SCION

Component Analysis

PANRG - IETF 114

28.07.2022

Nicola Rustignoli nicola.rustignoli@inf.ethz.ch
Corine de Kater corine.dekatermuehlhaeuser@inf.ethz.ch

draft-rustignoli-panrg-scion-components

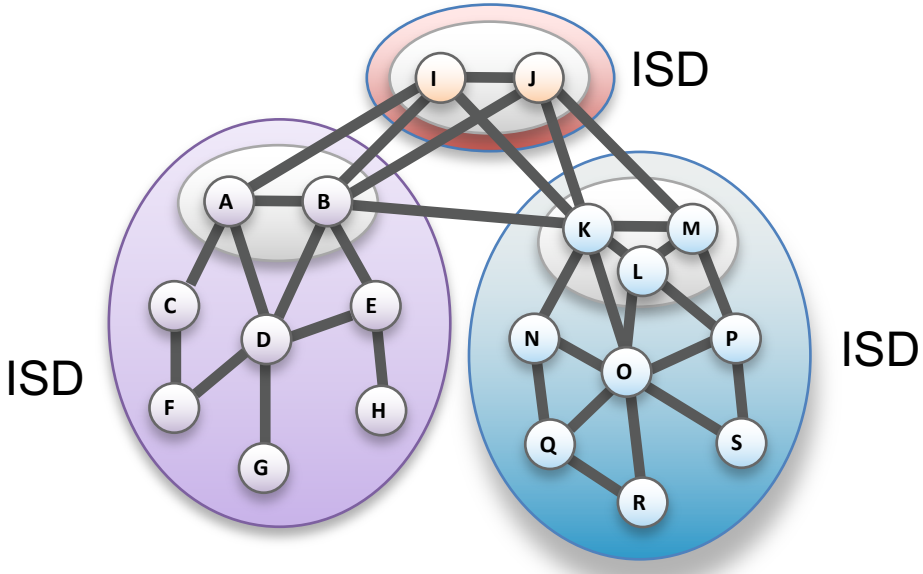
Background: the SCION Internet Architecture

- Path-aware inter-domain Internet Architecture, focused on
  - Availability (in presence of adversaries)
  - Security
  - Scalability
- Started in 2009 to study security of inter-domain routing protocols
- In production use by 7 ISPs, trial deployment by 5 ISPs serving the Swiss inter-banking network

For a general overview about SCION, see: draft-dekater-panrg-scion-overview

Background: SCION and Isolation Domains

- **Isolation Domain (ISD)**: grouping of Autonomous Systems (AS)
- **ISD core**: ASes that manage the ISD and provide global connectivity
- **Core AS**: AS that is part of ISD core
- **Two-level hierarchical routing**: inter-ISD and intra-ISD



draft-rustignoli-panrg-scion-components

Ongoing Work

- IETF 113: First discussions at RTGAREA open meeting & side meeting

- PANRG Interim June 1st 2022:
  → overview draft draft-dekater-panrg-scion-overview

- Today: SCION component analysis
  →draft-rustignoli-panrg-scion-components

Today's Questions

Goals:

- What are SCION components and their dependencies? Can they be split?

- What protocols are reused or extended? Why?

