



# Control Plane

RTGWWG - IETF 117

25.07.2023

Nicola Rustignoli ([nic@scion.org](mailto:nic@scion.org))  
Corine de Kater ([cdekater@scion.org](mailto:cdekater@scion.org))

# Background: the SCION Internet Architecture

- Path-aware *inter-domain* Internet architecture, focusing on
  - Availability (even in presence of adversaries)
  - Security (routing)
  - Scalability
- In production use by 7 ISPs, trial deployment by 5 ISPs, serving the Swiss inter-banking network [SSFN](#) & an [education network](#), being tested for the Swiss health network.
- For a general overview about SCION, see: [draft-dekater-panrg-scion-overview](#)

# SCION Drafts

SCION Overview

[draft-dekater-panrg-scion-overview-03](#)

Last discussion at RTGWWG was at IETF115, with a general introduction

SCION Component Analysis  
[draft-rustignoli-panrg-scion-components-02](#)

**Data Plane**  
Packet forwarding  
Available by Q3

**Control Plane**  
Routing  
[draft-dekater-scion-controlplane-00](#)

**Control Plane PKI**  
Authentication  
[draft-dekater-scion-pki-02](#)

[draft-dekater-scion-controlplane-00](#)

# SCION Core Components in a Nutshell

## Data Plane - Packet Forwarding

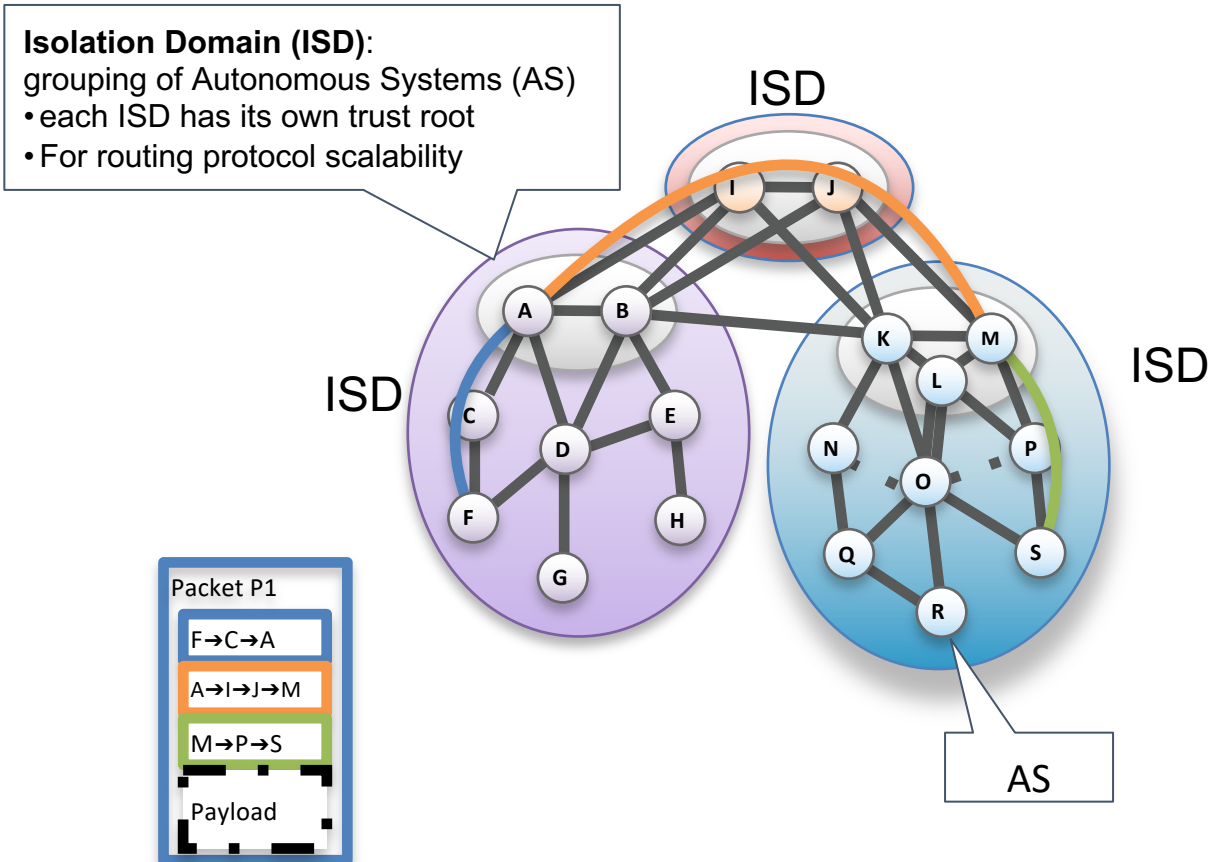
- Combine path segments into end-to-end path (ISD-AS level)
- Packets contain end-to-end ISD-AS path
- Forward packet based on e2e path, agnostic of end-host address

