Integrating PostGuard into FileSender

August 25, 2024

Bryan Rinders, s1060340

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

Institute for Computing and Information Sciences
Radboud University

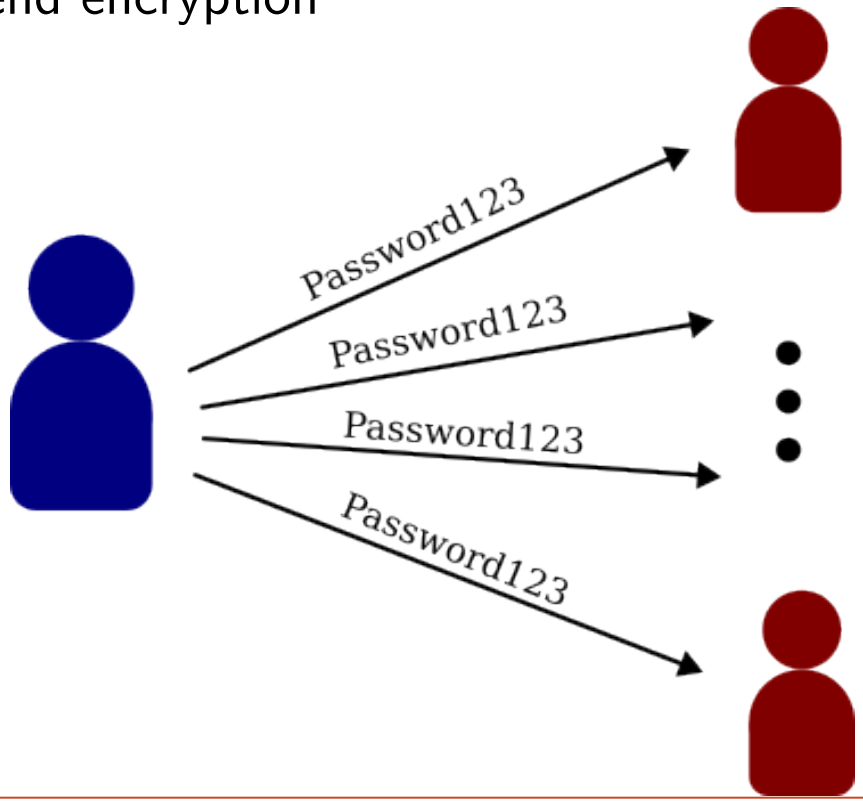
FileSender

- 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`

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)

Institute for Computing
and Information Sciences
Radboud University

Identity-based encryption (2)

