JOSE Working Group

7 November 2013, 0900-1130 PST
IETF 88 Vancouver

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Agenda

- Administrivia and Agenda Bashing
- Open issue resolution
  Issues to be discussed include:
  - #54, #55, #141
  - #74-C
  - #77
  - #93
  - #114-C
- Schedule and next steps (Chairs)
  - Cookbook document
  - Virtual interim schedule

Summary Issue Status

- draft-ietf-jose-use-cases
  - IESG processing
- JWS, JWE, JWK, JWA Issue Resolution
  - Total Issues = 185 (many with multiple parts)
  - Remaining Open Issues = 56 (Closed Issues = 129)
  - Co-chairs and editor have had several meetings this week and previously resulting in agreements for 49 issues:
    - Awaiting editor implementation,
    - Awaiting implementation verification, or
    - Awaiting external input or verification.
  - Issues for discussion today – 7 !

#54, #55, #141

- #54 (JWA) epk/apu/apv need to be REQUIRED
- #55 (JWA) Mandatory entropy in ECC KDF inputs
- #141 (JWS) Section 4.1.10 "crit" (Critical) Header Parameter

- concat issue
  - http://www.ietf.org/mail-archive/web/jose/current/msg03542.html

#74-C (JWK)

- #74-C (JWK) Section 3.5 - "x5u" (X.509 URL) Header Parameter
  - What happens if this JWK has only an x5u member in it? Is this a legal construct? How does one say that this matches the bare public key?

- Question: Is there a minimum set of fields which must be present in the JWK?

#77

- #77 – (JWK) Section 3.7 "x5c" (X.509 Certificate Chain) Parameter

- We currently require things to be presented as chains, but generally things are presented as bags
- Should we change from chains to bags?
- If we stay with chains, what happens to partial chains (are they legal)?

#93

- #93 (JWS)
  - There should be a new - informational - appendix added to this document that describes how to go from the various fields or lack of fields to get a key. This should include all of the methods of finding keys that Mike has described to me over the duration of this project. This would be everything from following a jku to the application provides a method to find the key. The description should contain a series of steps and a description of what information is retrieved by doing this.

- Jim Schaad and Richard Barnes provided proposals (see following slides):
  - Non-normative appendix to JWS

Jim Schaad proposal: http://www.ietf.org/mail-archive/web/jose/current/msg03447.html

A. Look for certificates:
   a. Identify an EE certificate and a certificate list
      i. Is there an x5u? Follow the link and down load the certificates to get a certificate list and set the EE certificate to the zero-th entry in the list
      ii. Is there an x5t? Locate the EE certificate in local storage and set the certificate list to that certificate
      iii. Is there an x5c? Set the EE certificate to the first item in the list. Set the certificate list to the array of certificates.
   b. Do path building from the EE certificate to a trusted root using the certificate list and local certificate stores.
   c. Validate the path to a trust point

B. Look for JWK Sets
   a. Create an empty JWK set KEYS
   b. Is there a jku? Down load from the pointer and add to KEYS we are maintaining.
   c. Is there a jkw? Add it to KEYS
   d. Are there application JWKs? Add them to KEYS
   e. Are there local JWKs? Add them to KEYS

C. Find viable keys in KEYS
   a. Is there a kid? Remove items from KEYS which have a kid and it does match, leave items with kid value in the KEYS
   b. Remove items from KEYS based on the algorithm in the alg member. If a key element in KEYS does not support the algorithm, remove it. This examines the ‘kty’ member and the ‘alg’ member if it is present.
   c. Remove items from KEYS based on the use member. If a key element in KEYS has a use member and it does not match the required use for the JOSE element, remove it from KEYS.

D. Check each of the key values in KEYS to see if it validates/decrypts the object.

Richard Barnes proposal: http://www.ietf.org/mail-archive/web/jose/current/msg03527.html

Look for self-describing keys (jwk, jku, x5c, x5u), then look for key references (kid, x5t)

0. Initialize KEYS to the empty set
1. If a key has been speciified by the application for use with this object, add that key to KEYS
2. If "jwk" in header, add value to KEYS
3. If "jku" in header, fetch URL and add all JWKs in set to KEYS
4. If "x5c" in header, extract public key and add to KEYS (or corresponding private key, if present)
5. If "x5u" in header, fetch URL and process first certificate as "x5c”
6. If "kid" in header and "kid" value represents a known key, add corresponding key to KEYS
7. If "x5t" in header and "x5t" value matches a known cert, add corresponding key to KEYS

#114-C

- #144-C (JWS) Section 4.1.10 "crit" (Critical) Header Parameter

- Question: If an extension is placed in a “crit” header, must that extension also be signed?

Next Steps

- Cookbook document
- Expected editor's drafts:
  - In the next week or so, all normative changes incorporated
  - In the next month or so, all remaining editorial changes
- Proposed tentative virtual interim
  - 13 January 2014