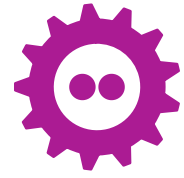
FOSDEM 2019



Vincent Breitmoser

Intro

- I'm Vincent
- Developer of OpenKeychain
- OpenPGP support in K-9 Mail
- More holistic approach required

Overview - Goals

1. Make it easy to encrypt e-mail
2. Don't rely on infrastructure
3. Minimize implementation complexity
4. Work on multiple devices

More importantly: Non-Goals

1. Disregard active attackers (for now)
2. Stick to a simple trust model
3. Don't impose encryption by default

UX: Writing Mail

From: Alice <alice@example.org>
To: Bob <bob@example.net>
Subject: Followup from Thursday's Meeting

☐ Encrypt this message

I think Susan was mistaken

Overview - Governance

1. This is a community effort!
2. Workflow via Github PRs
3. Where possible, sprints in meetings
4. Spec and implementation side-by-side

The Autocrypt Header


```
Autocrypt: addr=alice@gmail.com; keydata=BASE64
```

- Simple attribute-based format
- Typically ~2KiB in size
  - For an RSA3072+RSA3072 key
  - Currently moving to Ed25519+Cv25519
- Optional and critical attributes
  - basic forward and backward compatibility

Recommendation Algorithm

- "Unavailable"
- "Available"
- "Discouraged"
- "Encrypt"

The Autocrypt-Gossip Header


```
Autocrypt-Gossip: addr=bob@autocrypt.org; keydata=BASE64
```

- Lives in header of encrypted MIME part
- Contains keys of all Cc'ed recipients
  - This ensures "reply to all" works
- Direct Autocrypt headers take priority!

Current status

- It works
- Autocrypt headers coming up "in the wild"

Support released in:

- Enigmail
- K-9 Mail
- delta.chat

https://autocrypt.org

autocrypt@lists.mayfirst.org

#autocrypt on irc.freenode.net

Autocrypt Setup Message

- Transfer secret key as self-sent message via user's own inbox
- Symmetric encryption with strong setup code

```
Please enter the Setup Code displayed by
   your other e-mail app to proceed:

          17__ - ____ - ____ -
          ____ - ____ - ____ -
          ____ - ____ - ____

    [   Cancel   ]     [ Import Settings ]
```

The Future

Beyond "Level 1"

- Verification
- Better multi-device