Using the HiiMap Mapping System as a Public Key Infrastructure

Oliver Hanka
oliver.hanka@tum.de

SPONSORED BY THE
Federal Ministry of Education and Research

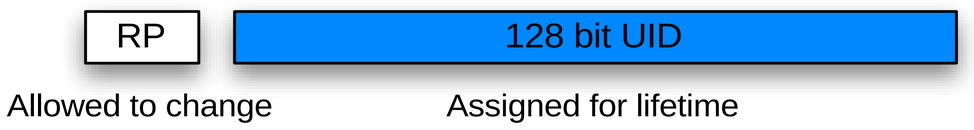
Motivation

- Why a Public Key Infrastructure?
  - Security is a key element of any Next Generation Internet architecture.
  - Functionality like integrity, confidentiality and authenticity can be provided by the private/public key principle.
  - This mechanism needs a means to distribute the public keys without the possibility to manipulate them.
  - To avoid the need of an additional infrastructure, the PKI should be integrated into the mapping system.
- Why not HIP?

  The Host Identity Protocol uses a 128-bit hash of the public key as the identifier (Host Identity Tag). The key is mathematically bound to the identifier and vise versa.
  - In case the key or identifier changes, the other one has to as well.
  - No possibility to withdraw a key.
  - Additional trust entity required to verify the relationship between the identifier and a legal-person.
  - Random key-pair guess.

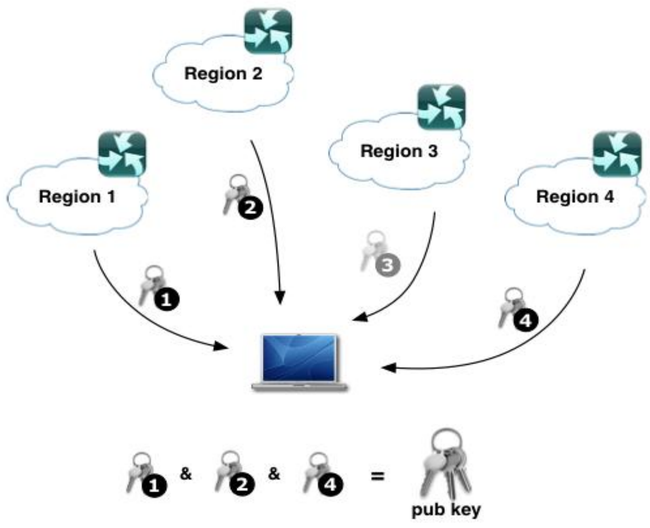
HiiMap

- Hierarchical Internet Mapping Architecture
  - A new concept for a Future Internet Architecture based on mapping regions.
  - Implements the locator/identifier-separation paradigm.
  - Divides the world into regions, whereby each region is responsible for the mapping of nodes residing in it.
  - A 8-bit *regional prefix (RP)* is pretended to each *unique identifier (UID)* to determine which region is responsible for the mapping.
  - The UID to RP resolution is done by a global authority (GA) which stores the RPs for all valid UIDs.
  - RP changes are expected to be rare. The RP of a node only changes if the node permanently moves to another region - not while roaming.
  - For legal and administrative reasons, one region represents one country.



PKI and the Mapping

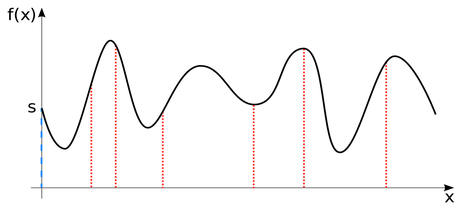
- Overview
  - Additionally to the locator, the mapping system also stores information about the public key.
  - The key is not stored in *plain text* in the mapping system.
  - Key-hints are generated by using Shamir's *Threshold Cryptography* paradigm (2).
  - `n` key-hints are generated, but only `k` hints are required to reconstruct the public key (`k<n`).
  - The key-hints are stored at different regions.
  - To reconstruct a key, a client needs to download `k` hints.
  - A malicious region is not able to disrupt or foreclose the key reconstruction.
  - A modified key-hint is detected during the reconstruction.
  - In case a modified hint is detected, another hint must be downloaded.



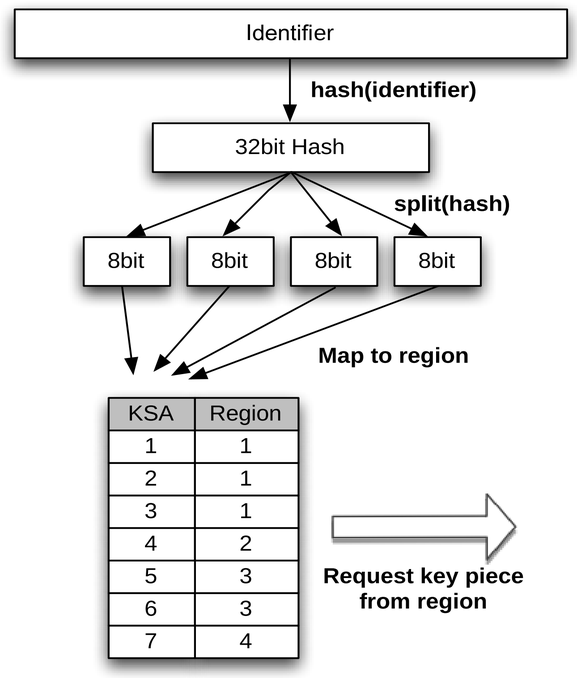
- Threshold Cryptography

  The paradigm is based on the construction of a polynomial like
  $f(x) = s + a_1 x + a_2 x^2 + ... + a_{t-1} x^{t-1}$

  whereby `s` represents the secret. All a_i values can be chosen freely. After constructing the polynomial, `n` arbitrary tuples `(x,f(x))` can be disclosed as key-hints. At least `k` hints are required to reconstruct the secret, whereas $k = x^t$.



- Determining the storage location
  - Each key-hint is stored at a different region.
  - A client is able the calculate the storage locations without the need to trust a single region.
  - The method is based on a simple cryptographic hash algorithm.
  - The algorithm allows for a fair distribution of storage requirements over the unequally sized regions.
- Example (using 4 regions)
  1. Hash the identifier to a 32-bit value.
  2. Split the hash value into four pieces.
  3. Each piece represents an 8-bit *key storage address space* (KSA).
  4. Since not all possible 256 regions numbers in the HiiMap architecture are reserved, a mapping directive must be downloaded from the global authority.
  5. The mapping directive maps the KSA to regions.
  6. In case the algorithm results in two identical regions, the next higher region number is used for the second number.



KSA	Region
1	1
2	1
3	1
4	2
5	3
6	3
7	4

- User key management
  - The private key is stored in a cryptographic smart card.
  - Before shipping the smart card to a client, the public key hints are generated by the card and out of band transmitted to the mapping system.
  - Ordering a new smart card can be linked with identity verification
  - All cryptographic operations are handled by the smart card (e.g., mapping update requests).

(1) Hanka, O.; Kunzmann, G.; Spleiß S.; Eberspächer. J.; Bauer, A.; *HiiMap: Hierarchical Internet Mapping Architecture.* In First International Conference on Future Information Networks, Oct. 2009
(2) Shamir, A.; *How to share a secret.* Communications of the ACM, 22, 612-613, 1979
(3) Hanka, O.; Eichhorn, M.; Pfannenstein, M.; Eberspächer, J.; Steinbach, E.; *A Public Key Infrastructure based on Threshold Cryptography for the HiiMap Next Generation Internet Architecture*. In Future Internet, 3, 14-30, Feb. 2011