Giegerich & Partner

gpg4o

Dealing with OpenPGP Key Pairs within the Company

Whitepaper

TABLE OF CONTENTS

1 Introduction

1.1 Motivation

In order to decrypt encrypted data, you always need a corresponding key. In no case can you rely on being able to simply calculate the key. This may work in exceptional cases with weak encryption or errors in the encryption algorithm; however, this is not always the case and can only be done with corresponding know-how. Thus, there is considerable motivation to back up key material.

- Possibility of recovering key material when the passphrase has been forgotten or accidentally deleted
- Possibility of access to encrypted data via authorised third parties within the company
- Possibility of access to encrypted data via authorised authorities (e.g. as part of GDPdU)
- Possibility of withdrawing issued key material, e.g. when employees leave or when private keys are lost

The use of encryption technologies within the company offers improved protection of valuable know-how. This is all the more true when sensitive information of whatever kind leaves (must leave) the company. Encryption is used here when implementing strategies for information security and for data protection.

However, not everyone should indiscriminately employ some sort of encryption. In many cases (legal regulations, employee departures, etc.) third parties (general management and possibly the authorities) must also be able to gain access to data encrypted by employees. For this reason, it is important to subject the issuance of key material within the company to uniform rules, preferably as part of an information security strategy.

1.2 Objective / Delineation

Three concepts for issuing and backing up key pairs used within the company are described in this document. Depending on the status of the organisation within the company and the company's size, different versions are conceivable / reasonable. Hybrid forms are possible here. Encryption often grows into the company. Therefore, it is a matter of setting up a status quo. The backing up of existing key pairs is described in section 5.

Ideally, a key concept is created before the introduction of encryption within the company. A process for issuing keys in small and micro companies or for work groups and role models is described in section 3. Section 4, on the other hand, describes the handling of personal key material in larger companies.

This document describes how to practically issue and back up key material within the company as part of a strategy for information security or for data protection. It does not replace the company's own plans on the subject of data security and data protection, nor will it offer any instructions for the design of processes to access encrypted data. The company's everyday reality as well as legal regulations or regional customs are to be observed for this.

This document does not replace the necessary training of employees when dealing with key material either.

1.3 Definition

gpg4o is an add-in for Outlook 2010® / 2013® to encrypt and decrypt emails. It is based on the asymmetrical **OpenPGP** encryption system in which a key pair consisting of a public and a private key is used.

gpg4o requires the private key to decrypt encrypted emails as well as to sign outgoing emails. This private key is protected by a passphrase (a password), which is defined when the key pair is generated. The passphrase can be changed at a later time.

The public key is made accessible to the communication partner in order to enable encrypted communication with you.

Keyservers collect and offer access to public keys which are published by people. Keyservers may be located within the internet (open key servers) or locally within an organization or company. In the second case they provide employees with necessary public keys. Published public keys cannot be deleted by users but may be disabled by a so called revocation certificate.

We always recommend to create revocation certificates during the creation process of a new key pair to enable revocation in case of compromised keys, lost passphrases, replacement of a key and in cases when a key should not be used anymore.

2 Archiving and backing up key pairs

2.1 Backup media

In contrast to classical data security, which is mostly done without encryption, private key material may not be encrypted without additional measures. In addition to organisational questions such as

- who collects / backs up key material, and
- who is permitted subsequent access to key material under what circumstances,

The question about suitable backup media and storage sites needs to be answered. Here, the selection is based on the highest conceivable level of security within the company.

