



URI Signing for CDNI

draft-ietf-cdni-uri-signing-07

Kent Leung (Cisco Systems)
Francois Le Faucheur (Cisco Systems)
Ray van Brandenburg (TNO)
Bill Downey (Verizon Labs)
Michel Fisher (Limelight Networks)

Key Concepts Incorporated from Version -05 to -06

- Support for URI pattern that represents a set of URIs
- Support privacy for Client IP address/prefix
- Sections that were updated to support the above:
 - Enforcement Information Elements
 - Signature Computation Information Elements
 - Creating the Signed URI
 - Validating a URI Signature
 - CDNI Logging Interface
 - Privacy

Privacy for Client IP Address/Prefix

- Client IP address/prefix is encrypted
- Introduced “Client IP Encryption Algorithm (CEA)” information element
- Introduced “Client IP Key ID (CKI)” information element

Support for URI Pattern

- Introduced “Original URI Container (OUC)” information element
 - Used to protect the Original URI
- Introduced “URI Pattern Container (UPC)” information element
 - Used to protect a set of URIs that matches the specified pattern
 - Literals for matching expression are ‘\$’, ‘*’, and ‘?’

Key Concepts Incorporated from Version -06 to -07

- Re-organize the “Creating the Signed URI” section to improve readability and procedure.

From:

1. “Calculating the URI Signature” and
2. “Packaging the URI Signature”

To:

1. “Compose URI Signing IEs with Protected URI”,
2. “Compute URI Signature”,
3. “Encode the URI Signing Package”, and
4. “Assemble the Signed URI”

Key Concepts Incorporated from Version -06 to -07

- Re-organize the “Validating a Signed URI” section to improve readability and procedure.

From:

1. “Information Element Extraction”,
2. “Signature Validation”, and
3. “Distribution Policy Enforcement”

To:

1. “Extract and Decode URI Signing Package”,
2. “Extract URI Signing IEs”,
3. “Obtain URI Signing IEs with Protected URI”,
4. “Validate URI Signature”, and
5. “Distribution Policy Enforcement”

IANA Considerations

- Thanks to Kevin Ma for writing up section
- Add URI Signing to “CDNI Payload Type” registry
- Add new CDNI Record Type version 2 to extend CDNI Logging Record version 1 to include URI Signing logging fields
- Add URI Signing logging fields to “CDNI Logging Field Names” registry
- Create the following new subregistries under "Content Delivery Networks Interconnection (CDNI) Parameters" registry:
 - "CDNI URI Signing Enforcement Information Elements“,
 - "CDNI URI Signing Signature Computation Information Elements“, and
 - "CDNI URI Signing Signature Information Elements"

Next Steps

- Resolved issues from Leif's expert review and incorporated review comments
- Brian Weis will review draft for early security review
- WG Last Call after that?

Thank you!