SML Use Cases for Opportunistic Email Encryption in pEp

SML @ IETF-116, Tue 28 March 2023

revision 006

Hernâni Marques / Bernie Hoeneisen

p≡p

Privacy by Default.

Background

- pEp aims to make text communications (i.e., email, chat, ...) **private by default**
- pEp systems must not depend on centralized elements
- “Good” tools for privacy (using, e.g., OpenPGP) already exist
- **However:**
  - Most users are unable to use existing encryption tools such as GnuPG (properly)
- Need to fix this usability challenge by automation
- This automation requires “Structured Emails”

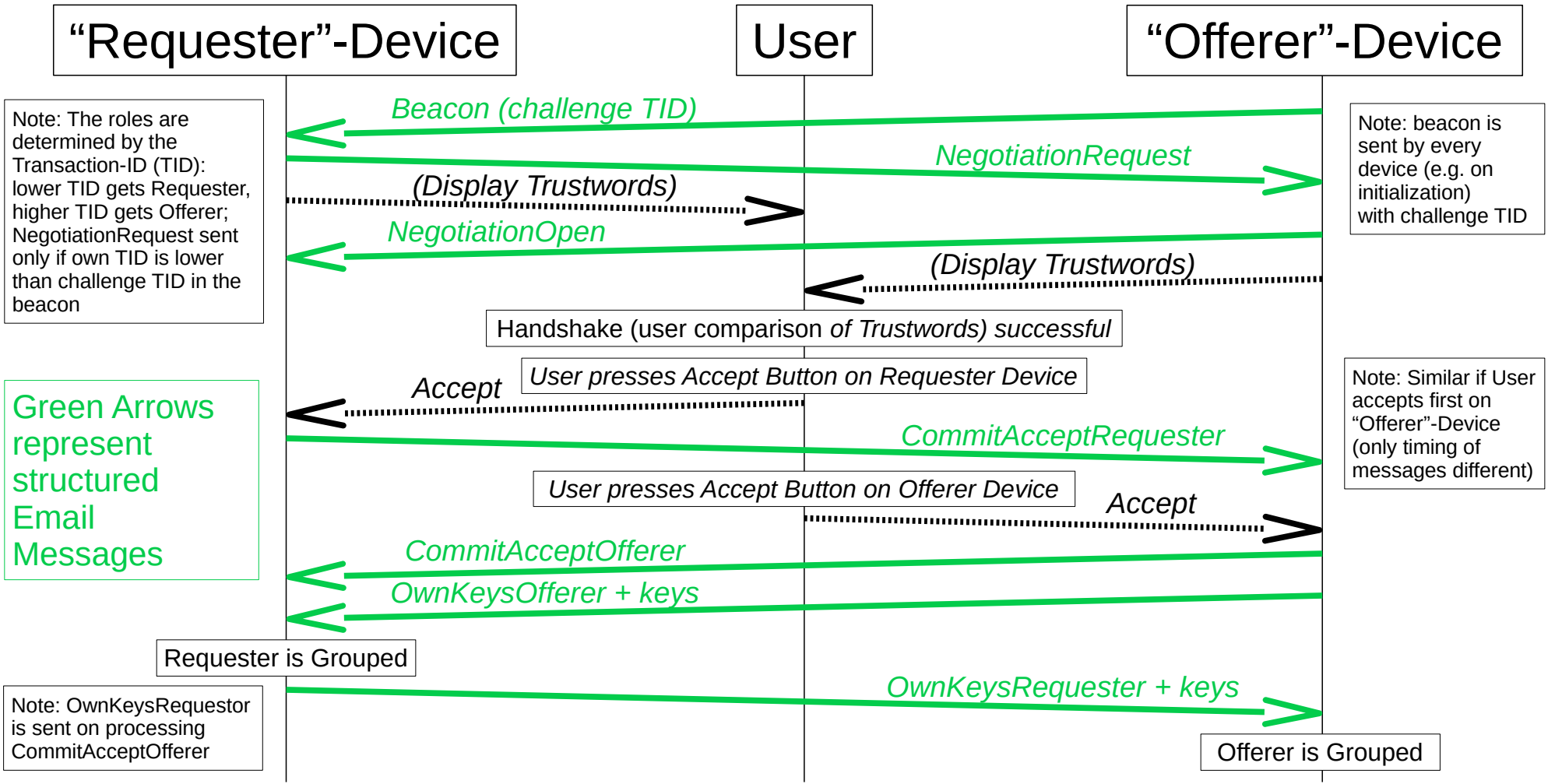
Use Case 1: Attached Public Key

- I-D: https://datatracker.ietf.org/doc/html/draft-pep-email
- Public key is attached to pEp email messages (by default)
- Properties (of this type) of Structured Email
  - Key to be automatically processed by receiving MUA
- Receiving users may get confused by “attachment that cannot be opened” (in absence of an OpenPGP-aware setup)
  - Do not (invasively) show such attachments to (ordinary) users

