MEDUP

Missing Elements for Decentralized Usable Privacy

PEARG @ IETF-106, Mon Nov 18, 2019

Bernie Hoeneisen
<bernie.hoeneisen@pep.foundation>

p≡p

Privacy by Default.

Background

- Decentralized (E2E / P2P)
  - Pervasive monitoring (RFC 7258) is an attack on Privacy
  - Centralized elements are more prone to attacks
- Usable
  - Message encryption is a hassle for most Internet users
    - Even for savvy users, setting up encryption may take several hours
  - Need to fix this usability challenge by automation
- Privacy
  - Privacy is a Human Right (RFC 8280)

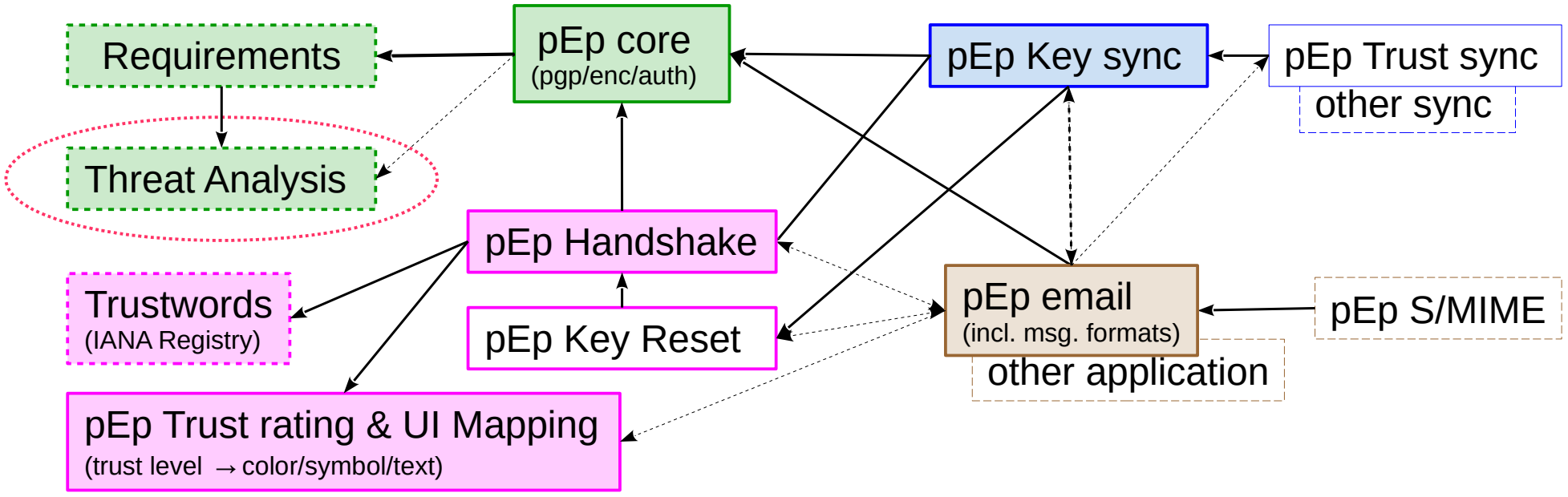
MEDUP in short

- Enhancements to application protocols for decentralized usable privacy
  - Based on Opportunistic Security (RFC 7435) principles
- Originally emerged from pEp (pretty Easy privacy)
  - Everybody working in this field (e.g. autocrypt) invited to participate & actively contribute to MEDUP
- Goal
  - Define the missing pieces (e.g. key management, private key synchronization, message formats, trustwords, handshake, etc.)

MEDUP Group

- Non-WG sessions during IETF meetings
- Mailing list discussion:
  - medup@ietf.org
  - To subscribe: https://www.ietf.org/mailman/listinfo/MEDUP
- Aims for BoF/ IETF WG

I-D Dependency Graph



Legend:

Core

Secure decentralized synchronization

Handshake & trust

pEp Applications

depends on

uses / may use

I-D exists

Not pEp specific

I-D coming soon

TBD

Questions

Backup Slides

What MEDUP is about?

