IRMAseal

Identity based encryption of email


nlnet
FOUNDATION

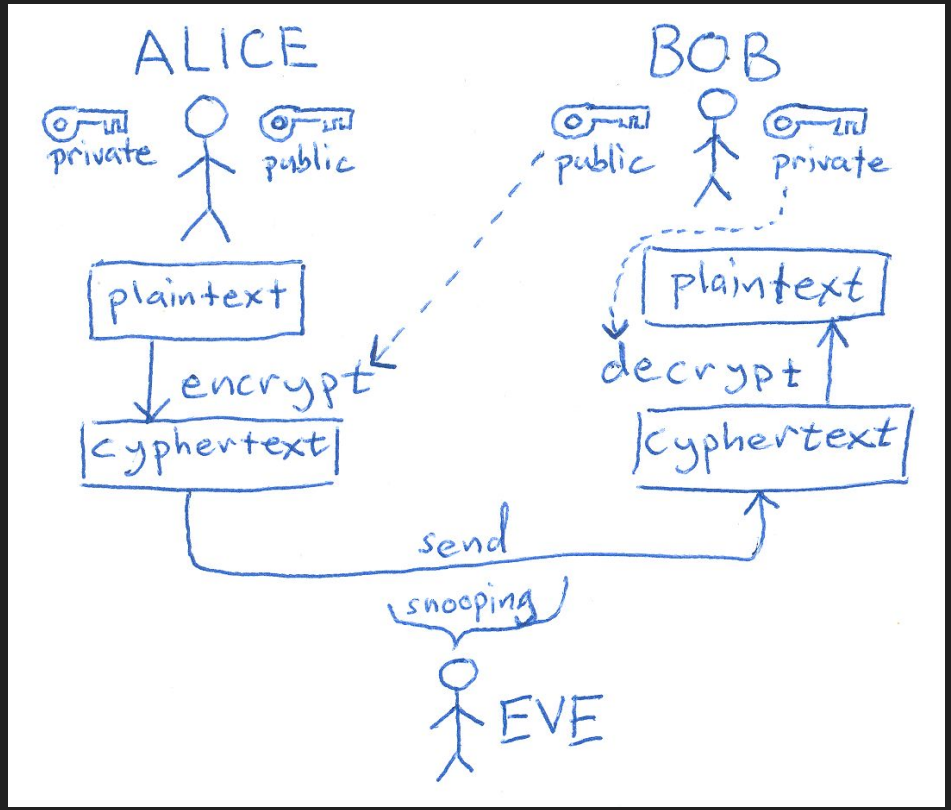

NGI
ZERO

Do not trust e-mail

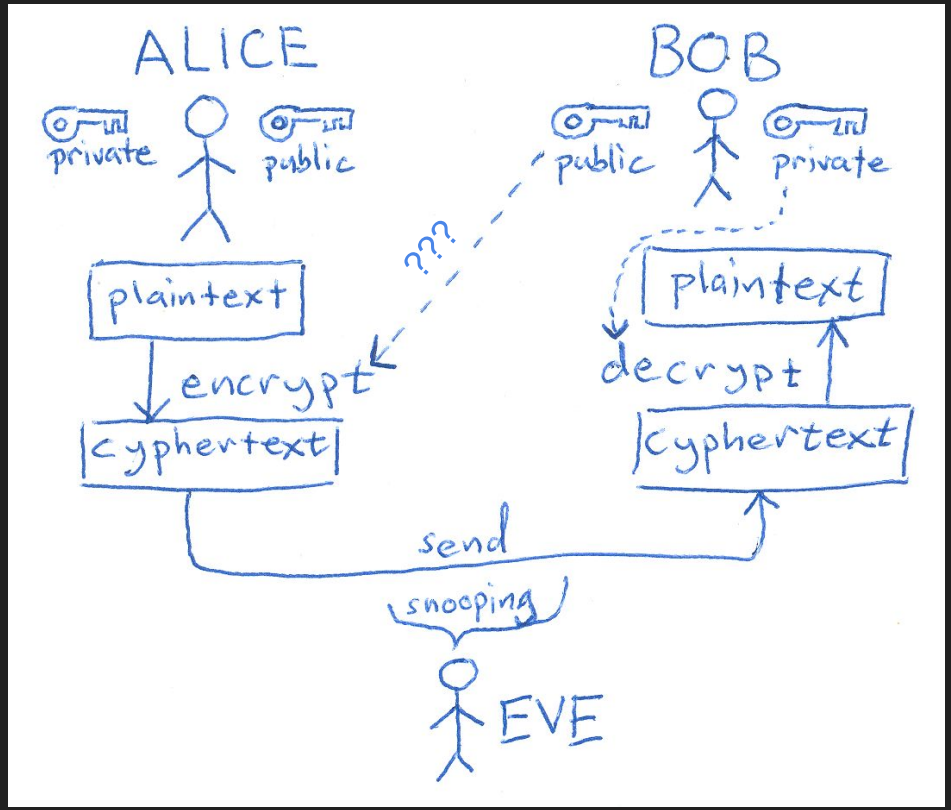
E-mail is not confidential or authenticated.

