SwissPKI™

libC TECHNOLOGIES

# Building solid foundations for digital trust in the finance industry with SCION PKI

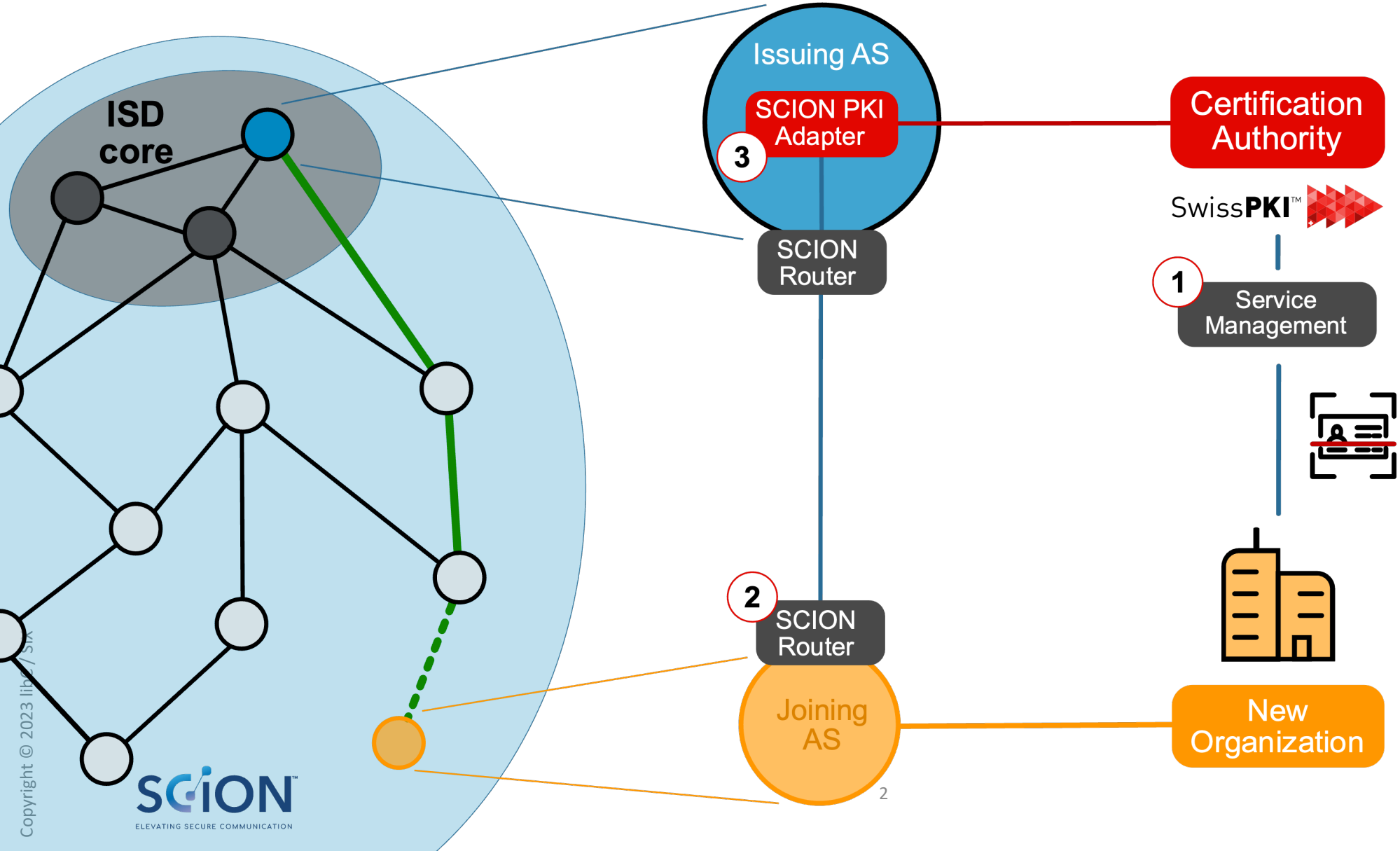
## SCION Day 2023

Marcel Suter, Partner, Director Solutions, libC Technologies | Switzerland
Fritz Steinmann, Senior Infrastructure Domain Architect, SIX | Switzerland

