Uniform Data Fingerprint

Phillip Hallam-Baker

draft-hallambaker-udf-00

PGP Requirements

- Want to use Base 32 instead of Hex
  - 25 digit fingerprint instead of 32
- Use a modern hash
  - SHA-2 or SHA-3

General Requirements

- Fingerprints identify a root of trust
  - Every type of root of trust should have one
    - OpenPGP keys
    - OpenPGP Software distribution
    - Operating system distribution
    - PKIX trust roots
    - Anything that can’t be trusted by digital signature

UDF proposal

- Fingerprint is a binary string.
- First byte is a version/alg identifier
  - 96 = SHA-2 ‘Mxxxx-xxxxx-xxxxx-…
  - 144 = SHA-3 ‘Sxxxx-xxxxx-xxxxx-…
- Following bytes are the result of

  H(<Content-Type> ‘:’ H (<Content>))

  Where <Content-Type> is a MIME media type

  application/openpgp-key
  application/pkix-keyinfo

Base-32 Presentation

- Data is converted to Base 32
- Truncated to a multiple of 5 characters
- Dashes placed between groups

- MB2GK-6DUF5-YGYYL-JNY5E
- MB2GK-6DUF5-YGYYL-JNY5E-RWSHZ
- MB2GK-6DUF5-YGYYL-JNY5E-RWSHZ-SV75J

Base 65536/32768 Presentations

- Dictionary of words
- Dictionary of images

- Allow shorter presentation: 1/3rd the size
- Faster
- Does not depend on Latin-1 familiarity
- One way, verify only!

In crypto libraries

- Can use fingerprint as name for any key
  - Public key
  - Secret key
- Can use fingerprint as name for any binding
  - PKIX Certificate
  - OpenPGP Key
  - Kerberos token
  - DNSSEC Record

Further Work

- Compressed Fingerprints
  - 100 bit fingerprint with strength of 125 bit
  - Takes time to generate
    - Generate random keys
    - Check for first n (e.g. 25) bits being 0
    - Specify in version field (192 ‘x’)