SCION: PKI Overview

Adrian Perrig

Network Security Group, ETH Zürich

ETH zürich

SCION

PKI Concepts: Brief Introduction

- PKI: Public-Key Infrastructure
- Purpose of PKI: enable authentication of an entity
- Various types of entities
  - Autonomous System (AS): ISP, university, corporation
  - Router
  - Service
  - Web site
- Important terms
  - Certificate: binds entity identifier to a cryptographic key
  - Root of trust: Axiomatically trusted key to start authentication
  - Certification Authority (CA): trusted entity that issues certificates

Desired PKI Properties

- Trust scalability: support heterogenous trust relationships
- Transparency
  - Possible to enumerate trust roots
  - Accountability of all PKI operations
- Resilient to trust root compromise
- Quick recovery from trust root compromise
- Trust control / agility
  - Entities can select which trust roots they need to rely upon
  - Hosts can select trust roots for verification

Overview

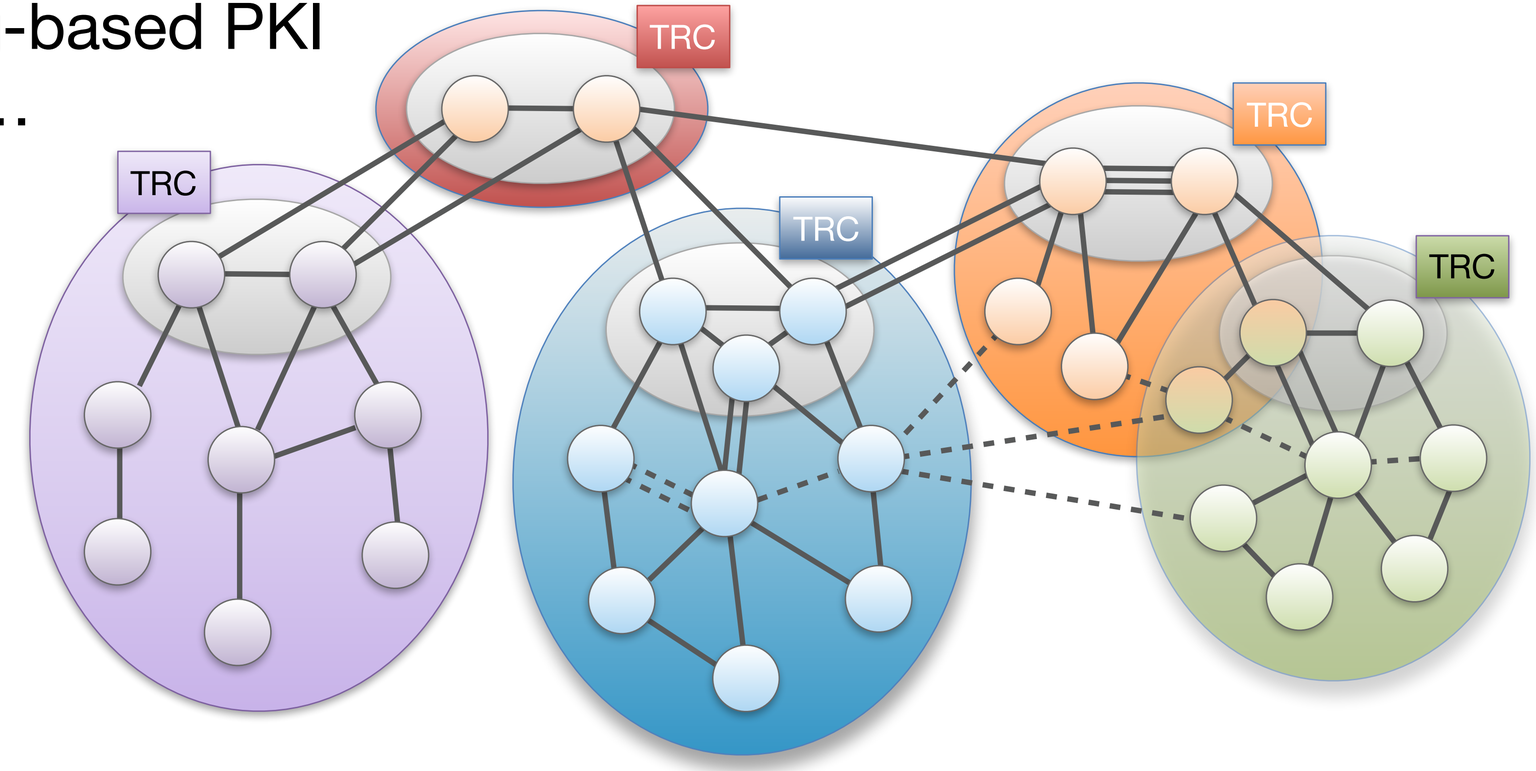
- Control-plane PKI
  - DRKey
- End-entity PKI
- Name-resolution PKI

