ICN+SCION Global Name-based Network Service

Thanks: NSF CNS-2512457
EAGER: NDN+SCION: Toward a global name-based network service
Also: David Hausheer, ETH

Jeremiah S. Davis
Jakob Duerstock, Ken Calvert
University of Kentucky

Agenda

I. What are we doing?
II. Why?
III. Background
   - SCION
   - RHINE
IV. ICN+SCION Design Goals, Initial Design & Status
V. Takeaways

I. What are we doing?

Combining existing network-layer protocols/services

- NDN/CCNx
  - Named-Data Networking/Content-Centric Networking (NDN/CCNx)
  - Network service delivers Data Objects requested by name
- SCION inter-domain routing/forwarding system
  - Secure, path-oriented replacement for BGP
  - Packets carry path indicating domains to traverse

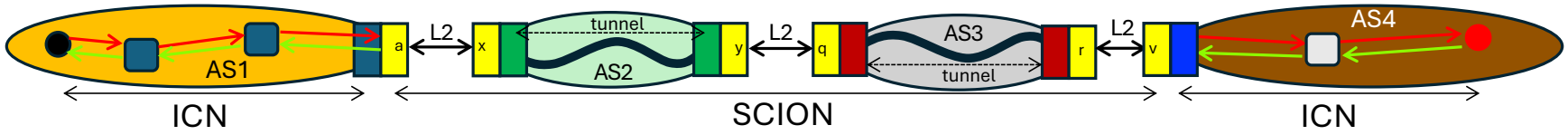
to create a scalable end-to-end network (layer 3) service, that:

- has trustworthiness of data as a fundamental, built-in feature
- is compatible with existing Internet ecosystem
- supports heterogeneous trust structures at network and application layers
- supports multipath transmission natively
- does not depend on IP at any level

Terms

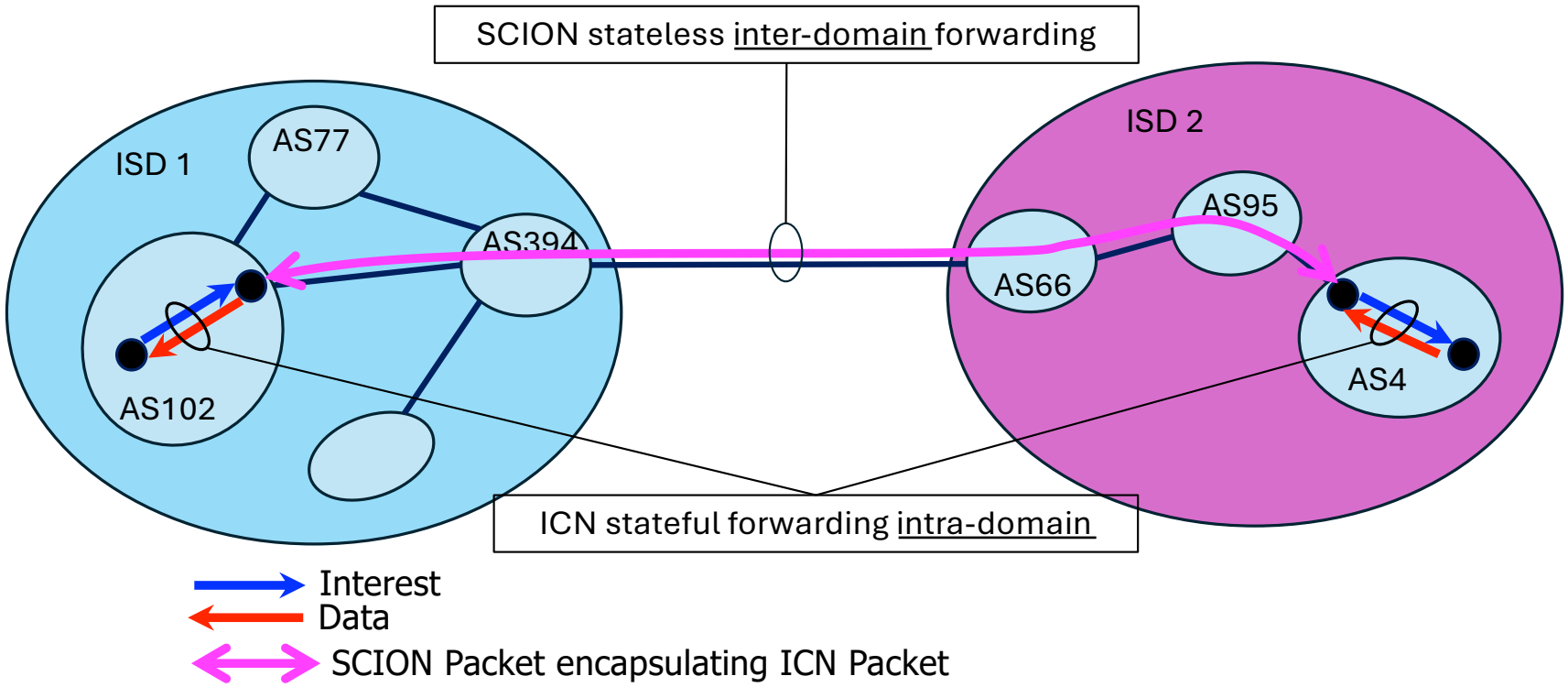
- AS = Autonomous System
  - = A collection of network elements (channels, switches, routers) under a single administration (think Internet Service Provider)
  - The basic unit of routing policy in the Internet
  - Identified by an AS number (ASN), used in BGP
- Intra-domain (routing/forwarding) = within an AS
- Inter-domain (routing/forwarding) = between/among ASes

