Empowered by Innovation NEC

Binding Self-certifying Names to Real-World Identities with a Web-of-Trust

(draft-seedorf-icn-wot-selfcertifying-00)

Jan Seedorf

IETF 90, Toronto
ICNRG
July 2014

Challenge: Binding in Naming Schemes

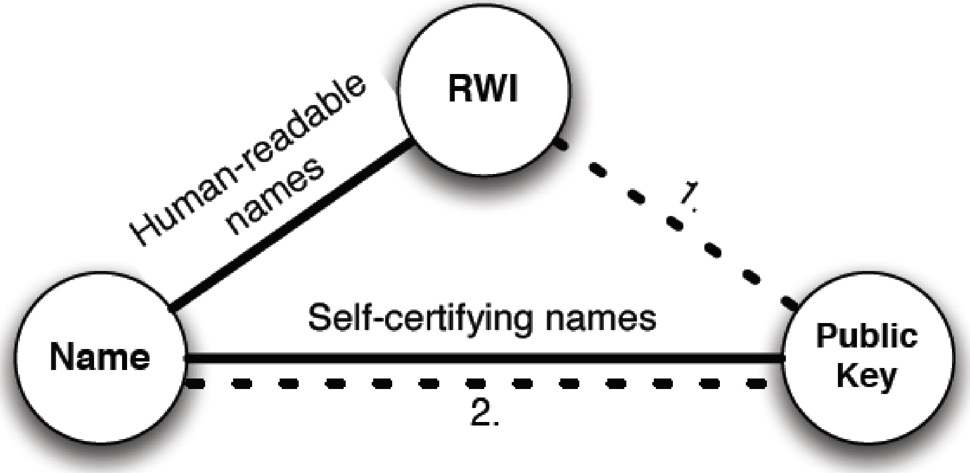

Figure 1: A depiction of the three entities and the different bindings between them. Two naming schemes provide different intrinsic bindings (solid lines) but require both an external authority to provide one additional binding (dashed line): with self-certifying names it's the binding (1), whereas with human-readable names it's the binding (2).

Ghodsi et al: "Naming in Content-Oriented Architectures", SIGCOMM ICN Workshop 2011

Self-Certifying Names

Self-Certifying Names

- **A name where ownership of the name can be verified without relying on a trusted third party**

How can this be done?

- **Name contains the hash of a public key**
  - Start with a private/public key pair
  - Represent the name as the hash of the public key
  - Sign the content that belongs to the name with the corresponding private key and append public key
  - Anybody can verify the signature by
    a) Checking that the hash of the public key is (part of) the name
    b) Verifying the signature with the public key

Self-Certifying Names in ICN

Self-Certifying Names are a key concept in ICN:

- A source can digitally sign data associated with a self-certifying name and append the public key to the signed data
- Any intermediate entity (e.g. ICN-router/Cache) or receiving entity (i.e. issuer of a request for the name) can verify the signature
  - without the need to verify the identity of the host that caches the object
  - without relying on a trusted third party, or a Public Key Infrastructure (PKI)

Problem: Binding to Real-World Identities

- Self-certifying names lack a binding with a corresponding real-world identity (RWI)
  - the concept enables to verify that whoever signed some data was in possession of the private key associated with the self-certifying name
  - but it does not provide any means to verify what real-world identity corresponds to the public key, i.e. who actually signed the data

Solutions

- Public Key Infrastructure [PKI] (hierarchical, central authority)
- **Web-of-Trust [WoT] (distributed, decentralised trust)**

Focus of draft-seedorf-icn-wot-selfcertifying

Decentralised Solution: Web-of-Trust

Binding of self-certifying names and RWIs in a Web-of-Trust[1]

- WoT key-ID is equivalent to the self-certifying name part used in the naming scheme
  - tying the self-certifying name with the ID of the corresponding public key in the WoT

Example

- PGP Web-of-Trust (RFC2240):
  - key ID (v4) is the lower 64 bits of the fingerprint of the public key, where the fingerprint is essentially the 160-bit SHA-1 hash of the public key
  - if a self-certifying name would be based on the same lower 64-bits of the fingerprint of a given public key, this public key would be tied to the self-certifying name and at the same time be tied to the real-world identity used in the WoT, e.g. an email- address or the real (i.e. non-self-certifying) name of a given ICN publisher

1 - Seedorf, J., Kutscher, D., and F. Schneider, "Decentralised Binding of Self-Certifying Names to Real- World Identities for Assessment of Third-Party Messages in Fragmented Mobile Networks", 2nd Workshop on Name Oriented Mobility (NOM), 2014

Standardisation Considerations (initial)

- Rules for forming a self-certifying name based on a public key
  - (List of) Asymmetric cryptography algorithm(s) and corresponding bit-length(s)
  - (List of) Hash algorithm(s) and corresponding bit-length(s)
  - Rules that define what part of the hash is used for forming the self-certifying part of the name
  - ➢ **E.g. based on “Naming Things with Hashes” (RFC6920)**

- Rules for relation to Web-of-Trust
  - Definition of the web-of-trust key-ID and how it relates to the self-certifying name
  - Semantics of a signature in the Web-of-Trust
  - ➢ **E.g. based on PGP (RFC2240)**

Acknowledgements

This work has been supported by the GreenICN project (GreenICN: Architecture and Applications of Green Information Centric Networking), a research project supported jointly by the European Commission under its 7th Framework Program (contract no. 608518) and the National Institute of Information and Communications Technology (NICT) in Japan (contract no. 167). The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the GreenICN project, the European Commission, or NICT.

\Orchestrating a brighter world

NEC brings together and integrates technology and expertise to create
the ICT-enabled society of tomorrow.
We collaborate closely with partners and customers around the world,
orchestrating each project to ensure all its parts are fine-tuned to local needs.

Every day, our innovative solutions for society contribute to
greater safety, security, efficiency and equality, and enable people to live brighter lives.

Empowered by Innovation

NEC