

Integrating PostGuard into FileSender

August 25, 2024

Bryan Rinders, s1060340

Supervisors:

Dr. Bram Westerbaan

Prof. Dr. Bart Jacobs





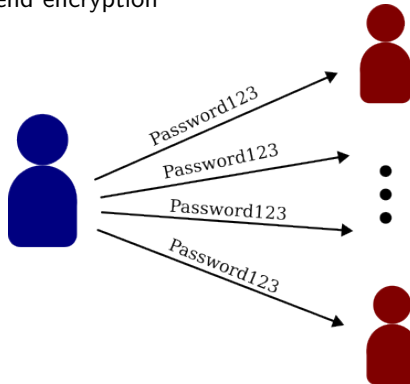
- Web application for sharing large (encrypted) files
- Comparable to WeTransfer¹
- Open source
- Focused on privacy and security
 - End-to-end encryption (E2EE) of files

¹ <https://wetransfer.com>



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**



Identity-based encryption (1)

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



Identity-based encryption (1)

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

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAQD0SuYs/jZl8V7ByNE/P5BQEZYSXxlQbrxMFg5mRcEe6rrZc0U6GTRiDJ2rUKS8v  
3NcljEZA8AjZx2qns2YW0TqXiXs71Zof7MmV73vPWxnKvFsUvt8EGJK19igAfeH95jJIVeF9tqpsXEwZqZ8rIh5S8C2/Fsy2wBA  
80BjmgcPx0kDvYEXn3mYgiZVzh8cZ/qUkxAWdwa+emizB0XScvx1AeDsDEyFwP7M4qxI/Ci641fFQfrQ+/T0/0We87K50bjQNLSB  
GQ6sTnlkEayHMFtlvRu1Q090dngG+N+bJzGyEE3/rppmQK/oaf3Nj1q6e7Kjwb94Mq0BnoiXnTUIjp57qc04bFwidc92tMN9uacE  
QE0dfqUSDmumy1XCWlai7EaibhX7QwKC+3Bj7LXY0Q8+RMJmBm670FRWNN6Ge+jA9CANH6Q40Zd+7AN40oa/JVMhCAYJnLhCL4Hn  
BDkoXiKAvjjJzVJN1qlzD9X7Nf/BQ55yIlc6kwBMw5YrFZdQ50414sbtft+qiDybtbJHzNpubmTyUb9rhqVJNMPdY8R200/kzgdT  
ZBMvoWzznqkYew== br@xps-arch
```



Identity-based encryption (2)

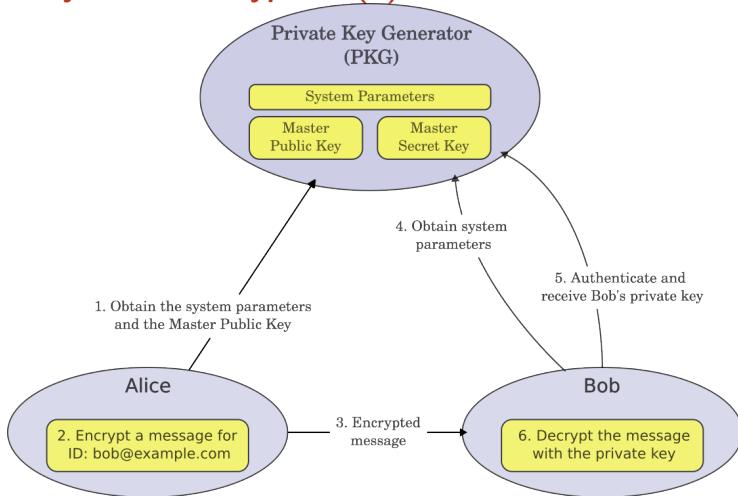


Figure 1: Identity-based encryption session flow, based on [1].

Yivi (identity wallet) (1)

With Yivi you can safely can securely share personal data.

- Passwordless authentication

Attributes

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



Yivi (identity wallet) (2)

Decentralized architecture

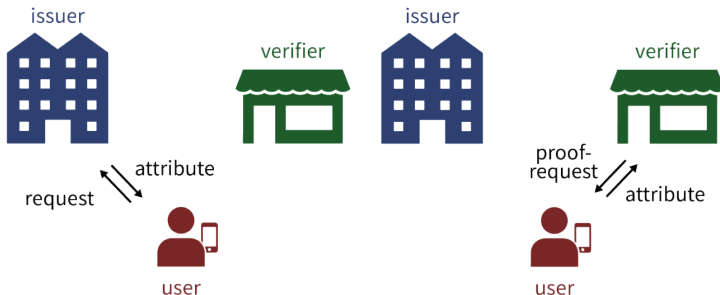


Figure 2: Issuance and sharing of attributes [2].

Yivi (identity wallet) (3)

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

Non Yivi

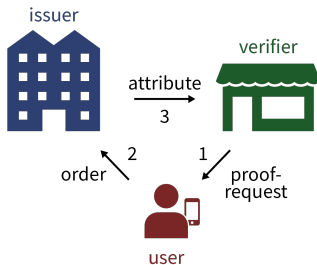


Figure 3: Centralized identity management architecture [3].

PostGuard

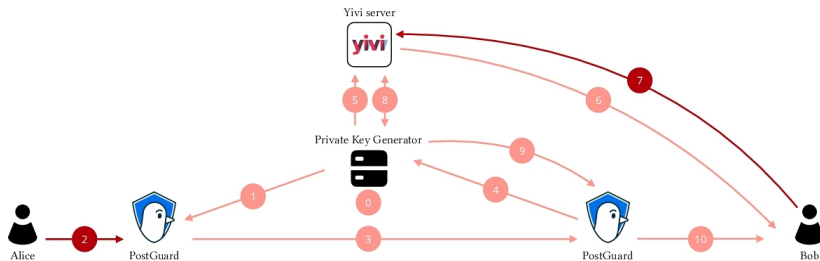


Figure 4: PostGuard session flow [4].

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

Demo

DEMO

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 :

2 To :

Enter recipient email(s)

Subject (optional) :

Message (optional) :

1 ☒ File Encryption

☒ Enable PostGuard for File Encryption

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

[Advanced PostGuard options](#)

Expiry date:

☒ 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](#)

Demo uploading (2)



Demo uploading (3)

vodafone NL 14:54 18%

Share my data



P

postguard-main.cs.ru.nl

Share my data with postguard-
main.cs.ru.nl



Demo Email address

Issued by:
**Demo Privacy by Design
Foundation via SIDN**

Email address
alice@example.com



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



Demo downloading (2)



Demo downloading (3)

signal Vodafone NL 14:54 18%

Share my data



P

postguard-main.cs.ru.nl

Share my data with postguard-main.cs.ru.nl



Demo Email address

Issued by:

Demo Privacy by Design
Foundation via SIDN

Email address

bob@example.com

Share data



Issues during development

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



Conclusion



Links

Prototype

- <https://filesender.bryanrinders.xyz>

Source code

- <https://gitlab.com/postguard-filesender/filesender>



Questions?



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.