## Control Plane – Inter-Domain Routing

- Discover valid inter-domain paths
- Construct and disseminate path segments
- Routing is based on <ISD>-<AS> tuple as “locator”
- Intra-AS communication reuses existing data plane and routing (e.g., IPv6/IPv4)

## Control Plane PKI (CP-PKI) - Authentication

- Authenticate path information
- Used by control plane
- Basis for unique ISD trust model



# Interoperability

- Transition mechanisms exist (e.g. SCION-IP gateway), however they are outside of scope of this draft. More info in [draft-dekater-panrg-scion-overview-03](#)
- There are no prefixes in SCION → Transition mechanisms based on SCION extensions leverage RPKI for origin validation
- Intra-AS routing and forwarding is used for intra-AS communication
- Path selection is left to endpoints – existing end-to-end mechanisms can be reused

# Routing Process Phases

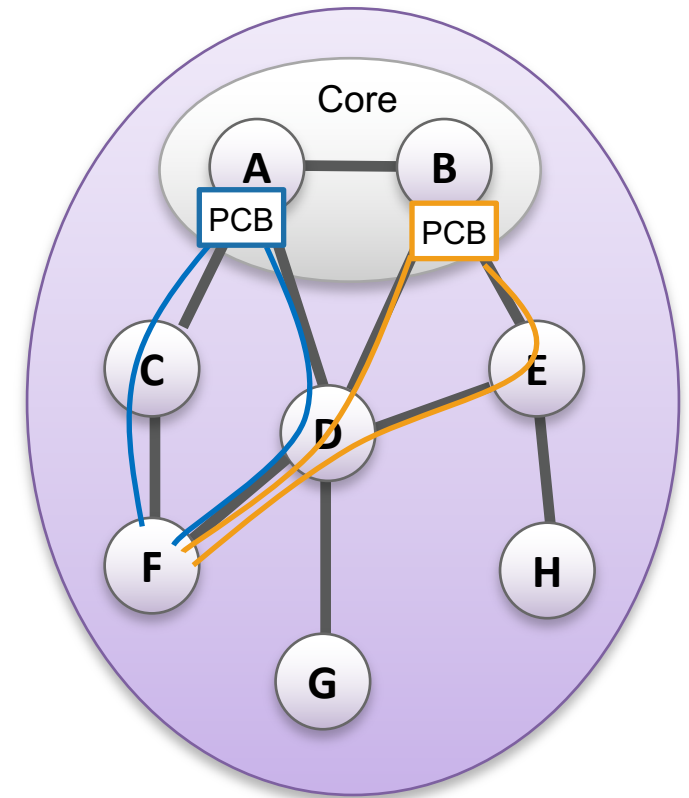
- **Exploration (beaconing):** SCION control plane discovers valid paths through “beaconing”
  - inter-ISD “core” beaconing (core to core)
  - intra-ISD “down” beaconing (parent to child)
- **Registration:** ASes select path segments and make them available to other ASes
  - Each AS can freely choose selection algorithm and criteria
  - Reversion of path segment direction is possible
- **Resolution (lookup and combination):** Source endpoint creates an e2e path by
  - looking up path-segments to destination AS (control plane)
  - combining path-segments into e2e path (data plane)
  - Endpoint chooses path based on application requirements

