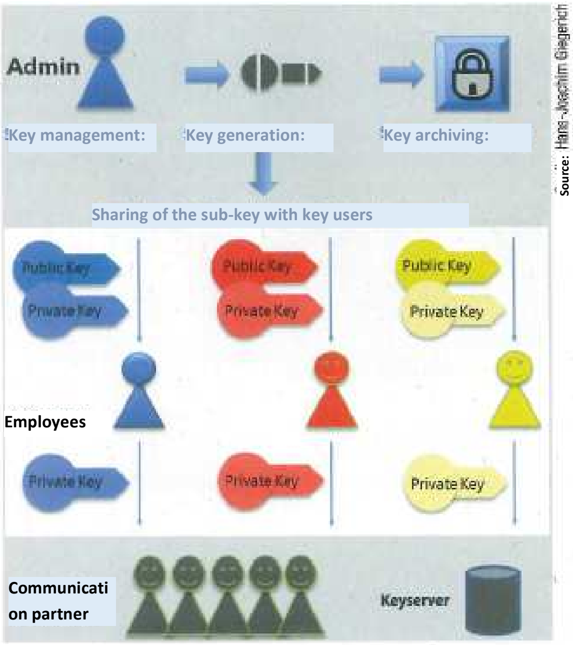
Guidelines for efficient email encryption

Setting up OpenPGP keys is less complex than what is often claimed

The person in charge in charge of encryption in accordance with the OpenPGP standard has already taken a decisive step towards safer email communication. The better the introduction is planned the smoother the use is in practice.

What you need to know: one needs to know what they want to protect themselves against in order to take the right measures of protection . Do you wish to save customer data securely, block secret services and corporate spies, adhere to legal data protection regulations or simply not lose the connection? And how is it with the employees: how strongly have they been sensitised in these domains and what experiences on every aspect of encryption do they already have? The latter can be decisive as to how complex the tool to be used may be and what training effort may be necessary.

It first needs to be clarified whether a key hierarchy should be used, who may generate and manage the keys in the company, how they will be archived and which keys are subject to which security level. The security level will be re-defined for every implementation of OpenPGP.



Source: Hans-Joachim Giegerich

Key management takes over the sharing and archiving of the OpenPGP key pairs.

An OpenPGP key achieves the highest level if it was generated on an extremely secure system and the secret key has either never left it or is saved on a safe data carrier until the next use. An example of this would be a live operating system and a USB stick that is only connected to this system and is otherwise kept in a safe.

Configuring and archiving the key correctly

An OpenPGP key pair consists of at least one or multiple User IDs. The User ID reveals the person (or group) to whom the key is allocated. It is generally made up of the complete name of the key owner as well as their email address. A comment field is available optionally, e.g. for entering the company name. The key can be allocated to different email addresses using multiple User IDs. The freeform User ID is also often used. It does not contain an email address, but serves as a type of basis. If the email address of the future user is then added as an additional User ID, it can be revoked in case of subsequent changes without having to withdraw the entire key in the process. Besides, companies should stick to a clear distinction between professional and private use of the company key for reasons of work safety and data protection.

In modern desktop environments, the key length hardly has any effect on the performance. Hence, it should be set as high as possible (4096 bit). The situation is different in case of keys for mobile devices, smartcards or automated systems, which need to process a lot of data in less time. A key length of 2048 bit is recommended in this regard; less (1024 bit) is not advisable.

Saving keys is an essential step for use in companies. In the simplest case, the keys of the employee will be issued with a known passphrase by a central authority in the company and archived at the same time. In less ideal cases, a passphrase – known to the archiving authority – must be set to the keys before they are saved. The selection of the storage medium defines how quickly the key or keys can be restored in case of a problem; it also directly influences the stability. Archiving on paper is feasible, but comparatively more time-consuming and error-prone. This works faster with the help of a container that has also been encrypted safely.

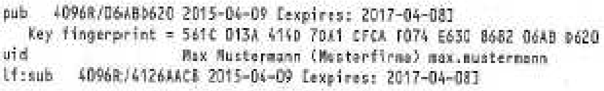
A key hierarchy is always sensible for companies. It makes it easier for the employees to work with OpenPGP as an administrator can centrally certify the keys (often also referred to as sign or undersign) for instance. A company key will be used for this, which is not assigned to any specific email address (free-form ID), but represents the company as a whole. This company key, preferably generated at a high level, will be used to carry out the certifications of the employee keys as well as incoming public keys after the necessary inspection. With the trust of the employees in the company key, a certification chain is formed from the individual employee right up to the external key. Moreover, duplicate keys can also be easily identified in this manner.

