



Welcome to COSE!

Justin Richer & Kepeng Li

IETF 93, Prague, July 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 - 5min (Justin/Kepeng)
- Introduction to the COSE Working Group - 10min (Justin)
 - Questions/transition - 5min
- ACE Requirements - 10min (Goran)
 - Questions/transition - 5min
- Key issues and choices for COSE - 10min (Mike)
 - Questions/transition - 5min
- COSE Messages Draft Current State - 10min (Jim)
 - Link: <http://datatracker.ietf.org/doc/draft-ietf-cose-msg/>
- Issues and open discussion - 30min

What is COSE?

- CBOR Object Signing & Encryption
- Brand new WG
 - Risen from the ashes of JOSE
- Pronounced like “cosy”

**Meet
Your
COSE
Chairs**



Kepong Li

- Works for Alibaba
- Also works as ACE co-chair
- Active in CoRE
- Wants to coordinate COSE with CoRE, ACE, and others



Justin Richer

- Founder/president/janitor of Bespoke Engineering
 - Independent consultant
 - Formerly of MITRE
- Editing a few OAuth specs
- Just wants COSE to work





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 Φ O?



Should we just copy JOSE?

Yes and no

Understand what works

- Which parts of JOSE work well?
- Which parts can be directly translated with little work?
- Which parts do people actually use?

What do actual JOSE libraries do?

- Compact serializations
- JWS validation, signing
- JWE encryption/decryption
- JWK parsing, generation



Pay attention to what people do

A standard is only a standard if someone implements it



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)
- Realize when “You Ain't Gonna Need It”
- Rough consensus, running code

A red velvet armchair is positioned on the right side of the frame, set against a wall with a rough, blue-painted stone texture. The lighting is dramatic, with the chair and the wall's texture highlighted. A semi-transparent dark horizontal band is overlaid across the middle of the image, containing the text.

cose@ietf.org

cose-chairs@ietf.org