Integrating PostGuard into FileSender

August 24, 2024

Bryan Rinders, s1060340

Supervisors:
Dr. Bram Westerbaan
Prof. Dr. Bart Jacobs

**Institute for Computing
and Information Sciences**
Radboud University

FileSender

- Web application for sharing large (encrypted) files
- Comparable to WeTransfer[1]
- Open source
- Focused on privacy and security
  - End-to-end encryption (E2EE) of files

---

[1] `https://wetransfer.com`

Institute for Computing
and Information Sciences
Radboud University

The Problem

- Distribution of the encryption password to the recipients
- How to do this securely?
  - Authenticate recipients
  - End-to-end encryption
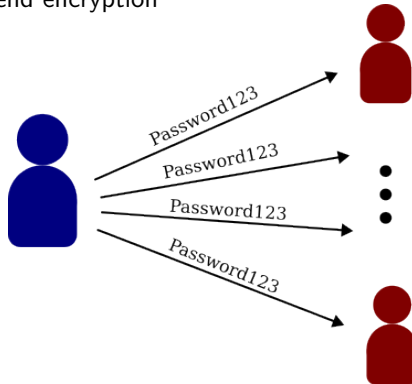
PostGuard

PostGuard is an encryption service that is privacy- and user-friendly.

PostGuard combines:

- Identity-based encryption
- Identity wallet yivi

Institute for Computing and Information Sciences
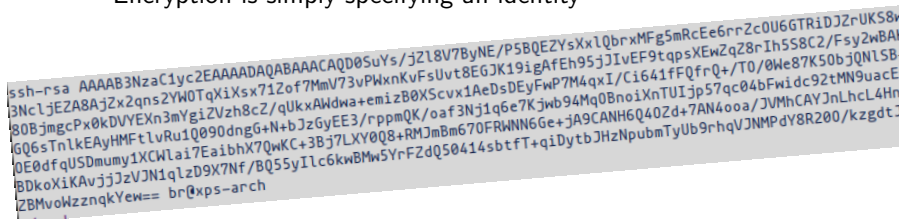Radboud University

Identity-based encryption (1)

- Private Key Generator (PKG) to manage the cryptographic keys
- Based on public key crypto
  - Use identities as public keys (usually something memorable e.g. email address)
  - Encryption is simply specifying an identity

Identity-based encryption (1)

- Private Key Generator (PKG) to manage the cryptographic keys
- Based on public key crypto
  - Use identities as public keys (usually something memorable e.g. email address)
  - Encryption is simply specifying an identity

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQD0SuYs/jZl8V7ByNE/P5BQEZYsXxlQbrxMFg5mRcEe6rr2cOU6GTRiDJZrUKS8W
3NcljEZA8AjZx2qns2YWOTqXiXsx71Zof7MmV73vPWxnKvFsUvt8EGJK19igAfEh95jJIvEF9tqpsXEwZqZ8rIh5S8C2/Fsy2wBAP
80BjmgcPx0kDVYEXn3mYgiZVzh8cZ/qUkxAWdwa+emizB0XScvx1AeDsDEyFwP7M4qxI/Ci641fFQfrQ+/T0/0We87K50bjQNlSBH
GQ6sTnlkEAyHMFtlvRu1Q090dngG+N+bJzGyEE3/rppmQK/oaf3Nj1q6e7Kjwb94MqOBnoiXnTUIjp57qc04bFwidc92tMN9uacEH
0E0dfqUSDmumy1XCWlai7EaibhX7QwKC+3Bj7LXY0Q8+RMJmBm670FRWNN6Ge+jA9CANH6Q4OZd+7AN4ooa/JVMhCAYJnLhcL4Hn
BDkoXiKAvjjJzVJN1qlzD9X7Nf/BQ55yIlc6kwBMw5YrFZdQ50414sbtfT+qiDytbJHzNpubmTyUb9rhqVJNMPdY8R200/kzgdtl
ZBMvoWzznqkYew== br@xps-arch
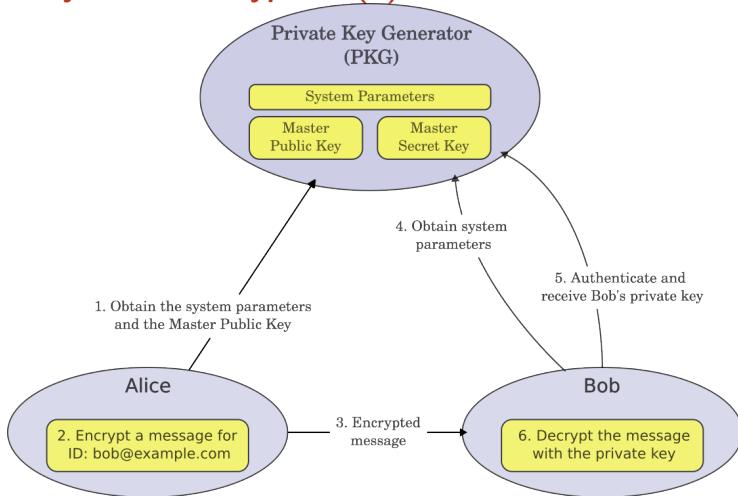
Identity-based encryption (2)

Figure 1: Identity-based encryption session flow, based on [1].

Institute for Computing
and Information Sciences
Radboud University

Yivi (identity wallet) (1)

With Yivi you can safely can
securely share personal data.