A key guideline should be defined for the key material used. It generally consists of three parts and summarises many of the specifications per key (or a group of keys). This includes the security level (How safely is a key stored/used?), the purpose of the key (For what and how is the key used?) and the certification guideline (How detailed is the procedure for the certification of external keys?). The key is not suitable for public certifications without a certification guideline.

Brief instructions for generating a key

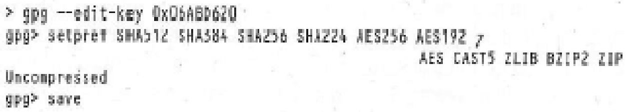
The following components are decisive for generating safe keys: a cryptographically safe passphrase, a free-form User ID, User IDs with the specification of the full name and email address of the user, a key length of minimum 2048 bit (better 4096 bit), an expiration date of maximum five years and an offline main key version. After generating the key, it will be hardened, i.e. it will be

As regards the format of the User IDs, it must be taken into account that, for security reasons, many OpenPGP users certify only User IDs whose name completely corresponds to the details on the ID card. The company key should be imperatively generated with high security, i.e. in a secure live operating system without an Internet connection. For this, the latest version of a GnuPG is most likely considered. After entering > gpg –gen-key in the GnuPG command line, the key will more or less look like this:



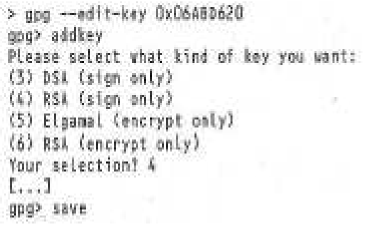
```
pub   4096R/06ABD620 2015-04-09 [expires: 2017-04-08]
   Key fingerprint = 561C D13A 416D 70A1 CFCA F074 E630 8682 06AB D620
uid                  Max Mustermann (Musterfirma) max.mustermann
Lf:sub   4096R/4126AAC8 2015-04-09 [expires: 2017-04-08]
```

In this example, “06ABD620” represents the Key ID in an abbreviated form saved in the metadata information that, preferably, the most powerful algorithms should be used. For generating a company key, the complete company name will be entered instead of the name of a person. The details of a personal email address will also be left out. If you wish to set up a central general email address for questions with respect to the company key, you can however specify it voluntarily.



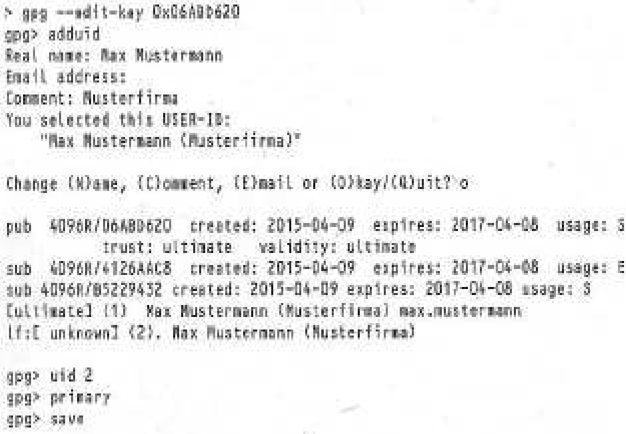
```
> gpg --edit-key 0x06ABD620
gpg> setpref SHA512 SHA384 SHA256 SHA224 AES256 AES192 ↗
                                              AES CAST5 ZLIB BZIP2 ZIP
Uncompressed
gpg> save
```

Subsequently, a sub-key will be generated as a rule for signing with the help of the separate main key.



```
> gpg --edit-key 0x06ABD620
gpg> addkey
Please select what kind of key you want:
(3) DSA (sign only)
(4) RSA (sign only)
(5) Elgamal (encrypt only)
(6) RSA (encrypt only)
Your selection? 4
[...]
gpg> save
```

You can now insert another User ID, in which an email address will not be mentioned. If the public key is supposed to be saved on a key server, this can be very useful if spam is avoided.