ICN+SCION In a Nutshell



- Network serves Data requested by application Name
- ICN provides Name-based intra-domain routing and forwarding
- SCION provides secure inter-domain routing and forwarding

Inter-domain Interest-Data Exchange



II. Why Do This?

- Today's Internet is a highly-tuned monoculture
  - Escaped lab experiment – now critical infrastructure
- Security not part of the original design
  - Some key protocols (BGP, DNS) are still largely insecure
- Synergy between the protocols
  - Security as a primary design goal of both ICN and SCION
  - Both support multi-path forwarding
  - Both are flexible with respect to trust (no single global trust root)
  - SCION systematizes inter-AS trust
  - ICN helps to reflection and other spoofing based attacks

Goal: Proof of concept for a global network layer with those properties

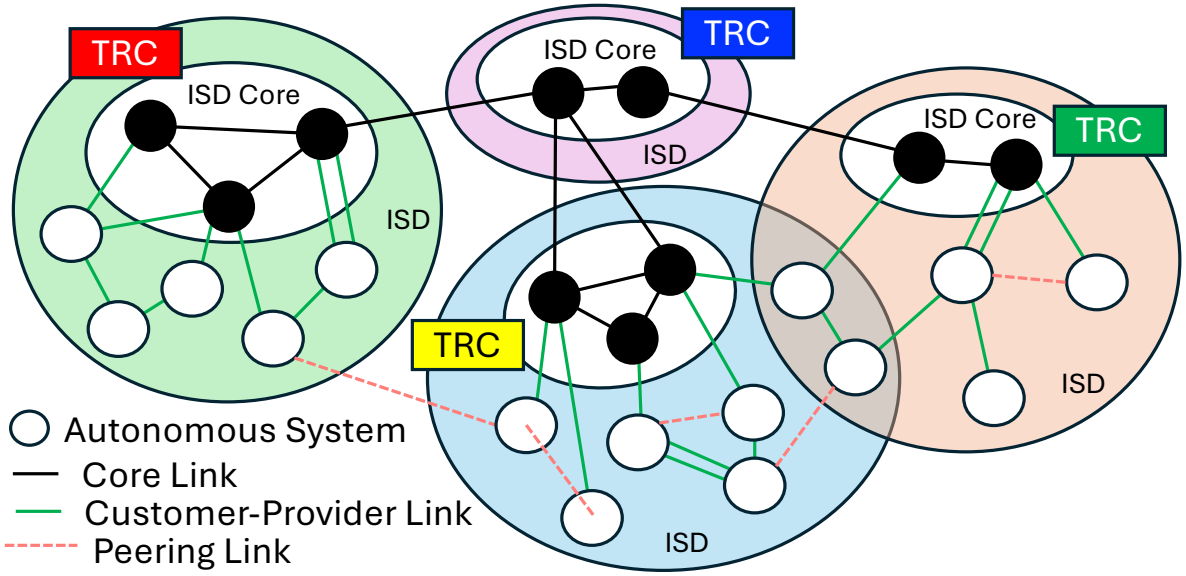
II. Background: SCION

The Complete Guide to SCION. Adrian Perrig *et al*, Springer, 2022.

