Encrypted and signed file transfer with PostGuard

Sjouke Mauw, Symposium, Luxemburg, 10/4/2026

Bart Jacobs — Radboud University, Nijmegen, NL
Joint work with Daniel Ostkamp

bart@cs.ru.nl

Outline

Encrypted and signed file

Where we are, so far

Security by Design: two perspectives

(1) security by design

- Security by default, not as afterthought in system design
- focus on architecture, (protected) data flows
- in GDPR art. 25, but restricted to personal data protection
- open norms: "...appropriate technical and organisational measures for ensuring that, by default, ..."
- subtle relationship to a priori and a posteriori security (resilience)

(2) security by design

- this is about usable or actual security
- bad user interfaces lead to uncertainties and bad/wrong choices
- e.g. after incomprehensible error messages (e.g. certificate expiry)
- or also through dark patterns

These two perspectives, for online voting

(1) Voting should be Putin-proof
- resistance against attack / manipulation, preservation of confidentiality

(2) Voting should be idiot-proof
- so that people express their intended vote, correctly
- recall the voting-by-mail drama in NL, during covid-times

EU / NL / Nijmegen / own perspective

- EU is regulatory power, but not a technology power
  - embedding EU values requires own technology
- Open source as a geopolitical instrument, to keep big-tech at bay
- Digital autonomy now at center stage in IT-debates in EU
  - finally! — with thanks to Trump
  - US technology is weaponised against us
- Nijmegen's interdisciplinary iHub for digitalisation and society
  - with value-driven research agenda and own development/design lab
- Own team projects with strong "usable security" focus:
  - Yivi.app, for attributed-based identity management
  - PostGuard.eu, for identity-based encrypted email & file transfer
  - PubHubs.net, for a new community network
- Today's point: there are subtle trade-offs — illustrated via Yivi & PostGuard

Where we are, so far

General remarks about Yivi

- Started around 2010, as academic research project, called "IRMA"
  - crypto-basis: zero-knowledge proofs, from Idemix (IBM, Zürich)
  - also for identifying attributes, like full name, email, mobile nr.
  - with smart card (first) and phone app (later) prototypes
  - new concept: proportional authentication — with data minimalisation
- In 2015 IRMA moved out of academia, to non-profit spin-off
  - called privacybydesign.foundation
  - roll-out 2019-24 with SIDN, non-profit domain registrar in NL
  - 2024-now, with commercial company Caesar Group (see later)
  - some academic Yivi research remains at university, e.g. PostGuard
  - Yivi has $\geq 100K$ users, but no (inter)national breakthrough
- Hugely influential, e.g. copied by EU in their wallet-ID plans
  - working app has been eye-opener for policy makers & others
  - **Message**: things can be done differently, there is a (political) choice, esp. relevant now for EU digital sovereignty.

Current cooperation with company Caesar

- The privacy by design foundation holds Yivi brand rights
  - and also web addresses like yivi.app and yivi.nl
  - the foundation does *not* have own employees
- Caesar is family-owned, Dutch IT-company, with ±150 employees
- The foundation and Caesar have signed a contract, saying in essence:
  - Caesar gets exclusive rights to (commercially) exploit Yivi brand
  - they run the infrastructure (backend servers, app) with EU hosting
  - they keep Yivi open source, privacy-friendly & secure, free for end-users
  - strategic decisions are taken jointly.
- The aim is to combine public values with corporate efficiency
  - this works well, so far
  - it solves the challenge of getting open source software actually supported and used outside academia