Control-Plane PKI

- Control plane: System to determine and disseminate end-to-end paths
  - Inter-domain control plane in current Internet: BGP + ICMP + support protocols
- Control-plane PKI mainly provides AS certificates to enable AS authentication
- Main requirement: high availability
  - Needs to work without reliance on availability of communication to PKI servers (to avoid cyclic dependency between routing and PKI operation)

Approach for Trust Scalability: Isolation Domains

- Observation: **subset** of the Internet can agree on roots of trust
  → form Isolation Domain (ISD) with those particular roots of trust
- Authenticate entities within each ISD
- Users & domains can select ISD based on root of trust
- Also supports modern log-based PKI approaches: CT, ARPKI, …
- Challenge: retain global verifiability



Trust Root Configuration (TRC)

- Each SCION ISD defines trust roots in a TRC
- Trust roots for three PKIs
  - Control-plane PKI: core AS certificates
  - End-entity PKI: root CA and log server certificates
  - Name-resolution PKI: root name server certificate
- Trust agility: hosts select TRC they want to use for verification
- TRCs enable efficient updating of trust roots
- TRC distribution is tied to path exploration and resolution

Sample TRC


```
{"ISD": 1,
 "Description": "The first (test) ISD",
 "Version": 2,
 "CreationTime": 1480927723,
 "ExpirationTime": 1483927723,
 "CoreASes": {
   "1-11": {"OnlineKeyAlg": "ed25519", "OfflineKeyAlg": "ed25519",
            "OnlineKey": "5n33hhBRT86/lS6LOOh0RUWweYranrnLkD8uqLzArB4=",
            "OfflineKey": "k0ScqpNRFMsal54sjlgbFxENWJq6ofdPOiazjiK9ta0="},
   "1-12": {"OnlineKeyAlg": "ed25519", "OfflineKeyAlg": "ed25519",
            "OnlineKey": "tuJOOW5bNrlzhoyohdifXo70Zc8zFl4nFyOT4JlgP1I=",
            "OfflineKey": "VYDONHZjckKqXHgprT9zmrDwGhL5dElakxNsGuxnd5I="},
   "1-13": {"OnlineKeyAlg": "ed25519", "OfflineKeyAlg": "ed25519",
            "OnlineKey": "cXRYKtY/L18KHs4dt8G6e4itodFhhj7f3LvBS5xo3as=",
            "OfflineKey": "wUw9f9wFov/kWykV/T94lJu6dfJ2aeQDOtzmnIbo32E="}},
 "RootCAs": {
   "VeriSign Class 3":   {"Certificate": "MIID3OwDQYJKoZIhvcNAQELBQA...",
          "OnlineKeyAlg": "ed25519", "OnlineKey": "F4tLPPhdEygoXidQK..."},
   "GeoTrust Global CA": {"Certificate": "MIID1jCCAr6gAwIBAgIIUuuzQL...",
          "OnlineKeyAlg": "ed25519", "OnlineKey": "pW2wH8DzCRVw2KGH4..."},
   "DigiCert Root CA":   {"Certificate": "MIIEOzCCA7ugAwIBAgIQGNrRni...",
          "OnlineKeyAlg": "ed25519", "OnlineKey": "uppd7OMBMQGGHrNAk..."}},
 "CertLogs": {
   "ISD 1, Log1": {"1-11 1.1.2.3": "MIIHOzCCBbugAwI..."},
   "ISD 1, Log2": {"1-13 3.0.8.7": "MIIDbTCCAlWgAwI..."}},
 "ThresholdEEPKI": 3,
 "RAINS": {"RootRAINSKey": "fQRbxC1lfznQgUy286dUV4otp6FO1vvpX1FQHKOt...",
           "OnlineKeyAlg": "ed25519", "OnlineKey": "VAsCtoEndLXAPtXVX..."},
 "QuorumTRC": 2,
 "QuorumCAs": 2,
 "GracePeriod": 18000,
 "Quarantine": false,
 "Signatures": {
   "1-11": "zQrFoqqaNfG62X5OyyraF8kQok4Ehh3POHooGemX+UwvhxhZnydw...",
   "1-12": "7DEAyG1ldO3jQqems22y9RZmD87VgBnbcvR7YxRIq58eLDkekV2O...",
   "1-13": "D+Eg1O++oGfqKVXB/bxufdz5GbXY5CTQFGQbOSJCPO7c8ebb3SzK...",
   "2-1": "ufTuR26sWp53MHu5suyQuChxWhWQM7gmgkLKJJI12KJPAdK98Ki8a...",
   "ISD 2, RAINS": "2BwAtQ4mG9rdnpo1VGVIj96f/Ueq1TNgdXPI9YSlEREm...",
   "ISD 2, CA: TestCA": "ZO9NkrvTJ/Vec8X5T9ja1IV+o2xvhTQ6FZatnsO..."}}
```