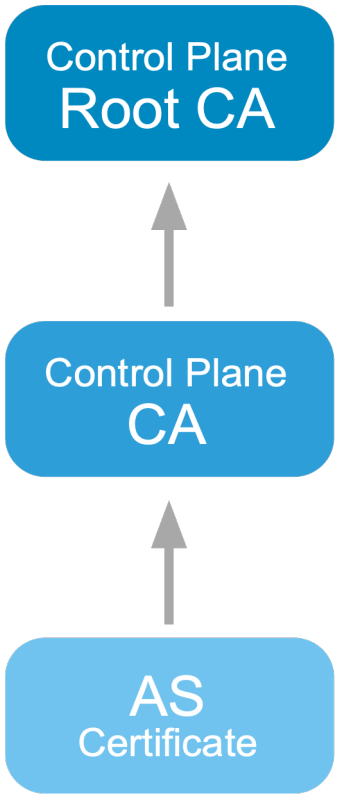
SCION
ELEVATING SECURE COMMUNICATION

SIX

# Building solid foundation for digital trust



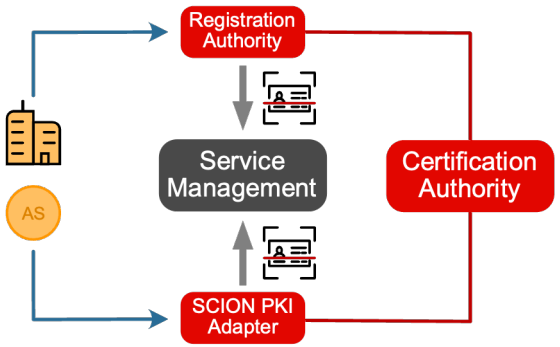
# SCION Certificate Lifetimes



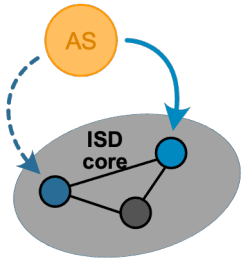

| | SCION Standard | SSFN |
|---|---|---|
| Control Plane Root CA | 1 year | 11 years |
| Control Plane CA | 7 days | 26 months |
| AS Certificate | 3 days | 3 days in regular issuance,<br>30 days initially |

# SCION Integration in SwissPKI

- The organization must be verified once before participation is possible
- An organizational service outside the PKI environment is usually responsible for the verification
- Service subscription is stored in the Identity Repository




- Autorenewal without human interaction
- Checking the identities against the stored service subscription
- Speed and reliability are important




- Short-lived certificates requires high PKI availability
- Failover to backup PKI provider with validation of the existing certificates
- Switch back to the master PKI provider

# Conclusion

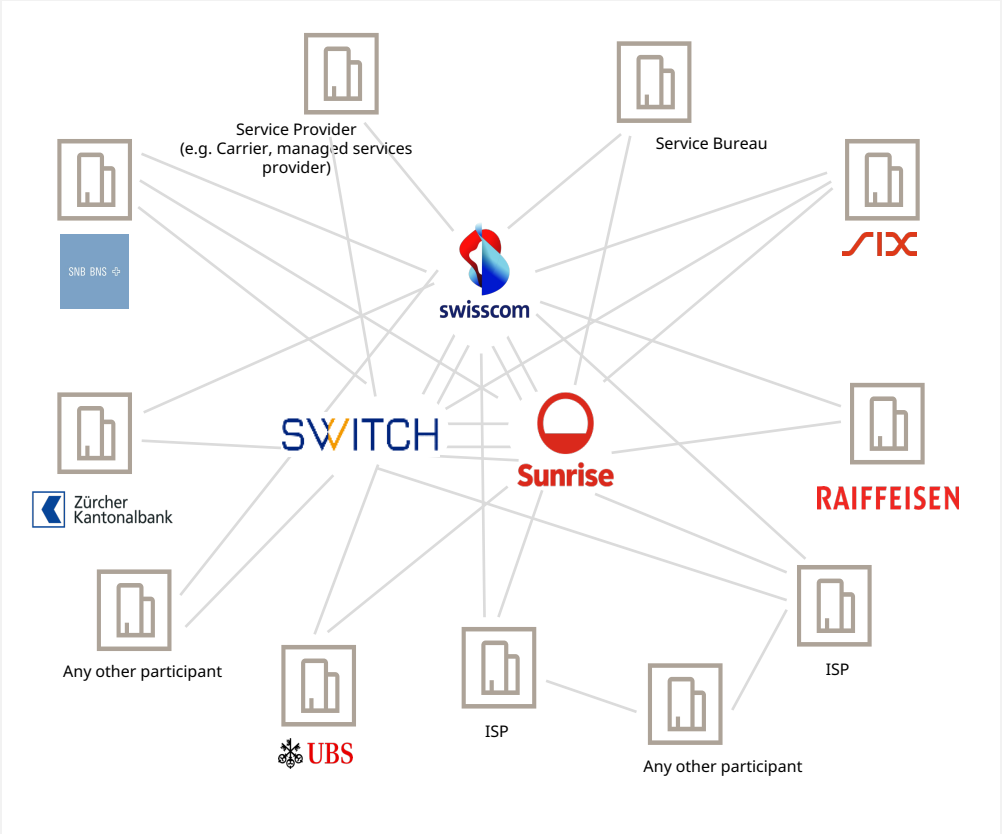
- **The PKI is usually underestimated** when setting up a SCION ISD. However, it is central to the trust within the participant group. Without certificate no participation and without clean processes no trust.
- Having **Enterprise Level PKI** in the portfolio has helped (audited according to Baseline Requirement / Public Trust).
- **Experience** in building a SCION PKI with high requirements (Closed User Group / Financial Network) / Don't re-invent the wheel for your own ISD!

