Giegerich & Partner

gpg4o

Umgang mit OpenPGP-Schlüsselpaaren im Unternehmen

Whitepaper

Inhaltsverzeichnis

1 Einleitung

1.1 Motivation

Um verschlüsselte Daten wieder entschlüsseln zu können, benötigen Sie in jedem Falle den entsprechenden Schlüssel. Keinesfalls können Sie sich darauf verlassen, den Schlüssel einfach errechnen zu können. Dies mag in Ausnahmefällen bei schwacher Verschlüsselung oder Fehlern im Verschlüsselungsalgorithmus funktionieren, ist jedoch nicht die Regel und nur mit entsprechendem Knowhow zu bewerkstelligen. Für die Sicherung von Schlüsselmaterial gibt es daher eine erhebliche Motivation.

- Möglichkeit der Wiederherstellung von Schlüsselmaterial bei versehentlicher Löschung oder bei vergessener Passphrase
- Möglichkeit des Zugriffs auf verschlüsselte Daten durch autorisierte Dritte im Unternehmen
- Möglichkeit des Zugriffs auf verschlüsselte Daten durch autorisierte Behörden (z.B. im Rahmen von GDPdU)
- Möglichkeit des Zurückziehens von verteiltem Schlüsselmaterial, z.B. bei Ausscheiden von Mitarbeitern oder bei Verlust privater Schlüssel.

Der Einsatz von Verschlüsselungstechnologien im Unternehmen bietet einen verbesserten Schutz von wertvollen Knowhows. Dies gilt umso mehr, wenn sensitive Informationen jedweder Art das Unternehmen verlassen (müssen). Hier dient Verschlüsselung bei der Umsetzung von Strategien zur Informationssicherheit und zum Datenschutz.

Allerdings darf nicht wahllos von jedermann irgendwie verschlüsselt werden. In vielen Fällen (gesetzliche Vorschriften, Ausscheiden von Mitarbeitern etc.) müssen Dritte (Geschäftsleitung, ggf. Behörden) Zugriff auch auf von Mitarbeitern verschlüsselte Daten erhalten können. Aus diesem Grunde ist es wichtig, die Verteilung von Schlüsselmaterial im Unternehmen einheitlichen Regeln, möglichst im Rahmen einer Informationssicherheitsstrategie zu unterwerfen.

1.2 Zielsetzung / Abgrenzung

In diesem Dokument werden drei Konzepte zur Verteilung und zur Sicherung im Unternehmen verwendeter Schlüsselpaare beschrieben. Je nach Stand der Organisation im Unternehmen und nach Unternehmensgrösse sind unterschiedliche Varianten denkbar / sinnvoll. Dabei sind Mischformen möglich. Häufig wächst Verschlüsselung ins Unternehmen hinein. Es gilt also, auf einen Status quo aufzusetzen. Die Sicherung vorhandener Schlüsselpaare ist im Abschnitt 5 beschrieben.

Idealerweise wird ein Schlüsselkonzept vor der Einführung von Verschlüsselung im Unternehmen erstellt. In Abschnitt 3 wird ein Verfahren zur Schlüsselverteilung in kleinen und kleinsten Unternehmen bzw. für Arbeitsgruppen und Rollenmodelle beschrieben. Abschnitt 4 beschreibt hingegen den Umgang mit persönlichem Schlüsselmaterial in größeren Unternehmen.

Dieses Dokument beschreibt, wie Sie praktisch im Rahmen einer Strategie zur Informationssicherheit oder zum Datenschutz Schlüsselmaterial im Unternehmen verteilen und sichern. Es ersetzt nicht eigene Planungen des Unternehmens zum Thema Datensicherheit und Datenschutz und will auch keine Anleitung für die Gestaltung von Zugriffsprozessen auf verschlüsselte Daten anbieten. Hierzu ist die Lebenswirklichkeit des Unternehmens ebenso zu beachten wie gesetzliche Vorschriften oder regionale Gepflogenheiten.

Dieses Dokument ersetzt auch keinesfalls die notwendige Schulung von Mitarbeitern beim Umgang mit Schlüsselmaterial.

1.3 Begriffsklärung

gpg4o ist ein Add-In für Outlook 2010® / 2013® zum Verschlüsseln und Entschlüsseln von E-Mails. Es basiert auf dem asymmetrischen Verschlüsselungssystem **OpenPGP**, bei der ein Schlüsselpaar bestehend aus einem öffentlichen und einem privaten Schlüssel zum Einsatz kommt.

