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.

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.
Do you have any questions? We would be happy to help you understand the next generation of internet architecture. Are you interested in SWITCHlan SCION access? Call us or send us a message. We advise you with expertise, commitment and a focus on your individual requirements.

Daniel Bertolo
Head Network
daniel.bertolo@switch.ch
+41 44 268 15 87

Diego Tres
Community Account Manager
hello@switch.ch
+41 44 268 16 57

SWITCH
PO Box
8021 Zurich
switch.ch/SCION