



SCION Integration

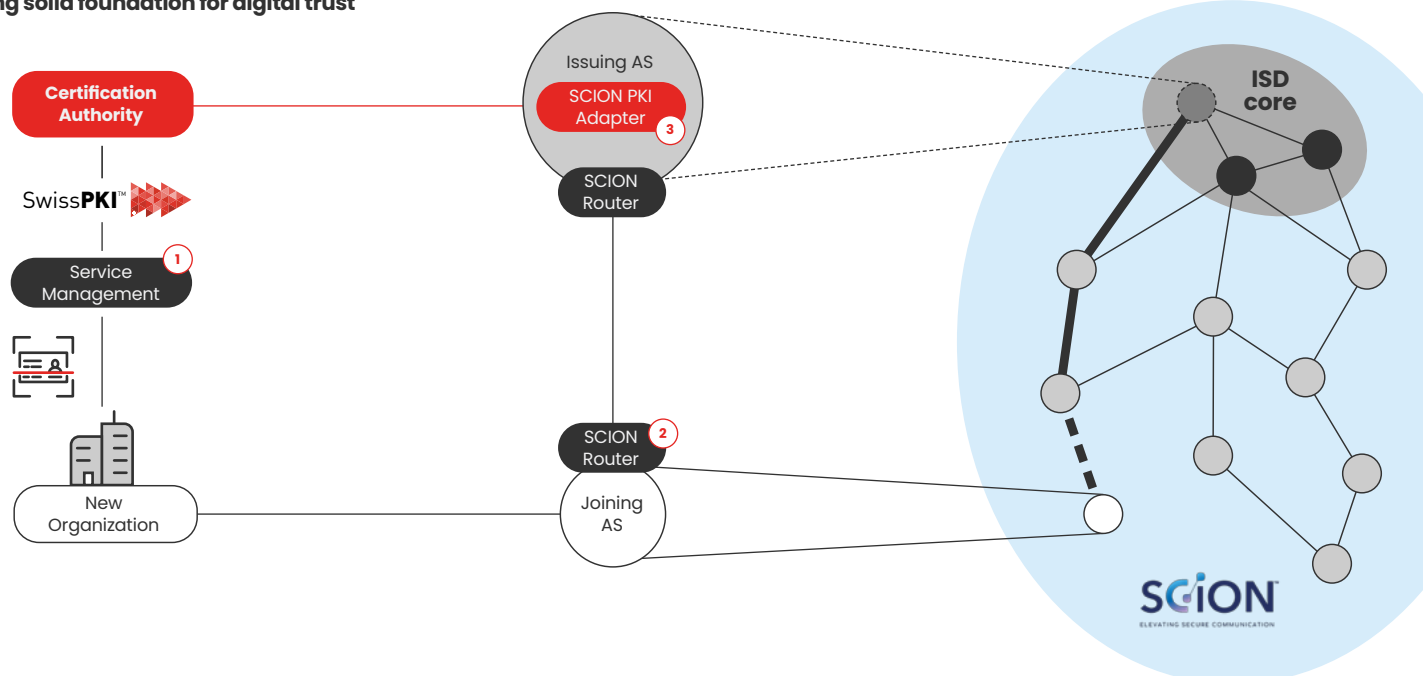
Fact Sheet



SCION Control Plane PKI

SCION is redefining how critical infrastructure operators think about network trust — but a SCION Isolation Domain (ISD) is only as trust-worthy as the PKI behind it. Every path, every control-plane message, and every participant identity in a SCION network is secured by X.509-based AS certificates with lifetimes measured in days, not years. Issuing, renewing, and revoking these certificates reliably, at scale, and without interrupting operations is a discipline in its own right — one that goes far beyond generating a keypair and signing a certificate. SwissPKI™ brings decades of enterprise PKI experience to this challenge, providing the certification backend that powers SCION deployments in Switzerland like the Secure Swiss Finance Network (SSFN), so that ISD operators can focus on their network instead of reinventing PKI operations from scratch.

Building solid foundation for digital trust



- ① Preregistration of participant
- ② Initial out-of-band certificate provisioning
- ③ Fully automated certificate renewal in operation

SCION Cryptography in General

- SCION control plane certificates are based on X.509 / RFC 5280.
- Uses elliptic curve cryptography only.
- No CRL / certificate revocation.
- Short certificate lifetimes for CA and end user certificates.
- Root Certification Authorities are registered in TRC which acts as an ISD's trust list for each ISD.