- Path-aware inter-domain routing/forwarding system
  - From Adrian Perrig's group at ETH Zurich
- Secure replacement for BGP
  - Internet-drafts being discussed in the IRTF/IETF (panrg)
- Designed for security "from the ground up"
  - Consistent with existing provider ecosystem
- Forwarding information carried in packets, not Routing Tables
  - Each packet carries the (cryptographically secured) AS path to follow
- Being commercially developed by Anapaya Systems (anapaya.net), and in real world production networks

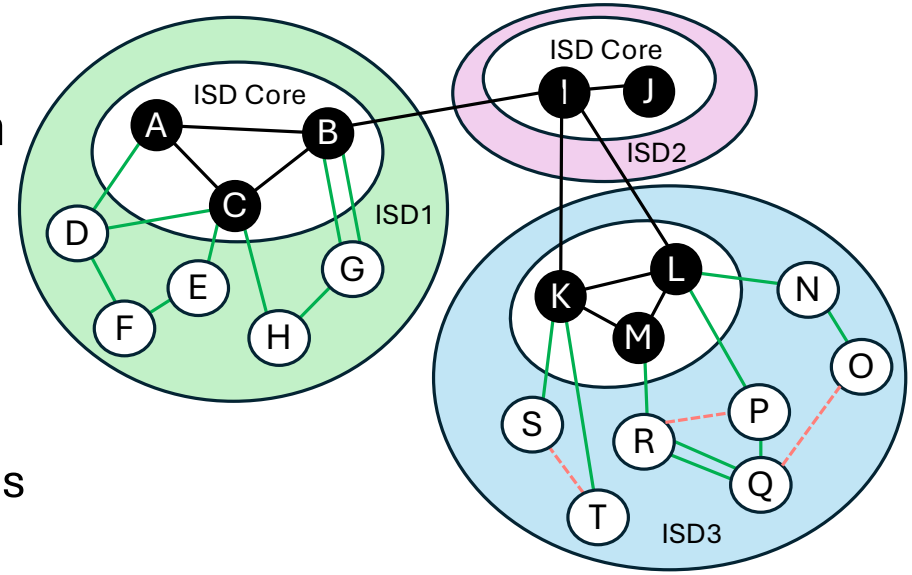
SCION Trust Structure

- Isolation Domain (ISD): group of ASes with common trust structure
  - TRC = trusted root config = CA keys + metadata for ISD
  - Think ISP customer cone
- ISDs connect via Core ASes