Finally, it is about central access to the data pool most worthy of protection. Both the key pair and the passphrase associated with and matching this key pair must be constantly safeguarded. There are the following possibilities:

- Paper print-out: The medium's proven long-term durability speaks in its favour. On the other hand, the passphrase being printed on paper speaks against it. It makes no sense without additional medium back up (e.g. in a bank vault). OCR systems obviate the tedious, error-prone typing work when accessing.
- Key material on DVD-R, USB stick, or other removable electronic media: The avoidance of media disruption facilitates the handling of the key material. Since the passphrases are also backed up, don't use them without encryption of the data by means of a suitable software; otherwise, it will create be a big security hole! The medium, in turn, belongs in a protected area such as a safe.
- Key material in key containers: Key containers address the technical challenge of backing up and archiving key material and passphrases. These containers can then be secured in traditional ways and also stored externally (e.g. in a bank vault). This version offers the best compromise between security and manageability for most small and medium-sized companies.
- Electronic key management solutions: Large, decentralised companies often coexist poorly with a central solution for key management. Here, appropriate enterprise solutions are an option. However, the expense of introduction is correspondingly large.

For whichever version you decide on, please keep in mind that the security of your encryption solution depends critically on the reasonable backing up of key pairs along with passphrases. Here, biometric access solutions can once again increase security.

2.2 Approach to key archiving

Backing up existing key material

This process is thoroughly explained in section 5.

Backing up newly created key material

1. The key pair is created with a high-quality passphrase and tested as well as backed up with this passphrase.
2. The passphrase is changed in a way to be communicated to the user.
3. The user may change the passphrase once again in a way agreeable to him.

Important note

By deleting the key files, you may permanently lose access to the encrypted emails!

2.3 Support from gpg4o

gpg4o supports administrators and users equally when creating and using key pairs. gpg4o's key management is thoroughly described in the *manual* from gpg4o. All of the tasks that the user can reasonably conduct can be conducted in key management.

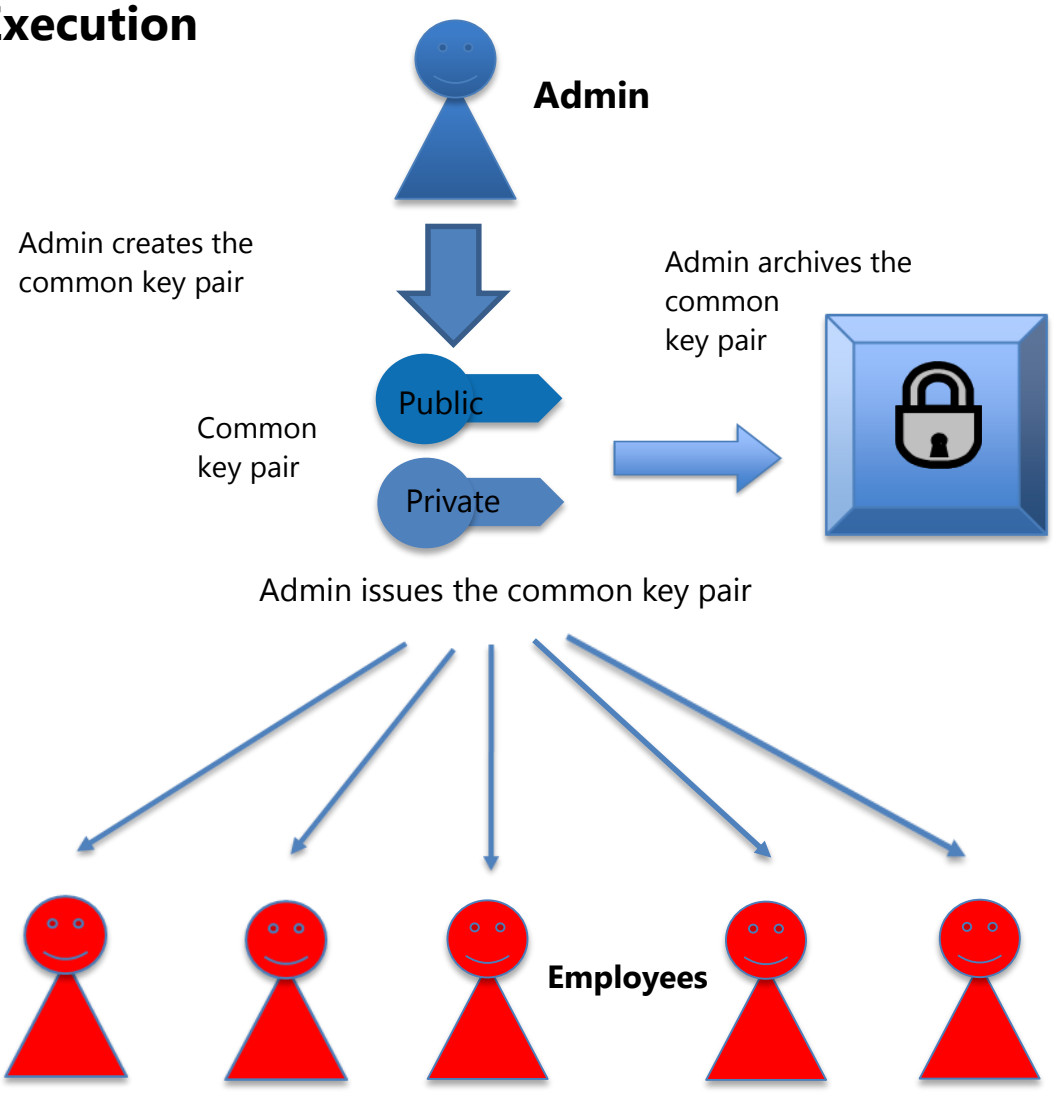
For administrators who would like to create a large number of keys in the company, gpg4o offers a batch function, which is described in the *Administrator's Manual*.

