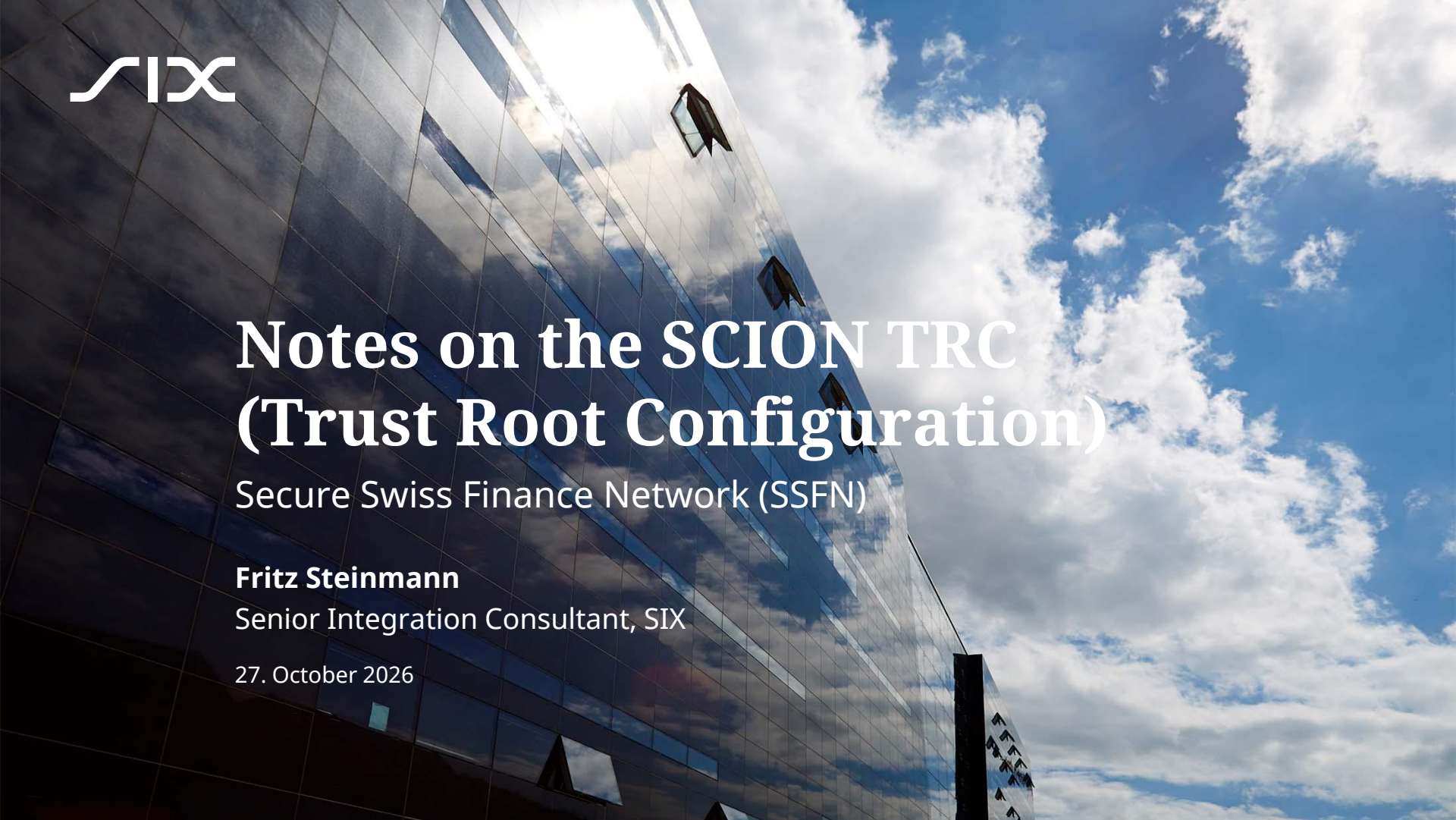


Notes on the SCION TRC (Trust Root Configuration)