Control-plane PKI roots

End-entity PKI root CAs

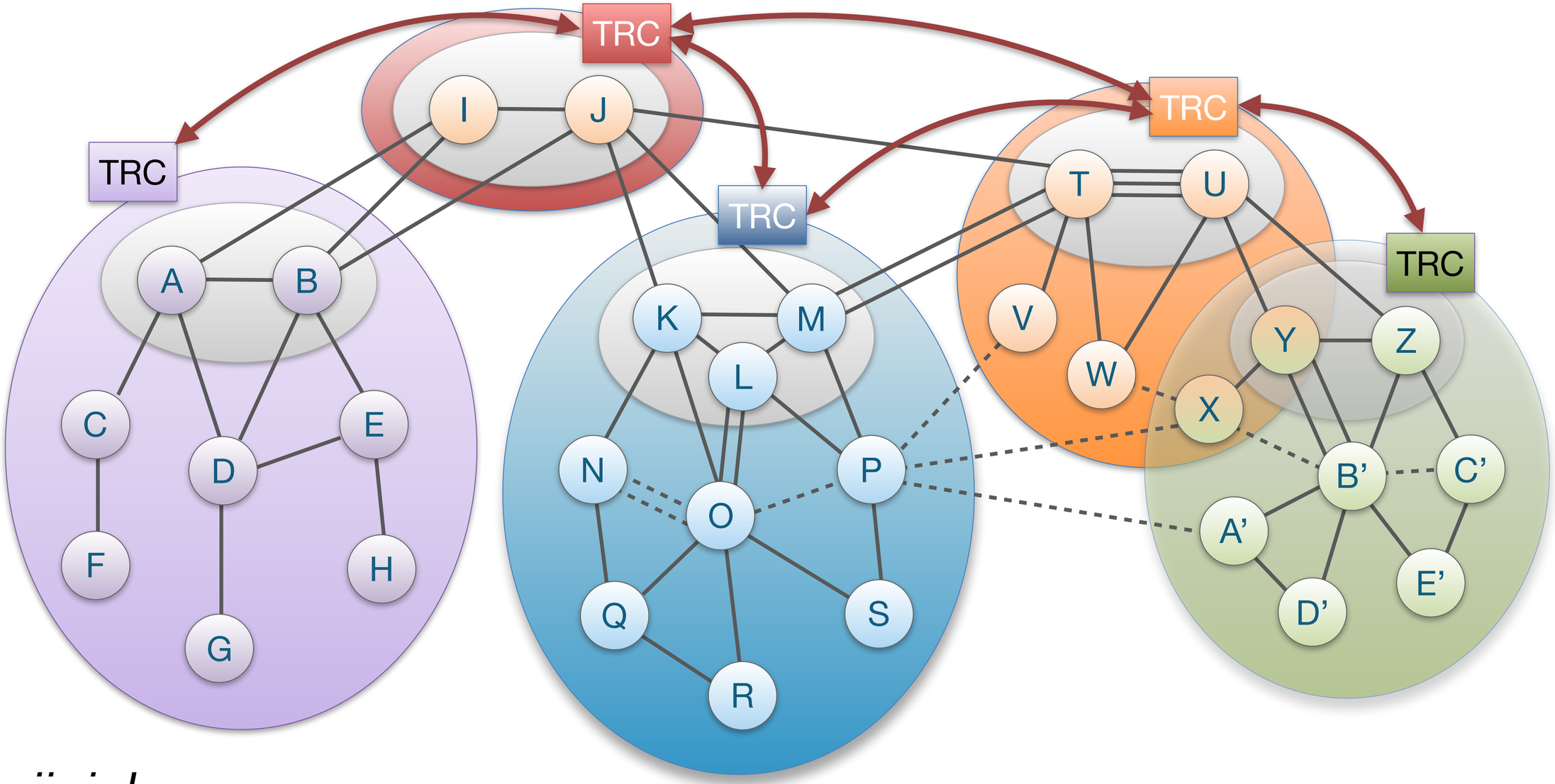
End-entity PKI Logs

Name-resolution PKI

Cross-signatures

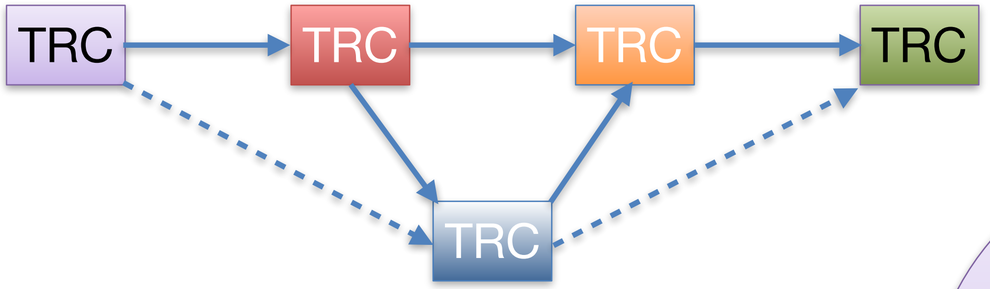
ETH zürich