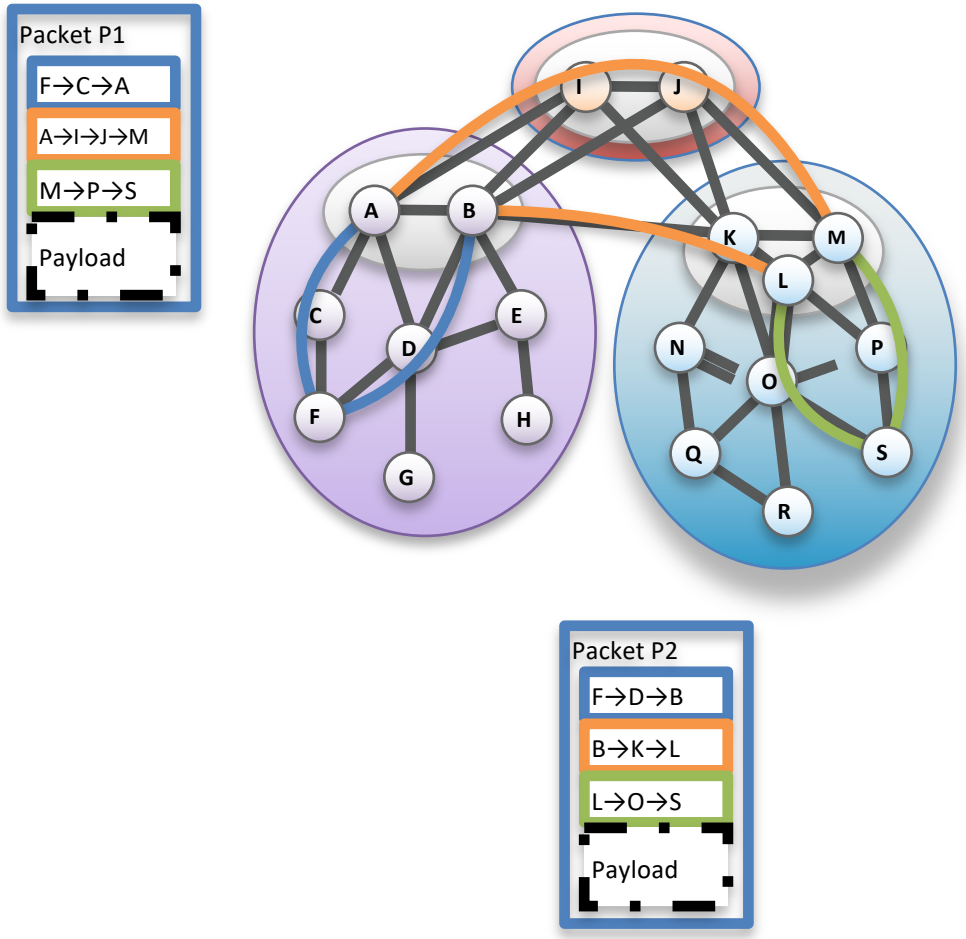
draft-rustignoli-panrg-scion-components

SCION Core Components in a Nutshell

Control Plane PKI (CP-PKI) - Authentication
- Authenticate path information
- Used by control plane
- Basis for unique ISD trust model

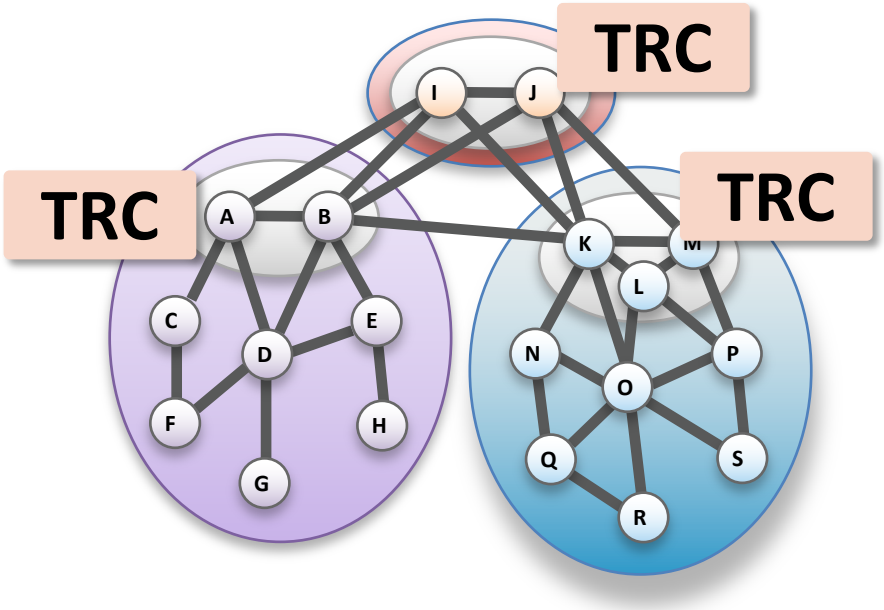
Control Plane - Routing
- Construct and disseminate path segments
- Authenticated with CP-PKI

Data Plane - Packet forwarding
- Forward packets based on path
- Combine Path Segments into end-to-end path
- Packets contain path



draft-rustignoli-panrg-scion-components

Control Plane PKI
Authentication



Required

- **Initial certificate** ceremony
- Coarse **time synchronization**
- **Communication** to other ASes

