URI Signing for HAS content

CDNI Meeting

IETF 93

Prague

Kent Leung

Francois Le Faucheur

Ray van Brandenburg

Bill Downey

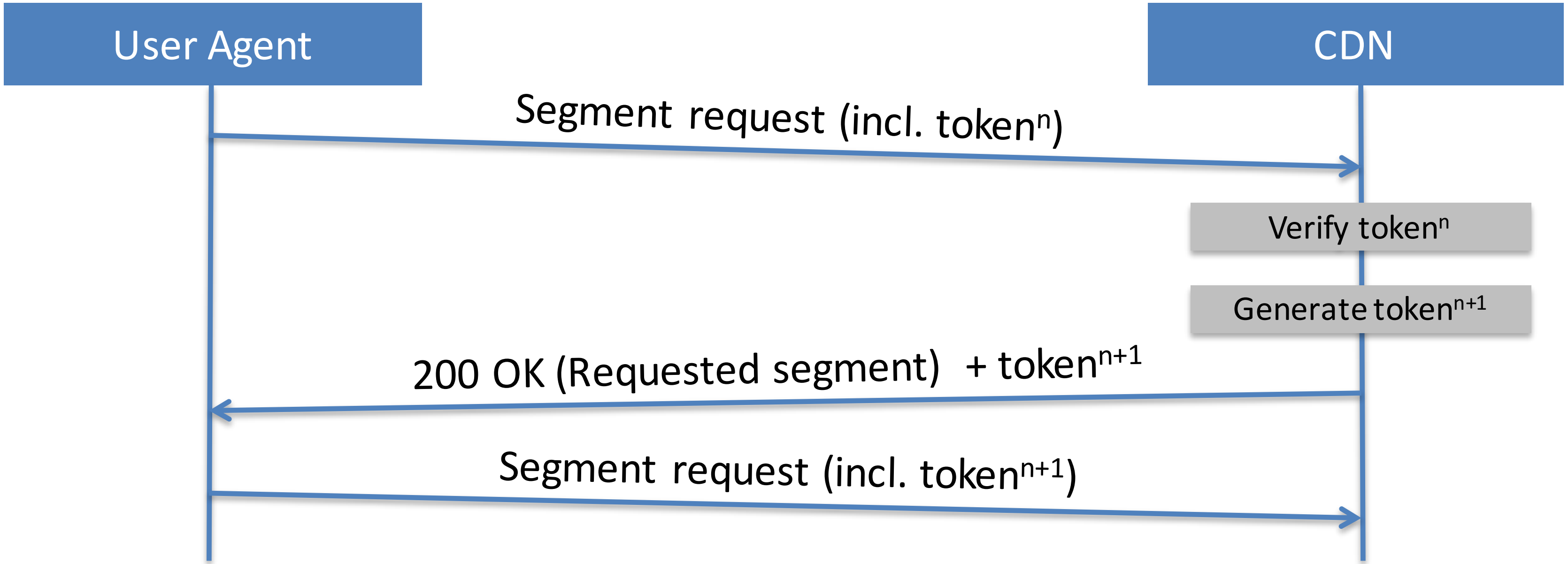
Michael Fisher

Update since Dallas

- New version (-04)
  - Adds chained token concept discussed in Dallas
  - Targeted at URI Signing for segmented content (e.g. DASH, HLS, etc.)
- Incoming liaison from MPEG
  - https://datatracker.ietf.org/liaison/1413/
  - Three questions:
    - User Agent
    - Long-term tokens
    - HTTP header name

Disclaimer: An IPR disclosure has been filed on this draft:
http://datatracker.ietf.org/ipr/2603/

Recap: Access control via chained tokens for segmented content (e.g. DASH)


User Agent
CDN
Segment request (incl. token^n)
Verify token^n
Generate token^n+1
200 OK (Requested segment) + token^n+1
Segment request (incl. token^n+1)

- Two options for token:
  - Cookie-based (works on existing UAs, and for non-DASH protocols)
  - URL-based (in line with URI Signing for non-segmented content)

New URI Signing elements

- Path Pattern: Defines scope of signed token
  - Example: */folder/content-83112371/quality_*/segment????.mp4
- URI Signing Cookie Flag: Specifies whether Cookies or HTTP Headers should be used in the response to the UA
- Expiration Time Setting: Specifies the value of the experitation time for the next signed token
- Question: Should we allow for more than one Path Pattern element?
  - Would for example allow different path patterns for for segments and manifests

Questions from MPEG - 1

- Long-term Tokens
  - MPEG sees a need for long-term tokens (from the liaison: ‘hours to days’)
  - Questionable whether such long-term tokens are actually useful
  - That said, if the validity time of a token is relatively short (order of minutes) but still significantly longer than a segment duration, then it might not be necessary to recalculate the signed token every cycle (unnecessary load on server)

  - Question: Do we want to include a mechanism which would allow servers to check whether a token needs to be refreshed or whether it can be re-used?
    - Advantage: might reduce load on server-side
    - Disadvantage: adds complexity, both on server and client side (needs to be aware when token was last refreshed)

Questions from MPEG - 2

- HTTP Header Name
  - Current situation: The HTTP Header name used for returning Signed Tokens to the client can be set via CDNI Metadata or via configuration. If none is set, it defaults to 'URISigningPackage'
  - Note: We use the same approach for signalling the token in the query string component of the URL (metadata/configuration with default to URISigningPackage)
  - Assumption: if we allow for dynamic HTTP Header fields, the actual header used needs to be communicated to the client via e.g. the DASH manifest file/MPD
  - Question: Do we stick with the current approach, or do we want to formally register this value with IANA?

Questions from MPEG - 3

- “According to the URI Signing specification, URI Signed Token may be transported with an HTTP response header. In that case, the User Agent is expected to extract the URI Signed Token from this specific HTTP header and reinsert it in the next HTTP request as a query string argument. **MPEG experts would like to know whether the IETF CDNI working group intended to mandate this behaviour in the User Agent, or whether it is up to the application to handle this operation.**”

- Fundamentally, what’s the difference?

Next steps

- We need reviews of the new features in the draft
- Keep working with MPEG on specifying the client-side elements necessary