TRC Cross Signatures

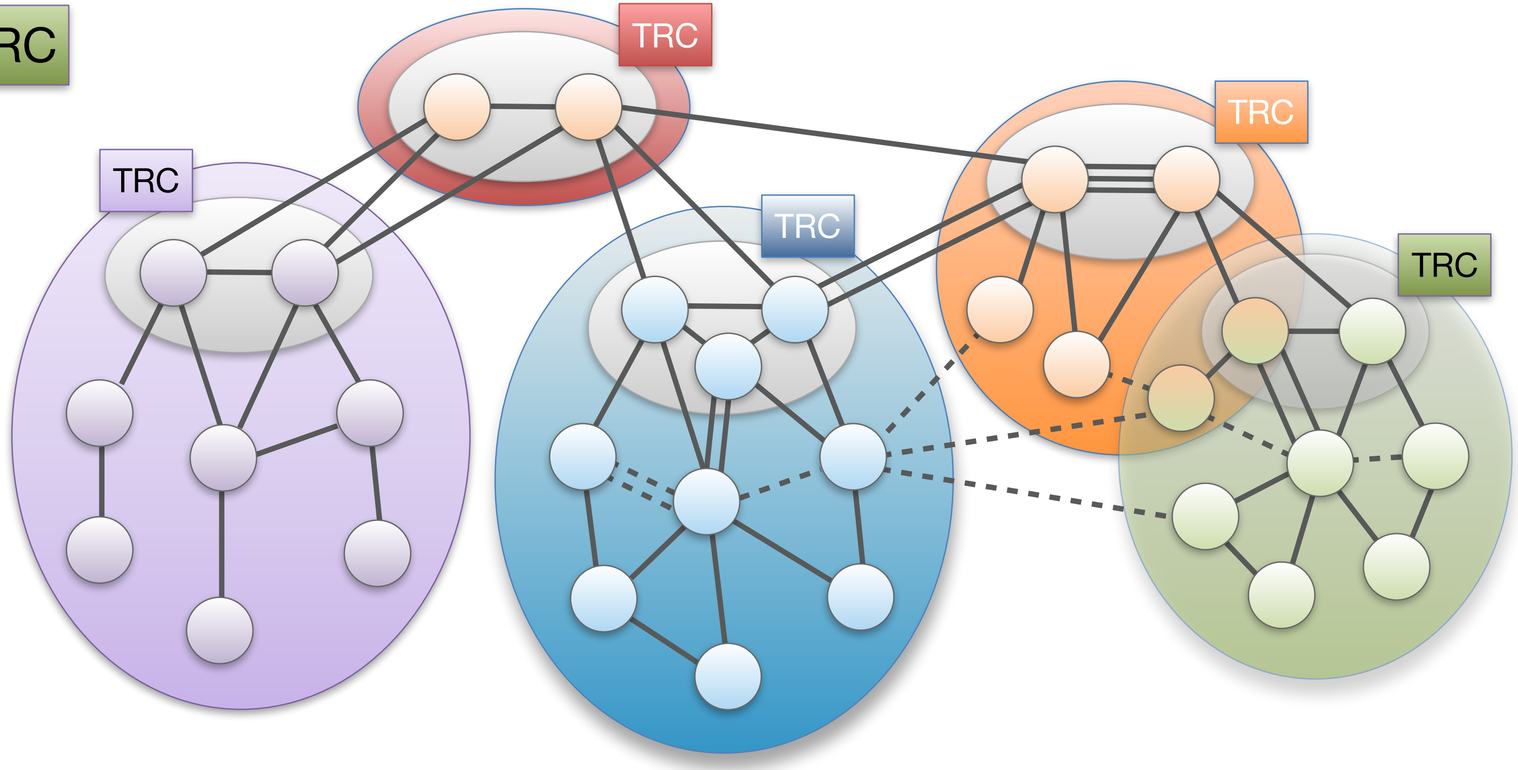


ISD-to-ISD TRC Verification

- TRC verification of other ISDs follows core paths
  - Additional cross-signatures are possible (dashed blue arrows)

