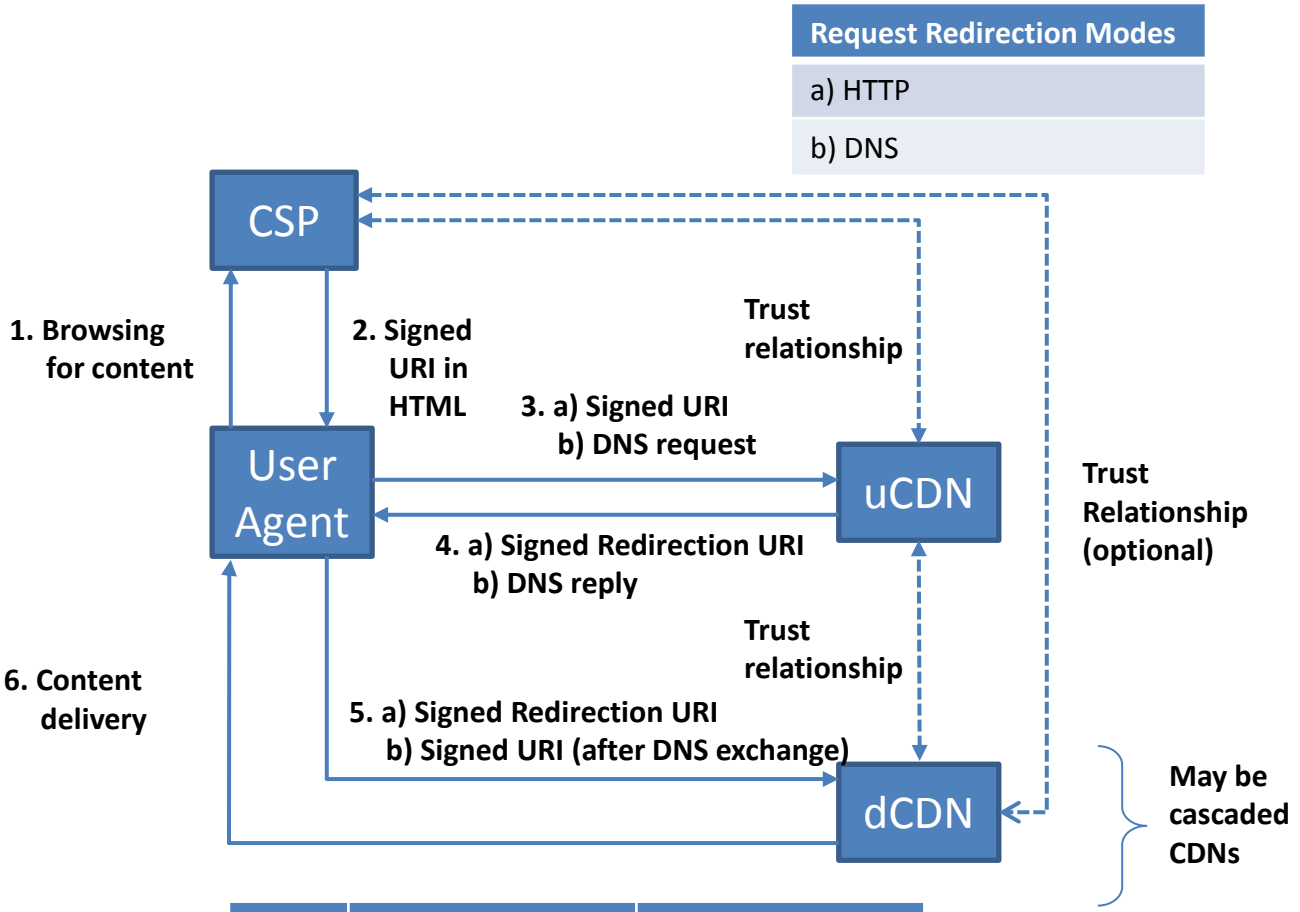
CDNI URI Signing
(draft-leung-cdni-uri-signing-02)

CDNI Working Group
IETF 87 Berlin, Germany
Aug 1, 2013

Kent Leung (kleung@cisco.com)
Francois Le Faucheur (flefauch@cisco.com)
Bill Downey (william.s.downey@verizon.com)
Ray van Brandenburg (ray.vanbrandenburg@tno.nl)
Scott Leibrand (sleibrand@llnw.com)

URI Signing in a CDNI Environment



Key	Asymmetric	Symmetric
HTTP	Public key (uCDN)	Shared key (uCDN)
DNS	Public key (CSP)	Shared key (CSP)

Signed URI Format

- Enforcement Attributes
  - Expiry Time (ET), Client IP (CIP)
- Signature Computation Attributes
  - Version (VER), Key ID (KID), Hash Function (HF)
- URI Signature Attributes
  - Message Digest (MD), Digital Signature (DS)
- URI Signing Token Attribute
  - URI Signing Token (UST)

Operations Summary

- Signing a URI
  - Exclude the “scheme name” part of original URI
  - Append enforcement/computation attributes (optional)
  - Compute message digest or digital signature
  - Generate the Signed URI (when URI Signing token is not used)
  - If URI Signing Token is used, then compute the token to generate the Signed URI
- Validating a URI signature
  - If URI Signing Token is in the Signed URI, then decode the token
  - Extract CDNI attributes
  - Exclude the “scheme name” part of Signed URI
  - If symmetric key is used, compute message digest
  - Verify message digest or digital signature
  - Enforce distribution policy

Next Steps

- Todo list
  - Address WG feedback
  - Considerations for CDNI interfaces
  - Recursive mode support for CDNI Request Routing Redirection interface
  - HTTP ABR
  - IANA Considerations
- Add URI Signing to charter?
  - Request interface between User Agent and CDN (outside scope of CDNI, draft-choi-cdni-req-intf)