SCION Challenges and Risks for Certificate Issuing and AS Number Assignment

Example of the Secure Swiss Finance Network (SSFN)

Fritz Steinmann, 17 May 2021

What is SSFN?

- The Secure Swiss Finance Network (SSFN) will become the network to interconnect Swiss financial infrastructure participants (Banks, other financial institutions, financial services companies)
- It forms a SCION isolation domain and is therefore the first industry ISD
- It is tightly governed by a set of parties who define its rules and regulations
- As governed SCION ISD it requires control over numbering and certificate issuing

Numbering

- ISD numbering for SSFN was not difficult – we went over to Anapaya and asked for a number, and there it was!
- AS numbering is more difficult. The current standard says:

1 - 4294967295 (~ `0:0:0/16`)	~4.3 bil	32-bit BGP AS numbers [2], formatted as decimal. If a BGP AS deploys SCION, it has the same AS number for both BGP and SCION.
`1:0:0`	1	Reserved.
`2:0:0/16`	~4.3 bil	Public SCION-only ASes (i.e. ASes that are created for SCION, and aren't existing BGP ASes). They should be allocated in ascending order, without gaps and "vanity" numbers.

- Some of the participants already have BGP ASes, so no issue there
- For those who are above 2:0:0/16 a numbering authority and a process to maintain the numbering lifecycle needs to be established

https://github.com/scionproto/scion/wiki/ISD-and-AS-numbering

Certificate Issuing – Key Questions and Risks

- Public or private trust
  - Not to be compared with TLS certificates
  - For a industry vertical ISD trust is established within the community, a CA therefore only needs to be trusted within this scope
- Liability
  - Since only routing and forwarding is cryptographically secured, identity is only certified on network and path level
  - There have been community requests to reuse SSFN certificates for other purposes, which we have strictly pushed back

Certificate Issuing – Key Questions and Risks

- CA Availability
  - As SCION certificates are short-lived (3 days for a typical AS certificate) CAs need to be designed for high availability
  - Failure to renew certificates in time can lead to complete participant network isolation!
  - Compensating measures for extended CA unavailability need to be in place from day one

Driving the Transformation for Financial Markets

Disclaimer

This material has been prepared by SIX Group Ltd, its subsidiaries, affiliates and/or their branches (together, "SIX") for the exclusive use of the persons to whom SIX delivers this material. This material or any of its content is not to be construed as a binding agreement, recommendation, investment advice, solicitation, invitation or offer to buy or sell financial information, products, solutions or services. It is solely for information purposes and is subject to change without notice at any time. SIX is under no obligation to update, revise or keep current the content of this material. No representation, warranty, guarantee or undertaking – express or implied – is or will be given by SIX as to the accuracy, completeness, sufficiency, suitability or reliability of the content of this material. Neither SIX nor any of its directors, officers, employees, representatives or agents accept any liability for any loss, damage or injury arising out of or in relation to this material. This material is property of SIX and may not be printed, copied, reproduced, published, passed on, disclosed or distributed in any form without the express prior written consent of SIX.