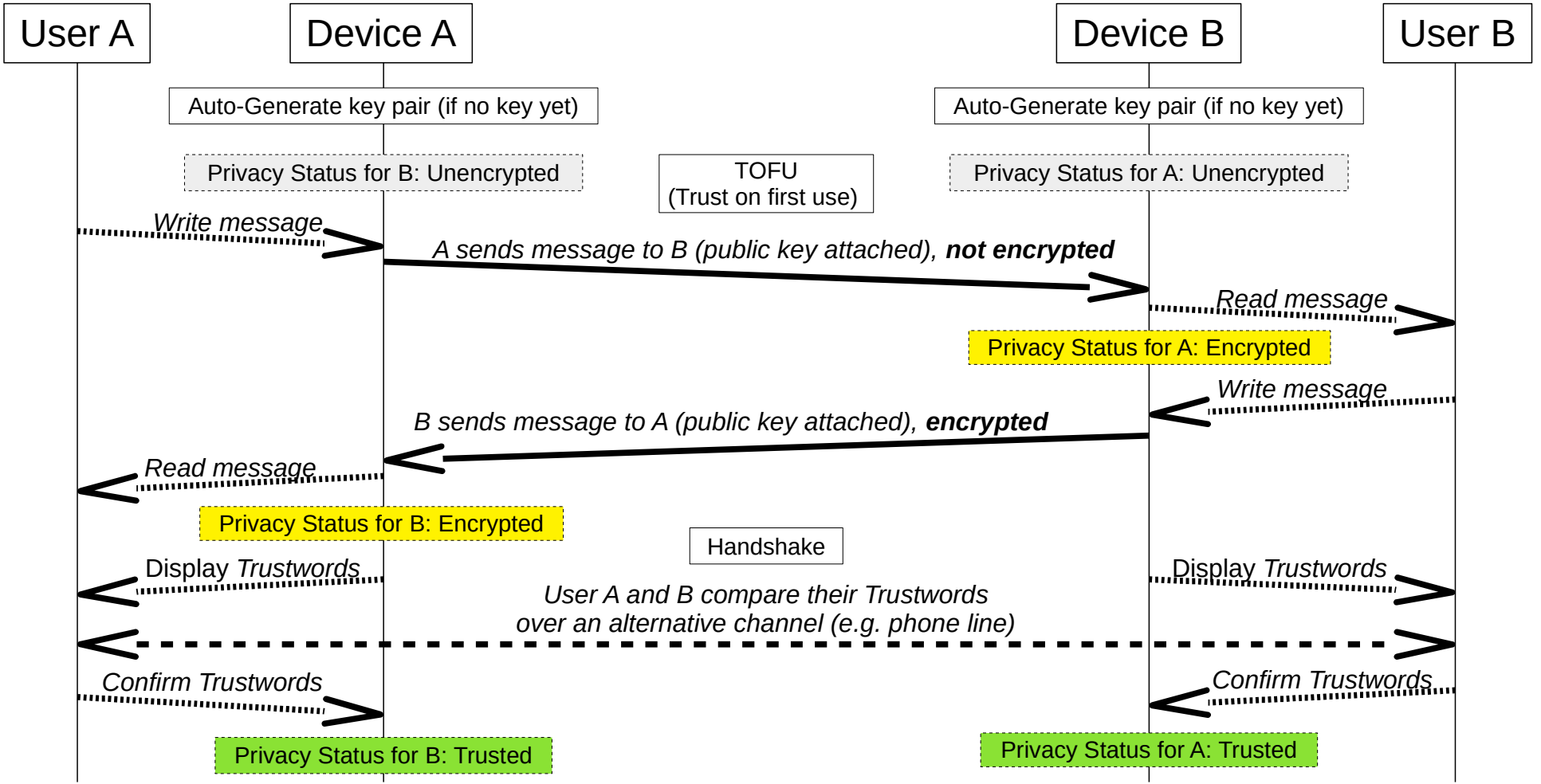
Missing Elements for Decentralized and Usable Privacy

The MEDUP list is for discussions of enhancements to application protocols for decentralized usable privacy.

RFC 8280 has identified and documented important principles in such as Data Minimization, End-to-End and Interoperability in order to enable access to Human Rights. While (partial) implementations of these concepts are already available, today's applications widely lack Privacy support that ordinary users can easily handle.

In MEDUP these issues are addressed based on Opportunistic Security (RFC 7435) principles. Updates/usage clarifications to application level protocols such as email and XMPP are in scope.

Example Msg. flow (simplified)



pEp Email Format 2