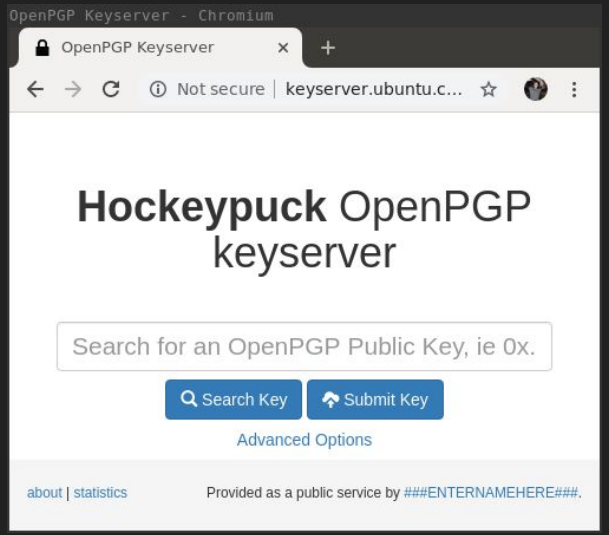
Security.nl 2017: “E-mail Tweede Kamer was kwetsbaar voor spoofing”

Basics: encrypting email



Basics: keysharing





Enigmail

Misconception: end-to-end encryption

We do not have an initial bi-directional communication channel.

What is IRMAseal?

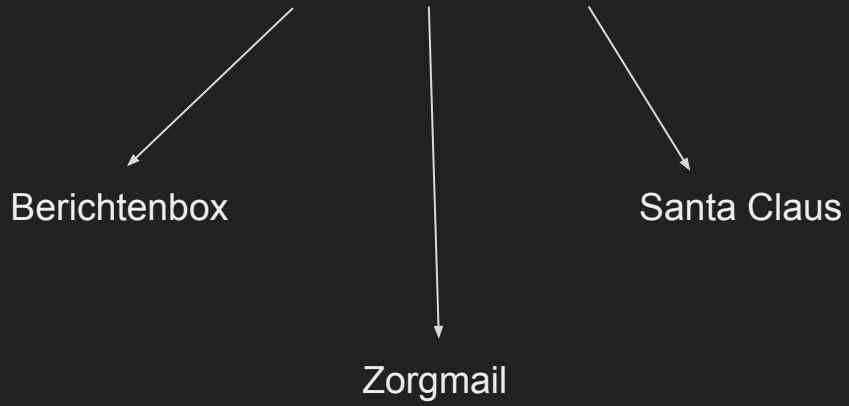
1. Proof of concept
2. Uses Identity based encryption
3. For encrypting e-mail
4. Uses IRMA

What can you do with IRMAseal?

