# OpenKeychain UX Decisions

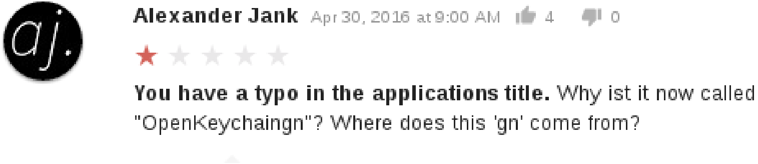
OpenPGP.conf, Cologne

Vincent Breitmoser, Dominik Schürmann

2016-09-09

# OpenKeychain

- OpenPGP implementation for Android
- Uses Bouncy Castle for OpenPGP



**Alexander Jank** Apr 30, 2016 at 9:00 AM 👍 4 👎 0

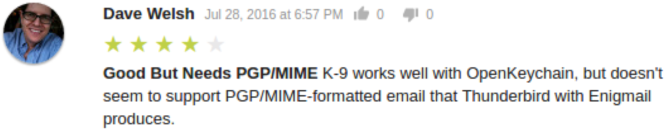
★☆☆☆☆

**You have a typo in the applications title.** Why ist it now called "OpenKeychaingn"? Where does this 'gn' come from?

# K-9 Mail

- E-Mail Client for Android

# K-9 Mail



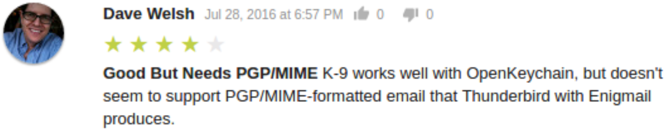
**Dave Welsh** Jul 28, 2016 at 6:57 PM 👍 0 👎 0

★★★★☆

**Good But Needs PGP/MIME** K-9 works well with OpenKeychain, but doesn't seem to support PGP/MIME-formatted email that Thunderbird with Enigmail produces.

- E-Mail Client for Android

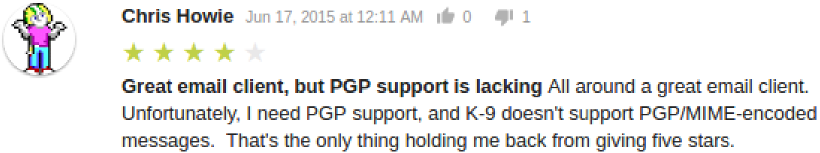
# K-9 Mail



**Dave Welsh** Jul 28, 2016 at 6:57 PM 👍 0 👎 0

★★★★☆

**Good But Needs PGP/MIME** K-9 works well with OpenKeychain, but doesn't seem to support PGP/MIME-formatted email that Thunderbird with Enigmail produces.

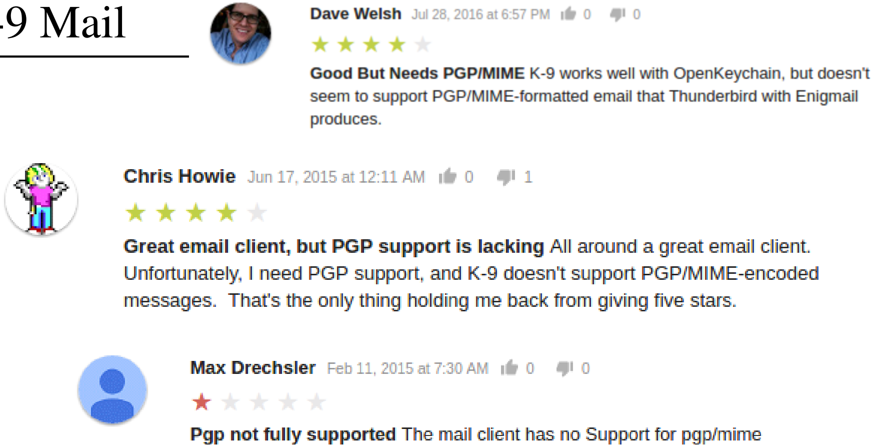


**Chris Howie** Jun 17, 2015 at 12:11 AM 👍 0 👎 1

★★★★☆

**Great email client, but PGP support is lacking** All around a great email client. Unfortunately, I need PGP support, and K-9 doesn't support PGP/MIME-encoded messages.  That's the only thing holding me back from giving five stars.