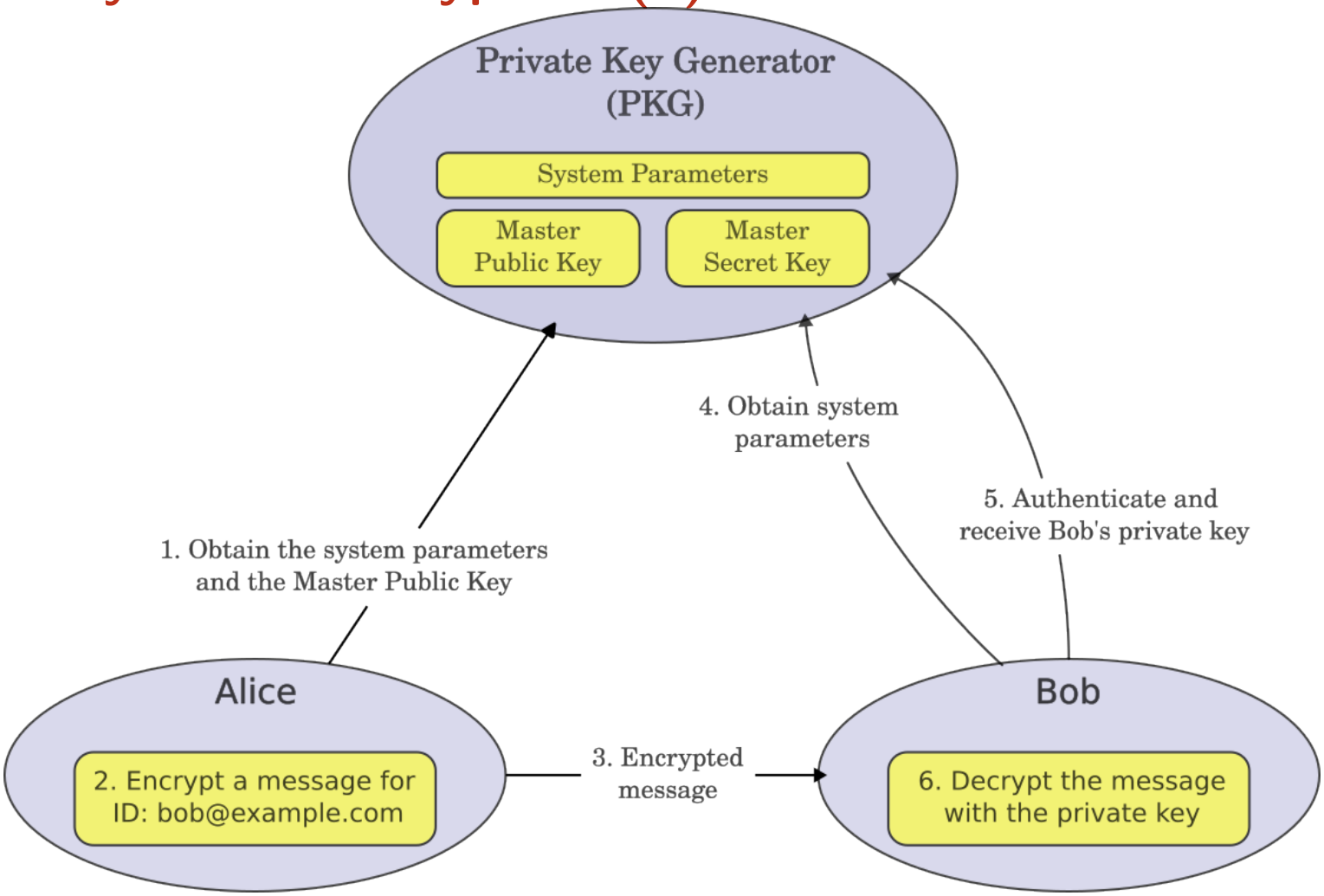


Figure 1: Identity-based encryption session flow, based on [1].