SCION AS  
control  
service

SCION  
endpoint

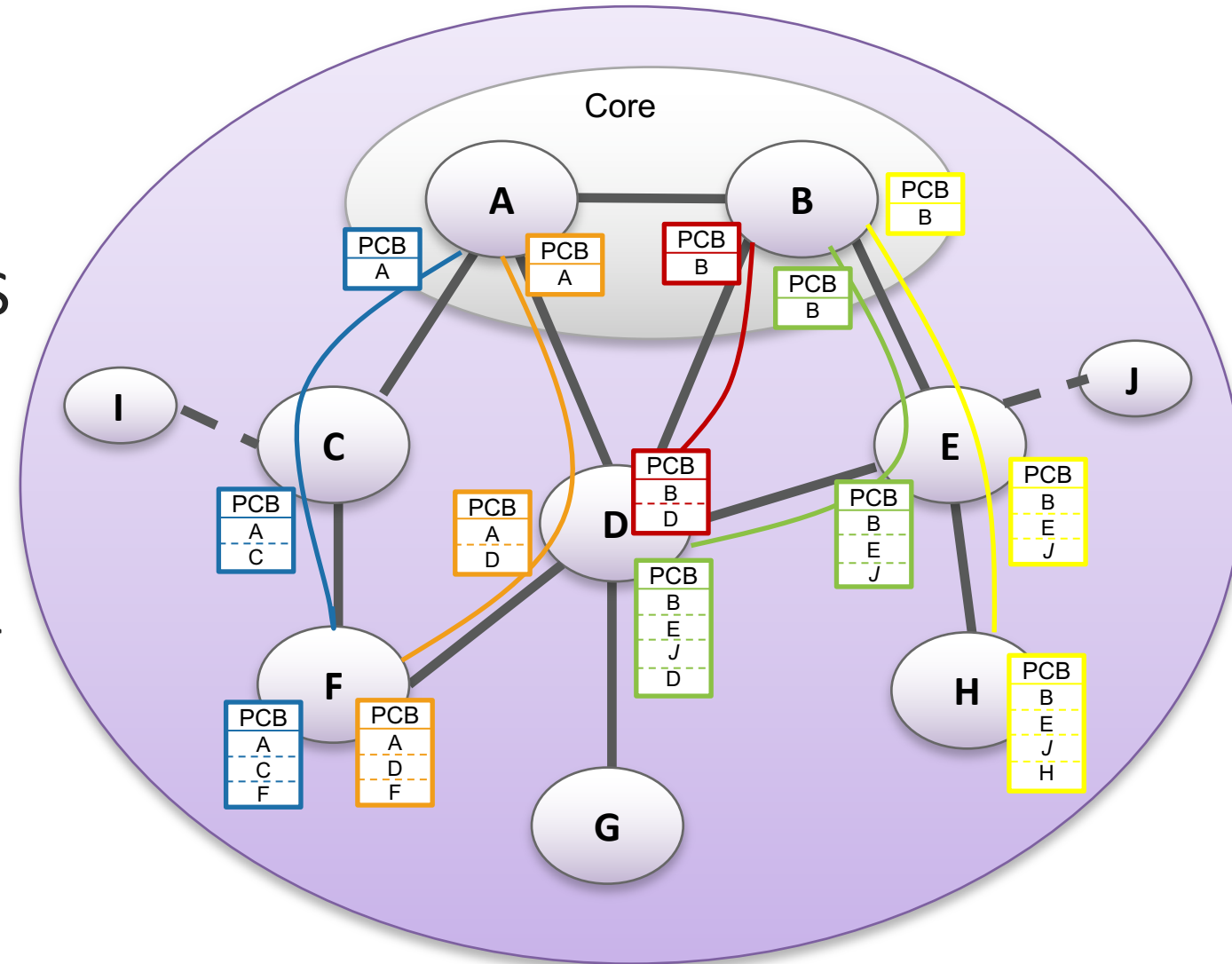
# Path Exploration: Beacons I

- Core ASes periodically send Path Construction Beacons (PCBs)
  - **Inter-ISD** “core” beacons are sent without direction
  - **Intra-ISD** beacons travel top-down (parent to child)
- Each AS stores received beacons in a beacon store
- Per propagation period, each AS
  - selects a subset of the received PCBs according to its needs,
  - appends its AS routing information, and
  - further propagates the selected PCBs to neighbors