# K-9 Mail



**Dave Welsh** Jul 28, 2016 at 6:57 PM 👍 0 👎 0

★★★★☆

**Good But Needs PGP/MIME** K-9 works well with OpenKeychain, but doesn't seem to support PGP/MIME-formatted email that Thunderbird with Enigmail produces.

**Chris Howie** Jun 17, 2015 at 12:11 AM 👍 0 👎 1

★★★★☆

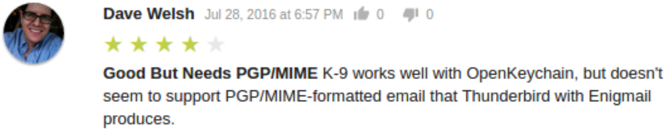
**Great email client, but PGP support is lacking** All around a great email client. Unfortunately, I need PGP support, and K-9 doesn't support PGP/MIME-encoded messages.  That's the only thing holding me back from giving five stars.

**Max Drechsler** Feb 11, 2015 at 7:30 AM 👍 0 👎 0

★☆☆☆☆

**Pgp not fully supported** The mail client has no Support for pgp/mime

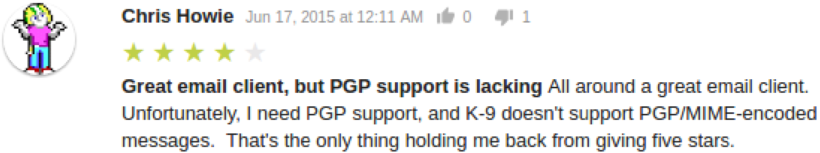
# K-9 Mail



**Dave Welsh** Jul 28, 2016 at 6:57 PM 👍 0 👎 0

★★★★☆

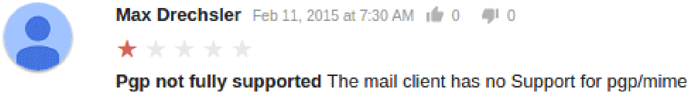
**Good But Needs PGP/MIME** K-9 works well with OpenKeychain, but doesn't seem to support PGP/MIME-formatted email that Thunderbird with Enigmail produces.



**Chris Howie** Jun 17, 2015 at 12:11 AM 👍 0 👎 1

★★★★☆

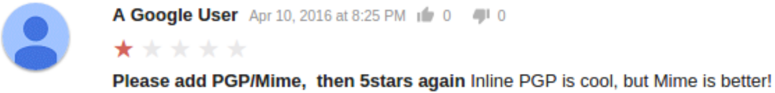
**Great email client, but PGP support is lacking** All around a great email client. Unfortunately, I need PGP support, and K-9 doesn't support PGP/MIME-encoded messages. That's the only thing holding me back from giving five stars.



**Max Drechsler** Feb 11, 2015 at 7:30 AM 👍 0 👎 0

★☆☆☆☆

**Pgp not fully supported** The mail client has no Support for pgp/mime



**A Google User** Apr 10, 2016 at 8:25 PM 👍 0 👎 0

★☆☆☆☆

**Please add PGP/Mime, then 5stars again** Inline PGP is cool, but Mime is better!

# K-9 Mail

- E-Mail Client for Android
- First party OpenPGP support coming up!
  - Beta available in PlayStore: https://openkeychain.org/k9testing.html

# K-9 Mail

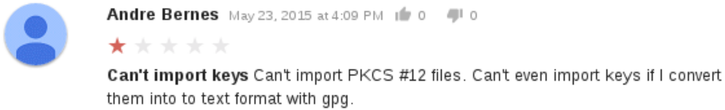
- E-Mail Client for Android
- First party OpenPGP support coming up!
  - Beta available in PlayStore: https://openkeychain.org/k9testing.html
- Unfortunately, rather outdated UI (help wanted!)

