Privacy by Default.

draft-birk-pep-00

p≡p

Privacy by Default.

p≡p – the problem

- There is nearly no privacy in the Internet
- No privacy is endangering free society
- Most users
  - are either bound to proprietary message systems (some with crypto)
  - or they’re using email, and S/MIME and OpenPGP need help there
- Jabber deserves help for gaining more users

We need answers for:

- Interoperability of Jabber with other IM, also in Crypto
- Interoperability OpenPGP ↔ S/MIME for Email
- Peer-to-peer Synchronization of Keys and Trust
- Hiding Metadata, Pseudonymity and Anonymity
  - Message Formats MIME and non-MIME
  - Protocols extending SMTP and adding DHT based Onion impl.
- Mapping different ways of Identity Management
- Common concept to signal Trust to users like with browsers
  => therefore standardized Trust rating

p≡p implementation status (1/2)

- Automated Key management (generation, revocation, etc.)
- p≡p Trust Rating, e.g. delivering traffic lights colors
- S/MIME and OpenPGP
- Message formats for more privacy
- First version of Key Sync
- Adapters for Java, C#, Python, Objective C, Swift, JavaScript, C++/Qt are available, more WIP

p≡p implementation status (2/2)

- First implementations of
  - p≡p for Android (release)
  - Enigmail/p≡p (beta)
  - p≡p for Outlook (release)
  - p≡p for iOS (alpha)
  - Kmail/p≡p (alpha)
- TODO
  - Extending GNUnet with DHT based Onion impl. based on CADET
  - Specifying and implementing p≡p Sync
    (P2P synchronization of Keys, Trust, Contacts and Calendar)

What does Sync need to work?

- Base protocol: inband Sync messages through Email and Jabber (encoding based on ASN.1 PER, i.e. as attachment)
- Sync: Beacon based auto-config for building Device Groups of user's devices
- Key Sync: sharing private keys with user authenticated devices
- Trust Sync: sharing trust ratings peer-to-peer
- Contact Sync, Calendar Sync: forming a peer-to-peer cloud via replication

Where can IETF help?

- MIME based message formats (message in message encapsulation)
- Key Sync
- Base protocol mapping for email, Jabber, …
- URI schemes for missing message addressing
  - mailto: irc: xmpp: are here, others are missing (like GNUnet MessageTransport, Signal, …)

Future additions

- Identity mapping
- Calendar mapping
- Key mapping
  - OpenPGP <=> S/MIME
  - Mapping on temporary symmetric keys
- Non-MIME message formats

IETF: Help!

- Interoperability is most important for p≡p,
  so please help keeping it up
- We need critics and input for already implemented code and I-Ds (first draft submitted draft-birk-pep-00)
- Open Standards need management
  - Interfaces of Standards have to be kept working
  - p≡p can be an Open Standard itself (and should be)
- We need guidance where in the IETF this will fit?

Questions? BarBoF!

- Bar**BoF** in Room Tyrolka (Mezzanine floor), today 19:30, including:
  - Demo of running code
  - Q & A
  - Discussion
- … likely to be followed up in a **Bar** close-by ;-)