Functions and properties

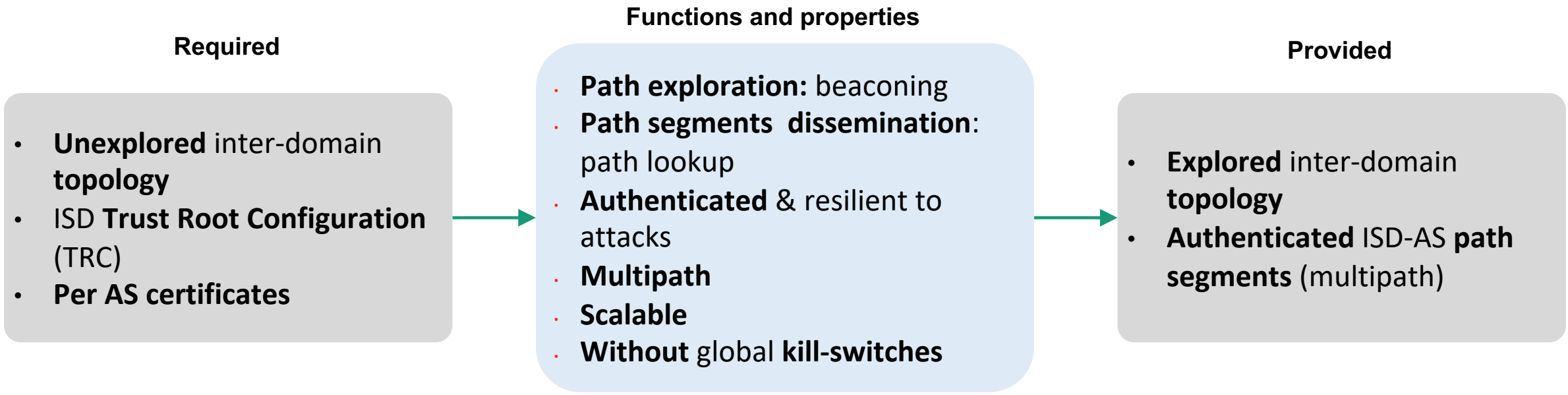
- **Flexible trust** (scoped per ISD)
- **Resilience to single entity compromise**
- **Multilateral governance**: ISD voting process
- Support for policy **versioning & updates** (TRC)

Provided

- **Per ISD Trust Root Configuration** (TRC) with ISD policies
- **Per AS certificates** (verified with TRC)

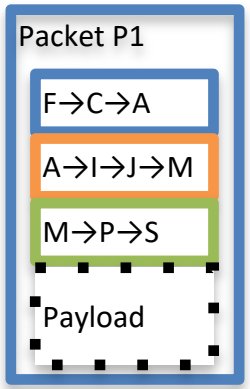
draft-rustignoli-panrg-scion-components

Control Plane
Routing



draft-rustignoli-panrg-scion-components

Data Plane
Packet forwarding



Required

- **Validated path segments** (per AS and interface granularity)
- **Authenticated error messages**
- **Application requirements** (e.g., latency, geofencing)