Den privaten Schlüssel benötigt gpg4o zum Entschlüsseln von verschlüsselten E-Mails sowie zum Signieren von ausgehenden E-Mails. Dieser private Schlüssel wird durch eine Passphrase (ein Passwort) geschützt, welches bei der Generierung des Schlüsselpaares festgelegt wird. Die Passphrase kann zu einem späteren Zeitpunkt geändert werden. Der öffentliche Schlüssel wird den Kommunikationspartnern zugänglich gemacht um mit Ihnen verschlüsselt zu kommunizieren.

Ein **Schlüsselserver** bietet Zugang zu den öffentlichen Schlüssel, die auf diesen Server veröffentlicht wurden. Ein Schlüsselserver kann auch lokal im Unternehmen eingerichtet werden, um Mitarbeitern, die für eine verschlüsselte Kommunikation notwendigen öffentlichen Schlüssel, zu Verfügung stellen. Einen auf ein Schlüsselserver veröffentlichten Schlüssel kann nicht mehr vom Server gelöscht, aber dieser Schlüssel kann unbrauchbar (mit einem Rückzugszertifikat) gemacht werden.

Es ist sinnvoll bei der Erstellung von Schlüsseln ein Rückzugszertifikat zu erstellen. Damit man diesen Schlüssel zurückziehen kann. Das kann aus den unterschiedlichsten Gründen geschehen.

Beispiele dafür: Schlüssel wurde kompromittiert, Passphrase vergessen, Schlüssel soll ersetzt werden oder der Schlüssel wird nicht mehr benutzt.

2 Archivierung und Sicherung von Schlüsselpaaren

2.1 Sicherungsmedien

Im Gegensatz zur klassischen Datensicherung, die meist unverschlüsselt erfolgt, darf privates Schlüsselmaterial nicht eben ohne zusätzliche Maßnahmen verschlüsselt werden. Neben organisatorischen Fragen wie:

- Wer sammelt / sichert Schlüsselmaterial
- Wer darf unter welchen Umständen gesichertes Schlüsselmaterial benutzen

Gilt es auch, die Frage nach geeigneten Sicherungsmedien und Aufbewahrungsorten zu beantworten. Hierbei orientiert sich die Auswahl an der höchsten im Unternehmen denkbaren Sicherheitsstufe. Wir sprechen schließlich vom zentralen Zugang auf schützenswertesten Datenbestand. Zu sichern sind stets sowohl das Schlüsselpaar als auch eine zu diesem Schlüsselpaar gehörende und passende Passphrase (testen!). Folgende Möglichkeiten bieten sich an:

- Ausdruck auf Papier: Dafür spricht die erwiesenermaßen langfristige Haltbarkeit des Mediums. Dagegen spricht unbedingt, dass auch die Passphrase im Klartext auf Papier gedruckt ist. Ohne zusätzliche Sicherung des Mediums (z.B. in Banktresor) nicht sinnvoll. Im Zugriffsfall sparen OCR-Systeme die lästige und fehleranfällige Tipparbeit.
- Schlüsselmaterial auf DVD-R, USB-Stick oder anderen elektronischen Wechselmedien: Die Vermeidung des Medienbruches erleichtert die Handhabung des Schlüsselmaterials. Da auch die Passphrasen gesichert werden, nicht ohne Verschlüsselung der Daten durch geeignete Software einzusetzen, anderenfalls entsteht ein großes Sicherheitsloch! Das Medium gehört wiederum in einen geschützten Bereich, z.B. Tresor.
- Schlüsselmaterial in Schlüsselcontainer: Schlüsselcontainer lösen die technische Herausforderung zur Sicherung und Archivierung von Schlüsselmaterial und Passphrasen. Diese Container können dann auf herkömmlichem Wege mitgesichert und zusätzlich extern gelagert werden (z.B. Banktresor) Für die meisten kleinen und mittleren Unternehmen bietet diese Variante den besten Kompromiss zwischen Sicherheit und Handhabbarkeit.
- Elektronische Schlüsselmanagementlösungen: Große, dezentral organisierte Unternehmen können oft schlecht mit einer zentralen Lösung zur Schlüsselverwaltung leben. Hier bieten sich entsprechende Enterprise-Lösungen an. Allerdings ist hier der Einführungsaufwand entsprechend.

Für welche Variante Sie sich auch entscheiden: Bitte führen Sie sich vor Augen, dass von der sinnvollen Sicherung der Schlüsselpaare samt Passphrasen die Sicherheit Ihrer Verschlüsselungslösung maßgeblich abhängt. Biometrische Zugangslösungen können hierbei die Sicherheit nochmals erhöhen.