# This talk

We're here to talk about

- Some of our UX decisions
- More importantly, our UX decision and thought process

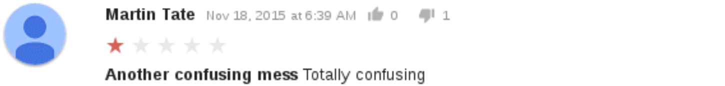
# Figure out Workflows



**Andre Bernes** May 23, 2015 at 4:09 PM 👍 0 👎 0

★☆☆☆☆

**Can't import keys** Can't import PKCS #12 files. Can't even import keys if I convert them into to text format with gpg.



**Martin Tate** Nov 18, 2015 at 6:39 AM 👍 0 👎 1

★☆☆☆☆

**Another confusing mess** Totally confusing

# Figure out Workflows

## Workflows

- Discover/exchange keys
- Confirm keys (“key signing”)
- Add/remove identities
- Send encrypted email

# Figure out Workflows

## Workflows for Key Manager

- Discover/exchange keys
- Confirm keys (“key signing”)
- Add/remove identities
- ~~Send encrypted email~~

# Figure out Workflows

## Workflows for Key Manager

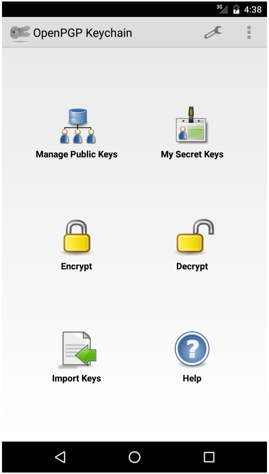
- Discover/exchange keys
- Confirm keys (“key signing”)
- Add/remove identities
- ~~Send encrypted email~~

## Examples

OpenKeychain 2.1, 09/2013 (first git tag)
vs.
OpenKeychain 4.1

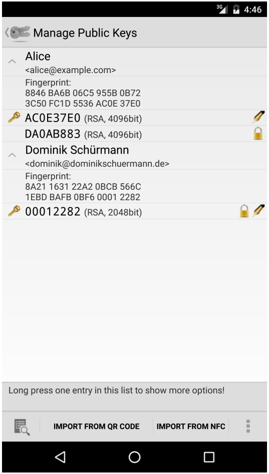
# Key List

- First screen
- Dashboard pattern



# Key List

- Expandable list (cf. Enigmail)
- Cluttered
- Why do people open the list?



Manage Public Keys

Alice
<alice@example.com>
Fingerprint:
8846 BA6B 06C5 955B 0B72
3C50 FC1D 5536 AC0E 37E0
AC0E37E0 (RSA, 4096bit)
DA0AB883 (RSA, 4096bit)

Dominik Schürmann
<dominik@dominikschuermann.de>
Fingerprint:
8A21 1631 22A2 0BCB 566C
1EBD BAFB 0BF6 0001 2282
00012282 (RSA, 2048bit)

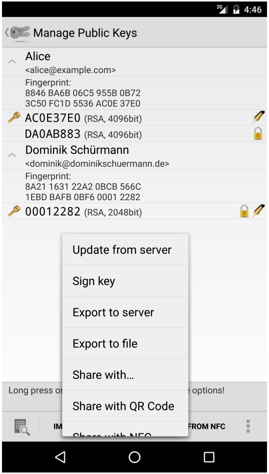
Long press one entry in this list to show more options!

# Key List

- Expandable list (cf. Enigmail)
- Cluttered
- Why do people open the list?