Functions and properties

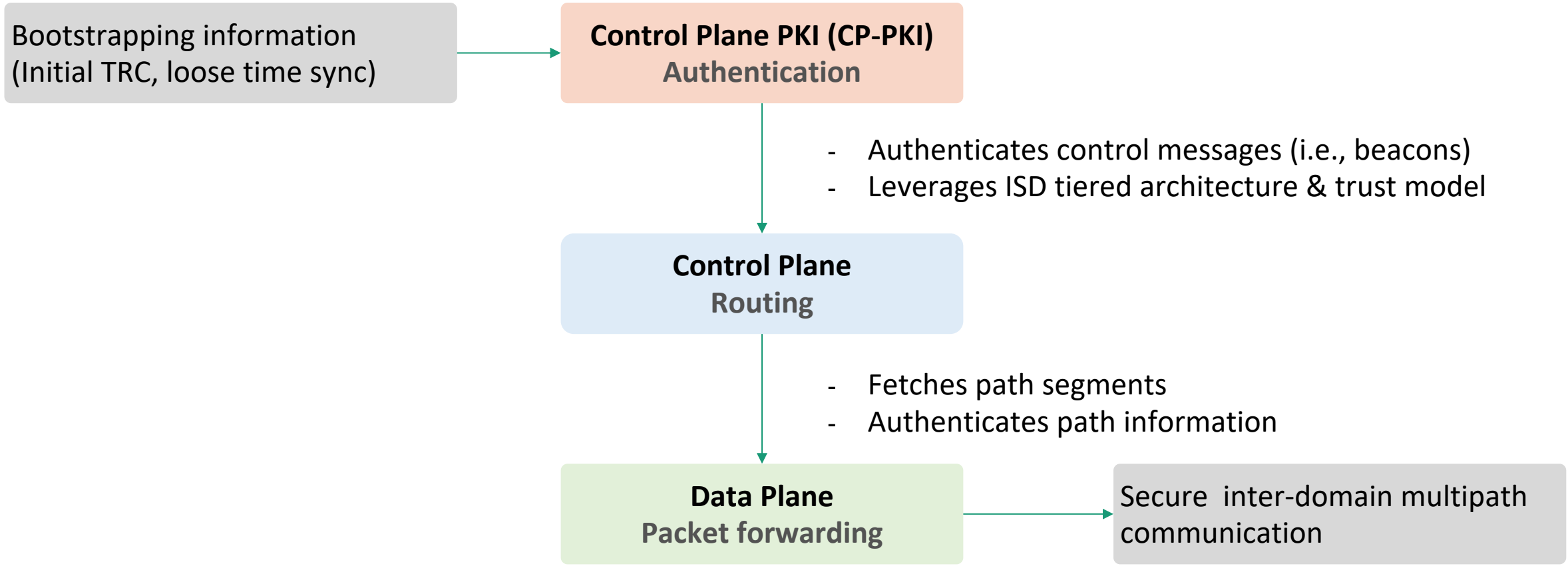
- Combine path segments into end-to-end Paths
- **Simple, stateless routers**
- Forward packets based on Path
- **Reuses intra-AS topology**
- **Decouples locator (ISD-AS) / identifier**
- **Handling of failures via alternate paths**

Provided

- **Secure inter-domain multipath communication**
- **Source-selected paths** (in packet header)

draft-rustignoli-panrg-scion-components

Core Components: Dependencies



draft-rustignoli-panrg-scion-components

Relationships to Existing Protocols

Control Plane PKI (CP-PKI)
Authentication

- Built on X.509 (RFC5280)
- Differs from other PKIs because of its trust model (there are no omnipotent entities, voting process)

Control Plane
Routing

- Existing intra-domain routing protocols are reused
- Transition mechanisms leverage RPKI for prefix origin attestation
- Path selection pushed to end hosts: existing end-to-end mechanisms can be leveraged
- Control messages are all authenticated

Data Plane
Packet forwarding

- Reuses intra-domain forwarding & network fabric (e.g., SR, MPLS, …)
- SCION routers are only deployed at edge
- Can reuse existing end-host addressing schemes (e.g., IPv6/IPv4)

draft-rustignoli-panrg-scion-components

Summary

- SCION is is based on 3 core components: control plane, data plane and PKI.
- The Control Plane PKI provides basis for other components
- SCION's approach allows to achieve properties that are not otherwise possible

draft-rustignoli-panrg-scion-components

Next Steps

- Discussion: feedback on draft & presentation

- How about starting further work?
  - Advance overview draft
  - Initial specification
  - Pave the way for later standardization work

draft-rustignoli-panrg-scion-components

Backup slides

Related Work

- RPKI
  - **SCION extensions use RPKI** for prefix origin validation
  - SCION has a distinct trust model
  - **Protects route origin, rather than path**
- BGP extensions
  - Routing decisions made by network, no end-to-end path control
  - BGP ADD-PATH and BGPSec face **scalability** challenges
- Transport protocols & multipath
  - **Multipath transport could perhaps use paths provided by SCION** → Ongoing path-aware networking API discussion (taps)
  - Allows to leverage multiple last-mile links, but not end to end path (including network core)
- Semantic Routing
  - Path selection at end hosts rather than in network
  - Semantics **limited to a trusted domain**