3 Issuing a common key pair

3.1 Classification

Administrative effort:	low
User effort:	low
Security level:	moderate
Utility for email signatures:	low to absent
Suitable for:	micro companies and role accounts with email

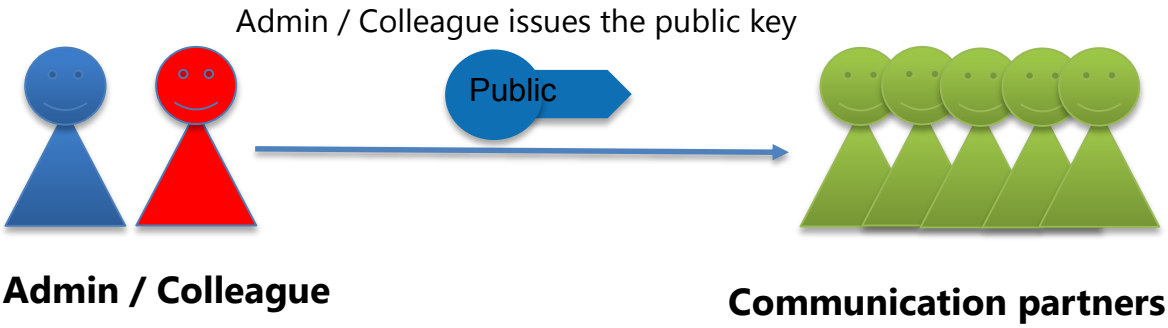
3.2 Execution



The concept is that a common key pair (general key pair) is created and used jointly in the company or work group, or for a role account. Here, all users know the passphrase. This key pair is archived with the passphrase valid at this time. All employees involved receive a copy of the common key, for instance to encrypt their emails and to sign new emails.

An authorised person ('administrator') creates, archives, and issues the common key pair to the users involved. Please note: if several users use a key pair, then the use of the private key to sign emails is of very limited benefit. Thus, the email's actual sender cannot be verified, particularly when role accounts are being used (e.g. personal@company.com). At this point, it cannot be said to which extent this is possible with additional information from the company's email infrastructure.

Your communication partners receive the common public key to encrypt emails to your colleagues.



An employee is free to change the passphrase of *his* copy of the key pair. The archived common key pair remains unchanged by this and can then still be used with the archived passphrase to decrypt the emails received.

