Guide

Encrypted e-mail for private use. All you need to know

Paweł Wałuszko 29.01.2020

During one of the online seminars conducted by CyberForces and Xopero on the topic of Internet security and social engineering, numerous attendees asked me to outline how encrypted e-mail works and how can one start utilizing it in their day-to-day operations. Since the topic is very broad, I thought this text might be a good introduction to the concept of using encrypted e-mail systems.

Digital transfer of private data

Today it's nearly impossible to utilize key Internet services without having an e-mail account. Our e-mail addresses, in fact, became verification methods for some services. For example, when we lose a password to a service, we usually can reset it by having a special link e-mailed to our address. The taxes we pay are linked to our e-mail addresses, as we utilize online tax services such as Turbotax, TaxAct, H&R Block Online Edition (and numerous others), which utilize e-mail as means of authentication. The tax forms themselves have a special field where the taxpayer can enter their e-mail address, so the government can send updates on tax returns. Consequently, e-mail is a critical hub for all important notifications about our business.

Unfortunately, the side effect of digitizing so much of our critical communication is the fact that identity theft has become easier than ever. Anyone who gains access to the contents of our mailbox has a wealth of data about us and can easily utilize this information to steal our identity. Meanwhile, the e-mail platform has not received much of an upgrade since the early 1990s. In fact, the basic principle of e-mail has not changed much over the course of three decades, with only a few modifications to the traditional e-mail protocols.

Standard e-mail security

It would be wrong to say that standard e-mail is outdated and insecure. In fact, most of the time e-mail is very secure, as protocols such as IMAP, SMTP, and POP3 are secured with SSL, TLS or STARTTLS, thus making sure that the authentication process is done in a secure, encrypted manner. Every major e-mail provider uses encryption for transfer and authentication of an e-mail; in fact, it would be hard to find a system that still sends authentication data in a plain text format.

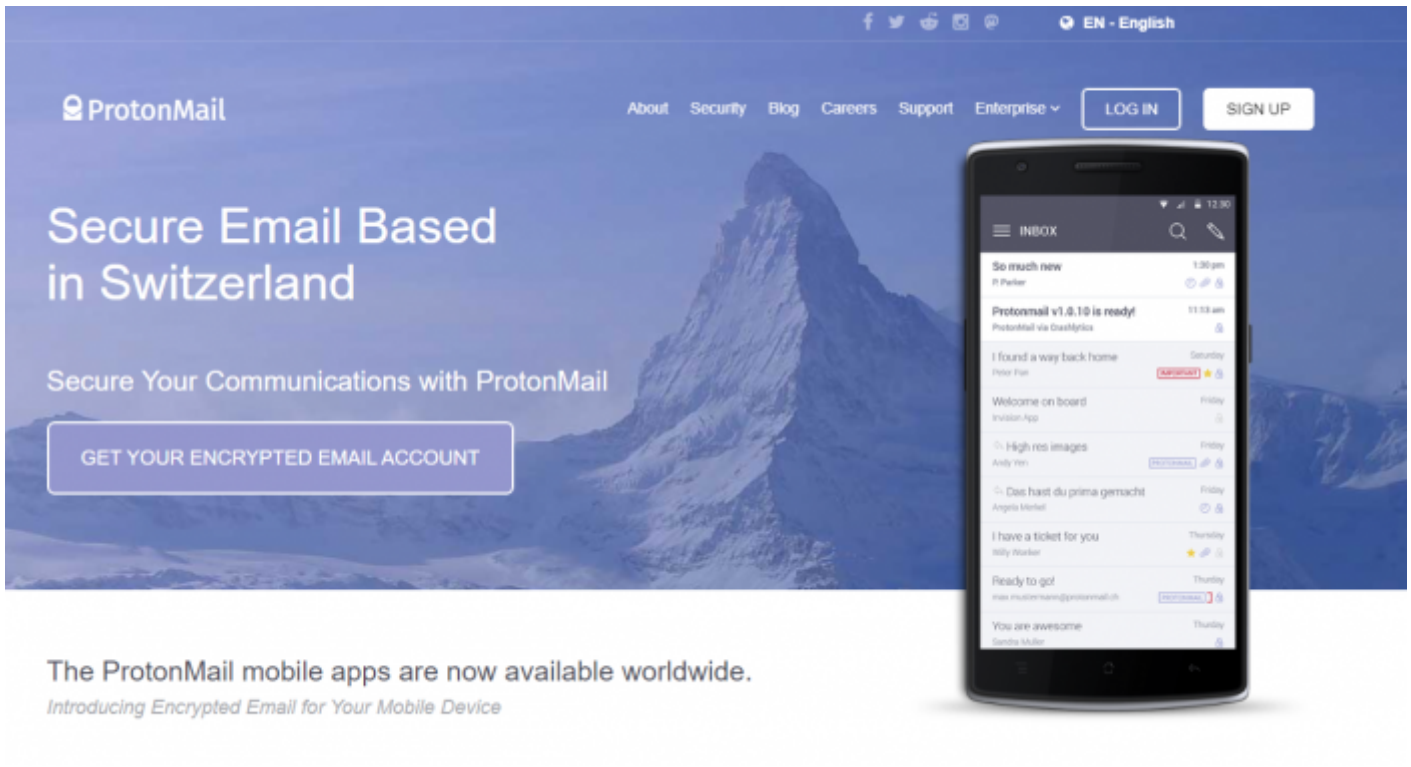
Nonetheless, there's an intrinsic problem with e-mail, and it has to do with the fact that by default, our messages are stored in plain text format. What this means is that while the authentication process is relatively secure, the storage method is completely unprotected. From the administrator's point of view, accessing someone's e-mail data is as easy as opening the text file on the computer.