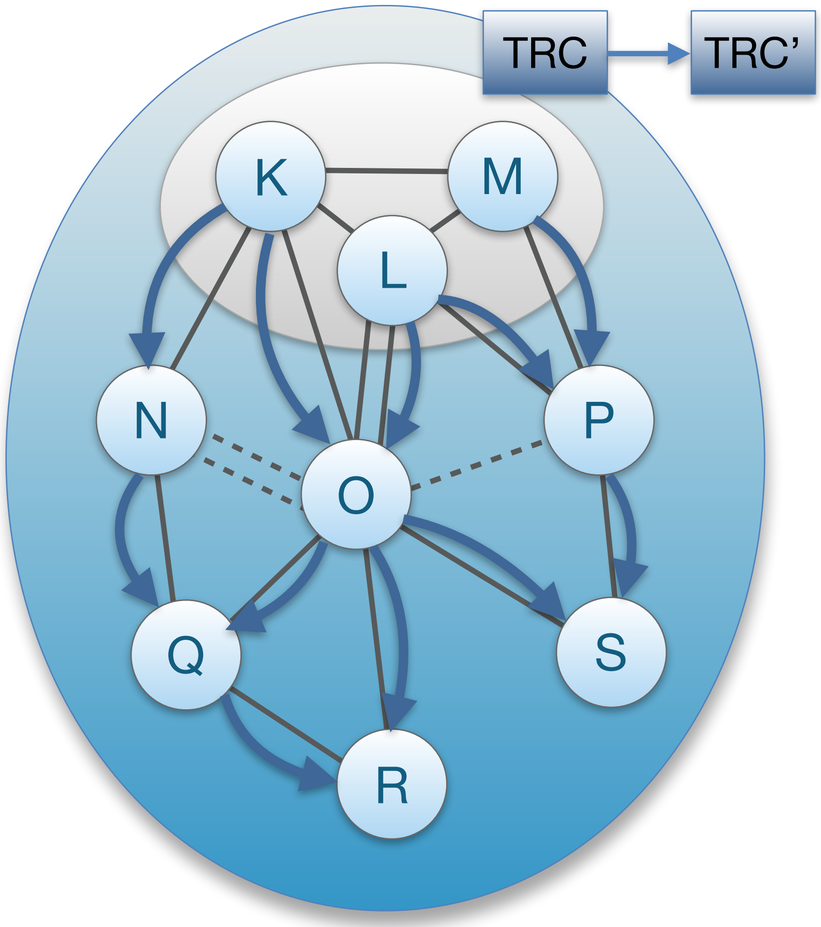


- Important property: each core segment provides a verification chain



TRC Update

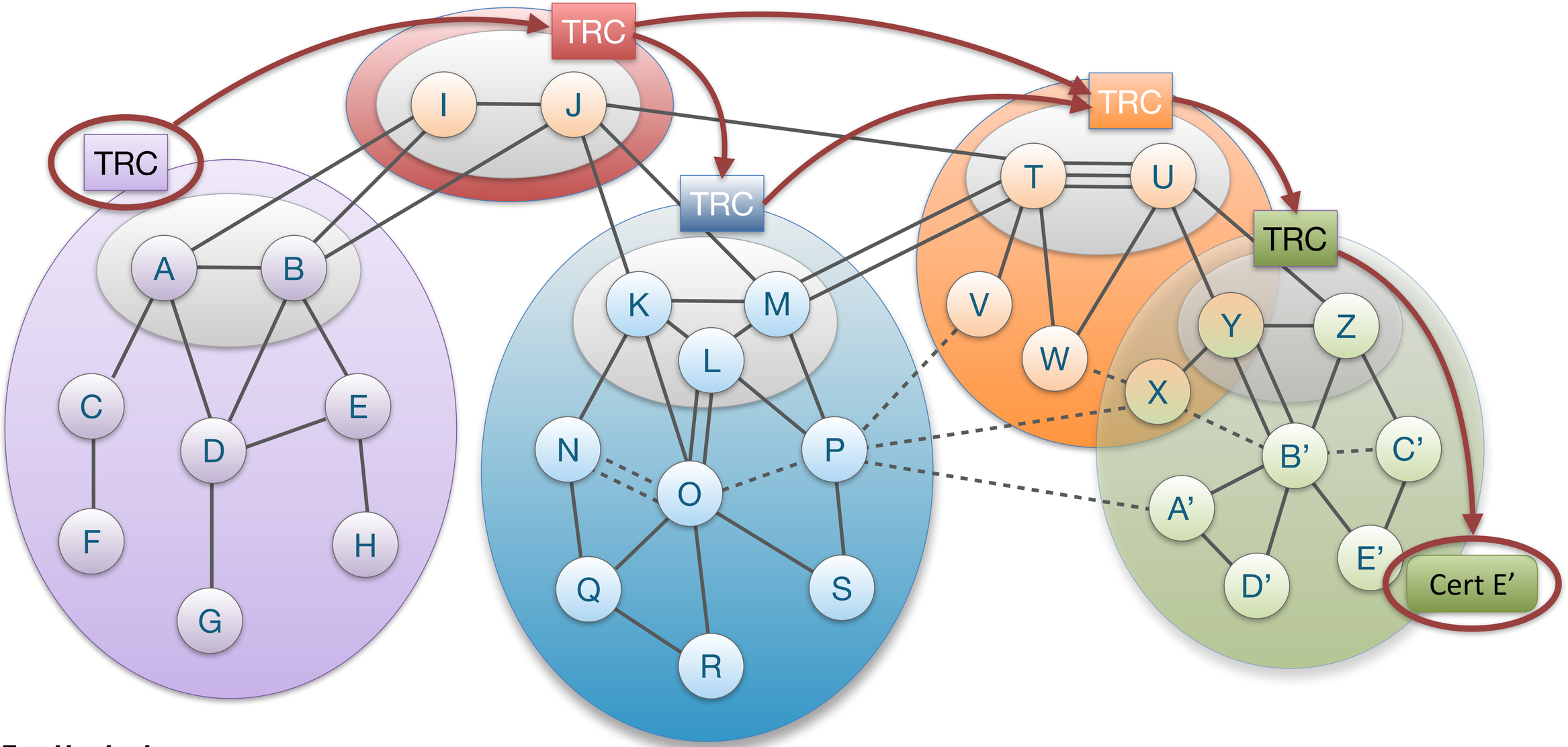
- New TRC’ is signed by quorum of trust roots defined in previous TRC
- Also cross-signed by neighboring ISDs
- TRC’ version is announced in PCB, ASes fetch TRC’ if they do not already have it
- Result: entire ISD rapidly obtains new TRC’ with new trust roots