Employees cannot create and use their own keys in this concept.

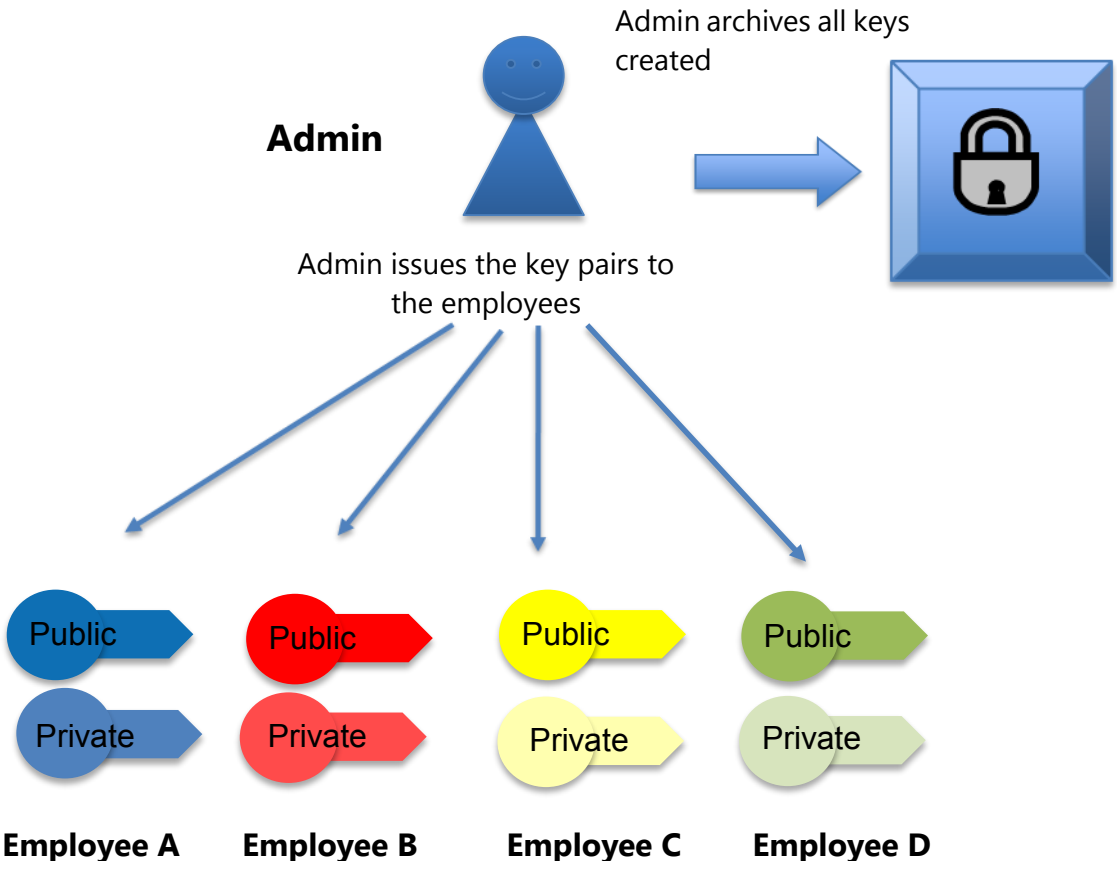
4 Issuing predefined key pairs

4.1 Classification

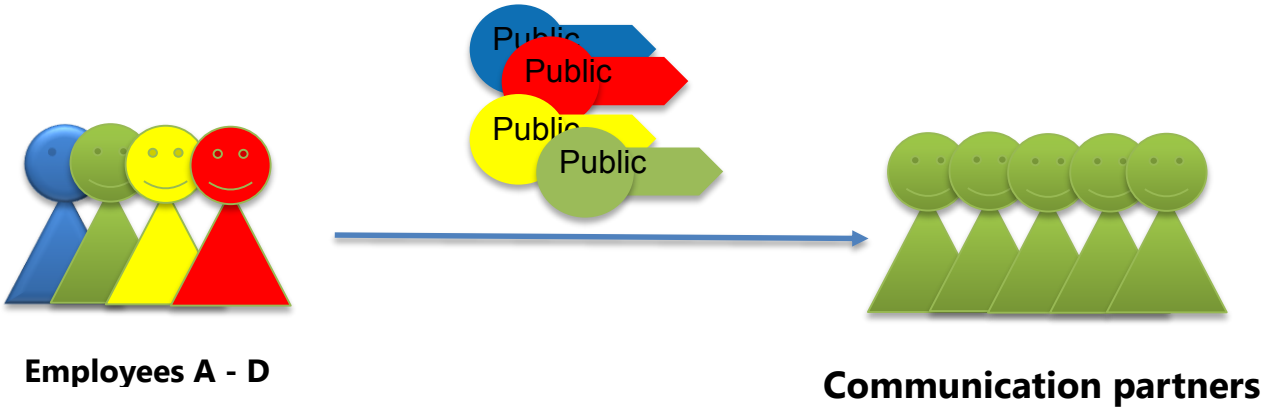
Administrative effort:	moderate
User effort:	low
Security level:	high
Utility for email signatures:	high
Suitable for	all companies

4.2 Execution

1. An authorised employee within the company (“admin”) creates a key pair with a secure passphrase for each employee.
2. The key pair is archived with the predefined passphrase.
3. The key pair is subsequently issued to the employee.
4. The employee can/should change the predefined passphrase.



Employee issue their public keys



Employees cannot create and use their own keys in this concept.

5 Backing up already existing key pairs

5.1 Cassification

Administrative effort:	high
User effort:	low
Security level:	high
Utility for email signatures:	high
Suitable for	companies with existing keys

Insofar as key pairs already exist within the company that are to be used further or possibly installed, or even withdrawn, as part of an information security strategy, they must be collected together and backed up centrally. This is the only way that the motivation issues identified in section 1 can be taken into account.