Use Case 2: pEp KeySync

- I-D: https://datatracker.ietf.org/doc/html/draft-pep-keysync
- Users usually have multiple devices; received messages cannot be decrypted on all devices
  - Missing private key
  - Encrypted with private key from another device
- pEp KeySync: Synchronization of private Keys
  - In a secure, peer-to-peer manner
- (Such types of) Structured Emails sent between the devices
  - Form (join or leave) a Device Group
  - Share keys among members of a Device Group

UC2: e.g., Form Device Group (simplified)



Use Case 3: pEp KeyReset

- I-D: https://datatracker.ietf.org/doc/html/draft-pep-keyreset
- pEp KeyReset protocol is used to revoke/replace/rotate public keys; relevant also for Zero Trust environments, rotating often
- pEp KeyReset also plays an important role in group communications:
  - Managed groups (admin adding or removing members)
  - Unmanaged groups (with members leaving)
- This is done in a peer-to-peer manner, by sending (such types of) Structured Emails:
  - Distribute Information about new keys to be imported, alongside with revocation certificates
  - Such “technical messages” are intended to be processed automatically, not to be read by users

Summary and Requirements

Structured Emails or attachments might be received, not intended to be read by users (in full), but to be processed automatically.

This may confuse users. Mechanisms to improve usability:

(1) Means to instruct receiving MUAs to not to render certain *attachments* to users

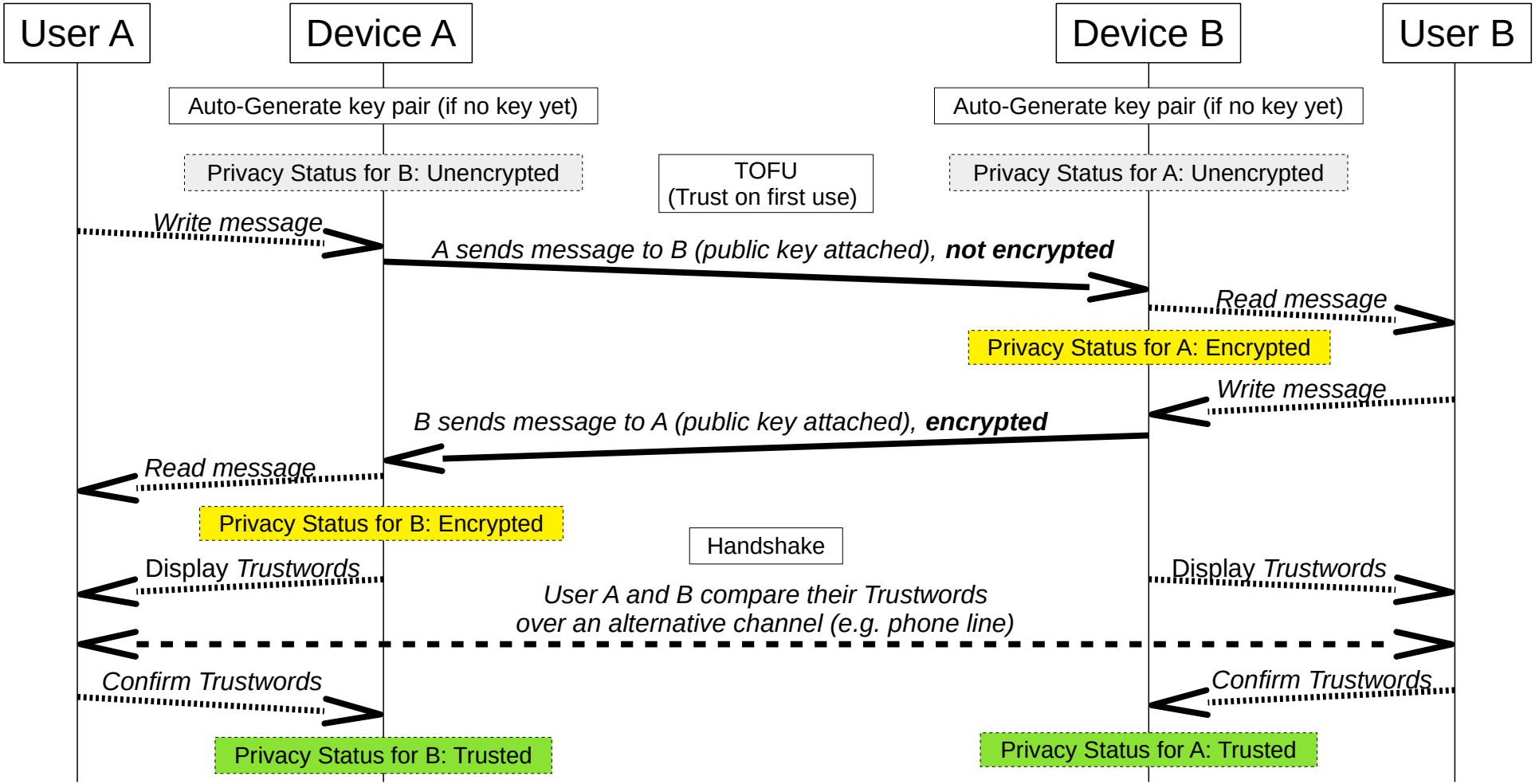
(2) Means to instruct receiving MUAs to not to display certain *emails* to users

