CDNI URI Signing
(draft-leung-cdni-uri-signing-01)

CDNI Working Group
IETF 86 Orlando, Florida
Mar 14, 2013

Kent Leung (kleung@cisco.com)
Francois Le Faucheur (flefauch@cisco.com)
Matt Caulfield(mcaulfie@cisco.com)

WG Feedback

- Draft is lacking the concept of URI signing from more of a system/high-level perspective (Next version)

- General concept of URI Signing along with specific algorithm (Next version)

- Clarify key terminology for asymmetric method (Asymmetric keying sections needed)

- Categorize attributes for validity of request vs. URI signature computation (Next version)

- Clarify semantics of Client ID vs Client IP (Remove CID in next version)

Topics under Discussion

- Eliminate Key Owner attribute
- Specify Key Index used for symmetric key
- Hash function used for symmetric key
- Need indicator for asymmetric keying; describe "digital signature" support
- Remove Version attribute, overlap with Algorithm
- How to add a new attribute for distribution policy and protocol extension? What's the best way to accomplish this? Further discussion needed.
- Request Routing interface support
- URI Signing kept in one document or disseminated into CDNI drafts (Metadata, Request Routing, Logging, etc.)

Issues Tracking

- Fix URI signing and validation for public key

X   Remove Client ID (CID) attribute or introduce IMSI, MSISDN, MEID, MAC address, etc. as separate attributes

- CDNI Metadata Interface contains URI Signing required indication means Downstream CDN ensures URI must be signed and validated before content delivery; otherwise, Downstream does not perform validation regardless if URI is signed or not

- Specify MUST/SHOULD/MAY in text

X   URI signing and validation steps are used as reference for operational logic and not specific implementation sequence

- Flexible URI signing work item

- CDNI Interfaces' work items