AS Certificates

- Each AS obtains certificate signed by a core AS
- Problem: AS certificate revocation check can introduce cyclic dependency between control plane and PKI operation
  - Solution: use short-lived certificates for non-core ASes, valid for up to 3 days
  - Core AS certificate can be revoked through TRC update
- Any AS can certify any other AS through chain of cross-signed TRCs and by verifying core AS signatures
- Certificate distribution is tied to path exploration and resolution

External ISD AS Certificate Verification



Desired PKI Properties: SCION CP-PKI

- ✔ Trust scalability: support heterogenous trust relationships
  - Transparency
    - ✔ Possible to enumerate trust roots
    - ✔ Accountability of all PKI operations
- ✔ Resilient to trust root compromise
- ✔ Quick recovery from trust root compromise
  - Trust control / agility
    - ✔ Entities can select which trust roots they need to rely upon
    - ✔ Hosts can select trust roots for verification

Dynamically Recreatable Key (DRKey)

- AS certificates (authenticated through TRCs) can be used to bootstrap authentication and secrecy
  - Unfortunately, asymmetric-key cryptography is quite slow and would not work well for the following cases:
    - A router needs to send an authenticated error message to a remote AS
    - An end host needs to encrypt a secret value for each router on a path
- Goals
  - Enable rapid establishment of a shared secret key between any two entities
  - Routers can derive per-host secret key efficiently without any per-AS or per-host state

DRKey: Deriving AS-to-AS Symmetric Keys

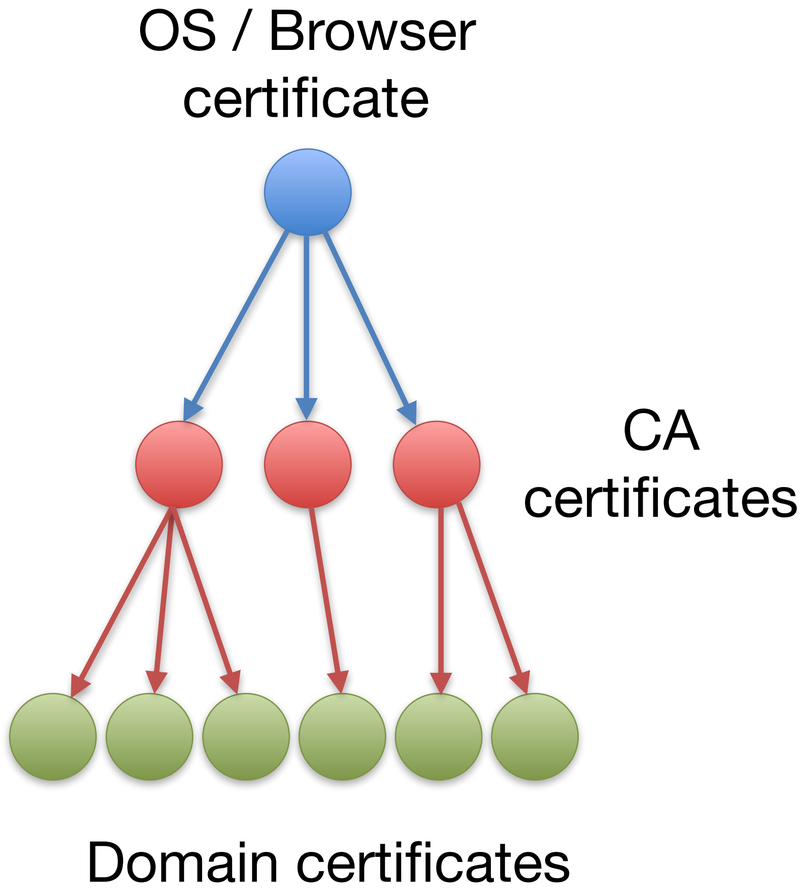
- Idea: use a per-AS secret value to derive keys through an efficient Pseudo-Random Function (PRF)
- Example: AS X creates a key for AS Y using X's secret value SV_X
  - $K_{X \rightarrow Y} = PRF_{SVx}$ ("Y")
  - Intel AESni instructions enable PRF computation within 50 cycles. Key computation can be faster than in-memory key lookup!
- Any entity in AS X knowing secret value SV_X can derive $K_{X \rightarrow *}$
  - Example: router inside AS X can derive $K_{X \rightarrow Y}$ on-the-fly
- AS Y can fetch $K_{X \rightarrow Y}$ from AS X through a secure channel set up based on AS certificates