draft-rustignoli-panrg-scion-components

SCION Contrasted to Segment Routing

SCION	Segment Routing
Inter-domain	Intra-domain
To be deployed between untrusted entities (security-focus)	To be deployed in trusted domain
Paths authenticated	Paths unauthenticated
L3 (directly on top of L2) or optionally encapsulated in IP/UDP	On top of IPv6 EH or MPLS
Full path control to endpoint (massive multipath)	Partial path control
AS granular	Router granular
Path encoded in header – no state at routers	
Support for Traffic Engineering	

draft-rustignoli-panrg-scion-components

SCION Contrasted to LISP

SCION	LISP
Decouples the routing locators and identifiers	
Secure path-aware networking (performance, availability, geofencing, flexible trust)	- no authentication
Mapping between two spaces: open	Mapping between two spaces
Routing Locator: ISD-AS Endpoint Identifier: any (i.e. IP)	Routing locator: RLOCs Endpoint Identifier: EID Using IP address format
Changes needed in the network (peering links between routers, optionally a SCION to IP GW at edge)	Change needed at the edge (LISP router)
Translation: SCION IP Gateway	Translation: Egress Tunnel Router (ETR)

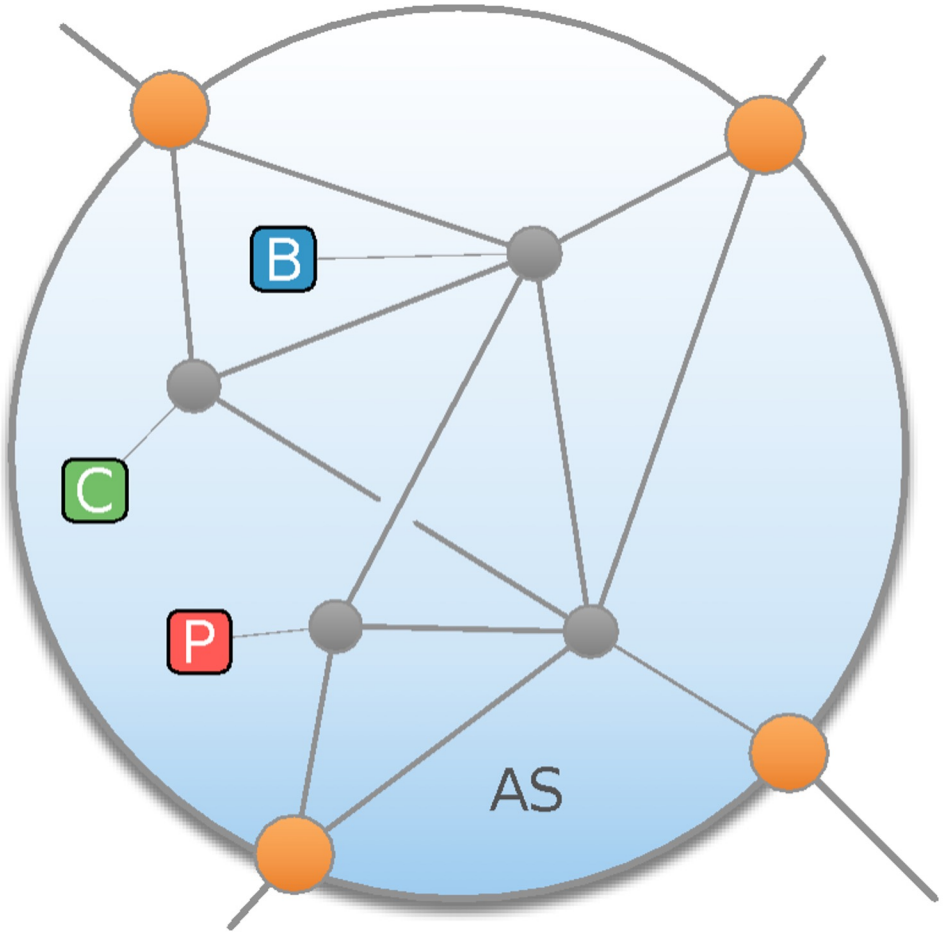
draft-rustignoli-panrg-scion-components

Bootstrapping a SCION AS

1. A set of core ASes founds an ISD with an initial TRC ceremony
2. An AS deploys control plane & PKI services, and a border router with links to an existing SCION AS
3. Trust: the AS devices are pre-loaded with a base root certificate of its own ISD (and optionally, of other trusted ISDs). Certs can be optionally distributed by the control plane.
4. The AS can start beaconing, register its paths into the core, and it becomes reachable

