JSON Signing and Encryption(JOSE)

Jim Schaad

August Cellars

JOSE Goals

- Create a method for providing Integrity Protection for JSON objects
  - Signature Protection for Long Term protection
  - MAC Protection for in transit protection
- Create a method for providing Encryption Protection for JSON objects
- Create a method for holding keys in JSON objects
- Define a set of must implement algorithms

JOSE Goals (2)

- Current targets
  - Adopt WG documents in Jan 2012
  - Submit to IESG consideration around Jul 2012

Signature Format

- Elements
  - Signature Header
  - Dot
  - Signature Body
  - Dot
  - Signature Value
- Example:
  eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQogImh0dHA6Ly9leGFtcGxlLmNvbS9pc19yb290Ijp0cnVlfQ.dBjftJeZ4CVP-mB92K27uhbUJU1p1r_wW1gFWFOEjXk

Signature Header

- base64url encoded JSON object
- Contains algorithm specific parameter information
- Key identification:
  - URL to JSON encoded key
  - URL to PEM encoded PKIX certificate/certificate chain
  - SHA1 hash of PKIX certificate

Signature Body

- Can be any value
- Discussions about detached bodies
  - Currently no support
- Base64url encoded value

Signature Value

- base64url encoded value
- Result of hashing and signing
  - Signature Header (in base64url)
  - Dot
  - Signature Body (in base64url)

Questions?