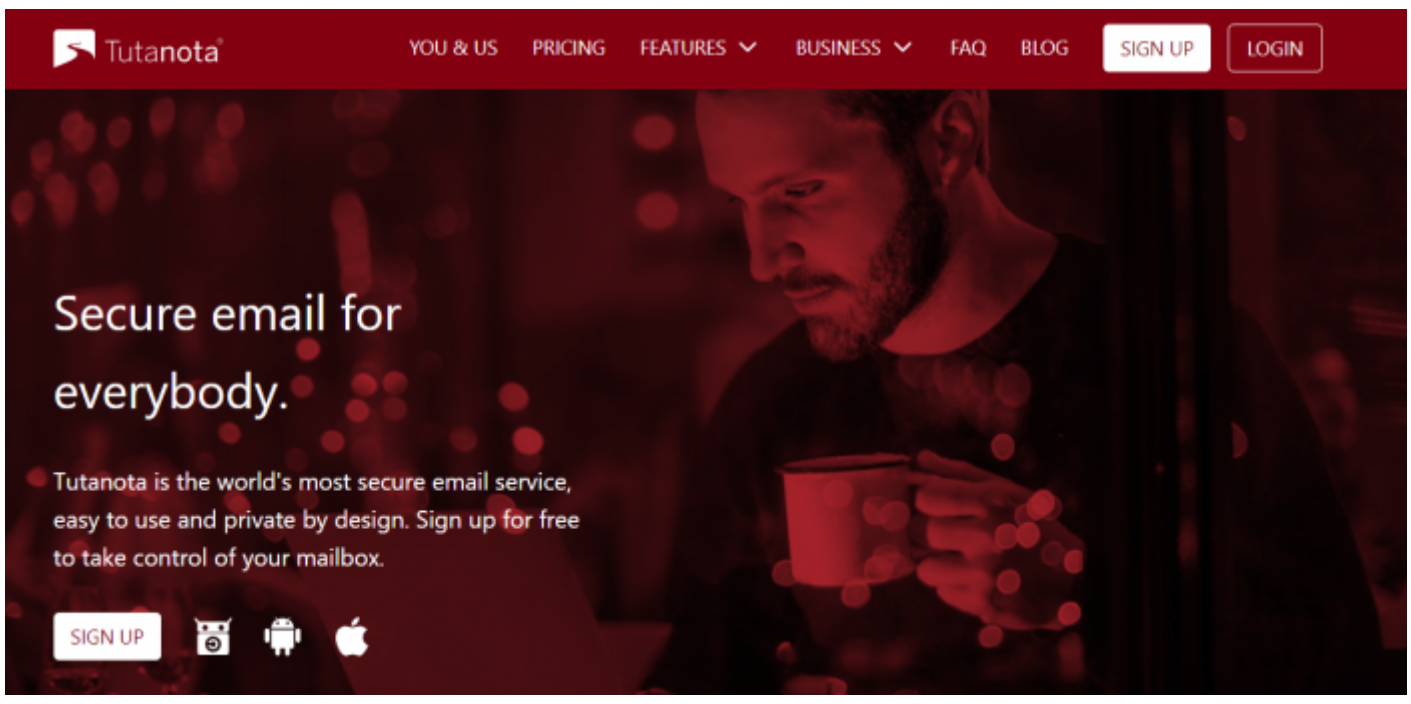
For some users, ramifications of this design flaw can be great. Let's take security, for example. While a user might do their best to keep their devices encrypted and secured, if someone gains access to the provider's credentials, all users data is at risk. With the profitability of identity theft, each compromised e-mail account has its worth on a black market – and there are plenty of "entrepreneurs" happy to mine this data for a potential exploit. Meanwhile, a single mailbox often has highly confidential information related to our identity, our business or personal life.