draft-rustignoli-panrg-scion-components

Deployment Model – SCION AS

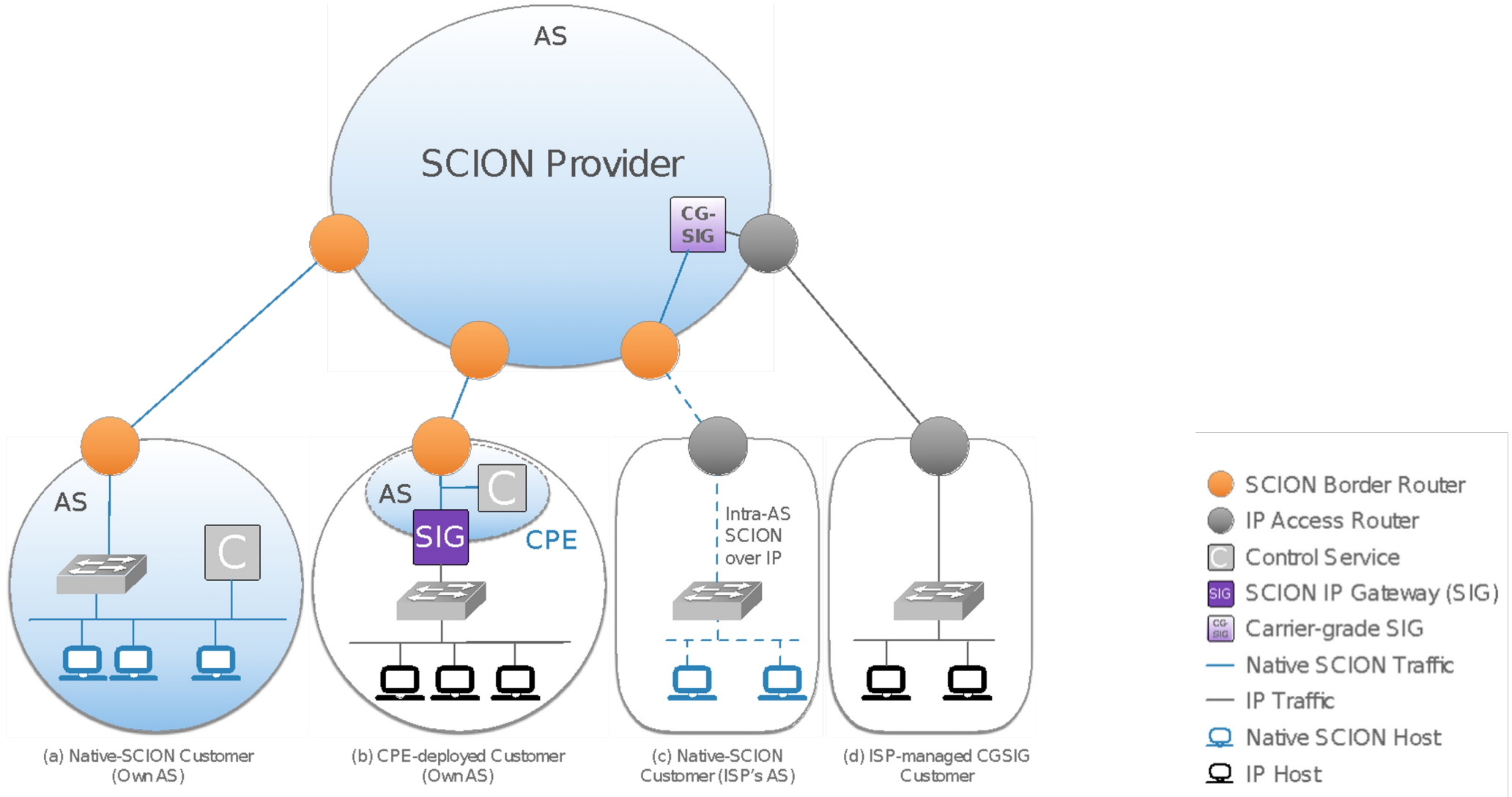


- CORE routers are set up at the borders of an ISP
  - to peer with other SCION-enabled networks
  - to collect customer accesses
- No change to the internal network infrastructure of an ISP needed

P Path service
B Beacon service
C Certificate service
Border router
Internal router

draft-rustignoli-panrg-scion-components

Deployment Model – End customer



draft-rustignoli-panrg-scion-components

Can we use the control plane PKI alone?