Overview

- Control-plane PKI
  - DRKey
- End-entity PKI
- Name-resolution PKI

Roots of Trust in Current Internet

- OS / browser CA certificate store: roots of trust of TLS PKI [Oligopoly model]
- Observation: Browser and OS manufacturer control roots of trust, thus their update keys become most fundamental root of trust [Monopoly model]
- Interesting question: how to become a root CA?
  - Pay ~$50’000 to two major browser vendors to add new root CA certificate, others will follow suit



PKI Properties: TLS PKI

- ❌ Trust scalability: support heterogenous trust relationships
  - Transparency
    - ❌ Possible to enumerate trust roots
    - ❌ Accountability of all PKI operations
- ❌ Resilient to trust root compromise
- ❌ Quick recovery from trust root compromise
  - Trust control / agility
    - ❌ Entities can select which trust roots they need to rely upon
    - ❌ Hosts can select trust roots for verification

Improvement: Certificate Transparency

- Google has leveraged market leader position to improve security of TLS PKI ecosystem (Chrome browser market share in May 2017: ~60%)
- Certificate Transparency: public log servers that create public ledger on which certificates are valid
  - If a certificate does not appear on any ledger, it is invalid
- Google has made CA compliance with CT mandatory by October 2017

PKI Properties: Certificate Transparency

❌ Trust scalability: support heterogenous trust relationships

- Transparency
  - ✅ Possible to enumerate trust roots
  - ✅ Accountability of all PKI operations

❌ Resilient to trust root compromise

❌ Quick recovery from trust root compromise

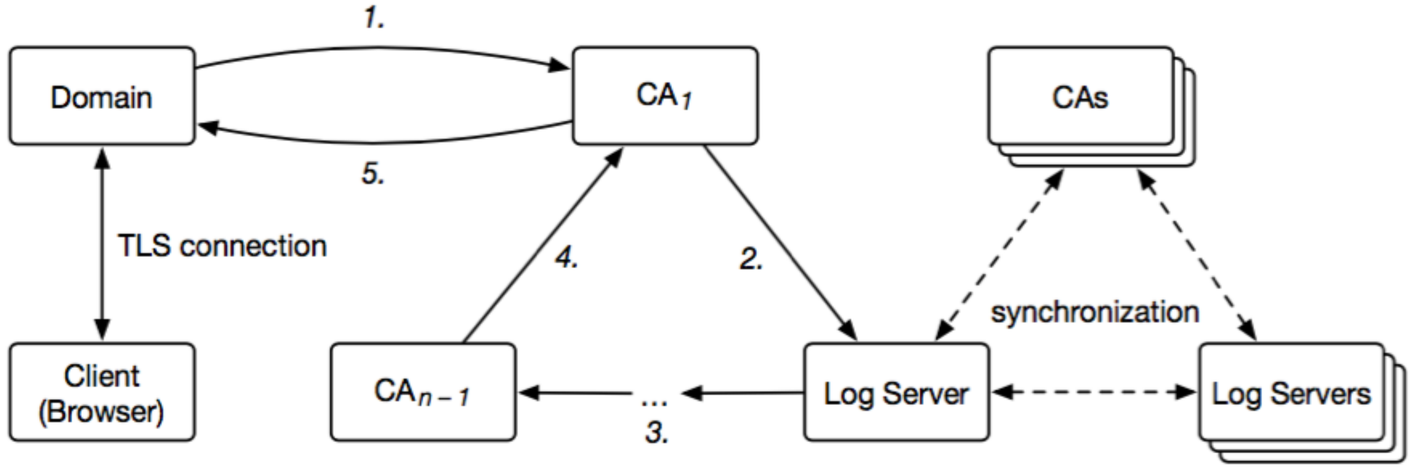
- Trust control / agility
  - ❌ Entities can select which trust roots they need to rely upon
  - ❌ Hosts can select trust roots for verification

Goal: Increase Security of TLS PKI

- Observation: for man-in-the-middle attack, adversary creates new bogus certificate
- Basic idea: cross-validate TLS certificate by multiple parties
- Perspectives [Wendlandt et al. 2008]
  - Network of Notary servers record certificates from multiple vantage points
  - Browser contacts a random subset of notaries
- CT [Laurie et al. 2012], Sovereign keys [Eckersley 2012]
  - Public ledger containing all valid certificates
- ARPKI [Basin et al. 2014]
- PoliCert [Szałachowski et al. 2014]

SCION End-Entity PKI: ARPKI + PoliCert

- Subject certificate policy (SCP): policy that all of a domain's certificates need to adhere to
- Multi-signature certificate (MSC): domain certificate signed by multiple entities + signed by SCP
- Observation: Domain's Subject Certificate Policy (SCP) changes infrequently → invest more effort to secure it
- SCP registration:



