An introduction to mailbox.org Guard

Our new mailbox.org Guard offers the first PGP implementation for Webmail that combines both convenience and security to facilitate the easy and widespread use of secure e-mail for everyone.

The days are over when encryption remained largely unavailable to the masses because of complex installation procedures or a lack of support for Webmail and cloud-based systems.

The mailbox.org Guard is 100% OpenPGP-compatible and can be used in addition to regular end-to-end encryption for e-mail clients. This means the mailbox.org Guard is not a replacement but an extension to OpenPGP, and integrated into the front end of our Webmail system.

Other solutions that work as plug-ins for web browsers, or tools such as Mailvelope typically fail when it comes to using attachments from cloud storage; or cannot be used safely in untrusted environments like computers in Internet cafes, or those public PCs in hotels, for instance. Consider also that a range of cryptography experts have discovered various loopholes and uncertainties in the current encryption mechanisms of Javascript, and expressed doubts about whether reliable cryptographic methods could ever be realised using Javascript alone.

mailbox.org Guard is a server-side implementation of PGP where all users can create individual encryption keys without needing any particular technical expertise. Those users who are technically adept may of course still upload their own keys to mailbox.org Guard if they wish to do so, and can then use our system together with their local PGP setup. The advantage of this parallel configuration is that it allows secure access to communication data on the go, which includes any untrusted, public Internet terminals. Meanwhile, all encryption keys are kept safe on our servers, managed in a secure environment by our experienced team of IT professionals.

The encryption keys are secured by a password that only the users themselves will know. In other words, our administrators do not have this password and thus, cannot decode any user communication. Decrypting any private key requires the relevant user to log in explicitly, and the protection mechanisms on our servers will make sure that we, the server operators, will never have access to a decrypted key. Our systems are also designed such that any of these keys will never be stored in program memory unencrypted.

We acknowledge that it requires trust for anyone to hand over their private encryption keys to us so that we may store and manage these on our servers, and we wish to make customers explicitly aware of the fact that this is how it works.

However, one might argue that encryption keys, which remain password-protected as they sit on our infrastructure, are probably stored more safely and securely with us than on a private PC or smartphone.

Security experts like M. Cardwell have explicitly warned users to not store or use their private OpenPGP keys on devices that are not secure (like smartphones).

Since mailbox.org Guard offers a browser-based solution, we do not need any keys to be stored on the device itself, yet can still provide secure access to your e-mails at any time.

However, as the processes of encrypting and decrypting happen exclusively on the server, mailbox.org Guard can not offer true end-to-end encryption. **This means the level of security offered here will not be sufficient for users with extremely high security requirements (like whistleblowers, for example). The primary aim of mailbox.org Guard is to combine security and convenience to facilitate so-called “sufficient security”.**

In any case, the mailbox.org Guard presents an interesting alternative for anyone who would like to use our service conveniently, on a daily basis. We encourage everyone else with higher security requirements to continue using their local PGP setups for secure access to e-mail.

By the way, even if your communication partner happens not to be a mailbox.org customer and does not have an OpenPGP key, you can still communicate securely via mailbox.org Guard. We use temporary mailboxes for external users, which they can then use to receive, read, and reply to encrypted e-mails. Of course, these temporary accounts are also protected by dedicated login credentials, two-factor authentication, and SSL.

Overview of the advantages:

- mailbox.org Guard is 100% compatible with the established OpenPGP standard.
- Activating and using encryption is accessible to everyone, even if they do not have any technical expertise.
- Easy to use and transparent, runs in your web browser on the PC or on the phone.
- Server-side PGP implementation – your actual PGP key is not transmitted to a (potentially unsafe) web browser.
- Read and compose OpenPGP-encrypted messages in your web browser, without any restrictions.
- Business users benefit from group accounts and shared key management.
- Temporary mailboxes for secure communication to everyone worldwide, even those who do not use Open-PGP yet.

Overview of the disadvantages:

- Encryption and decryption both happen on the server side, hence there is no true end-to-end encryption.
- Users need to hand over their private PGP keys to be stored on our servers.
- mailbox.org Guard offers “sufficient security” for those who want the convenience but cannot provide “absolute security”.

Related Articles

- Can I trust the staff at mailbox.org
- An introduction to mailbox.org Guard

- Import existing PGP keys into Guard
- Activate your mailbox.org Guard
- Read encrypted e-mails with Guard