

draft-fieau-https-delivery-delegation-02

A CDNi Use case

Lurk BoF

Frédéric Fieau Orange
Emile Stephan, Benoît Gaussen

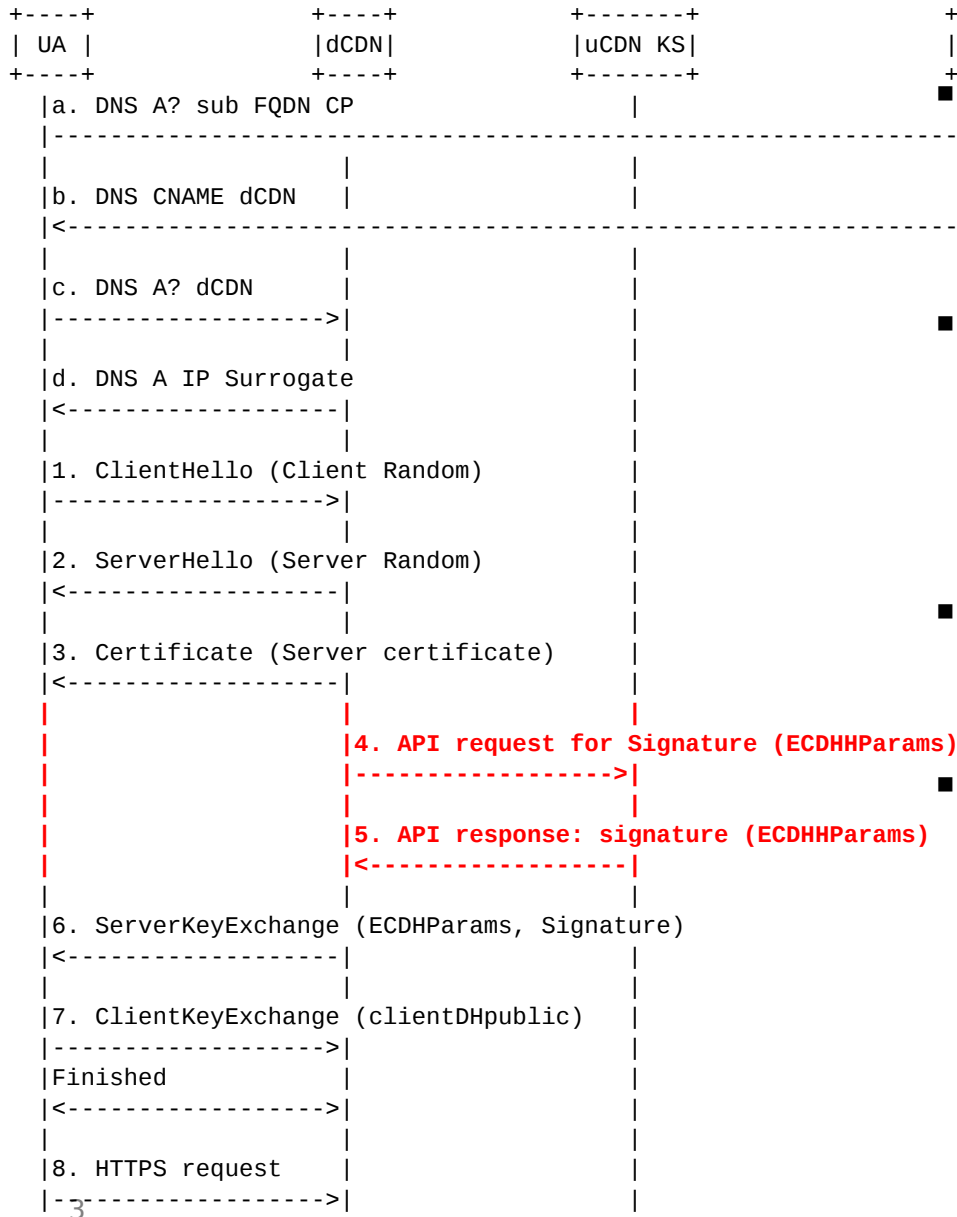
IETF 95 – Buenos Aires

CDNi delivery delegation

From HTTP to HTTPS delivery

- CDNi HTTP delivery delegation
 - CDNi WG has specified interfaces for handling HTTP delegation in CDNi
 - Content Distribution Network Interconnection (CDNI) Problem Statement <https://datatracker.ietf.org/doc/rfc6707>
 - Request Routing Redirection interface for CDN Interconnection <https://datatracker.ietf.org/doc/draft-ietf-cdni-redirection>
 - HTTP redirection and DNS routing are be used to redirect a user from a uCDN to a dCDN that will deliver content
- CDNi HTTPS delegation (work in progress)
 - In a CDN interconnection model, a uCDN delegates the HTTPS content delivery to a dCDN.
 - In a particular use case, the uCDN doesn't want to provide the dCDN with its private keys (i.e. for legal/trusting/security reasons)
 - Using Lurk, only the uCDN needs valid certificates received by the Content Provider (CP), whereas the dCDN would rely on security materials received from the uCDN Key Server (KS) for the TLS session establishment.
 - The dCDN will deliver HTTPS content to the user agent using the uCDN (or CP)

HTTPS delegation example



- In a common HTTP use case of CDNi, the CP delegates the delivery of a HTTP sub domain to the uCDN.
- To work with HTTPS it requires a Key Server that owns the CP subdomain certificate & private key.
- The dCDN does not possess any CP subdomain credentials.
- The dCDN queries the KS to get the necessary security materials to establish the secure connection to the end-user and serve the content.

Next Steps

- The interface between the dCDN and uCDN Key Server is common to other use cases
- It should be specified by the IETF.