- SCION PKI has no strict dependencies on other components (but it does need some sort of transport)
- There is no connectivity nor forwarding in the PKI
- Its unique trust model can be leveraged by other systems
  - Symmetric keys could be used for further development of authentication between ASes (i.e. control-plane messages)
    - e.g., providing internet-wide symmetric key derivation between ASes based on a hierarchical key derivation (draft-garciapardo-panrg-drkey)

Can we use the control plane alone?

- How are paths authenticated?
  - Could reuse existing PKI (i.e. web PKI) with one global ISD?
    → Missing a flexible trust model
  - If we have a “global ISD”, who would be the core ASes administering the network?

- Control plane would miss the critical ISD model
  - Scalability concerns (as there would be one global routing process)

draft-rustignoli-panrg-scion-components

Can we use the data plane alone?

- How are paths fetched and authenticated?
  - Need a control plane to discover, disseminate and authenticate path segments
  - Needs authenticated control messages
- Data plane would miss the critical ISD model
  - No scoped trust (i.e. used in the finance industry deployments)
  - Presence of kill switches
  - No distinction of core/non-core ASes causes additional issues (e.g., scalability on the CP, raising questions on how to limit the amount of paths)

draft-rustignoli-panrg-scion-components

Control Plane

Control Plane - Routing
- Constructs and Disseminates Path Segments
- Authenticated with CP-PKI

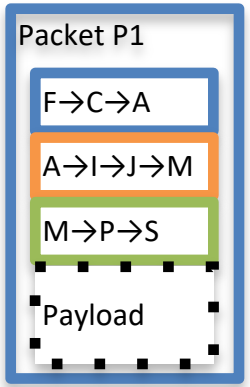
- Main functions
  - Path exploration → path segments
  - Path dissemination → senders request segments
  - Certificate dissemination/renewal → needed for segment verification
- Properties:
  - **Hop by hop path authorisation**: segments are authenticated with Message Authentication Codes (MACs). Control messages are authenticated.
  - **Multipath**: multiple (possibly disjoint) paths made available to hosts
  - **Scalable**: 2-tiered structure (intra & inter-ISD) helps scale routing process
  - **Fast**: routing information is disseminated to create path segments, which can be immediately used for communication. There is no need to iteratively converge.
  - **Address-agnostic**: routing based on locator (ISD, AS), not on end-host identifier (i.e. IP)

draft-rustignoli-panrg-scion-components

Data Plane

Data Plane - Packet forwarding
- Forward packets based on Path
- Combine Path Segments into end-to-end Path
- Packets contain Path
- Simple routers, stateless operation

- Main functions:
  - Inter-domain forwarding → with authentication
  - Path revocation → signal failures to end hosts
- Properties
  - **Routing decisions pushed to end hosts**: Forwarding information is encoded in the packet header.
  - **Scalable**: no forwarding tables. Routers only verify the authenticity of path segments. One AES operation replaces longest-prefix match
  - **Highly available:** failures are securely signalled, end hosts can immediately use alternative paths (within RTT)
  - **Secure**: paths are validated at each hop
  - **Extensible**: support for extension headers (similarly to IPv6)



draft-rustignoli-panrg-scion-components

Control Plane PKI

Control Plane PKI (CP-PKI) - Authentication
- Authenticates path information
- Used by Control and data plane
- Basis for unique ISD trust model

- Main functions
  - Provides the control and data plane ways to authenticate control information
- Properties:
  - **Unique trust model**: trust scoped within an ISD, there is no omnipotent entity and no global kill-switches.
  - **Resilient to compromise:** cone compromised entity does not compromise the whole ISD
  - **Trust flexibility**: ISDs can define their own trust policy

draft-rustignoli-panrg-scion-components