2.2 Vorgehensweise bei der Schlüsselarchivierung

Sicherung vorhandenen Schlüsselmaterials

Dieser Ablauf ist ausführlich im Abschnitt 5 erläutert.

Sicherung neu erzeugten Schlüsselmaterials

1. Das Schlüsselpaar wird mit einer sicheren Passphrase erzeugt und mit dieser Passphrase getestet sowie gesichert.
2. Die Passphrase wird auf eine dem künftigen Benutzer mitzuteilende geändert
3. Ggf. wird die Passphrase vom Anwender nochmals in eine ihm genehme geändert.

Wichtiger Hinweis

Durch das Löschen von Schlüsseldateien verlieren Sie dauerhaft den Zugriff auf die verschlüsselten E-Mails!

2.3 Unterstützung durch gpg4o

gpg4o unterstützt Administratoren und Anwender gleichermaßen bei der Erstellung und Verwendung von Schlüsselpaaren. Die Schlüsselverwaltung von gpg4o ist ausführlich im *Handbuch* von gpg4o beschrieben. Alle vom Anwender sinnvoll durchführbaren Aufgaben können in der Schlüsselverwaltung durchgeführt werden.

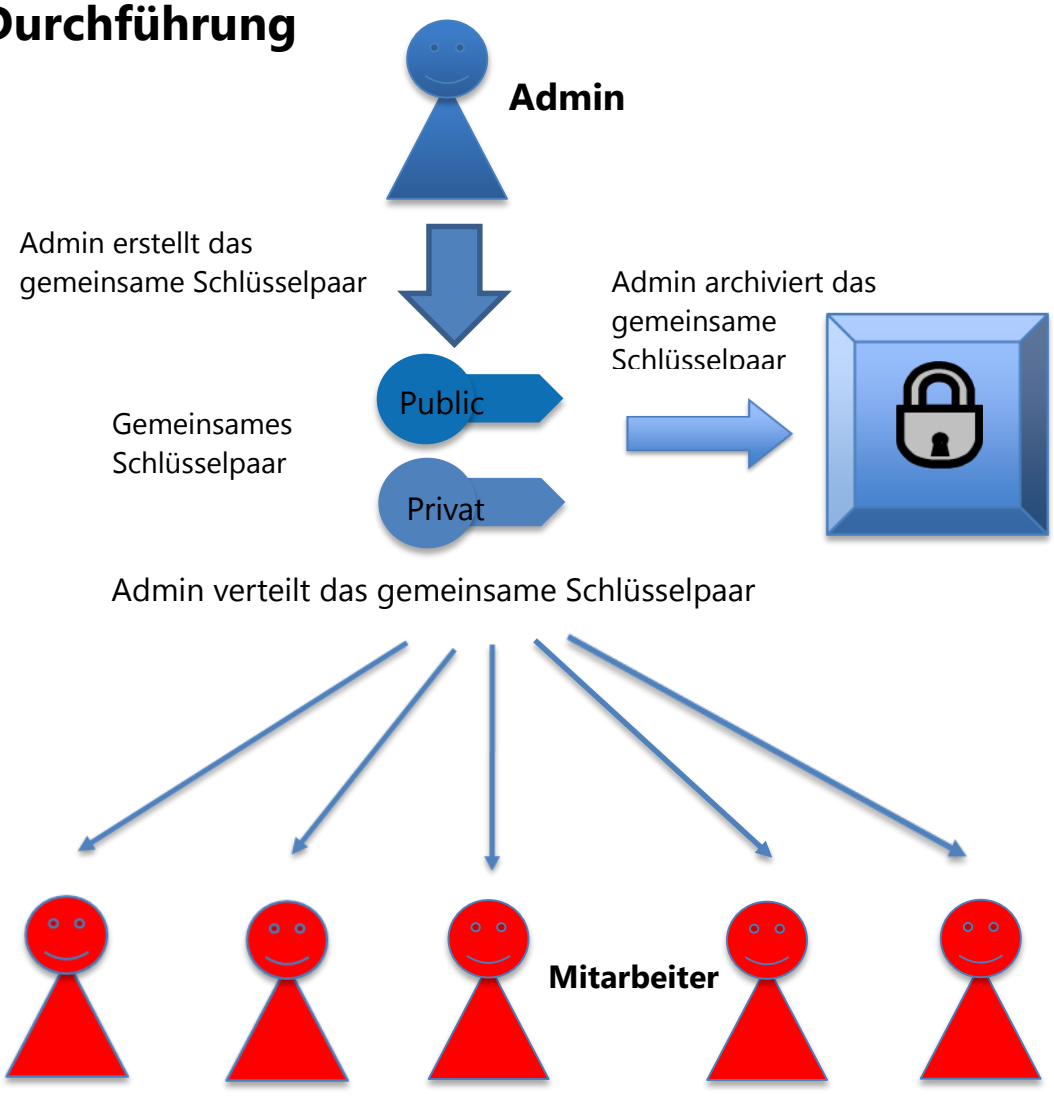
Für Administratoren, welche im Unternehmen eine größere Anzahl von Schlüsseln erzeugen möchten, bietet sich die Batchfunktion von gpg4o an, welche im *Administratorhandbuch* beschrieben ist.