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

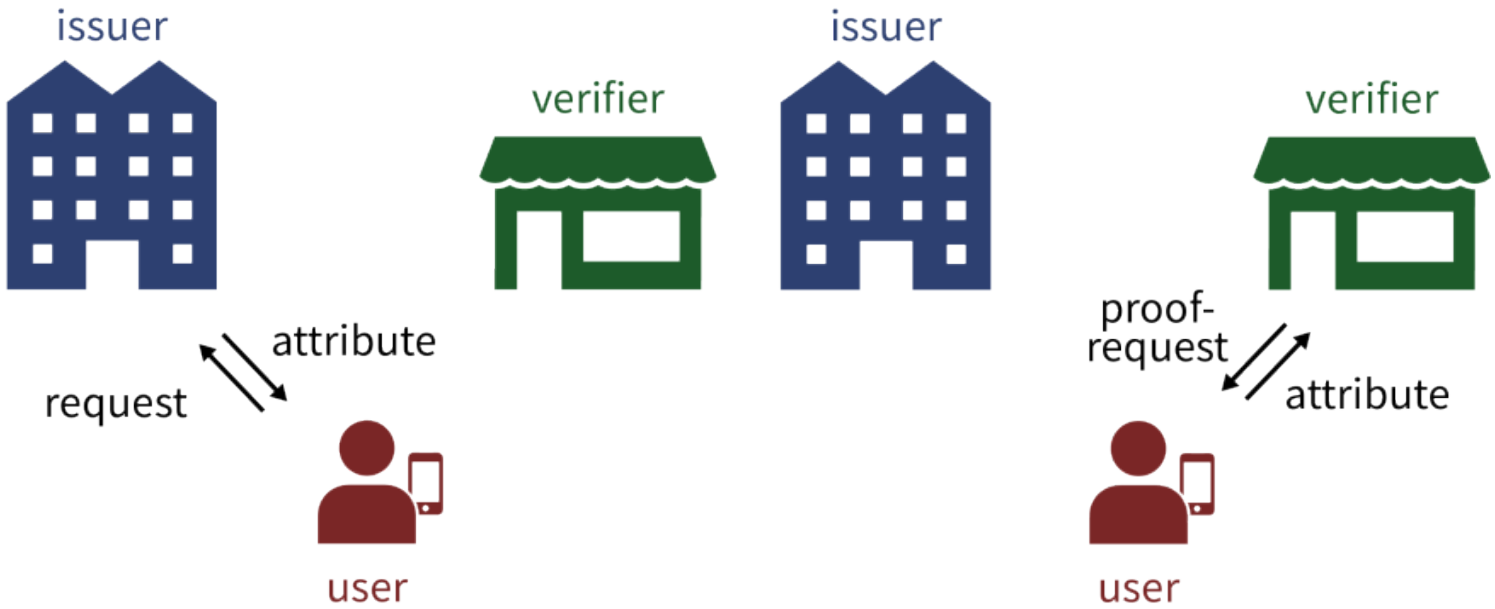


Figure 2: Issuance and sharing of attributes [2].

Institute for Computing
and Information Sciences
Radboud University

Yivi (identity wallet) (3)

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

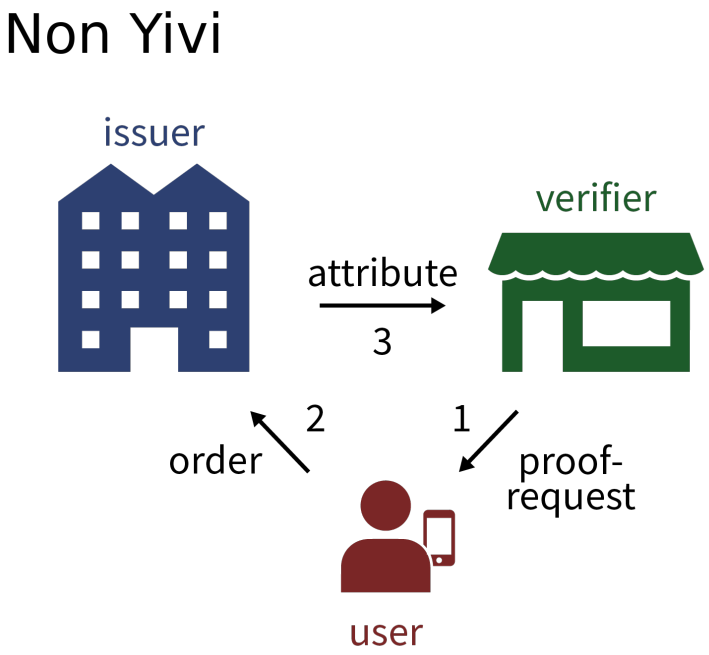


Figure 3: Centralized identity management architecture [3].