# Path Exploration: Beaconing II

- PCBs accumulate cryptographically protected path- and forwarding information per traversed AS
- Key content of one PCB:
  - Initiation timestamp
  - Expiration time
  - ID
  - List of all ASes on the path so far
  - Signed routing information per AS



# Path Registration

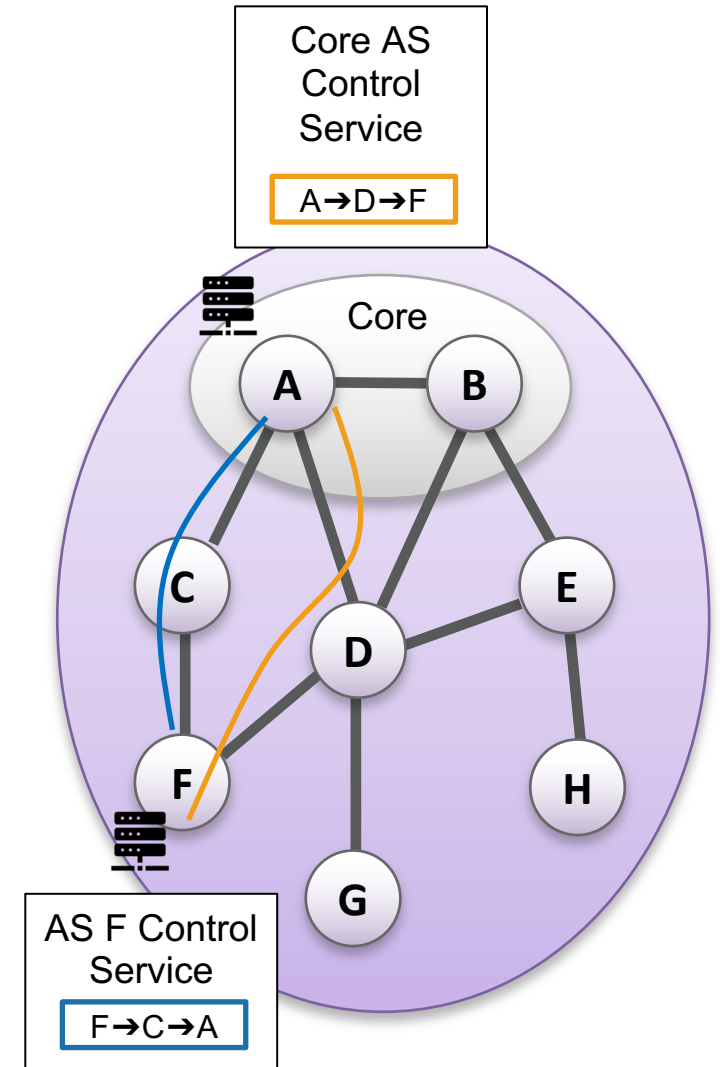
Each AS periodically stores/registers selected PCBs as **path segments** (**up-path** or **down-path**)

- **Up-path** segments
  - How the AS wants to reach its core AS(es)
  - Stored at the AS's local control service
- **Down-path** segments
  - How the AS wants to be reached by other ASes
  - Registered with the control services of the relevant core ASes

## Example

AS F selects PCBs **A-C-F** and **A-D-F** (in beaconing direction), and

- Turns PCB **A-C-F** into the **up-path** segment **F-C-A**, storing it at its own control service
- Turns PCB **A-D-F** into the **down-path** segment **A-D-F**, registering it with the control services of its core ASes.