- Passwordless authentication

Attributes
- email address
- name
- date of birth
- nationality
- ...

Institute for Computing
and Information Sciences
Radboud University

Yivi (identity wallet) (2)

Decentralized architecture
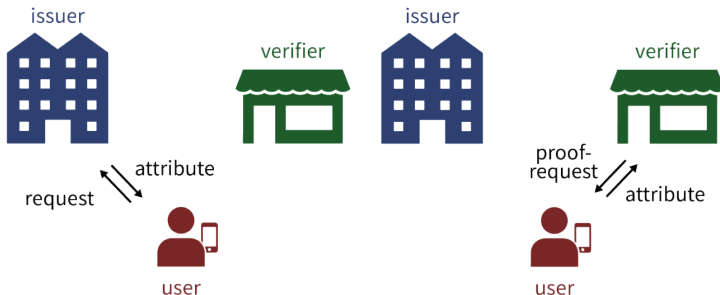
Figure 2: Issuance and sharing of attributes [2].

Institute for Computing
and Information Sciences
Radboud University

Yivi (identity wallet) (3)

Comparison with a centralized architecture (e.g. Google)

Non Yivi
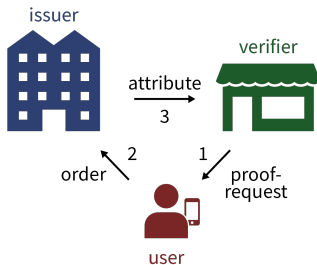
Figure 3: Centralized identity management architecture [3].

Institute for Computing
and Information Sciences
Radboud University

PostGuard

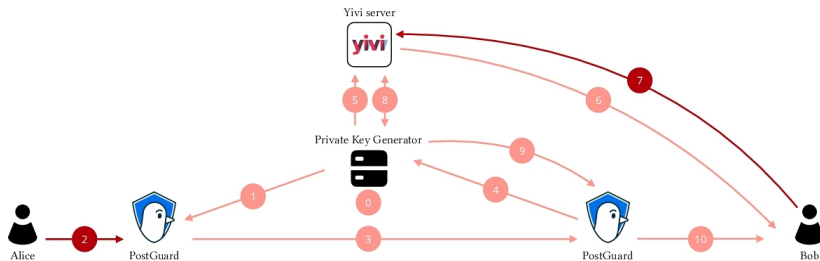Figure 4: PostGuard session flow [4].

- Note: no digital signing
- Simplifies the decryption process to a simple authentication

Institute for Computing
and Information Sciences
Radboud University

Demo

**Institute for Computing
and Information Sciences**
Radboud University

Demo uploading (1)

secret-message.txt : 20 B

drag & drop your files here

Clear all — **4** Select files

Number of files : 1/30
Size : 20 B/20 MB

3 From : alice@example.com

To :

2 bob@example.com

Enter recipient email(s)

Subject (optional) :

Message (optional) :

☑ File Encryption

1 ☑ Enable PostGuard for File Encryption

PostGuard is an encryption service that simplifies the en- and decryption process.

Advanced PostGuard options

Expiry date: 01/09/2024

☑ Notify me when expired
☐ Notify me when upload is done
☑ Notify me upon downloads
☑ Send me a report when expired
☐ Include me as a recipient
☐ Get a link instead of sending to recipients
☐ User must login to FileSender to download file(s)

Advanced settings

5 Send

Demo uploading (2)

Institute for Computing
and Information Sciences
Radboud University

Demo uploading (3)

Institute for Computing
and Information Sciences
Radboud University

Demo downloading (1)

Download

1 PostGuard attribute: `bob@example.com ▾`

Advanced PostGuard options

Click on a file to download the data and decrypt it on your computer.

From : alice@example.com
Created : 22 Aug 2024
Expires : 31 Aug 2024
Size : 20 B

secret-message.txt   20 B   **2** ⬇ PostGuard Download

**Institute for Computing
and Information Sciences**
Radboud University

Demo downloading (2)

Institute for Computing and Information Sciences
Radboud University

Demo downloading (3)

**Institute for Computing
and Information Sciences**
Radboud University

Issues during development

- Encryption
  - Signing?
- Content Security Policy (CSP)
- Webpack (a JavaScript bundler)

Conclusion

File Sender + Post Guard = ❤️

Links

Prototype

- `https://filesender.bryanrinders.xyz`

Source code

- `https://gitlab.com/postguard-filesender/filesender`

**Institute for Computing
and Information Sciences**
Radboud University

Questions?

**Institute for Computing
and Information Sciences**
Radboud University

Bibliography

[1] Y. Sheffer, *File:Identity Based Encryption Steps.png*, May 26, 2009. [Online]. Available: `https://en.wikipedia.org/wiki/File:Identity_Based_Encryption_Steps.png` (visited on 08/04/2024).

[2] Privacy by Design Foundation, *What is IRMA?* Version 0.15.0. [Online]. Available: `https://irma.app/docs/what-is-irma/`.

[3] Privacy by Design Foundation, *Yivi in detail*, [Online]. Available: `https://privacybydesign.foundation/irma-explanation/` (visited on 08/04/2024).

[4] L. Botros, M. Brandon, B. Jacobs, D. Ostkamp, H. Schraffenberger, and M. Venema, "Postguard: Towards easy and secure email communication," in *CHI Extended Abstracts*, ACM, 2023, 232:1–232:6.

**Institute for Computing
and Information Sciences**
Radboud University