PostGuard

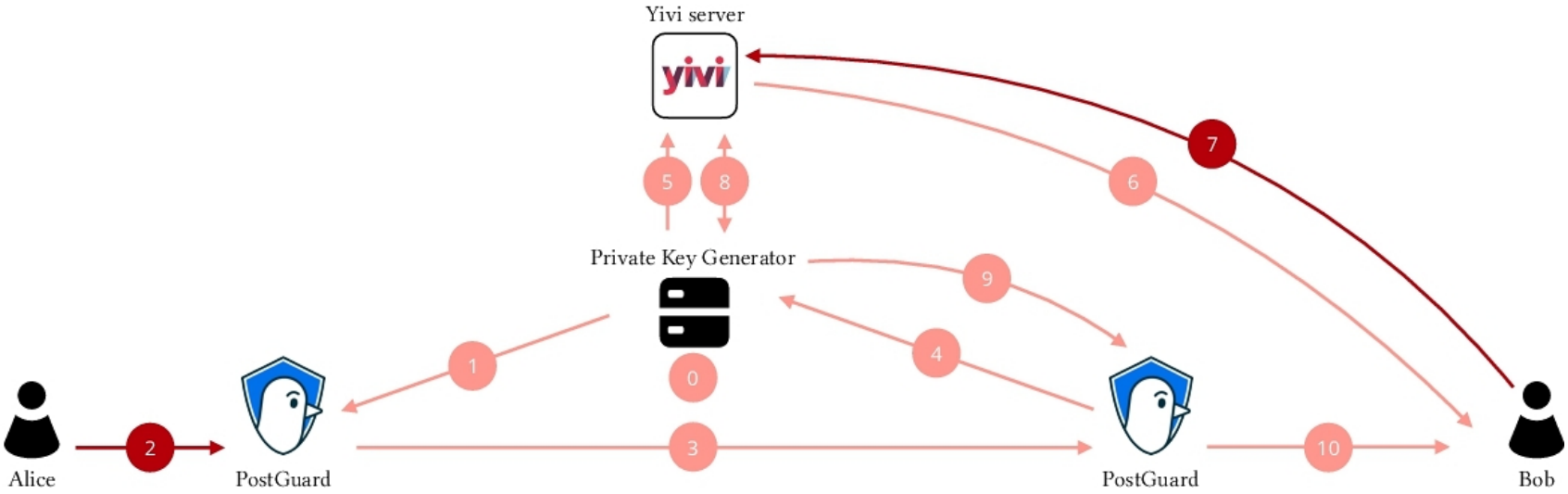
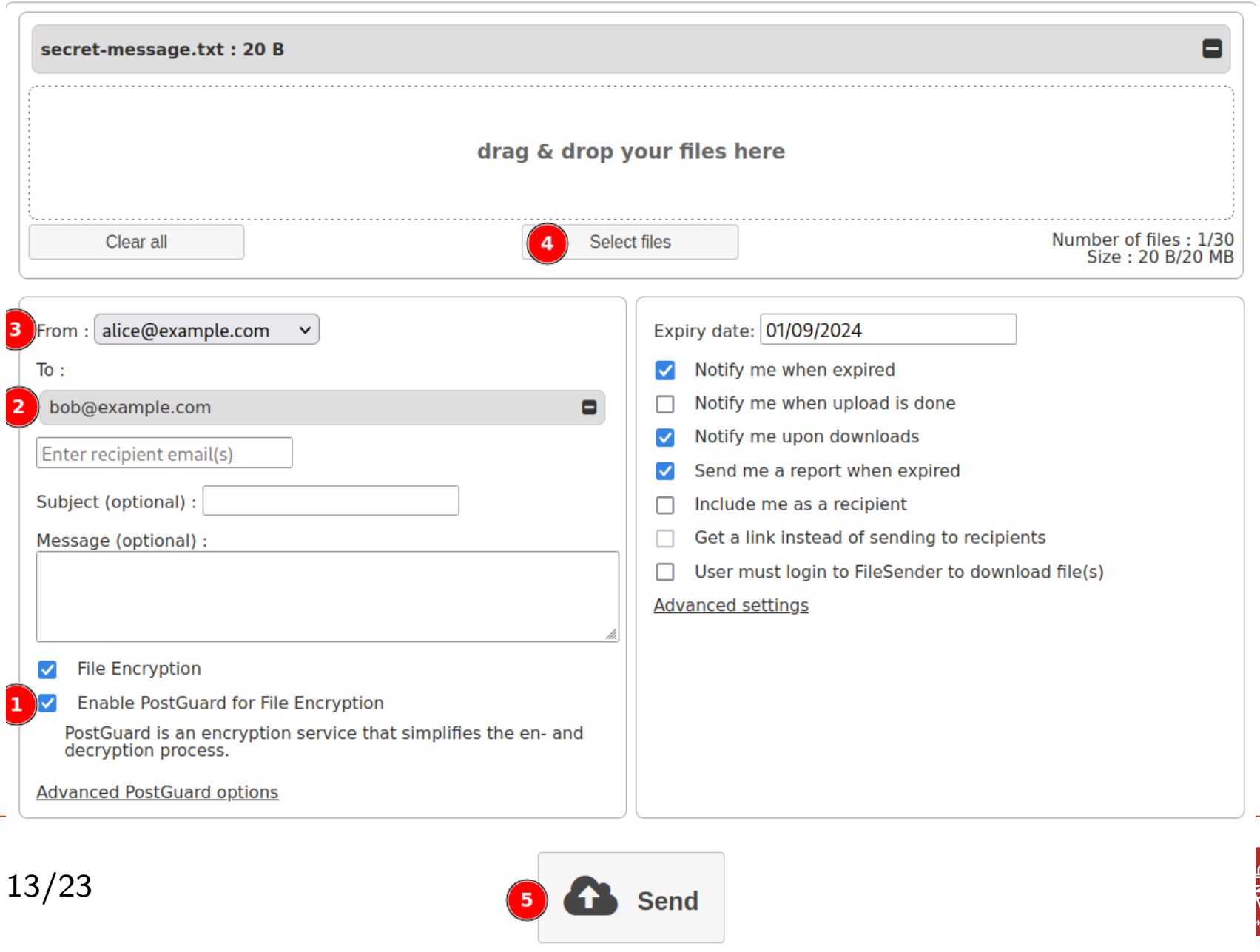


Figure 4: PostGuard session flow [4].