## Identified Workflows in List

- Exchange your key
- Add a new keys



4:46

Manage Public Keys

Alice
<alice@example.com>
Fingerprint:
8846 BA6B 06C5 955B 0B72
3C50 FC1D 5536 AC0E 37E0

AC0E37E0 (RSA, 4096bit)

DA0AB883 (RSA, 4096bit)

Dominik Schürmann
<dominik@dominikschuermann.de>
Fingerprint:
8A21 1631 22A2 0BCB 566C
1EBD BAFB 0BF6 0001 2282

00012282 (RSA, 2048bit)

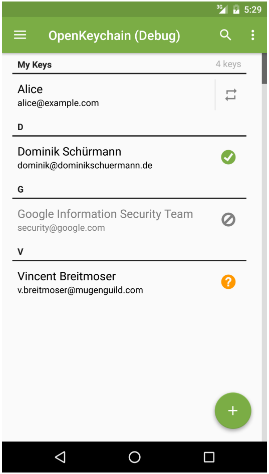
Long press o ... options!

# Key List

- First screen
- Names and confirmation status
- Secret keys on top

## Identified Workflows in List

- Exchange your key
- Add a new keys



5:29

OpenKeychain (Debug)

My Keys 4 keys

Alice
alice@example.com

D

Dominik Schürmann
dominik@dominikschuermann.de

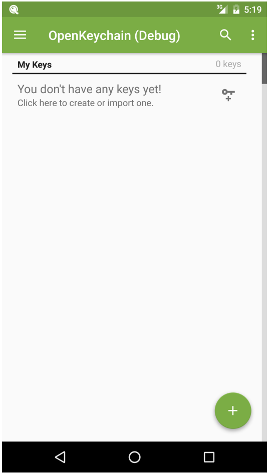
G

Google Information Security Team
security@google.com

V

Vincent Breitmoser
v.breitmoser@mugenguild.com

# Key List



5:19

OpenKeychain (Debug)

My Keys

0 keys

You don't have any keys yet!

Click here to create or import one.

+

## Special Workflow: No Secret Key

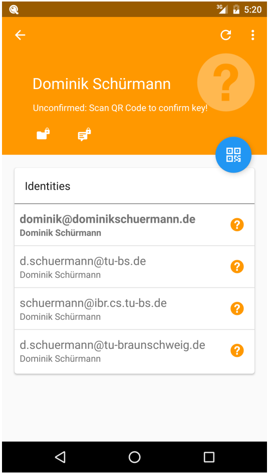
- Weird status
- “I imported my key but cannot decrypt!”

⇒ Encourage import

# Key View

## Identified Workflows for Public Keys

- Confirm key (“key signing”)
- Check verification status
- Encrypt text/file to key
- Manual refresh from keyservers



**dominik@dominikschuermann.de**
**Dominik Schürmann**

d.schuermann@tu-bs.de
Dominik Schürmann

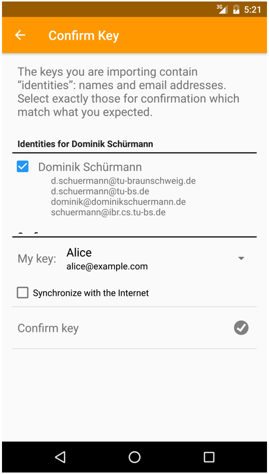
schuermann@ibr.cs.tu-bs.de
Dominik Schürmann

d.schuermann@tu-braunschweig.de
Dominik Schürmann

# Key View

## Identified Workflows for Public Keys

- Confirm key (“key signing”)
- Check verification status
- Encrypt text/file to key
- Manual refresh from keyservers



Confirm Key

The keys you are importing contain “identities”: names and email addresses. Select exactly those for confirmation which match what you expected.