# Secure Swiss Finance Network (SSFN) CA Insights

Fritz Steinmann, Infrastructure Domain Architect, SIX

# SSFN Implementation
## SSFN Specific Attributes

### Schematic view of the SSFN network

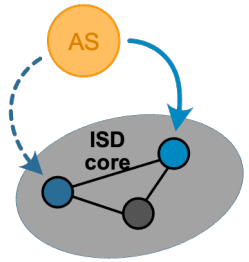



- SSFN is NOT connecting other ISDs
- Based on Anapaya SCION IP gateways (SIG) at customers
  (No SCIONabled Hosts)
- Onboarding via SIX → Identification Process
- Certificate validity
  - Initial AS certificate: 30 days
  - Regular AS Certificate: 3 days
  - CP Intermediate Certificate: 26 months
  - CP Root Certificate: 11 years
- Requirements for admission to SSFN
  - Participant of Swiss financial market (SIC, euroSIC, or SECOM participant) or service providers for participants (e.g. Service Bureau)
  - Not limited to participants in Switzerland
- Only global unique public addressing allowed
- Dedicated DNS service/namespace available

# What Process? It's all about Technology, isn't it?

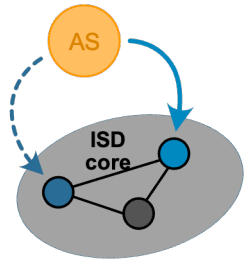
- Identification is key in SCION – else trustworthiness is limited right from the start
- Building and running a (SCION) CA is no easy task, but it's manageable technically
- The challenge is to clearly identify participants:
  - Due to limited SCION adoption needs to be done out of band
  - There is no (established) process like proof of ownership
  - …back to the roots → identification via public or semi-public records issued by some level of (government) authority, ideally certified by notarial act

# How many CA's per ISD?




- A single CA instance in a single AS per ISD is not enough
- Even if built in high-redundant architecture there is risk of failure
- If the CA fails, the ISD fails (eventually)
- Thus, in SSFN a second CA in a different AS was created:
  - Separate instance
  - Different implementation / product
  - Different operator
  - Path diversity due to different AS
- …but also, more challenges:
  - Same or different participant identification process?
  - Signaling, Monitoring?