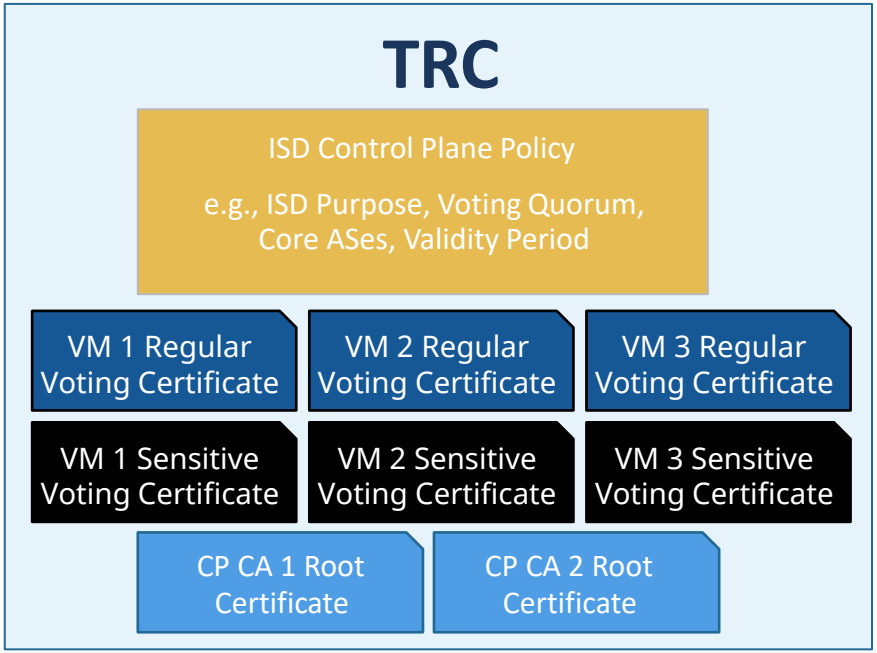
Secure Swiss Finance Network (SSFN)

Fritz Steinmann
Senior Integration Consultant, SIX

27. October 2026

What is the TRC?

- TRC (Trust Root Configuration) is a container for various certificates, declarations and statements
- A TRC consists of:
  - Purpose statement
  - Core and authoritative participants (ASes) → participants with special duties
  - Parameters: ISD ID, base/serial number, Validity period, Voting Quorum etc.
  - Certificates (all CA root certificates, regular and sensitive voting certificates of every voting members)
- A TRC is signed by all the Voting Members to certify its validity and authenticity

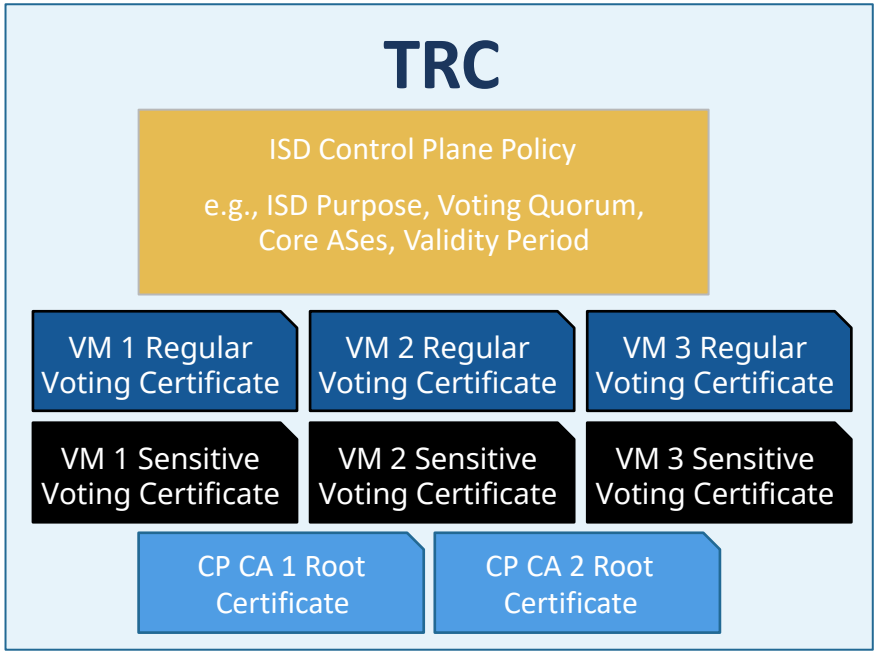


VM: Voting Member, CP: Control Plane, CA: Certificate Authority

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…)