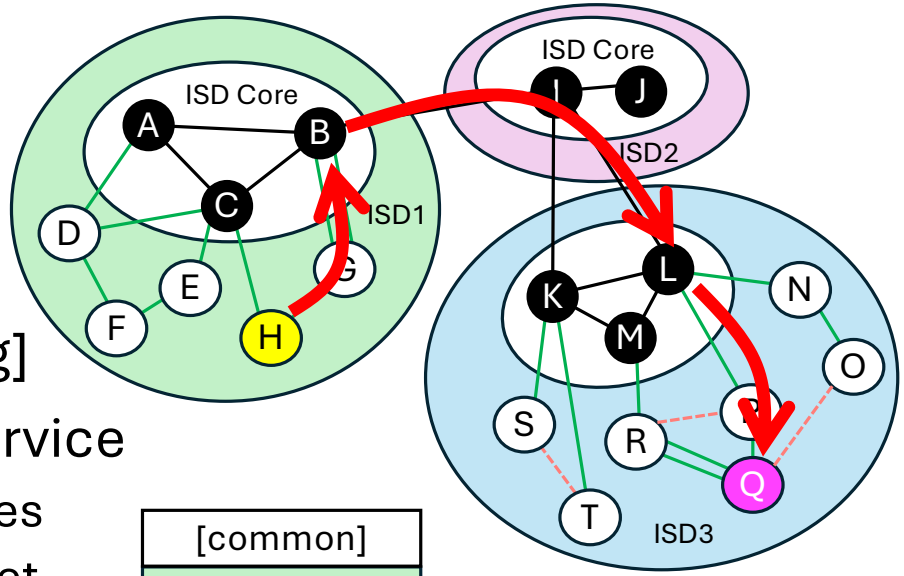
SCION Control Plane

- AS path segments constructed via beaconing within ISDs
  - Protected cryptographically
  - Beacons emitted from Core ASes, propagate away from Core
  - Applying policy along the way
  - Cores beacon across ISD boundaries
- Path segments are oriented
  - Down Segments, e.g.: M➛R, K➛S➛T
  - Core Segments, e.g.: C➛A, B➛I➛L
  - Up Segments, e.g.: F➛E➛C, T➛S➛K



SCION Data Plane

- Packets carry AS Path
  - Sequence of ASes to be transited
  - Optional: E2E HMAC covers path
- Path: [up-seg][core-seg][down-seg]
- Paths collected by AS's Control Service
  - Endpoints request paths to other ASes
  - Source selects path to place in packet
- Paths are reversible



[common]
H➔G➔B
B➔I➔L
L➔P➔Q
payload

III. Background: RHINE

RHINE: Robust and High-performance Internet Naming with E2E Authenticity

Huayi Duan, Rubén Fischer, Jie Lou, Si Liu, David Basin, and Adrian Perrig, *NSDI 2023*

- Name Resolution System
- Designed to replace and solve problems with DNS
  - E.g., uky.edu can override netlab.uky.edu even with DNSSEC
- More flexible and secure trust/delegation system
  - Separate mechanisms to secure delegation status vs zone data
  - Leverage WebPKI-type CAs to certify binding between Name prefixes and keys
  - Multiple roots of trust ("assertion contexts")

Design Goals for ICN+SCION

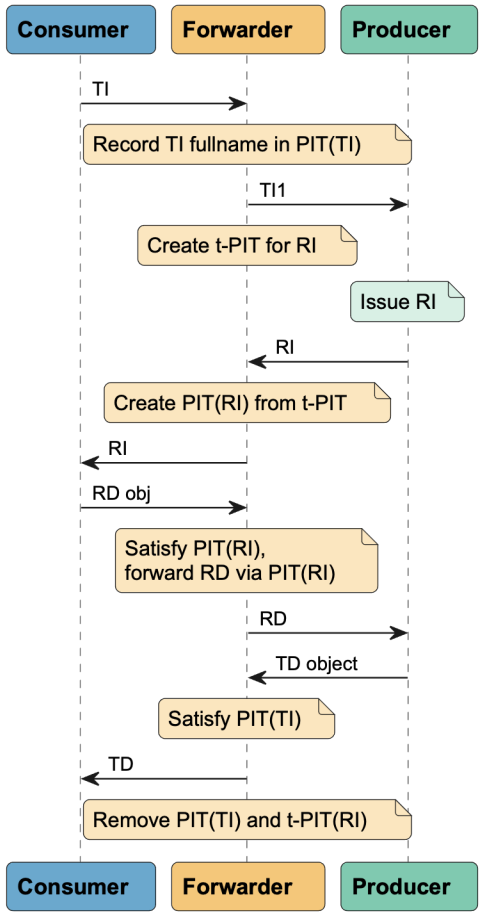
- Minimize changes to existing ICN & SCION protocols
- Support varied application classes (with auxiliary infrastructure if needed)
  - Mass content delivery, e.g., streaming video
  - Point-to-point, e.g., mobile telephony
- Maintain support for:
  - Location-independence of data
  - Multipath forwarding
  - Flexible trust policies/roots of trust
- Ensure ability of sources to produce authentic content before advertising in routing system
- Applications do not *need* to be aware of SCION or the inter-domain topology (but may be)
- Does not depend on IP at any level (in complete implementation)
- ASes can provide multiple tiers of services, including ICN consumer-only.