# Certificate issuing and renewal

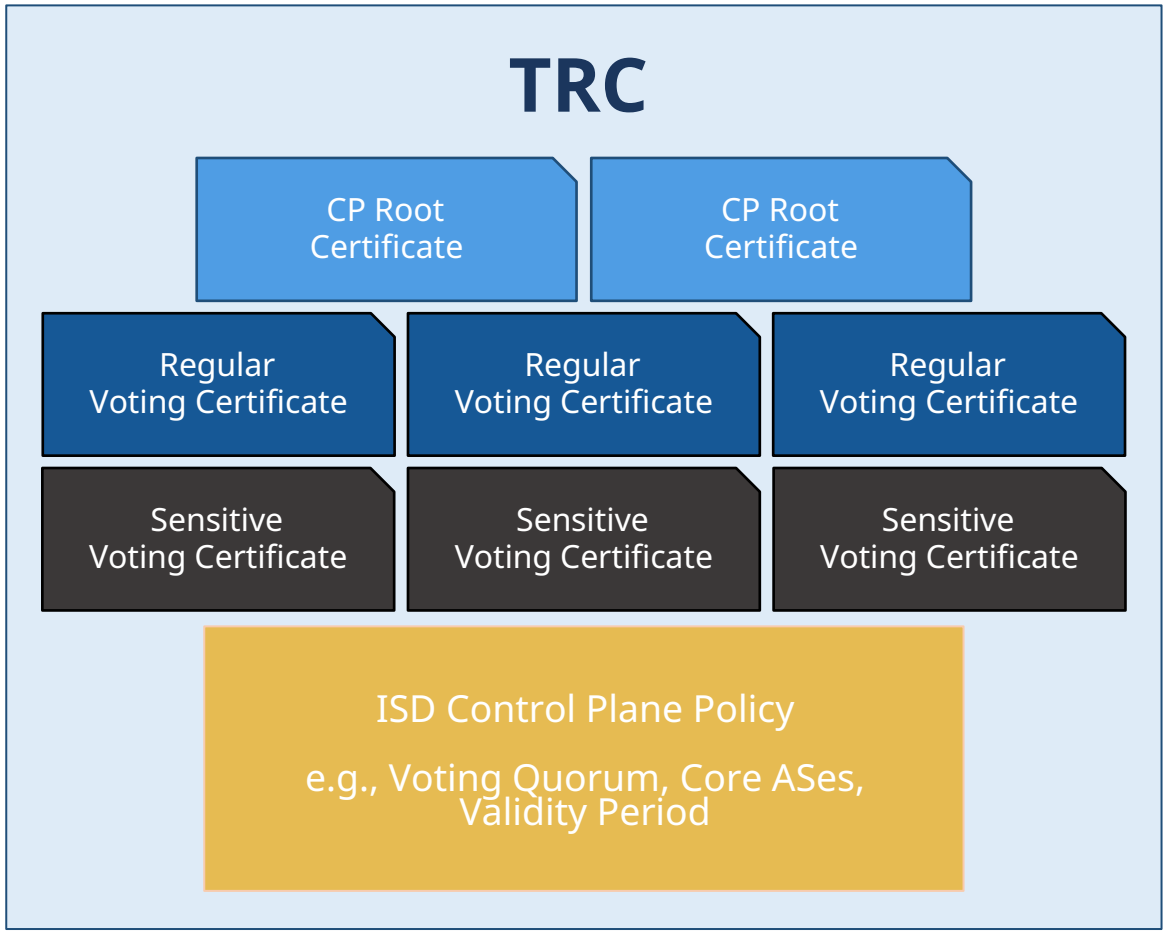


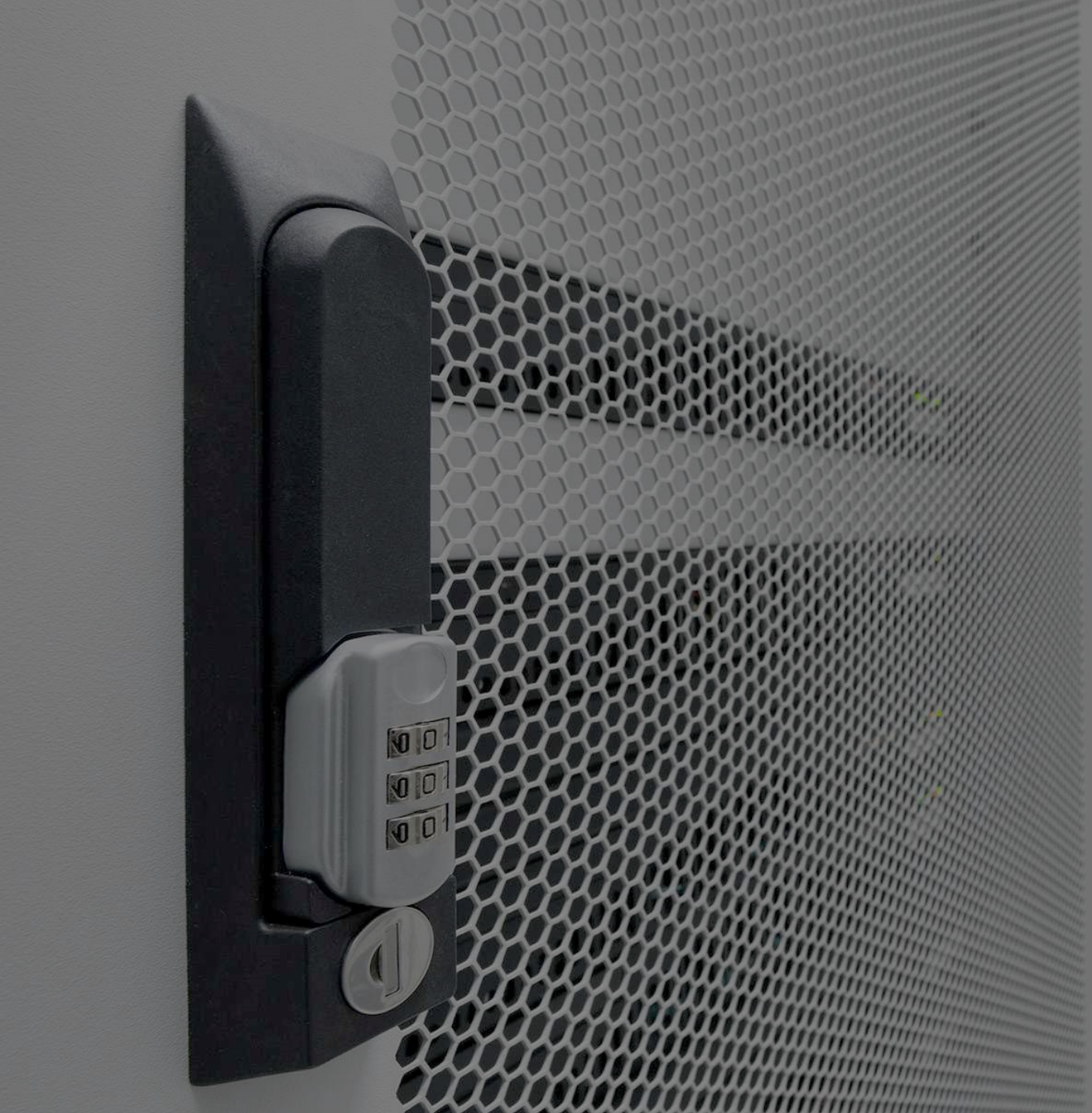

- In SSFN, there is a concept of primary and secondary CA
- Only primary CA will guide participants through identification process
- Secondary CA will refuse participants certificate applications
- Only primary CA issues initial certificate, secondary also refuses initial requests
- Upon first renewal request, secondary could issue certificates, but only does if primary CA is unavailable
- Thus, secondary CA acts as “independent” monitoring instance
- Secondary CA is tested periodically to ensure availability

# Sidenote on TRC's

- TRC's are valid for a predefined period
- Typically, a one-year period is chosen; it could be longer (up to the certificate validity period)
- Renewal (freshly signing the TRC) needs to be done before expiry of the currently valid TRC
- (Yearly) Renewal means access to signing keys, typically kept offline in (network) HSM's
- Yearly access to offline HSM material involves a certain risk of incapability of succeeding (aging, software incompatibilities, loss of know-how…)

→ Make sure you design your TRC validation process properly, including backup and safeguarding. Serious heart attack risks ensue if not tested and proven!





# RESOURCES

www.swisspki.com
www.libc.ch

**SSFN:**
PM-SSFN@six-group.com
www.six-group.com/ssfn
(including Link to Webinar Slides)

**SSFN Service Providers:**
Check complete and up-to-date list of providers on SSFN SSFN homepage

# CONTACT


**SIX Group Services Ltd**
Hardturmstrasse 201
CH-8021 Zürich
www.six-group.com

**libC Technologies SA**
Avenue d'Ouchy 18
1006 Lausanne
Basteiplatz 5
8001 Zürich
call: +41 21 550 1562
info@libc.ch