Encrypted e-mail

With all the problems of ‘traditional’ e-mail outlined above, one might be inclined to turn to message content encryption in order to solve this weak-point. In many ways, this is a logical and reasonable solution. However, for those trying to upgrade, lack of ubiquity is the problem: most popular e-mail providers simply do not provide encrypted e-mail services, and even when they do, sending and receiving mail can be… unergonomic at least.

If you are inclined to start utilizing an encrypted e-mail service, one of the easiest ways to jump on the bandwagon would be to utilize an encrypted e-mail provider. Over the last few years several companies came out with a reliable, standard and encrypted e-mail service offering – some even for free.





Two of the most prominent encrypted e-mail providers on the market today are Protonmail (Switzerland) and Tutanota (Germany). As one may notice, obtaining an encrypted mailbox is just as easy as signing up for a regular e-mail account from Gmail, for example. After the signup process, we’re presented with a clean user interface, and we can start e-mailing right away. Both Protonmail and Tutanota combine standard with encrypted e-mail service, so users can seamlessly transition into the more secure technology as they utilize the new mailbox in their day-to-day operations.

However, whereas sending e-mails between two encrypted providers works out of the box, sending an encrypted e-mail to a non-encrypted mailbox ends up with an extra step in the reading process.

When a user of an encrypted service sends an encrypted message to a ‘standard’ user, he/she will only receive an invitation to read the message through their Internet browser. Clicking on a special link will forward the user to a password form, where they will have to enter a password earlier obtained from the sender. Here it’s important to notice that giving someone the password

to a message should be ideally be done through a different means of communication – for example, during a phone conversation. When the receiving party is done reading the message, they will have the opportunity to reply in the same window. Once the “send” button is clicked, the message is encrypted and sent off to the receiving user.

While this additional step might not constitute a sizable inconvenience for the price of additional security, not all users are inclined to switch, however. This is partly due to the fact how ubiquitous traditional e-mail has become in our daily life: many of us have dozens, if not hundreds of services registered to our current e-mail address and switching to an entirely new address might not only be highly problematic, but downright impossible. So, can a standard e-mail account be used for sending encrypted messages?

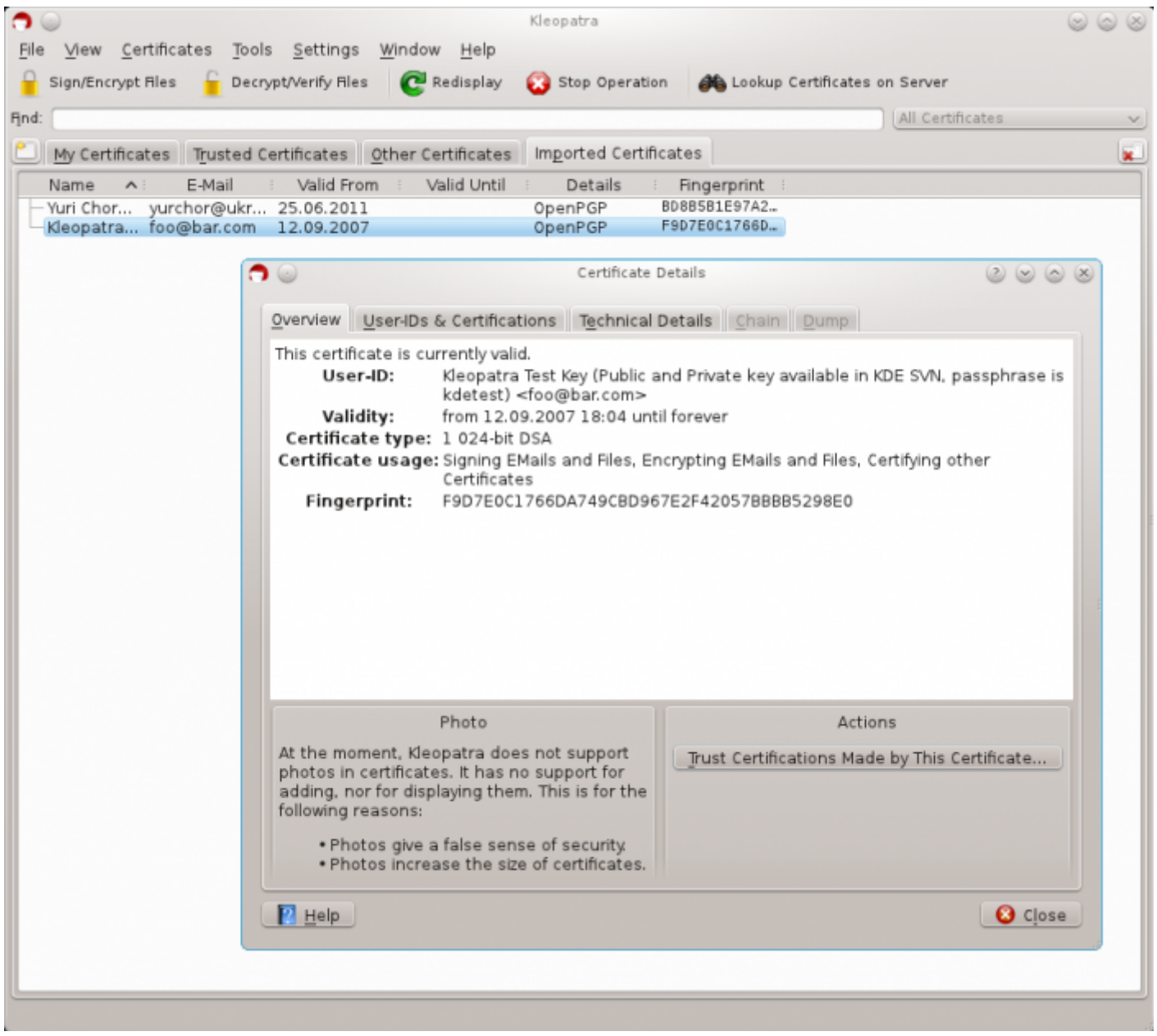
Using standard e-mail accounts to send and receive encrypted messages

