JSON Web Key Thumbprint

Mike Jones

November 10, 2014

IETF 91

Overview

- draft-jones-jose-jwk-thumbprint-01
- Defines “jkt” (JSON Web Key SHA-256 Thumbprint) values for JWK keys
  - Analogous to “x5t#S256” for X.509 keys
- Hash input uses JWK w/ required key fields
- Sorts them into lexicographic order
- Hashes UTF-8 representation of resulting JWK

Example

- For JWK containing "kty":"RSA", "n", "e", and possibly optional fields, sort fields lexicographically into order "e", "kty", "n"
- Create hash input as a JWK with no white space and unescaped char representations:
  - E.g., {"e":"AQAB","kty":"RSA","n":"0vx7…"}
- Hash UTF-8 representation
- "jkt" value is base64url encoded hash value

Incorporated input from IETF 90

- Spec now says result is undefined if chars requiring escaping are needed in hash input
  - If a canonical JSON representation standard is ever adopted, spec could be revised to use it, resulting in unambiguous definitions for those (unlikely to ever occur) values as well
- Added instructions for representing integer numeric values in the hash input

Adopt as WG document?

- Used by OpenID Connect Core standard
- IoT applications another possible use case
- Can we add a charter item for this?