**Identities for Dominik Schürmann**

☑ Dominik Schürmann
d.schuermann@tu-braunschweig.de
d.schuermann@tu-bs.de
dominik@dominikschuermann.de
schuermann@ibr.cs.tu-bs.de

My key: Alice
alice@example.com

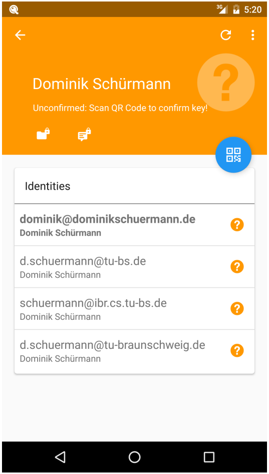
□ Synchronize with the Internet

Confirm key ✓

# Key View

## Identified Workflows for Public Keys

- Confirm key (“key signing”)
- Check verification status
- Encrypt text/file to key
- Manual refresh from keyservers



**dominik@dominikschuermann.de**
**Dominik Schürmann**

d.schuermann@tu-bs.de
Dominik Schürmann

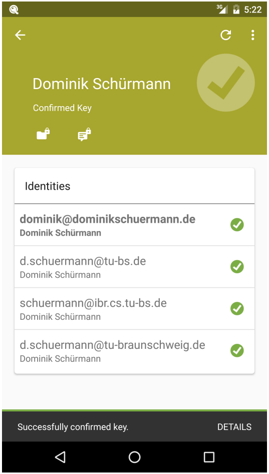
schuermann@ibr.cs.tu-bs.de
Dominik Schürmann

d.schuermann@tu-braunschweig.de
Dominik Schürmann

# Key View

## Identified Workflows for Public Keys

- Confirm key (“key signing”)
- Check verification status
- Encrypt text/file to key
- Manual refresh from keyservers



5:22

Dominik Schürmann

Confirmed Key

Identities

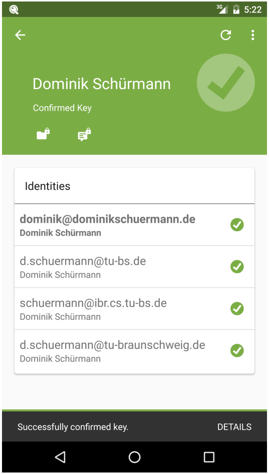
| | |
|---|---|
| **dominik@dominikschuermann.de**<br>**Dominik Schürmann** | ✓ |
| d.schuermann@tu-bs.de<br>Dominik Schürmann | ✓ |
| schuermann@ibr.cs.tu-bs.de<br>Dominik Schürmann | ✓ |
| d.schuermann@tu-braunschweig.de<br>Dominik Schürmann | ✓ |

Successfully confirmed key.

# Key View

## Identified Workflows for Public Keys

- Confirm key (“key signing”)
- Check verification status
- Encrypt text/file to key
- Manual refresh from keyservers



5:22

Dominik Schürmann

Confirmed Key

Identities

**dominik@dominikschuermann.de**
**Dominik Schürmann**

d.schuermann@tu-bs.de
Dominik Schürmann

schuermann@ibr.cs.tu-bs.de
Dominik Schürmann

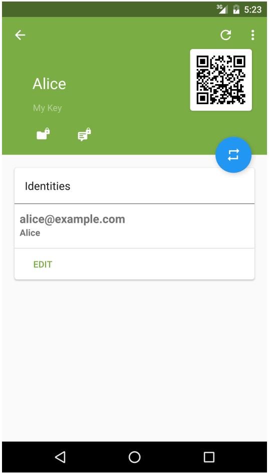
d.schuermann@tu-braunschweig.de
Dominik Schürmann

Successfully confirmed key. DETAILS

# Key View

## Identified Workflows for Secret Keys

- Show confirmation QR Code
- Exchange key
- Add/remove identities



Identities

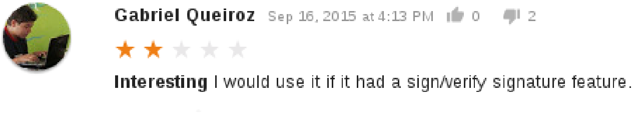
alice@example.com
Alice

# Interim Conclusion

## Advice for developers

- Do shoulder surfing and ask users
- Identify encouraged workflows
- Context aware workflows
- Make them accessible from the focus area