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

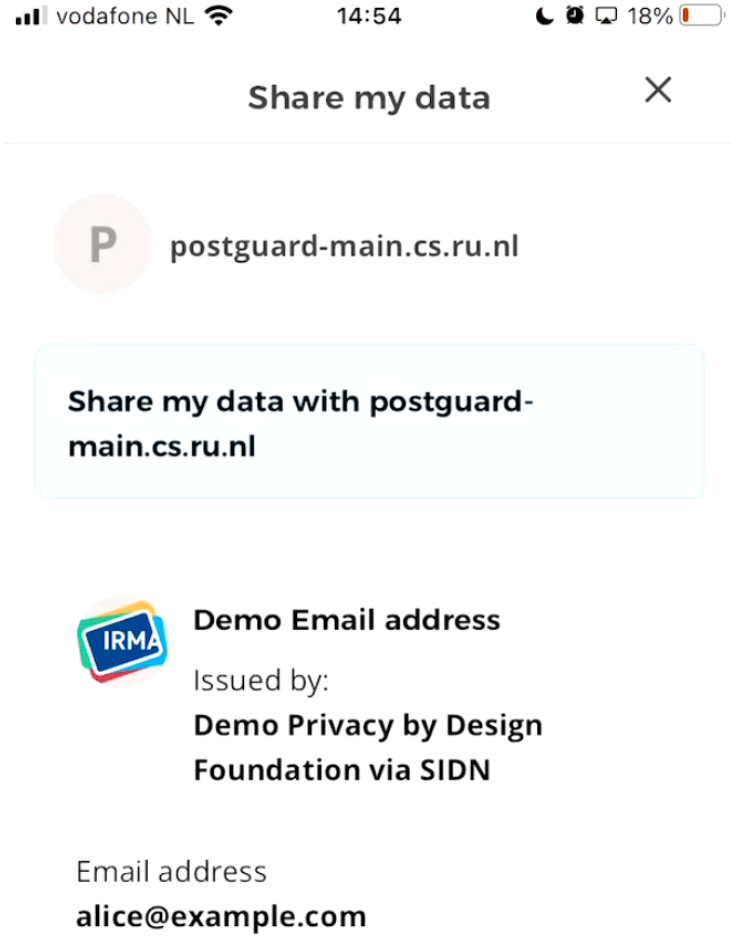
Demo

Demo uploading (1)