Advantages of an Enterprise Grade SCION PKI

Setting up a SCION Control Plane PKI is often underestimated: it looks like “just” issuing short-lived X.509 certificates according to an open specification. In practice, an ISD’s trust model lives and dies with the processes around the CA — participant identification, key custody, renewal automation, and resilience against outages. A basic implementation of the SCION cryptography specification gives you certificate signing, but not the organisational and operational scaffolding an ISD needs to run safely:

- **Participant identification is the real challenge.** Before any AS can receive its first certificate, the operating organisation must be reliably vetted — typically out-of-band, since a joining AS has no SCION connectivity yet. This vetting must be documented, repeatable, and tied to an authoritative Identity Repository, not left to ad-hoc scripts around a bare CA.
- **Autorenewal must run unattended, at speed, and reliably.** Certificates with 3-day lifetimes leave little room for error. Renewal requests must be authenticated against stored subscription and identity data automatically, with no human in the loop — something that requires a real service-management layer, not only cryptographic verification.
- **Short lifetimes mean the CA itself becomes a single point of failure.** With no certificate revocation in SCION, availability of the issuing CA is paramount. A production-grade ISD needs a failover concept — a backup CA that can take over, validate existing certificates, and hand back control to the master CA — which is an operational capability, not a protocol feature.

Advantages of an Enterprise Grade SCION PKI

SwissPKI™ with its SCION integration was built from the ground up to cover exactly this layer: identity vetting, service subscription management, automated renewal, and CA redundancy — proven in production for two of Switzerland's most demanding high-security networks.

Benefits

SwissPKI™ acts as the certification backend for SCION ISDs, integrating directly with Anapaya's SCION Control Plane components via the SCION PKI Adapter — a dedicated integration module using a REST/HTTPS interface and protocol jointly developed by libC and Anapaya, which has since become the quasi-standard for CA/Control Service integration in the SCION ecosystem.



Registration Authority Web application for the manual, out-of-band initial certificate issuance process, giving joining ASes a self-service portal to submit CSRs and retrieve certificate chains — before they have SCION connectivity of their own.



Identity Repository integration ensures every certificate only ever contains vetted, verified identity attributes (organisation, country, trade register number, ISD-AS number) — never unverified client input.



Fully automated, unattended certificate renewal over the SCION protocol stack, with signature verification against previously issued AS certificates — no manual steps, no downtime risk from missed renewals.



Multi-tenant CA hierarchies support several ISDs and Issuing ASes from a single platform, with clean separation of Root CA, CP CA, and AS certificate layers, and a naming scheme that keeps generations and instances unambiguous over time.



HSM-backed key protection, including partitioning, role segregation and enabling extended CA certificate lifetimes without compromising security — reducing operational overhead compared to the SCION standard's default weekly/yearly CA rotation.



Primary/secondary CA and failover concepts supported natively, so an ISD can run a second, independently operated CA instance for path diversity and resilience, with defined behaviour for which CA issues, refuses, or takes over during outages.



Exclusion and governance processes for ISD-AS numbers are supported end-to-end, letting an ISD Governance Body enforce exclusions consistently across all Issuing ASes.

The result: ISD operators and Trust Service Providers get a PKI that is operationally boring in the best sense — predictable, automatable, and auditable — instead of a bespoke stack of scripts around raw certificate tooling.

Economies of SwissPKI™ as SCION PKI

- **Full lifecycle, not just issuance.** From out-of-band initial enrolment to unattended machine-to-machine renewal, exclusion handling, TRC-signing support, and CA generation management — the entire certificate lifecycle is covered.
- **Direct, standardised integration with Anapaya's SCION stack** via the REST-based PKI Adapter interface jointly established with Anapaya — proven in production.
- **Proven mature platform, extended for SCION.** SwissPKI™ already supports use cases from small private PKIs to full Public Trust CA operations. Its SCION Control Plane capability builds on this same trusted, audited foundation rather than a purpose-built one-off tool.
- **Built-in resilience.** Native support for primary/secondary CA architectures and failover procedures addresses the single-point-of-failure risk inherent in short-lived, non-revocable SCION certificates.
- **Trusted by Switzerland's most demanding networks.** SwissPKI™ is the certification backend behind both the Secure Swiss Finance Network (SSFN) and the Swiss Secure Utility Network (SSUN) — two closed-user-group ISDs with some of the strictest security and availability requirements in the SCION ecosystem.
- **PKI is our core business, not a side project.** libC has decades of dedicated expertise in building and operating PKI solutions — SwissPKI™ customers benefit from this concentrated know-how.

Your consultation is
just a click away:

[ARRANGE A MEETING](#)

Schedule an appointment with
our experts today.