# Path Resolution

Source endpoint creates e2e path by

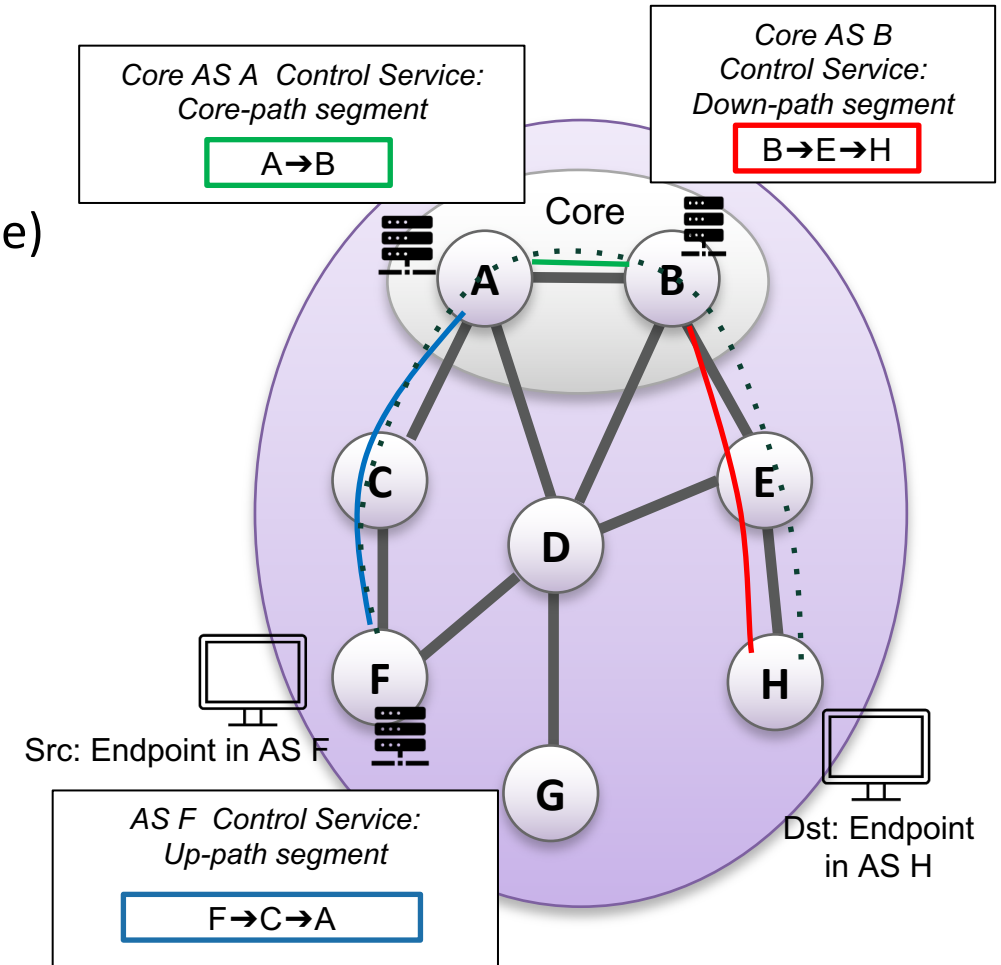
- looking up path-segments to destination AS (control plane)
- combining path-segments into e2e path (data plane)

Requires lookup of max. **3** path segments:

- **Up-path segment**
  - To reach **core AS** in **source ISD**
  - Responsible: control service of **source AS**
- **Core-path segment**
  - To reach **core AS** in **destination ISD**
  - Responsible: control service of **core AS** in **source ISD**
- **Down-path segment**
  - To reach **destination AS**
  - Responsible: control service of **core AS** in **destination ISD**

To improve efficiency:

- Cache returned path segments
- Send requests for path segments in parallel



# Security Considerations\*

- **PCBs are signed** in an onion fashion in order to avoid path hijacks/splicing. Every AS can verify all routing messages by following the certificate chain.
- **Hop-by-hop path authorisation:** Information on each hop is authenticated with a MAC (Message Authentication Code), checked by routers at forwarding → Each AS only forwards traffic on paths that are explicitly authorized
- **Lack of global kill-switches:** Roots of trust are ISD-scoped, thanks to the use of own PKI (CP-PKI [draft-dekater-scion-pki](#))