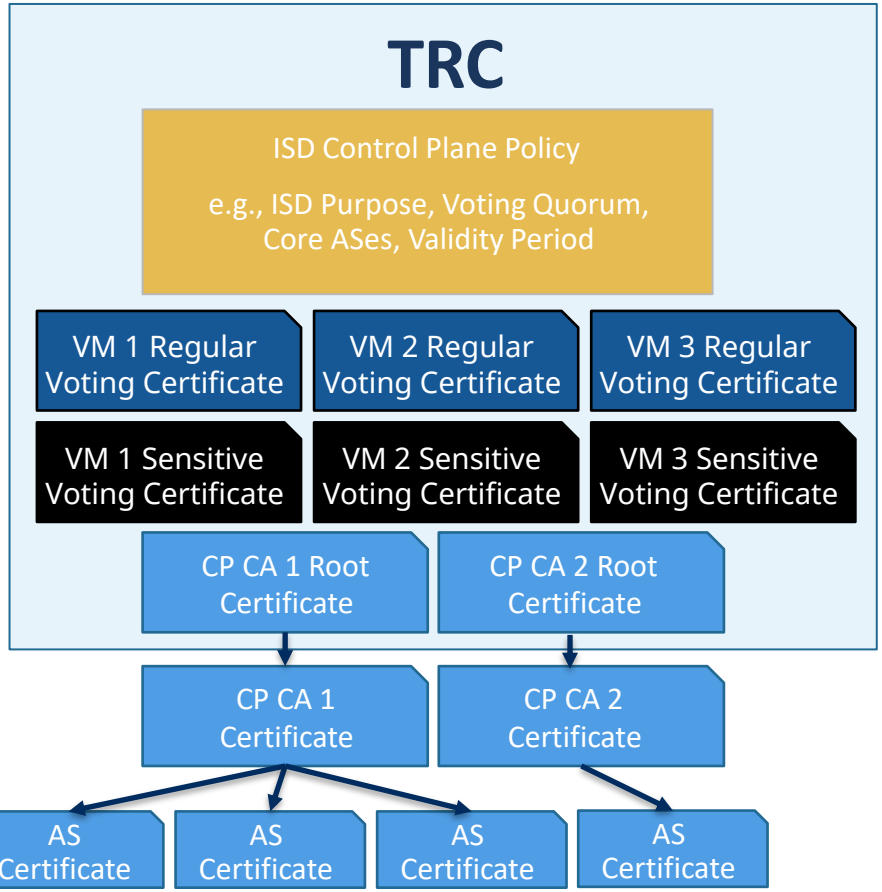
→ Make sure you design your TRC validation process properly, including backup and safeguarding!



VM: Voting Member, CP: Control Plane, CA: Certificate Authority

Certificate Hierarchy

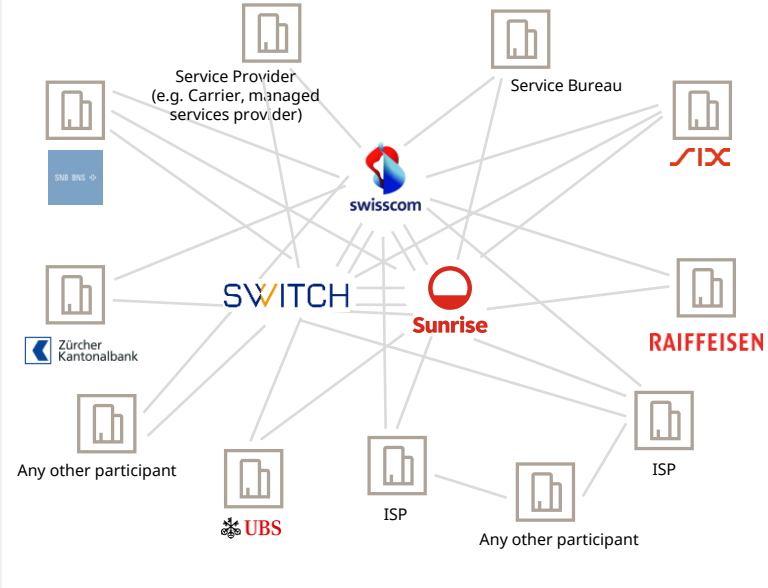
- Designated CAs create their own Root key, and use this key to self-sign their CA Root Certificate (long validity, kept offline)
- The Root Certificate is integrated in the TRC, for everybody to use to verify signatures and certificate hierarchy
- The CAs generate the intermediate (“signing”) key and use it to sign the intermediate Certificate (medium validity, kept online)
- The signing key is then used to sign individual AS CSRs and issues the respective AS certificates (short validity)



VM: Voting Member, CP: Control Plane, CA: Certificate Authority, AS: Autonomous System

SSFN Implementation
SSFN Specific Attributes

Schematic view of the SSFN network



- SSFN is NOT connected to 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
  - Ordinary AS Certificate: 3 days
  - CP Intermediate Certificate: 26 months
  - CP Root Certificate: 11 years
- Requirements for admission to SSFN
  - Participant of Swiss financial market…
  - …but not limited to participants in Switzerland!
- Only global unique public addressing allowed
- Dedicated DNS service/namespace available

Contact & Resources

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

Resources

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