# Figure out Non-Workflows



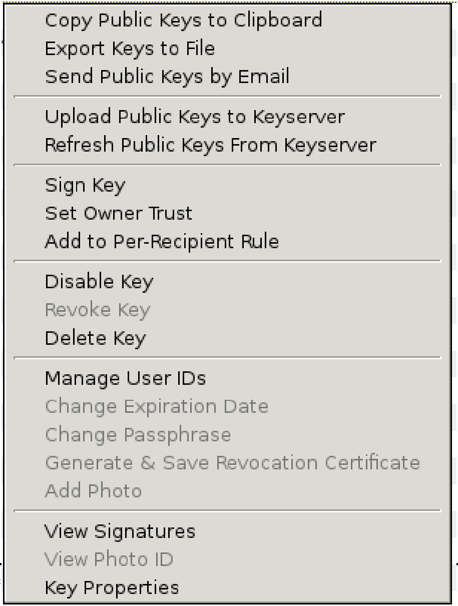
**Gabriel Queiroz** Sep 16, 2015 at 4:13 PM 👍 0 👎 2

★★☆☆☆

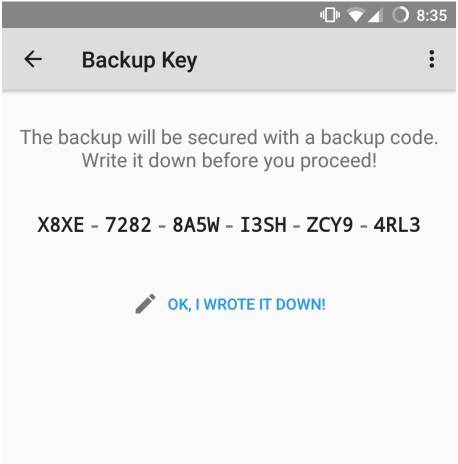
**Interesting** I would use it if it had a sign/verify signature feature.

# Figure out Non-Workflows

- Stay focused
- Get rid of distractions


Copy Public Keys to Clipboard
Export Keys to File
Send Public Keys by Email
Upload Public Keys to Keyserver
Refresh Public Keys From Keyserver
Sign Key
Set Owner Trust
Add to Per-Recipient Rule
Disable Key
Revoke Key
Delete Key
Manage User IDs
Change Expiration Date
Change Passphrase
Generate & Save Revocation Certificate
Add Photo
View Signatures
View Photo ID
Key Properties

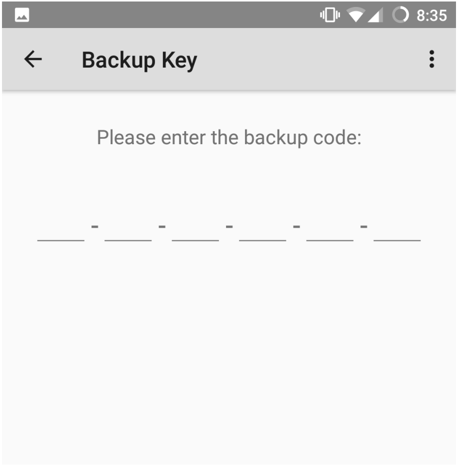
# Figure out Non-Workflows



The backup will be secured with a backup code. Write it down before you proceed!

X8XE - 7282 - 8A5W - I3SH - ZCY9 - 4RL3

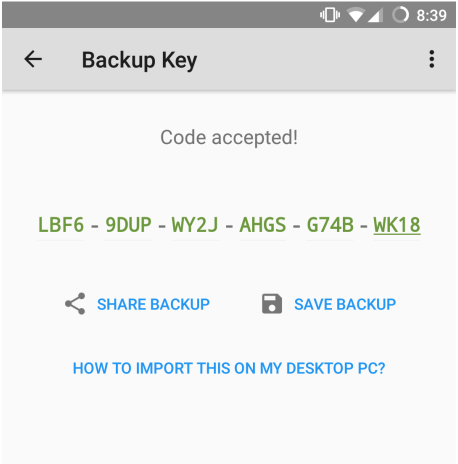
# Figure out Non-Workflows



Please enter the backup code:

____ - ____ - ____ - ____ - ____ - ____

# Figure out Non-Workflows



Backup Key

Code accepted!

