Definition of End-to-end Encryption

https://datatracker.ietf.org/doc/draft-knodel-e2ee-definition

Authors

- Mallory Knodel, Center for Democracy and Technology
- Fred Baker, ISC
- Olaf Kolkman, ISOC
- Sofia Celi, Cloudflare
- Gurshabad Grover, Centre for Internet and Society India

Goal

A priori definition of end-to-end encrypted communications.

Outcomes

Things that are not e2ee can’t easily be called e2ee.

Parallel drafting in MLS to compliment other work.

Articulation of norms- and principles-driven implementations.

Anti-goals

Anti-definition.

Directly invoking threats in order to define e2ee.

Public record of discord and disagreement about what is e2ee.

TOC

Changes

Since -00

- Broke out separate subsection in the formal definition on “end”.

Since -01

- Nits and edits from Britta
- Added functional definition as a formal definition subsection from Chelsea
- Linked concept of identity and endpoint in first section

Future of the draft

- Incorporating feedback in an initial review from Raphael. -- thanks
- More thorough definitions of features in second section. -- but still precise
- Information around how metadata is protected (or should!) in end-to-end communications
- More ideas around forward secrecy and backwards security

Dispatch question

We think this draft should be in MLS and we propose to keep the draft open as long as MLS is at work.

MLS might agree as per last virtual interim.

But then other WGs might want to weigh in: OpenPGP, LAMPS, et al?

PRs, reviews welcome

https://github.com/mallory/e2ee