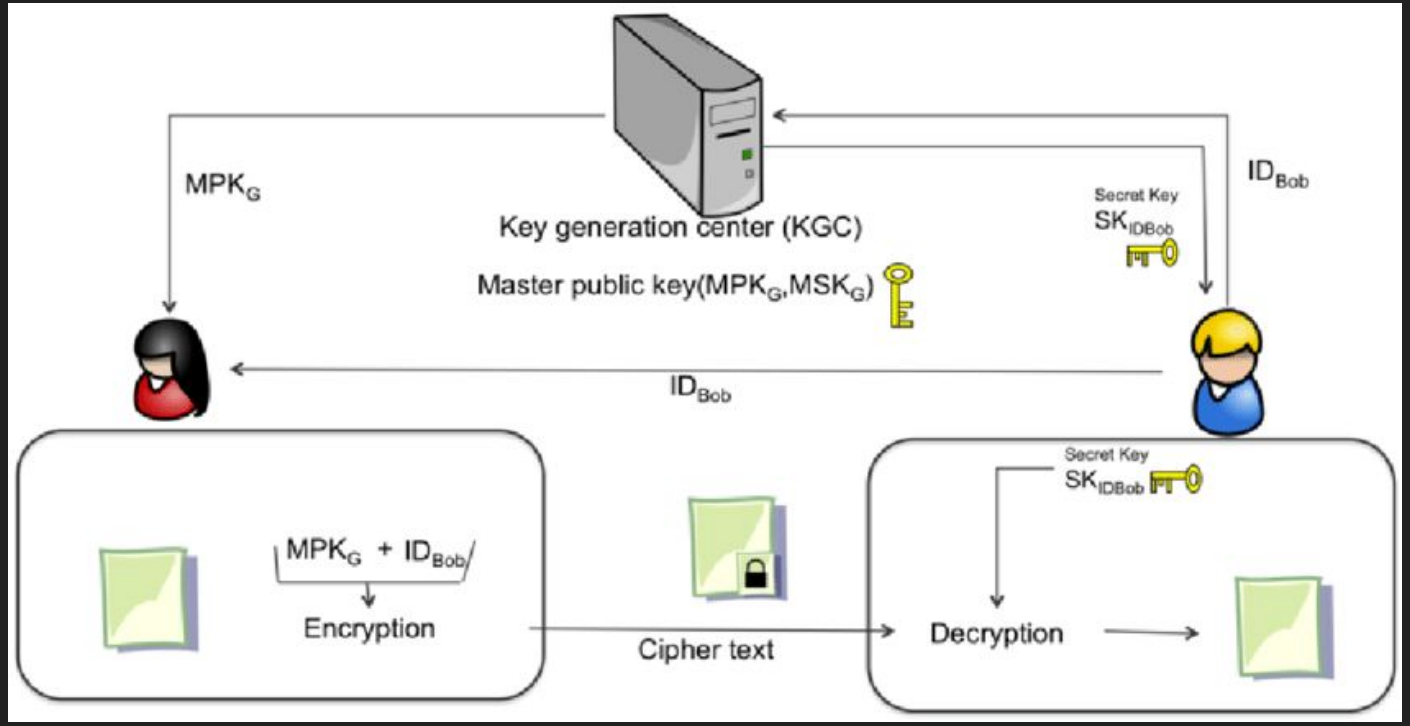
Encrypt an e-mail or file for an {address, BSN, BIG, over 18, name, company}.

What can you do with IRMAseal?

Encrypt an e-mail or file for an {address, BSN, BIG, over 18, name, company}.



Identity based encryption



Properties of IRMAseal

1. Has a root of trust
2. Key distribution does not violate privacy
3. No prior key requirement
4. Identities can be any set of IRMA attributes

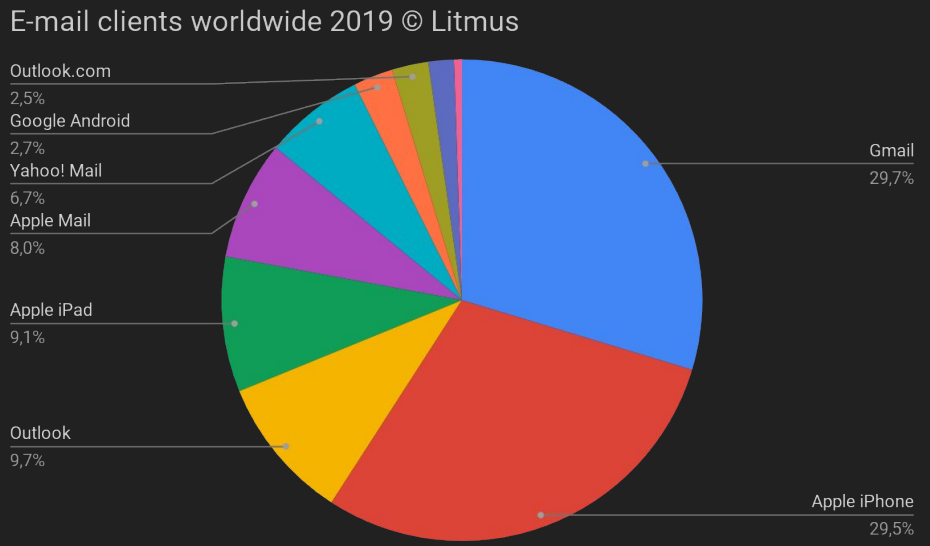
Scope of IRMAseal

1. General libraries
2. Public Key Generator (PKG) daemon
3. Command line application
4. Thunderbird plugin
5. *(optional) Browser plugin (WebExtension) for web e-mail clients*
    a. *GMail*
    b. *Outlook 365*
    c. *Protonmail*

Demo

Challenges: e-mail clients

1. Most people use GMail.
2. Thunderbird is declining.
3. Outlook has best extensions.
4. MailExtensions (WebAssembly!)
5. E-mail is a horrific standard.