\*Section not available in -00 draft yet, will come soon

# Summary & Next Steps

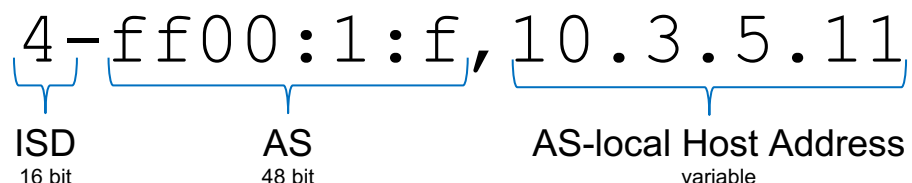
SCION is a future Internet architecture with productive deployment  
Its control plane provides path-aware, secure inter-domain routing

- Feedback is welcome
- More work to do on draft:
  - Security considerations, IANA section

# Backup slides

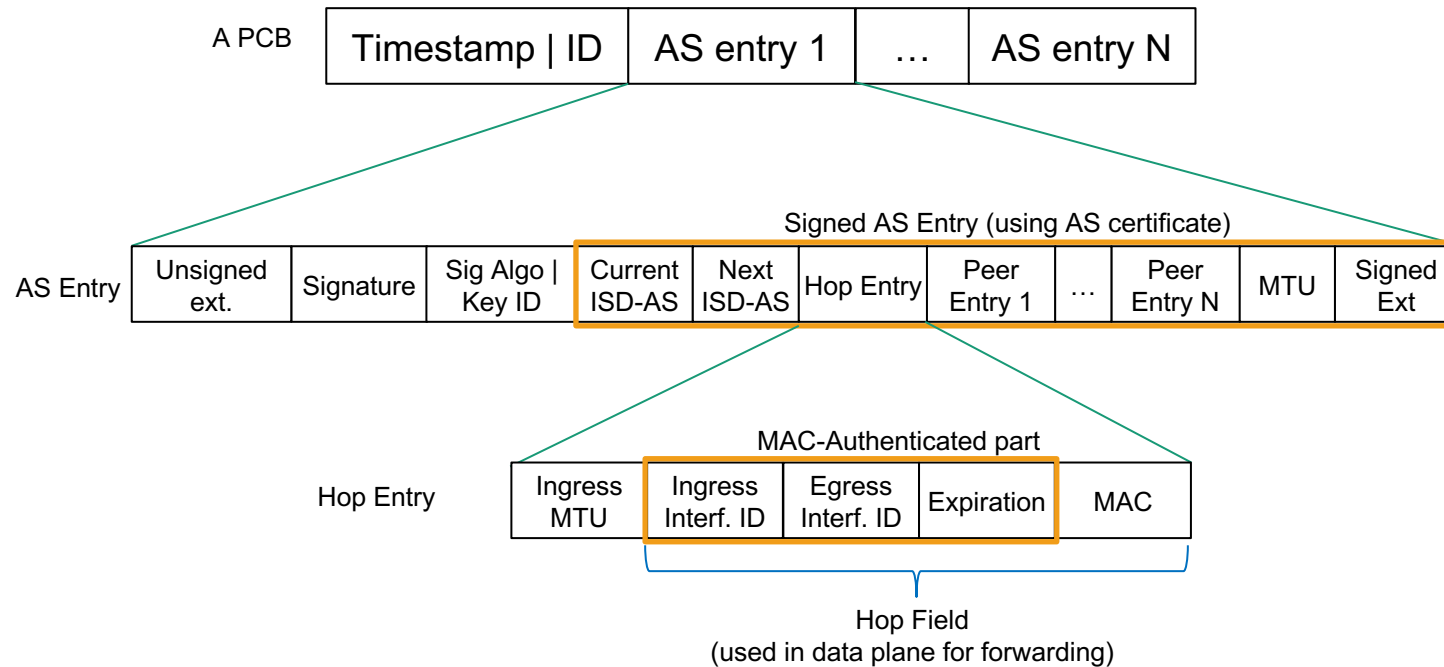
# SCION Addresses

SCION provides communication between SCION endpoints. A SCION address looks like:



- Routing is AS-granular and it is based on the <ISD>-<AS> tuple as “locator”
- *Intra-AS* communication reuses existing data plane and routing (e.g. IPv6/IPv4)

# PCB Message Format



PCBs support signed and unsigned extensions