(3) Means to instruct receiving MUAs to automatically process (or not process) an *attachment* (or MIME sub-tree) [optional]

Questions / Discussion

Backup Slides

Example Msg. flow (simplified)



UC1: e.g., wire message format (pubkey attached)

```
From: Alice <alice@example.org>
To: Bob <bob@example.org>
Date: Tue, 31 Dec 2019 05:05:05 +0200
X-pEp-Version: 2.1
MIME-Version: 1.0
Subject: Saying Hello
Content-Type: multipart/mixed; boundary="boundary"

--boundary
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: quoted-printable

Hello Bob

If you reply to this email using a pEp-enabled
client, I will be able to send you that sensitive
material I talked to you about.

Have a good day!

Alice

--
Sent with pEp for Android.
```

```
--boundary
Content-Type: application/pgp-keys;
name="pEpkey.asc"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
filename="pEpkey.asc"; size=2639

-----BEGIN PGP PUBLIC KEY BLOCK-----

[...]

-----END PGP PUBLIC KEY BLOCK-----

--boundary--
```

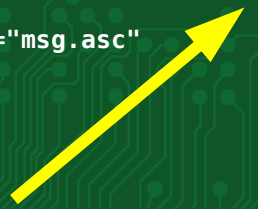
UC2: e.g., wire message format (KeySync)

```
From: alice@example.org
To: alice@example.org
Date: Tue, 31 Dec 2022 23:23:23 +0200
Subject: =?UTF-8?Q?p=e2=89=a1p_key_management_message_-
_please_ignore?=
X-pEp-autoconsume: yes
X-Pep-Version: 2.1

This is a multi-part message in MIME format.
--------------boundary
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 8bit

This message is part of pEp's concept to manage keys.

You can safely ignore it. It will be deleted
automatically.

--------------boundary
Content-Type: application/pEp.sync; name="sync.pEp"
Content-Disposition: attachment; filename="sync.pEp"
Content-Transfer-Encoding: base64

QAEIGAA=
```

```
--------------boundary
Content-Type: application/pEp.sign;
name="electronic_signature.asc"
Content-Disposition: attachment;
filename="electronic_signature.asc"
Content-Transfer-Encoding: base64

[...]

--------------boundary
Content-Type: application/pgp-keys; name="file://sender_key.asc"
Content-Disposition: attachment;
filename="file://sender_key.asc"
Content-Description: OpenPGP public key
Content-Transfer-Encoding: 7bit

-----BEGIN PGP PUBLIC KEY BLOCK-----

[...]

-----END PGP PUBLIC KEY BLOCK-----

--------------boundary--
```

UC3: e.g., wire message format (KeyReset)

```
From: alice@example.org
To: bob@example.org
Subject: pEp
X-pEp-Version: 2.1
X-pEp-autoconsume: yes
MIME-Version: 1.0
Content-Type: multipart/encrypted;
boundary="boundary";
 protocol="application/pgp-encrypted"

--boundary
Content-Type: application/pgp-encrypted

Version: 1
--boundary
Content-Type: application/octet-stream
Content-Transfer-Encoding: 7bit
Content-Disposition: inline; filename="msg.asc"

-----BEGIN PGP MESSAGE-----

[... {PGP-encrypted payload} ...]

-----END PGP MESSAGE-----

--boundary--
```



```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="boundary2"

--boundary2
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: quoted-printable

Subject: pEp key management message - please ignore

This message is part of pEp's concept to manage keys.

You can safely ignore it. It will be deleted automatically.

--boundary2
Content-Type: application/pEp.distribution
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="ignore_this_attachment.pEp"

BAAEHnBlcC50ZXN0LmFsaWNlQHBlcC1wcm9qZWN0Lm9yZzCVfHVes1hln8nwygFSgjou3+AdLhzg
iuC+3u7cvurmyuSSyCaC2NLGykDS3ECu3tzIyuTYwtzJ/kaYmzzJOmibEWcIKpDIB2akY+Q5y3E=

--boundary2
Content-Type: application/pgp-keys
Content-Disposition: attachment; filename="pEpkey.asc"

-----BEGIN PGP PUBLIC KEY BLOCK-----

[...]

-----END PGP PUBLIC KEY BLOCK-----

--boundary2--
```

Running Code

https://pep.software/

- p≡p for Outlook (release: add-on)
- p≡p for Android (release: app)
- p≡p for iOS (release: app)
- p≡p for Thunderbird (release: add-on)

Join the discussion

- MEDUP (Missing Elements for Decentralized and Usable Privacy) side meeting at IETF-116
  - Room G-301 on Tue 2023-03-28 (today), 18:30-19:30 JST

- Mailing list discussion:
  - medup@ietf.org
  - To subscribe: https://www.ietf.org/mailman/listinfo/MEDUP

- Contact us directly:
  - hernani.marques@pep.foundation
  - bernie@ietf.hoeneisen.ch