URI Signing

draft-ietf-cdni-uri-signing-09

CDNI
IETF 96
Berlin

Kent Leung
Francois Le Faucheur
Ray van Brandenburg
Bill Downey
Michael Fisher
Update since BA

• Currently in WGLC

• Two new versions posted since BA (-08, -09)

• New in -08
  – Addressed comments from Leif, Phil and Gancho based on implementation experience
  – Percent-encoding of URI Pattern Container
  – Recommendations on parsing of UPC to increase performance
  – Brought algorithm notation in line with NIST (e.g. “ECDSA” versus “EC-DSA”)
  – Added support for signalling of URI Signing Package as a URL Path Parameter

• New in -09
  – Added CDNI Metadata Auth Type registration to IANA section
    • (Will probably be removed again)
Open Issues - 1

• Matt Miller reviewed draft from a security perspective. Issues he found:

• Implicit algorithms: when using the default algorithms, the HF/DSA field is optional. This should be changed
• Implicit key sizes
• Currently using AES-ECB for Client IP Encryption. Potential for oracle and substitution attacks
• Mixing of hashing algorithm: better to use a single one throughout
• No recommendations regarding use of ECDSA (specific curves etc.)

• In summary: we need some work here
Open Issues - 2

• Proposal from Ben to make ECDSA optional instead of mandatory
• Proposal to merge KID and KID_NUM information elements
  – Both are used for communicating Key Index
    • KID as string (e.g. for public key URLs), KID_NUM as 32-bit int
  – Original intention for introducing KID_NUM was that it might be slightly better in terms of performance
  – Questionable whether that’s still the case given that we now have mandatory Signing Package
• Proposal to merge HF and DSA
  – HF and DSA are used to signal the used hash function or digital signature algorithm respectively
  – In practice, no real benefit of having two elements, since actual algorithm value has to be parsed anyway
• Proposal to merge MD and DS
  – MD and DS for signalling the message signature itself (MD when HF is used, DS when DSA is used)
Open Issues - 3

• One way to deal with security issues would be to simply adopt JSON Web Token/Signature (JWT/JWS) as format for URI Signing
  • draf-ietf-cdni-uri-signing would become profile of JWT/JWS that defines additional ’claims’ and explains how JWT/JWS with the new claims may be used to perform URI Signing

  + Would benefit from thorough security review JWT/JWS went through
  + Would benefit from existing JWT implementations
  - Would require very significant rewrite of draft at this late stage (and probably delay it)
  - Current implementation would need to be overhauled

- Thoughts? Do the benefits outweigh the costs?
Next steps

• Make decision on whether to adopt JWT/JWS
  – If yes: rewrite draft
  – If no: address comments received during WGLC, including security issues

• Submit to IESG