Challenges: some attributes are better than others

E-mail is a pretty bad IRMA attribute.

Challenges: keeping the private key safe

If your laptop gets stolen, identity is stolen as well.

Challenges: trusting the trusted third party

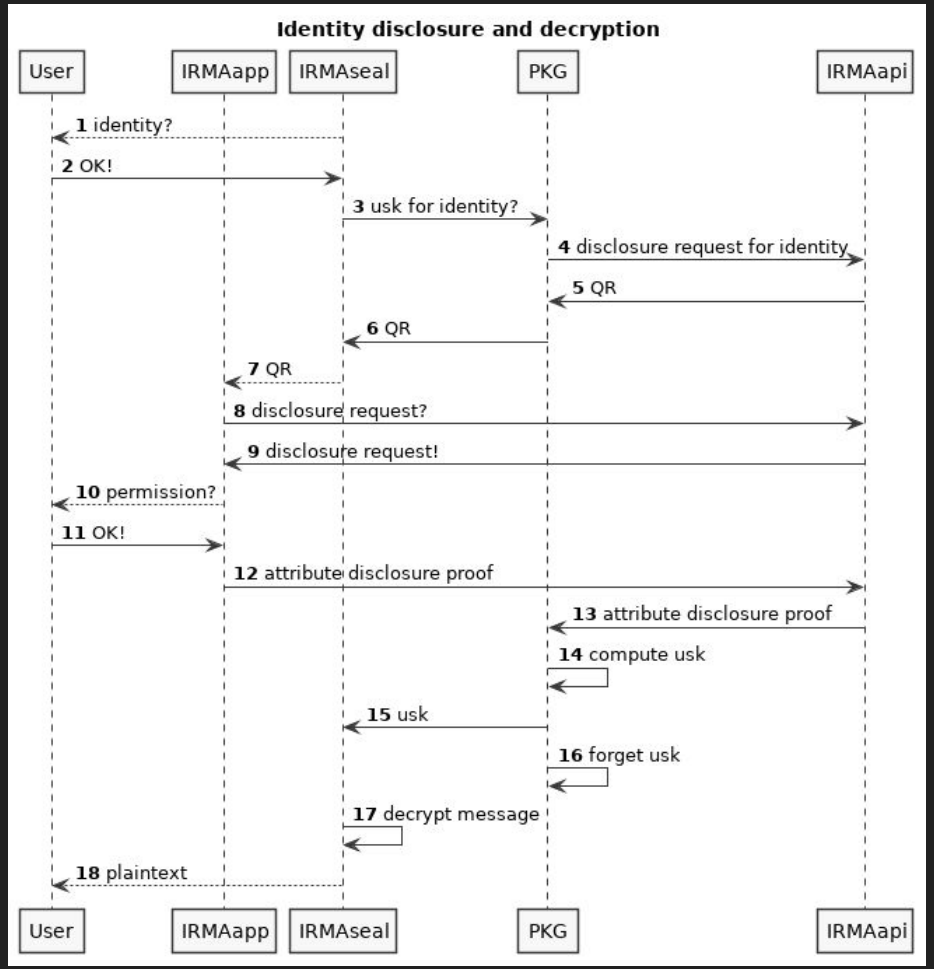
Trust TTP to keep private key available and confidential.

- Hardware modules (Rust!)
- Distributed trusted third parties
  - Tactical choices in TTPs
  - I.e. { BoF, universities, PbdF, ISPs, ... }
- Limited set requirement

Challenges: I want my own trusted third party

Federation over DNS.

Decryption


Identity disclosure and decryption
User
IRMAapp
IRMAseal
PKG
IRMAapi
1 identity?
2 OK!
3 usk for identity?
4 disclosure request for identity
5 QR
6 QR
7 QR
8 disclosure request?
9 disclosure request!
10 permission?
11 OK!
12 attribute disclosure proof
13 attribute disclosure proof
14 compute usk
15 usk
16 forget usk
17 decrypt message
18 plaintext
User
IRMAapp
IRMAseal
PKG
IRMAapi