SCION End-Entity PKI: ARPKI + PoliCert

- TRC contains:
  - Trust roots of CAs and log servers
  - Threshold for number of signatures required for SCP
- SCP defines domain-specific policy
  - List of trusted CAs
  - Threshold for number of signatures required for MSC
  - Hard fail or soft fail in case MSC parameter violation

Security of SCION End-Entity PKI

- Consider domain D has an SCP and MSC registered in ISD with TRC A
- Important property: any client that uses TRC A as its root of trust can be assured that at least a threshold number of trusted entities defined in TRC A must be malicious in order to forge an SCP or MSC
- Therefore, any client that obtains an SCP or MSC defined by a TRC other than TRC A, needs to obtain a proof of absence that there's no SCP in the end-entity PKI defined by TRC A

PKI Properties: End-Entity PKI

- ✔ Trust scalability: support heterogenous trust relationships
  - Transparency
    - ✔ Possible to enumerate trust roots
    - ✔ Accountability of all PKI operations
- ✔ Resilient to trust root compromise
- ✔ Quick recovery from trust root compromise
  - Trust control / agility
    - ✔ Entities can select which trust roots they need to rely upon
    - ✔ Hosts can select trust roots for verification

What about DNSSEC-based PKI?

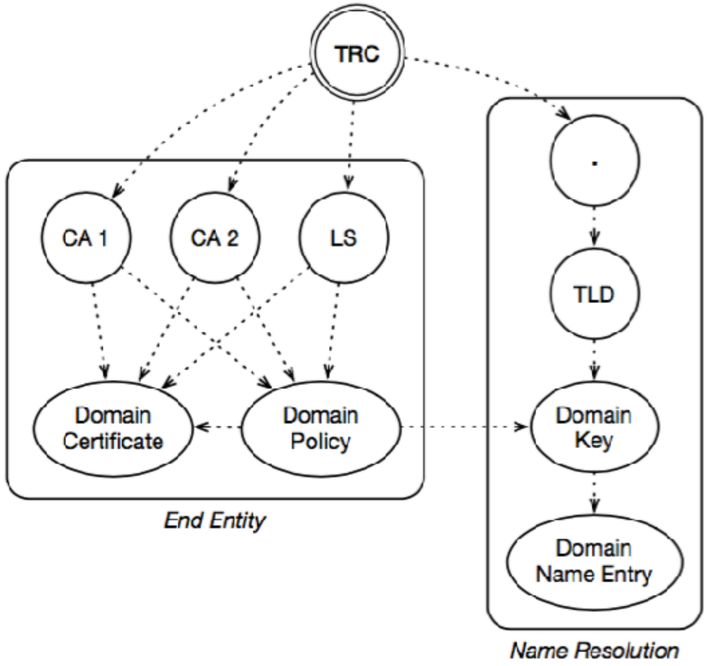
- DANE: DNSSEC entry also contains domains' certificate
- Problems
  - All entities on the verification chain need to be trusted
    → system only as secure as the weakest link
  - Kill switch: revocation of a key invalidates all child entries

PKI Properties: DANE

- ❌ Trust scalability: support heterogenous trust relationships
  - Transparency
    - ✅ Possible to enumerate trust roots
    - ❌ Accountability of all PKI operations
- ❌ Resilient to trust root compromise
- ❌ Quick recovery from trust root compromise
  - Trust control / agility
    - ❌ Entities can select which trust roots they need to rely upon
    - ❌ Hosts can select trust roots for verification

SCION Name-Resolution PKI

- Double verification path:
  - All delegations in name resolution process are signed, each step is verified
  - Domain entry is also signed by SCP
- Advantages
  - Name-resolution PKI used for availab
  - SCP used for high security



PKI Properties: Name-Resolution PKI

- ✔ Trust scalability: support heterogenous trust relationships
  - Transparency
    - ✔ Possible to enumerate trust roots
    - ✔ Accountability of all PKI operations
- ✔ Resilient to trust root compromise
- ✔ Quick recovery from trust root compromise
  - Trust control / agility
    - ✔ Entities can select which trust roots they need to rely upon
    - ✔ Hosts can select trust roots for verification

Summary

- SCION integrates three innovative PKI systems
  - Control-plane PKI
    - High availability with simple operation
    - TRC provides trust root transparency, control, and easy updatability
    - DRKey provides highly efficient and scalable symmetric key derivation
  - End-entity PKI
    - High security: requiring several “trusted” entities to collude to create bogus certificate
    - First PKI where domain can limit the set of trust roots for the certification of its certificate
  - Name-resolution PKI
    - DNSSEC-style PKI only used for availability
    - End-entity PKI used for high security

For More Information …

- … please see our web page:
  www.scion-architecture.net
- Chapter 4 of our book “SCION: A secure Internet Architecture”
  - Available from Springer this Summer 2017
  - PDF available on our web site
- Following presentations
  - Control-plane PKI
  - DRKey
  - End-entity PKI
  - Name-resolution PKI
  - ISD coordination