Encryption of our Email Communication
Motivations and Challenges

Hernâni Marques <hernani@vecirex.net>

2025-10-29 @ L200, Langstr. 200, 8004 Zurich

Internet Society
Switzerland Chapter

Motivations: Cypherpunk & Privacy

"Privacy is necessary for an open society in the electronic age. [...]. A private matter is something one doesn't want the whole world to know [...]. Privacy is the power to selectively reveal oneself to the world."

Motivations

- Email usage still grows: it won't die. It's the most important and largest federated identity system. Free identity choice possible by principle.
- We have **Mass Surveillance**, now even widespread in countries we considered safe.
- Emails flow between people like postcards, even if encryption (in transit) since Snowden revelation as of 2013 increased a lot.
- Citizens, enterprises and public offices have a right to be protected.

  Mass Encryption and **Mass Anonymization** are needed to counter this.
- Messages should be encrypted and signed by default, for privacy and security reasons (e.g., phishing attacks).

(TS//SI//NF) PRISM Collection Details

Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)? It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

Example 4

- $acwitems = 'machine gun' or 'grenade' or 'AK 47'
- $acwpositions = 'minister of defence' or 'defense minister'
- $acwcountries = 'somalia' or 'liberia' or 'sudan'
- $acwbrokers = 'south africa' or 'serbia' or 'bulgaria'
- $acwports = 'rangood' or 'albasra' or 'dar es salam'

```
topic('wmd/acw/govtorgs') =
    email_body($acwitems and $acwpositions and
  ($acwcountries or $acwbrokers or $acwports));
```

Challenges: Need for automation

- For email, “good”privacy already exists (i.e., with PGP/OpenPGP implementations).
- **But:** Most users are not able to use email encryption tools like GnuPG, Sequoia PGP etc. (properly): its usability must be fixed through automation.
- We need not just good, but **automatic** and **easy** privacy.
- Email architecture as a challenge, other than chat / instant messaging systems, not a silo, no vendor lock-in; not just “one app”.
- That is, **coverage** / **interoperability** as a major problem
  - in terms of clients and platforms and keeping compatible to existing S/MIME and OpenPGP systems (cf. https://openpgp.org/).
  - in terms of the underlying crypto engine involved (e.g., GnuPG, Sequoia PGP, NetPGP etc. (cf. https://sequoia-pgp.gitlab.io/openpgp-interoperability-test-suite/results.html)

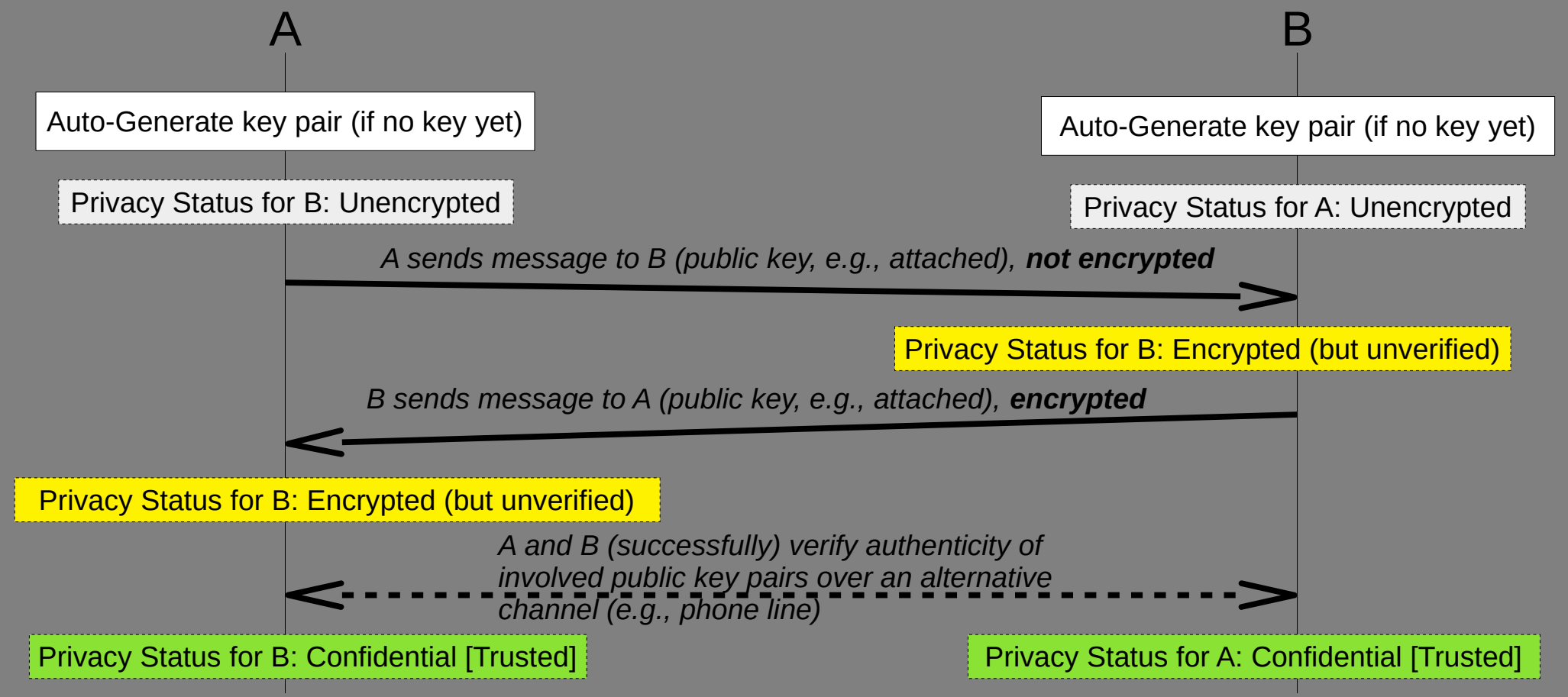
Stream: Internet Engineering Task Force (IETF)
RFC: 9787
Category: Informational
Published: August 2025
ISSN: 2070-1721
Authors: D. K. Gillmor, Ed. *ACLU*
A. Melnikov, Ed. *Isode Ltd*
B. Hoeneisen, Ed. *pEp Project*

RFC 9787
Guidance on End-to-End Email Security

Abstract

End-to-end cryptographic protections for email messages can provide useful security. However, the standards for providing cryptographic protection are extremely flexible. That flexibility can trap users and cause surprising failures. This document offers guidance for Mail User Agent (MUA) implementers to help mitigate those risks and to make end-to-end email simple and secure for the end user. It provides a useful set of vocabulary as well as recommendations to avoid common failures. It also identifies a number of currently unsolved usability and interoperability problems.

Example Msg. flow (simplified)



Questions

- ???
- ...
- Ask!