Certificate-based Namespace for HIP

René Hummen, Tobias Heer
HIP Namespace in the Stack

- Implementation of the id/loc split
- Public key as stable host identity
  - Statistically unique
  - Cryptographically verifiable

HIP Namespace and identity life cycles?
Phasing out “old” HIs

- Host Identity bound to public key’s life cycle
  - New key == new identity
  - New HITs in ACLs, DBs, …
- Re-bootstrapping of trust
  - ... but host is still same trustworthy entity
What is the HIT?

• Representation of HI
  – IPv6 format
  – Can be mapped to HI (locally)
  – Mapping is of cryptographic nature

• Current mapping
  – Hash function

• Other alternative
  – Certificates
New Namespace?

- 3 components of a host identity
  - Descriptive host identifier
  - Public Key equating to traditional HI
  - Binding certificate

- Stable description identifies host
- Public key authenticates host
  - May change over time
  - Allows for key negotiation
Scoping Identifiers

- Inherent naming conflicts

- Certificate confines scope of host identifier
  - Binding certificate (CA-specific scope)
  - Common root/intermediate cert. (coordinated scope)
Replacing a HI (revisited)

- Public key and certificate change
- Host identifier remains stable

→ Host identity stays intact
1. Deeper look into and specification of coordinated namespace scenario
2. Generation of HITs from certificate-based HIs
3. Integration of namespace in HIP exchange