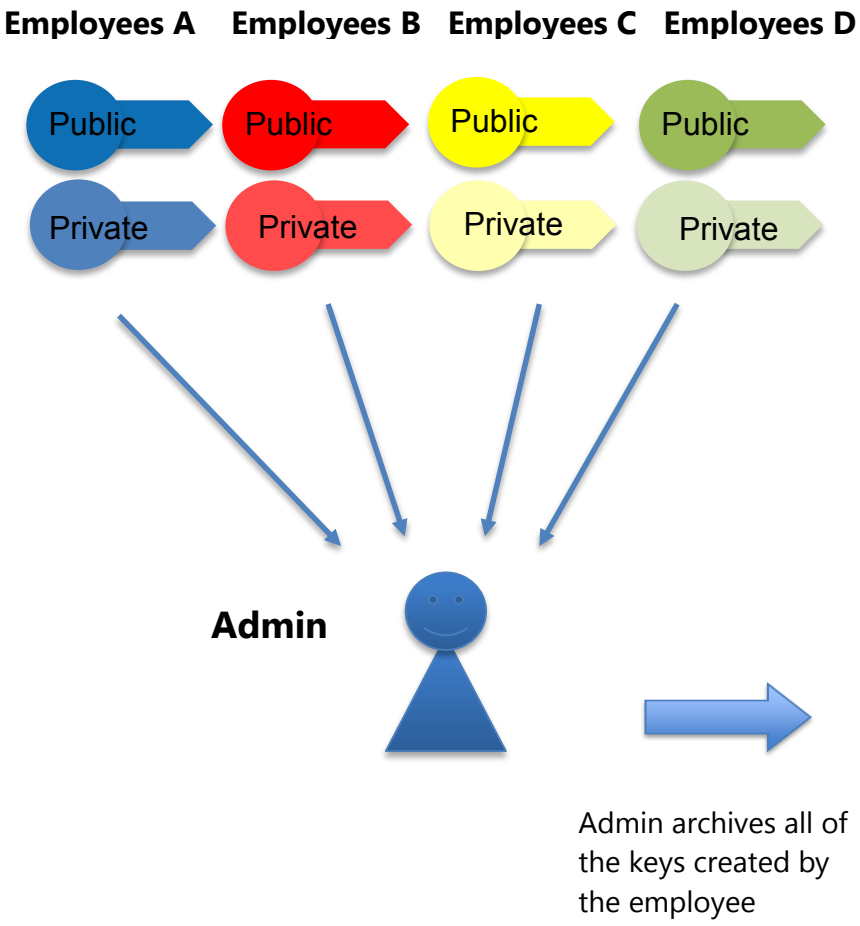
5.2 Execution

1. The user changes the key pair's passphrase to a passphrase prescribed by the administrator.
2. The key pair is tested with the new passphrase.
3. The key pair is exported and archived along with the passphrase.
4. After successful archiving, this key pair's passphrase is changed back to the user's desired passphrase.

The key pairs to be collected together are entered into a previously prepared archive along with the passphrase.

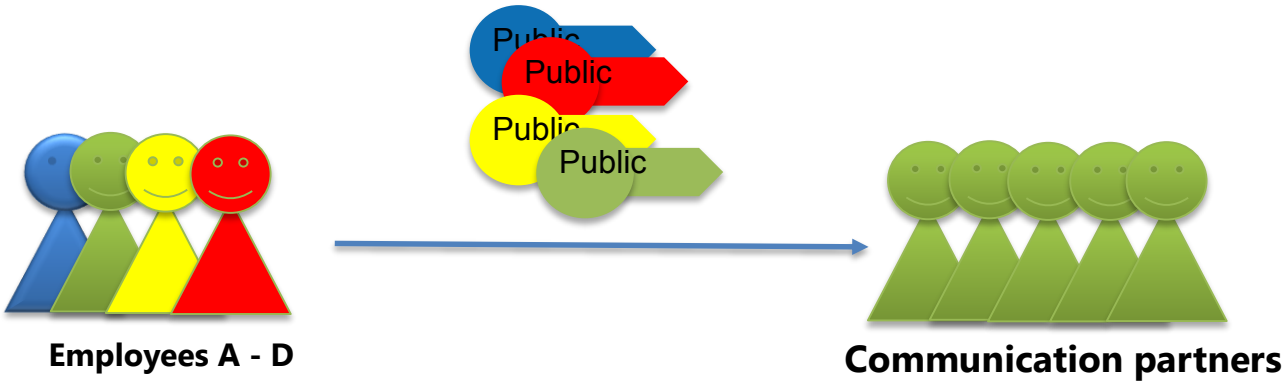
Please note: the requisite processes and tools in the context of an overall strategy are not a part of this document.

After consolidation of the existing key material, additional keys can be created and issued from the central location. It cannot be recommended that the user arbitrarily create and use key material unsupervised. In that way, the company may lose access to important encrypted information.



Admin archives all of the keys created by the employee

Employees issue their public keys



Recommendation: employees may not create or use any new keys after their own key is activated.

6 Contact & Information

The IT-solution provider Giegerich & Partner GmbH based in Dreieich near Frankfurt on the Main specializes in the smooth and safe operation of networks and computer-controlled applications. In addition to consulting and conception the company undertakes the entire execution of IT projects as well as the operation of IT-systems and IT-solutions as outsourcing. Customer-specific individual solutions and the adaptation of IT-standard products to the requirements of companies belong to the strength of the IT-specialist.

From consulting to conception, realization and support –
Giegerich & Partner offers it all.

Further information can be found under: http://www.giepa.de