Sidebar: Reflexive Forwarding

Reflexive Forwarding for CCNx and NDN Protocols (Workgroup: ICNRG, Internet Draft)

David R. Oran, Dirk Kutscher, Hitoshi Asaeda, Ken Calvert.

- Facilitates multi-exchange handshakes in ICN **without** resorting to persistent consumer names and/or push semantics
- *Trigger Interest* establishes temporary forwarder state (PIT entries), permitting one or more *Reflexive* Interest-Data exchanges
- Final *Trigger Data* packet tears down temporary state



Design Choices – Initial Approach

- Where to implement ICN/SCION protocol transition?
  - AS Border routers?
  - End hosts (origin of Interest)?
  - Somewhere in between? (Gateway node)
- How/where do Network & Application trust regimes interact?
  - In the control plane
    - Prevent spoofing (DoS attack on intra-domain routing system)
    - Sources must prove authority to publish in their namespace to the AS
- How to find nonlocal (extra-AS) sources for a given Name?
  - Every AS operates RHINE Name service
  - Info about top-level authoritative name servers propagated in ISD

Problem: Namespace Authority

- Different producers, with different signing keys, can claim the same prefix, e.g /etc/example
- Signature verification and Interest re-issuing falls to applications
- How to indicate a producer is undesirable?
- May lead to routing-based DoS
- Previous attempts to address the problem:
  - Interest-Key Binding (Ghali et. al. 2019)
    Interests carry the signer's public key (or its digest)
  - Trust Engines (Tschudin et al. 2016)
    Requires that at least some forwarders have knowledge of application trust structures

Solution: Producer Verification

Producers prove to their AS that they are authorized to advertise under a particular namespace + prefix.

Example: A producer wants to advertise under /etc/example under the ICANN/DNS namespace

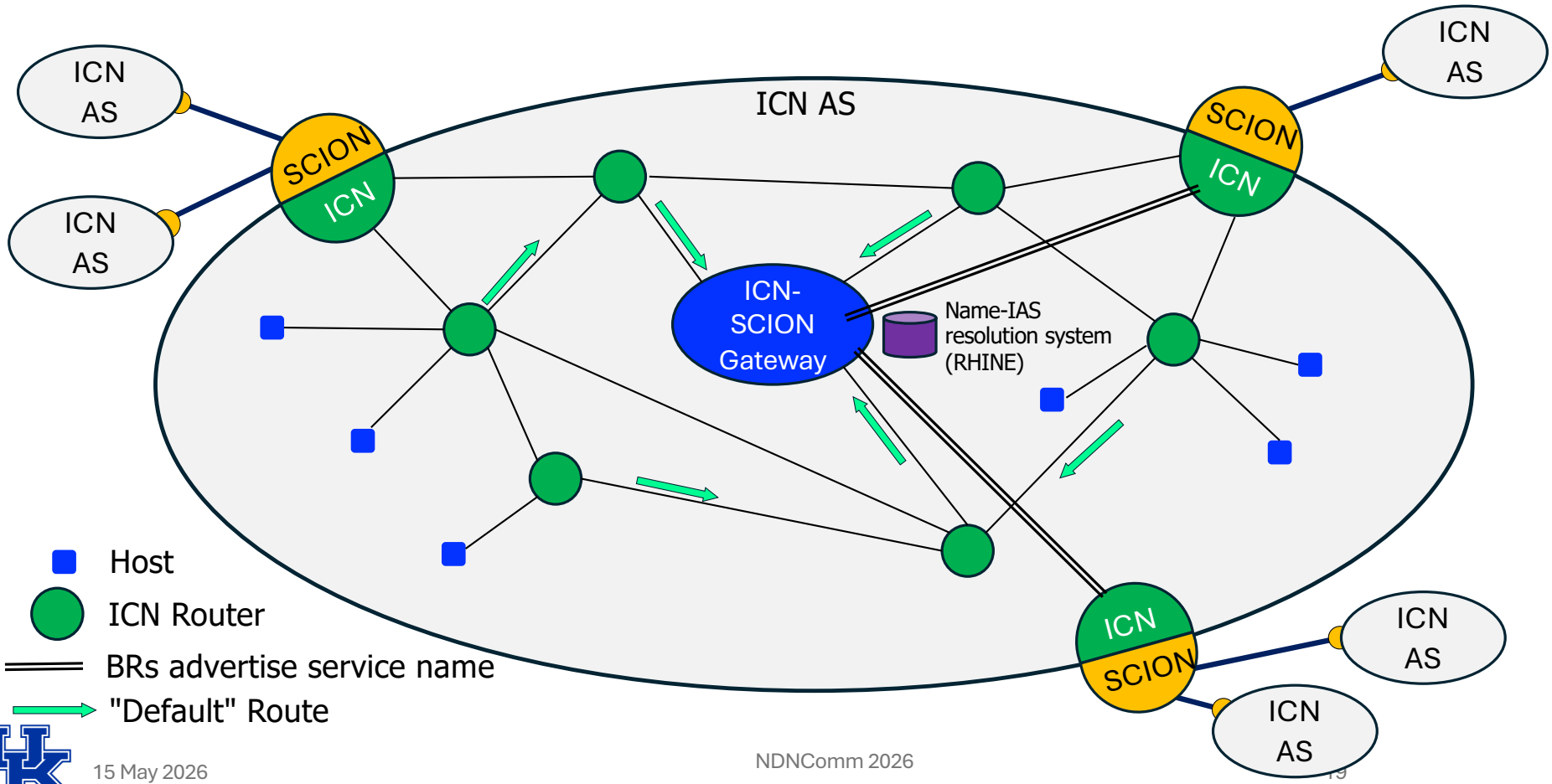
1. The producer initiates the enrollment process, requesting permission to advertise
2. The nearest AS forwarder retrieves a (proposed) RHINE ICNKey record for the prefix, which returns a public key corresponding to the Data signing key. The forwarder verifies the record
3. The forwarder issues a challenge nonce to the producer, which must respond with a signed Data packet containing the nonce
4. The forwarder verifies the Data packet signature using the retrieved public key.
5. The AS allows the prefix to be advertised
6. The namespace and name-key binding are indicated in a four-byte ScopeID included as a (custom) field in Interests and Data