In short – yes, it’s possible to use standard e-mail accounts for sending and receiving encrypted e-mails. However, this process usually entails downloading software, manually encrypting and decrypting e-mail messages.

Let’s dig in.

We begin with downloading a piece of software – such as Kleopatra – which will allow us to create a pair of keys: private and public. A private key is made specifically for one user and should be kept in secrecy at all times. This key is used in the process of decrypting received messages and should be treated as a password – that is, whoever has this key, they have access to all our message data. A public key, on the other hand, is a complimentary key to the private one and as the name suggests, can be published freely on the Internet. By using our public key, someone sending us a message will be able to encrypt it in such a manner, that only we will be able to decipher it. It’s important to point out that keys are made in such a way that it’s impossible to decrypt a message only by using someone’s public key.

By exchanging their public keys and retaining the private ones to themselves, users can compose and send encrypted messages in plain text format. With the private key in hand, the appropriate user will be able to decode the message. The administrator of the service, on the other hand, will only see nonsensical, scrambled text information that will bear no useful data.



Kleopatra

Making life easier with encrypted e-mail

Although there are countless tutorials and YouTube videos on how to use Kleopatra and similar software, for the purposes of this text, it makes little sense to publish step-by-step instructions. Regardless of which option we choose, there is a great amount of literature explaining the process of setting up and using the software to generate keys and encrypt/decrypt messages. Moreover, the logical foundations of how key management and message encryption software works is very similar.

However, as one may notice, the process of using standard e-mail accounts to deliver encrypted e-mails is by far more complicated, than composing an unencrypted message on a traditional e-mail service. This is the reason why there are very useful browser extensions that can help automate the process – such as Mailvelope and FlowCrypt. Additionally, popular e-mail clients such as Microsoft Outlook and Mozilla Thunderbird already have similar plugins available, as well as standardized methods of encryption and sender identity verification.

When it comes to corporate customers – using encrypted e-mail inside a business entity can be quite uncomplicated, as long as the IT department rolls out appropriate protocols and authentication procedures company-wide. Microsoft Outlook, for example, has been supporting this technology for years, so the process of transitioning into all internal e-mail encrypted by default has very little technological and financial constraints. The security benefits of this solution are definitely worth the upgrade.

Rate the article:

5 / 5 (1 vote)

29.01.2020

[Paweł Wałuszko]

Business Development Manager i Ekspert ds. Bezpieczeństwa. Doświadczony menedżer w branży IT, który swoje doświadczenie zdobywał m.in. w Dolinie Krzemowej; entuzjasta oprogramowania open - source.

VPN for private use – a good idea?

How CEOs fall victim to hackers. The example of Jeff Bezos

Search

To search, type and hit enter.

Recent Posts

Archives