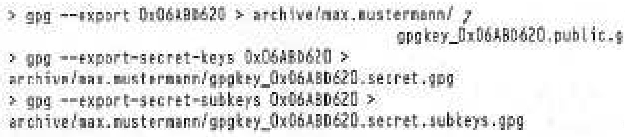
```
> gpg --edit-key 0x06ABD620
gpg> adduid
Real name: Max Mustermann
Email address:
Comment: Musterfirma
You selected this USER-ID:
    "Max Mustermann (Musterfirma)"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o

pub  4096R/06ABD620  created: 2015-04-09  expires: 2017-04-08  usage: S
            trust: ultimate   validity: ultimate
sub  4096R/4126AAC8  created: 2015-04-09  expires: 2017-04-08  usage: E
sub 4096R/85229432 created: 2015-04-09 expires: 2017-04-08 usage: S
[ultimate] (1)  Max Mustermann (Musterfirma) max.mustermann
[f:[ unknown] (2). Max Mustermann (Musterfirma)

gpg> uid 2
gpg> primary
gpg> save
```

In the end, the key must be further divided so that the sub-keys can be issued to the employees.



```
> gpg --export 0x06ABD620 > archive/max.mustermann/ ⁊
                                     gpgkey_0x06ABD620.public.g
> gpg --export-secret-keys 0x06ABD620 >
archive/max.mustermann/gpgkey_0x06ABD620.secret.gpg
> gpg --export-secret-subkeys 0x06ABD620 >
archive/max.mustermann/gpgkey_0x06ABD620.secret.subkeys.gpg
```

All the actions on the keys have now been carried out and it is exported to the archive. The gpgkey_0x06ABD620.secret.subkeys.gpg file goes to the employee (Max Mustermann) and the gpgkey_0x06ABD620.secret.gpg file remains in the archive in order to revoke or regenerate existing sub-keys or User IDs. The public key can now be shared with the communication partner, e.g. on an in-house key server. Otherwise it will be shared elsewhere in the company so that all the employees can communicate with each other in an encrypted manner, which is immensely helpful in case of a comprehensive implementation in the company. If the company uses an encryption solution, which works only with a specific key server, it is also possible to accurately specify which public keys may be used. For transmitting the key pairs to the employees, an automatically connected network drive is suitable for instance, which only the relevant user can access. Manual sharing via a data carrier is naturally possible too.

Private keys of the employees can fall into the hands of unauthorised persons, who then read the communication as well or make incorrect information appear authentic with a The corresponding private key or the key component can then no longer sign any data, and the public key can no longer be used for the encryption. The decryption of data is however still possible.

Without an offline main key, the entire key pair must be revoked. If the employee receives a new key pair after this, it must again be signed from all the communication partners. If only a sub-key was issued to the employee, it is sufficient to revoke only this sub-key. Previously established trust-based relations are thus maintained. A public key marked as unsuitable should be shared real-time with all the communication partners. Ideally, the new key is also communicated in this case and the existing key servers are updated.

Regulating the rights management

A topic that is often neglected is the stipulation and implementation of general guidelines for working with keys within the company. If the encryption software allows it, the Administrator can choose to take away or grant specific rights to individual users and groups. On the one hand, guidelines save a lot of work in daily usage and on the other hand a ban on uploading public keys ensures that the “social graph” of the trust-based relations of a user cannot be viewed publically – and thus (incorrect) conclusions as regards company strategies cannot be drawn.

A frequent objection to the use of email encryption is that encrypted messages in archives cannot be read easily. This is indeed correct, but this is also desired when it comes to encrypted communication. Auditors of email archives can be granted access to the archived key material. For this, it is best to define corresponding access rights at the time of planning itself.

At times, the email encryption gradually grows into the company as individual employees are already working with key material generated by them with or without approval of the company management.

However, from the business point of view, it is not possible to approve of an access to encrypted messages only in collaboration with the respective key owner. During vacation or illness or even if the employee leaves the company, the access to important information is possibly lost. Such keys should be collected along with a functioning passphrase and archived safely. By revoking the older key and sharing the new key, the situation can however be settled in terms of the company.

Verdict

Fortunately, the effort for implementing email encryption with OpenPGP is kept within limits. Extensive investments too are not mandatory. However, the workflows need to be defined and communicated with the employees so that the newly acquired safety is not rendered void again. However, at the same time, the acceptance should not suffer from it. Careful planning is thus required in this regard – irrespective of whether OpenPGP-based solutions are already available in signature. If an employee leaves the company, his public key should no longer be used. In these cases, a key can be revoked with a revocation certificate. Alternatively, only parts of a key can be revoked. However, this is not done using a revocation certificate, but using a special certificate of the main key.

the company or need to be rolled out in the first place.

Hans-Joachim Giegerich
Managing Director Giegerich & Partner