Where we are, so far

iCIS | Digital Security
Radboud University

Basic observations

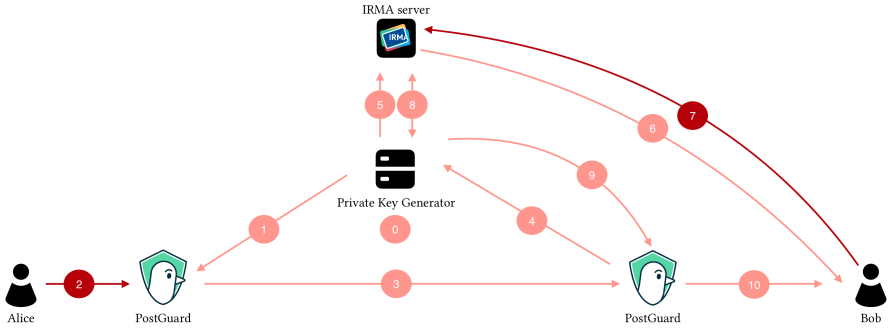
- Email encryption exists for decades, but is hardly used
  - most well-known: PGP
  - only 0.06% encrypted, out of 82 million analysed mails
    (Stransky et al. https://doi.ieeecomputersociety.org/10.1109/SP46214.2022.9833755)
  - "manual key management is unusable for novice users"
    (Ruoti at al. https://dl.acm.org/doi/10.1145/3313761)

- Many variations exist, with both local and central key storage
  - popular in NL: portal-based approaches, like *Zorgmail*, where one party stores all messages — aarghh!
  - another NL service Zivver for secure file transfer was recently taken over by American company Kiteworks
- GDPR pressure increases
  - passport copies via email is getting unacceptable
  - easy-to-use solutions are needed, for the masses
  - focus of Encryption4All NWO-project, leading to PostGuard
  - main idea: combine identity-based encryption (IBE) and Yivi

iCIS | Digital Security
Radboud University

PostGuard flows

- Sender Alice and receiver Bob have the PostGuard email client plugin
- There is a central Private Key Generator, with a Yivi server behind it



Demo time!

iCIS | Digital Security
Radboud University

File/email encryption: explanation and adoption

- Encryption is a very complex concept — for an outsider
  - certainly in combination with cryptographic key management
  - especially with public-private key pairs
- What is the right mental model to convey?
  - the actions that users have to perform must match this model
- We have chosen the following model / explanation:
  With PostGuard you ensure that only your intended recipient can read your message
- Thus, conceptually, confidentiality is reduced to authentication

Results from user studies

- Recall, confidentiality is reduced to authentication
  - Thus, we avoid talking about keys or encryption altogether
  - scanning a QR for authentication is familiar (from banks) and feels secure
- The actions of users are aligned with the mental model:
  - senders choose attributes of recipients, with emailadress as default
  - receivers prove who they are, i.e. that they possess the chosen attributes.
- Requirement to install addon/plugin into email client is a problem
  - extra work, not-entirely trivial
  - the addon requires full access and the user is warned
  - why would anyone trust "PostGuard"?
- PostGuard UX is entangled with Yivi UX
  - revealing own attributes via an app is poorly understood
  - people just click OK, without realising what really happens

Observations about PostGuard and its security

- It is intended to offer a easy-to-use basic level of protection
  - e.g. for direct email contact with your GP etc, not via portals
  - with a reasonable level of security & privacy
  - and fall-back decryption via website
- The IBE + central PKG set-up takes keys out of users' hands, but there is a price to pay:
  - PKG is vulnerable to DDOS — but it can be distributed
  - PKG can be hacked, so messages can be decrypted
  - PKG sees public key requests from senders and attributes of receivers — but not message contents
  - Key escrow: authorities can demand decryption keys — advantage?
- Trade-off: usability versus security/privacy!
  - of course: die-hards can keep on using PGP!
  - better than portal-based solutions with contents centrally visible

Where we are, so far

Concluding remarks

- Security by design may refer to a design attitude
  - not focused on functionality, but on (data) protection
  - in practice one needs security / privacy / usability by design
  - . . . in an approriate combination & balance (with trade-offs)
- The usability part of security (and privacy) requires much attention
  - it may have been underestimated in academia in NL
  - it is popular among students — at Nijmegen
  - it may be the deciding factor for adoption
- Deploying actual systems (Yivi/PostGuard/PubHubs) involves much user experience (UX) research, including mental models
  - do get in touch if you wish to contribute (both kinds of design)
- Recently, Caesar professionalised also PostGuard
  - usage is free, up to a certain file size
- More technical details about Postguard in the paper, including Sjouke's frameworks of attack trees and message sequence charts

Thanks for your attention. Questions/remarks?