Result: Application and Network Trust intersect *here*, in the control plane.

Table 1: Proposed NKBCs

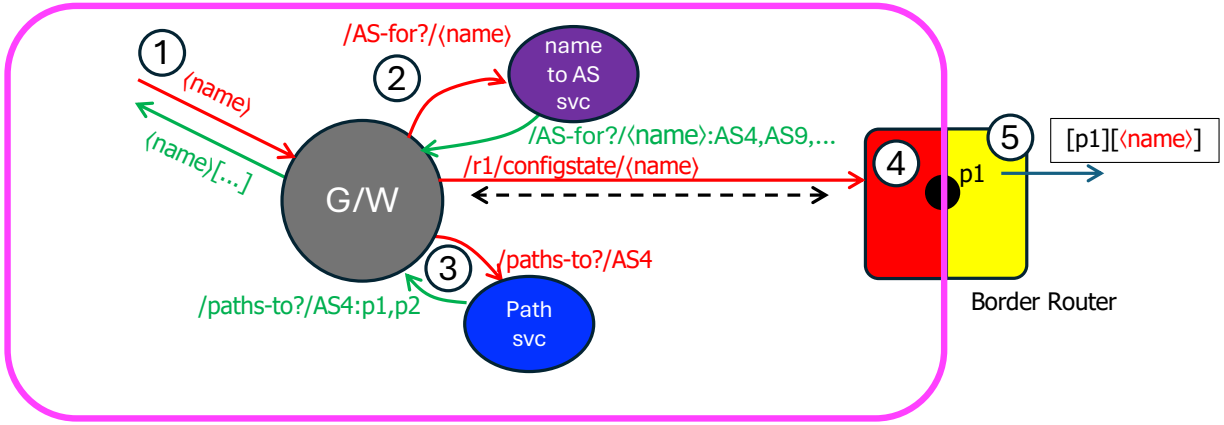
NKBC	Name	Brief Description	Examples
0	*Local*	*Default intra-domain name-key binding for AS.*	
1	SignedRecord	Chain of trust secures a signed record binding names to keys.	DNSSEC+DANE [11], RHINE with proposed NDNKey record type.
2	DirectSign	Chain of trust binds name to key via direct signature.	WebPKI.
3	SelfCert	Name is the cryptographic hash of the public key.	DONA [9].
4	TrustSchema	Signed schema binds names to keys.	NDN Trust Schemas [12].
5	CoupledNameKey	Key or key digest sent together with name in all requests/responses.	Interest-Key Binding [8].
6	Blockchain	Distributed, cryptographic ledger binds names to keys.	Namecoin.
7–64	*Reserved Global*	*Future global classes.*	
65–255	*Private use*	*ISD assigned.*	