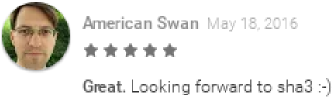
LBF6 - 9DUP - WY2J - AHGS - G74B - WK18

# Figure out Non-Workflows

- Not supported: custom backup code
- Not supported: unencrypted export

# Caveat: Expert Freedom

- But there are expert users, who don’t like to be patronized...
  - Let the user roll their own dice!



American Swan May 18, 2016

★★★★★

**Great.** Looking forward to sha3 :-)

# Caveat: Expert Freedom

# Caveat: Expert Freedom

1. Users are not crypto experts - you are!
   - If users are generating 16k RSA keys, that’s on us!

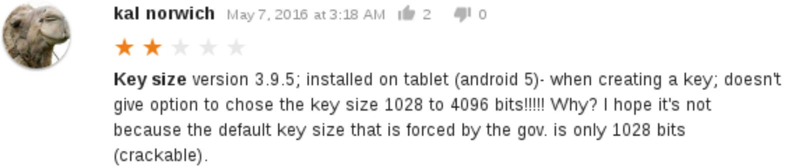
# Caveat: Expert Freedom

1. Users are not crypto experts - you are!
2. Expert settings introduce complexity to the ecosystem
   - If users are putting comments on their user ids, that's on us!

# Caveat: Expert Freedom

1. Users are not crypto experts - you are!
2. Expert settings introduce complexity to the ecosystem
3. Expert settings lead to expert culture
   - If users get yelled at by “experts” for not creating detached revocation certificates, that’s on us!

# Hide Complexity



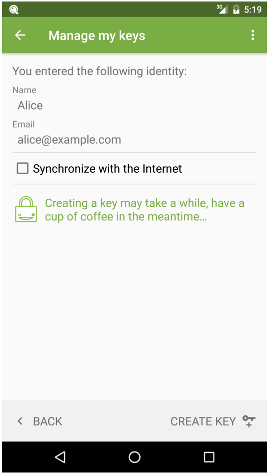
**kal norwich** May 7, 2016 at 3:18 AM 👍 2 👎 0

★★☆☆☆

**Key size** version 3.9.5; installed on tablet (android 5)- when creating a key; doesn't give option to chose the key size 1028 to 4096 bits!!!!! Why? I hope it's not because the default key size that is forced by the gov. is only 1028 bits (crackable).

# Advanced Create Key

- By default generates 3072 bit RSA
- Recommended default according to keylength.com



You entered the following identity:

Name
Alice

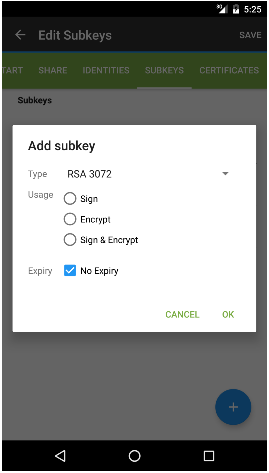
Email
alice@example.com

□ Synchronize with the Internet

Creating a key may take a while, have a cup of coffee in the meantime…

# Advanced Create Key

- Limited set of key configurations
- Gives clear guidance to user
- ECC supported, but not yet encouraged
- Not supported: ElGamal, DSA, custom RSA key sizes



Add subkey

Type RSA 3072

Usage ○ Sign
○ Encrypt
○ Sign & Encrypt

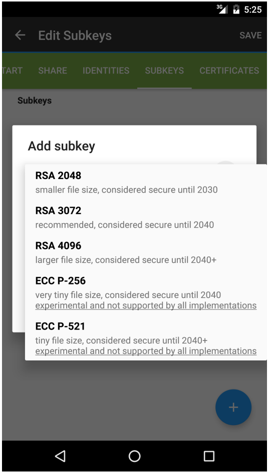
Expiry ☑ No Expiry

## Supported Workflows

- Authentication subkey
- ECC subkey
- Subkey with special expiry
- …

# Advanced Create Key

- Limited set of key configurations
- Gives clear guidance to user
- ECC supported, but not yet encouraged
- Not supported: ElGamal, DSA, custom RSA key sizes



