CYD) campuses in Lausanne, Thun, and Zürich
    - All campuses are now connected through the SCION network, including CCDCOE NATO campus in Tallinn
- CYD researchers are studying vulnerabilities and defenses for critical infrastructures
- SCION is now an active research project

CYD CYBER DEFENCE CAMPUS



CCDCOE
Tallinn, Estonia

ETH zürich

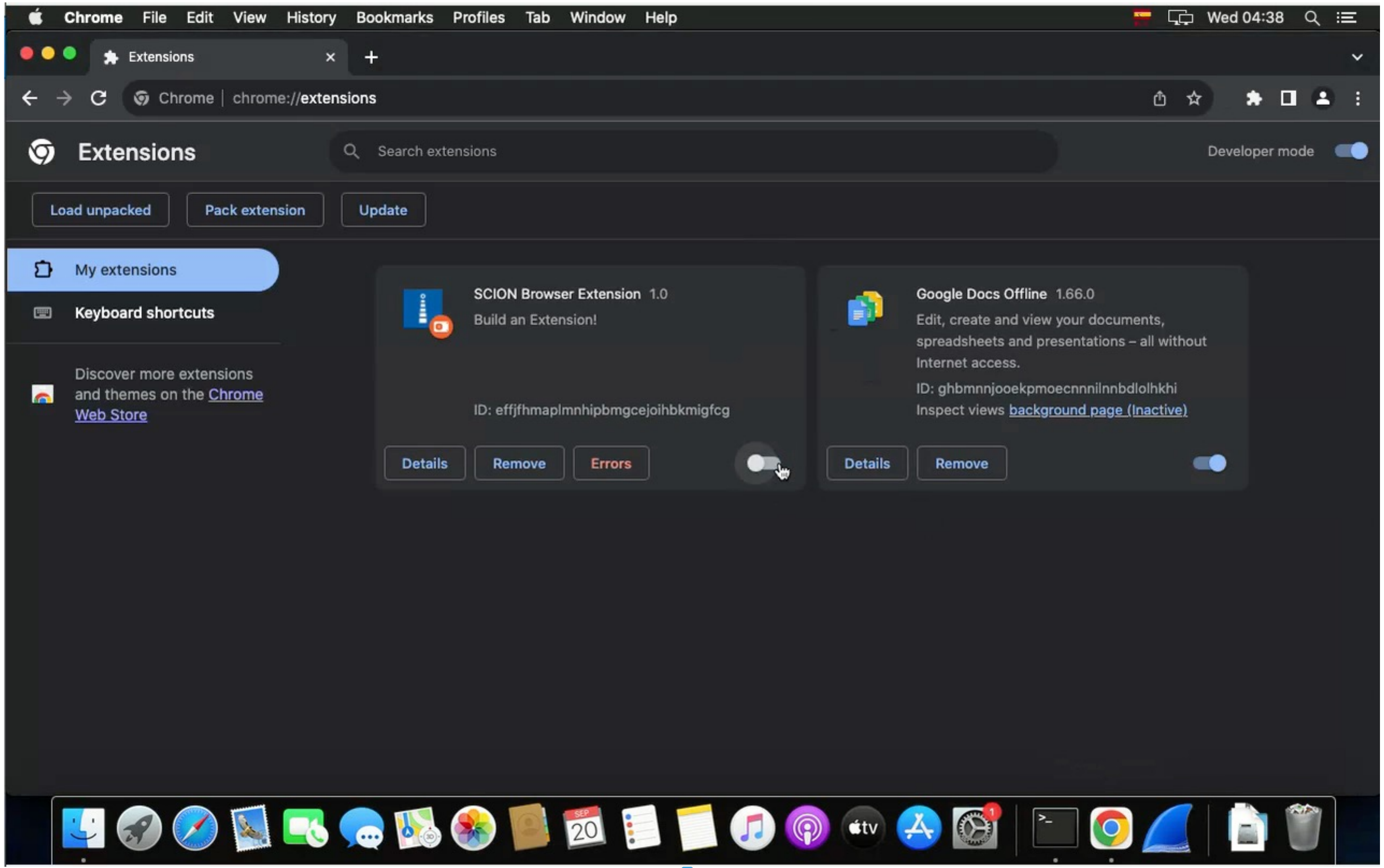
SCION™

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

brave SCION

- Collaboration with Brave browser team to build native SCION communication into browser
- Without OS support, SCION-enabled browser can directly fetch web pages over the SCION network if host is within SCION-enabled network
- Compelling advantages
  - Download speed optimization
  - Specific optimizations possible: low carbon footprint paths, low delay, high bandwidth, low jitter, low loss, …
- 60M enabled devices would help spur SCION adoption

brave Demo



Discover more extensions and themes on the Chrome Web Store

SCION Browser Extension 1.0
Build an Extension!
ID: effjfhmaplmnhipbmgcejoihbkmigfcg

Google Docs Offline 1.66.0
Edit, create and view your documents, spreadsheets and presentations – all without Internet access.
ID: ghbmnnjooekpmoecnnnilnnbdlolhkhi
Inspect views background page (Inactive)

ETH zürich

SCION™

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

Conclusion

- SCION production network is expanding
- Ambitious goal: Provide 1M hosts access to native SCION connectivity through global education network
- Native SCION applications emerging
  - Possibility to use SCION after app update

- More information:
  https://sciera.readthedocs.io/
  https://cloud.inf.ethz.ch/s/NRi3Za6pEd8Wyfy

SCION ACCESS FOR UNIVERSITIES AND RESEARCH INSTITUTES

BRINGING THE NEXT-GENERATION INTERNET TO YOUR CAMPUS

SCION

SCION

SCALABILITY, CONTROL, AND ISOLATION ON NEXT-GENERATION NETWORKS

SCION is a next-generation Internet architecture already in production use to protect critical infrastructure communication, for example in the Swiss financial ecosystem. A SCION connection combines the security, reliability and control of private networks with the flexibility of the public Internet.

In addition, thanks to its multipath functionality, SCION can offer higher performance and communication quality.

FURTHER INFORMATION

Book: The Complete Guide to SCION
SCION Project: scion-architecture.net
SCION Association: scion.org
wirzf@inf.ethz.ch

-1-