ICN+SCION Initial Approach



ICN-SCION Interoperation

1. Interest for ⟨name⟩ finds no match in FIB, forwarded to ICN-SCION Gateway (G/W)
2. G/W gets ASes that contain authorized sources for ⟨name⟩ from RHINE name-to-AS mapping (AS4, AS9)
3. G/W gets paths p1, p2 to AS4 from SCION path service
4. G/W sets up state in border router (via reflexive forwarding), associating p1 with PIT entry for ⟨name⟩
5. Border router encapsulates Interest, adds SCION path header, forwards along path p1

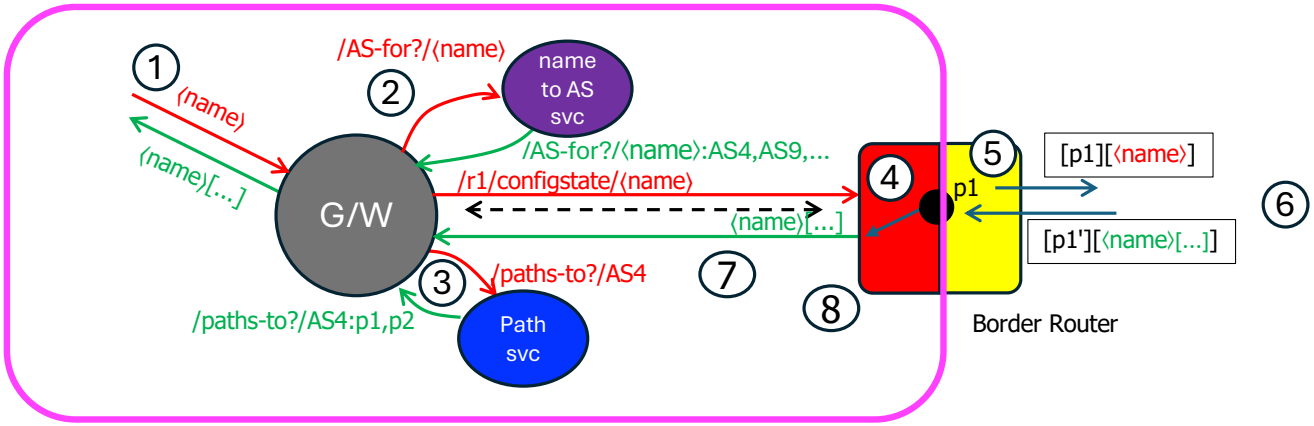


ICN-SCION Interface

⑥ At AS4, routing system forwards Interest to source for ⟨name⟩ and returns Data via reverse path (including reversed AS path)

⑦ At ingress router, Data packet is decapsulated and and matched to PIT entry ⟨name⟩, forwarded back to G/W and thence to source

⑧ Border router eventually advertises availability of ⟨name⟩ in intra-domain routing system



ICN+SCION Research

- Producer verification protocol
- How to find authoritative name servers for given Name
- Scalability of ICN-SCION Gateway and Border Router functions
- Namespace design for SCION control functions to use ICN
  - Initially: UDP/IP

ICN+SCION Status

- Component protocols running in FABRIC
  - Cefore implementation of CCNx
  - SCION's open-source implementation
  - RHINE's open-source implementation
- ICN-SCION Gateway and Border Routers under development
- FABRIC facility port for connection to SCIERA research network

V. Takeaways

1. Combining "mature" research implementations is not straightforward
2. Building on ICN/SCION/RHINE, can we do better than IP?
   - Security-first design
   - Multipath capability
   - Policy & trust flexibility
3. Long-term goal: off-the-shelf ICN, SCION, RHINE capabilities