Welcome to COSE!

Justin Richer & Kepeng Li

IETF 94, Yokohama, November 2015

Meeting logistics

- XMPP Scribe?
- Note Taker?
- Are you sure you're in the right meeting?

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

- Opening & Welcome 5 min (Justin/Kepeng)
- COSE Tokens 10 min (Justin)
- ACE Object Security 15 min (Goran)
  - https://tools.ietf.org/html/draft-selander-ace-object-security-03
- COSE Messages and open issues 55 min (Jim)
  - https://datatracker.ietf.org/doc/draft-ietf-cose-msg/
  - https://github.com/cose-wg/cose-issues/issues
- Wrap-up 5 min (Justin/Kepeng)

What is COSE?

- CBOR Object Signing & Encryption
- Pronounced like “cosy”


Meet
Your
COSE
Chairs

About the Working Group

What are we building?

XML : **XML DSIG** :: JSON : **JOSE** :: CBOR : **COSE**

What are our goals?

- JOSE in CBOR
  - Signing/validation
  - Encryption/decryption
  - Key representation (public/private)
- Other things are out of scope
  - Key management, identity management, stuff you wish JOSE had

Focus on Constrained Environments

- There are different kinds of constraints
  - Memory
  - Processor power
  - Network usage
- All of these need to be considered in decisions

The question we should ask ourselves:

What Would Jose Do?

How we'll get work done

Driving consensus

- Discussions on mailing list
- In person IETF sessions
- Phone calls where needed
  - None are planned right now

cose@ietf.org

Active spec work in GitHub

- Editors and Chairs have write access
  - Other contributors work via pull requests
- Issues via GitHub trackers

https://github.com/cose-wg

Let’s build this thing

- Keep it as simple as possible
  - (But no simpler)
- Learn from what’s being used elsewhere
  - Particularly in JOSE
- Realize when “You Ain’t Gonna Need It”
- Rough consensus, running code


cose@ietf.org
cose-chairs@ietf.org

COSE Tokens

What's a COSE Token?

- JWS/JWE/JWA :: COSE Messages
  - Cryptographic methods and envelopes
- JWT :: COSE Token
  - Common payload description

Should we build it?

- JWT has driven use of JOSE more than any other factor
- ACE drafts already mention an abstract “COSE Token” concept

Where should we build it?

- Here in COSE?
- In OAuth (where JWT was made)?