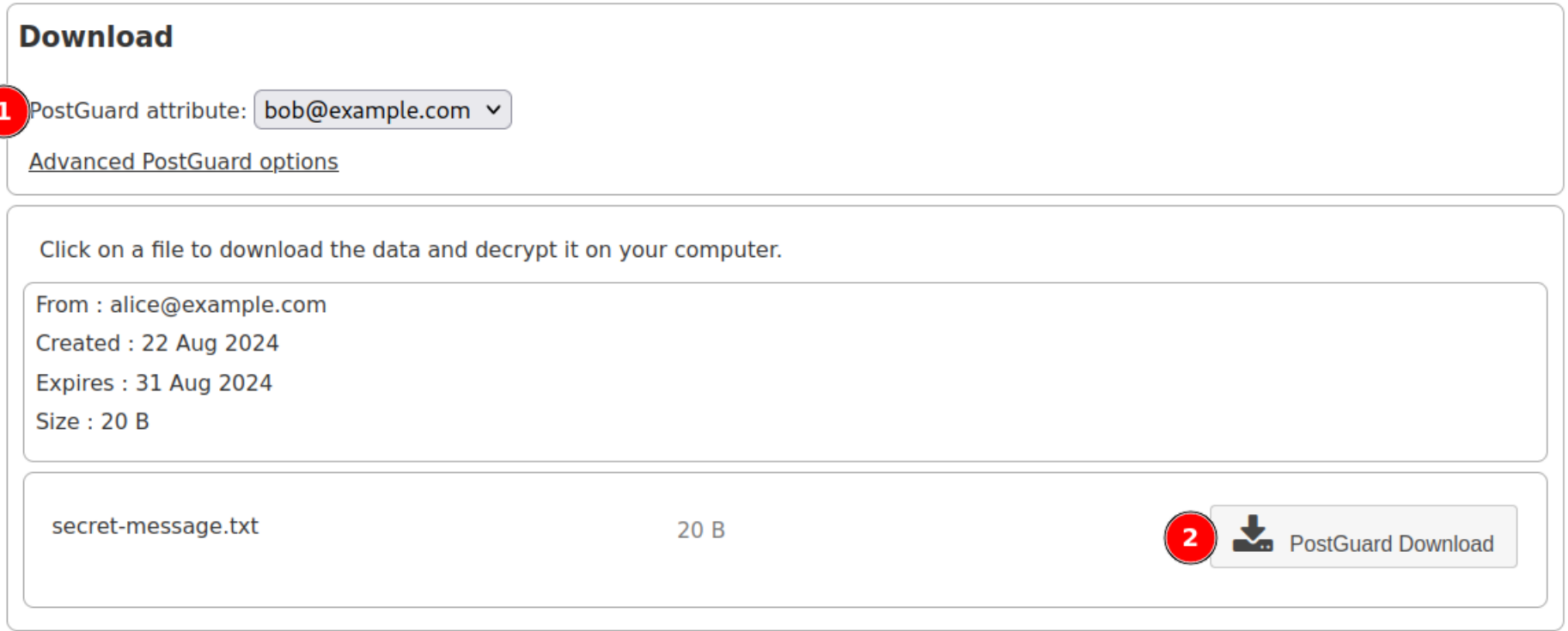


Demo uploading (2)

Demo uploading (3)



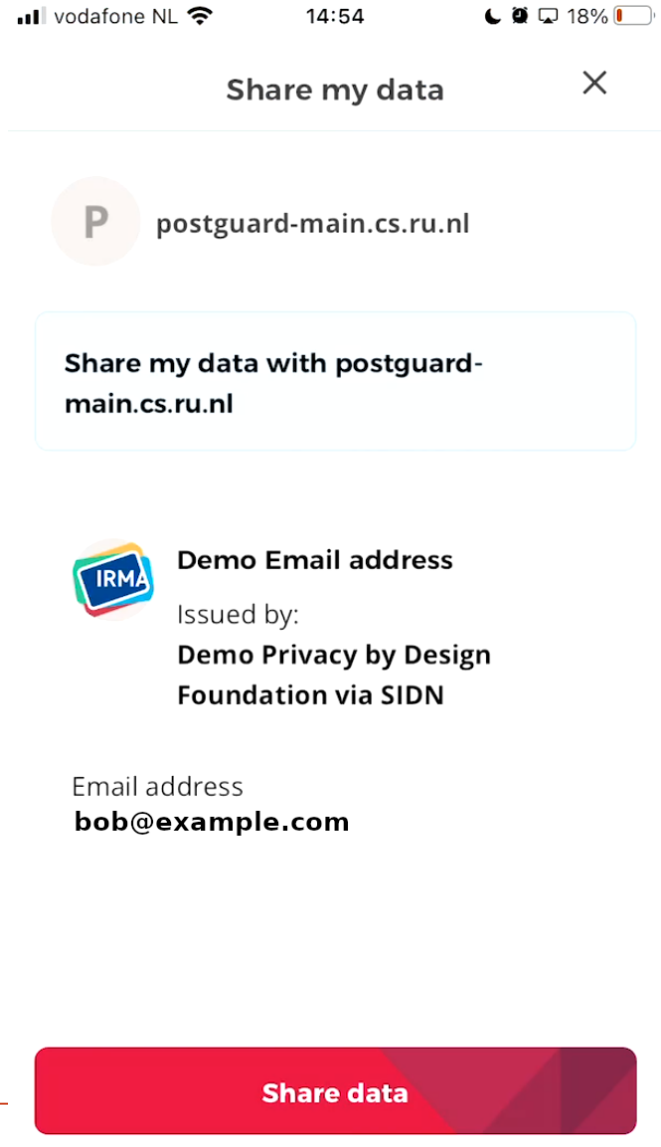
Demo downloading (1)



Institute for Computing
and Information Sciences
Radboud University

Demo downloading (2)

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

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.

Institute for Computing and Information Sciences
Radboud University