Add subkey

**RSA 2048**
smaller file size, considered secure until 2030

**RSA 3072**
recommended, considered secure until 2040

**RSA 4096**
larger file size, considered secure until 2040+

**ECC P-256**
very tiny file size, considered secure until 2040
experimental and not supported by all implementations

**ECC P-521**
tiny file size, considered secure until 2040+
experimental and not supported by all implementations

## Supported Workflows

- Authentication subkey
- ECC subkey
- Subkey with special expiry
- …

# Summary: Takeaways

1. Figure out your user's workflows

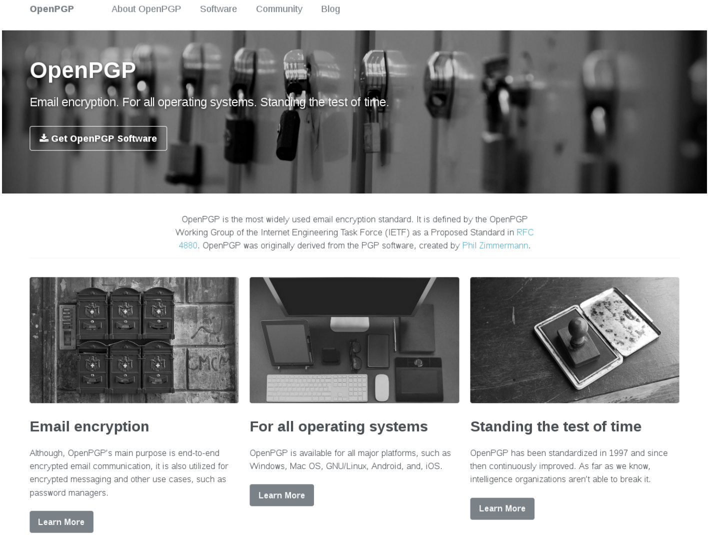
# Summary: Takeaways

1. Figure out your user’s workflows
2. Categorize each workflow
   - Is it "Encouraged", "Supported" or "Not Supported"?

# Summary: Takeaways

1. Figure out your user's workflows
2. Categorize each workflow
   - Is it "Encouraged", "Supported" or "Not Supported"?
3. Act on it!
   - Encouraged: Optimize for it
   - Supported: Display secondarily
   - Not supported: Remove it

# Jealous of xmpp.org? ⇒ Resurrect openpgp.org to promote the standard!



## OpenPGP

Email encryption. For all operating systems. Standing the test of time.

OpenPGP is the most widely used email encryption standard. It is defined by the OpenPGP Working Group of the Internet Engineering Task Force (IETF) as a Proposed Standard in RFC 4880. OpenPGP was originally derived from the PGP software, created by Phil Zimmermann.

### Email encryption

Although, OpenPGP's main purpose is end-to-end encrypted email communication, it is also utilized for encrypted messaging and other use cases, such as password managers.

### For all operating systems

OpenPGP is available for all major platforms, such as Windows, Mac OS, GNU/Linux, Android, and, iOS.

### Standing the test of time

OpenPGP has been standardized in 1997 and since then continuously improved. As far as we know, intelligence organizations aren't able to break it.

# Backup: OpenPGP's Terminology

| Traditional phrase | Replacement | Comment |
|---|---|---|
| User ID | Identity | |
| Key ID | - | They serve no purpose |
| Passphrase | Password | People know passwords |
| Public/Secret Key | Key | Don't try to explain public key cryptography |
| Sign/Certify Key | Confirm Key | Makes no sense without public key crypto |
| Cache Password | Remember Password | Cache is technical language |
| Smartcard | Security Token | Smartcard does not fit for YubiKeys |