3 Verteilen eines gemeinsamen Schlüsselpaares

3.1 Einordnung

Aufwand Administration:	Gering
Aufwand Anwender:	Gering
Sicherheitsniveau:	Mäßig
Nutzen für E-Mail Signaturen:	Gering bis nicht vorhanden
Geeignet für:	Kleinstunternehmen sowie Rollenaccounts bei E-Mail

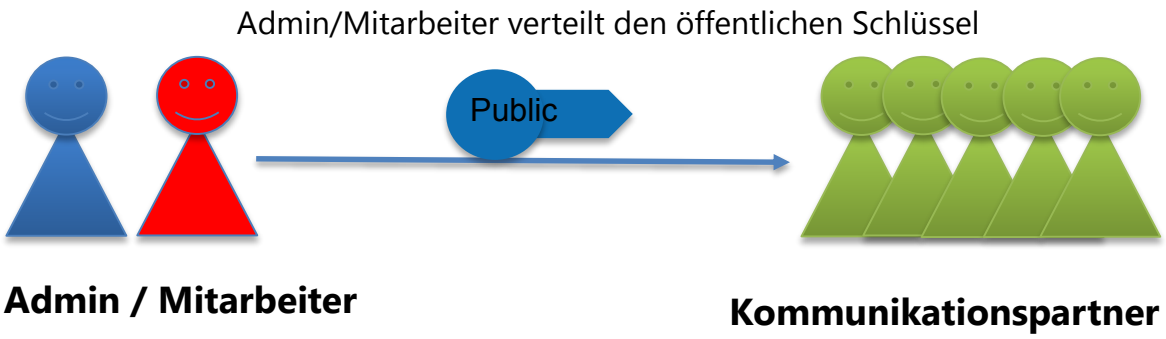
3.2 Durchführung



Das Konzept besteht darin, dass im Unternehmen / einer Arbeitsgruppe / für einen Rollenaccount ein gemeinsames Schlüsselpaar (General-Schlüsselpaar) erstellt und gemeinsam genutzt wird. Die Passphrase ist dabei allen Anwendern bekannt. Dieses Schlüsselpaar wird mit der zu diesem Zeitpunkt gültigen Passphrase archiviert. Alle betroffenen Mitarbeiter erhalten eine Kopie des gemeinsamen Schlüssels, um z.B. ihre E-Mails zu entschlüsseln und neue E-Mails zu signieren.

Das gemeinsame Schlüsselpaar wird durch eine befugte Person („Administrator") erstellt, archiviert und an die betroffenen Anwender verteilt. Bitte beachten: Verwenden mehrere Anwender ein Schlüsselpaar, so ist die Verwendung des privaten Schlüssels zum Signieren von E-Mails nur von sehr begrenztem Nutzen. Der tatsächliche Absender der E-Mail kann, insbesondere bei der Verwendung von Rollenaccounts (z.B.: personal@unternehmen.de) so nicht verifiziert werden. Inwieweit das mit zusätzlichen Informationen aus der E-Mail-Infrastruktur des Unternehmens möglich ist, kann an dieser Stelle nicht gesagt werden.

Ihre Kommunikationspartner erhalten den öffentlichen gemeinsamen Schlüssel, um E-Mails an Ihre Mitarbeiter zu verschlüsseln.



Einem Mitarbeiter steht es frei, die Passphrase *seiner* Kopie des Schlüsselpaares zu ändern. Das archivierte gemeinsame Schlüsselpaar bleibt dadurch unverändert und kann dann trotzdem mit der archivierten Passphrase verwendet werden, um die empfangenen E-Mails zu entschlüsseln.

Die Mitarbeiter dürfen bei diesem Konzept keine eigenen Schlüssel erstellen und verwenden.

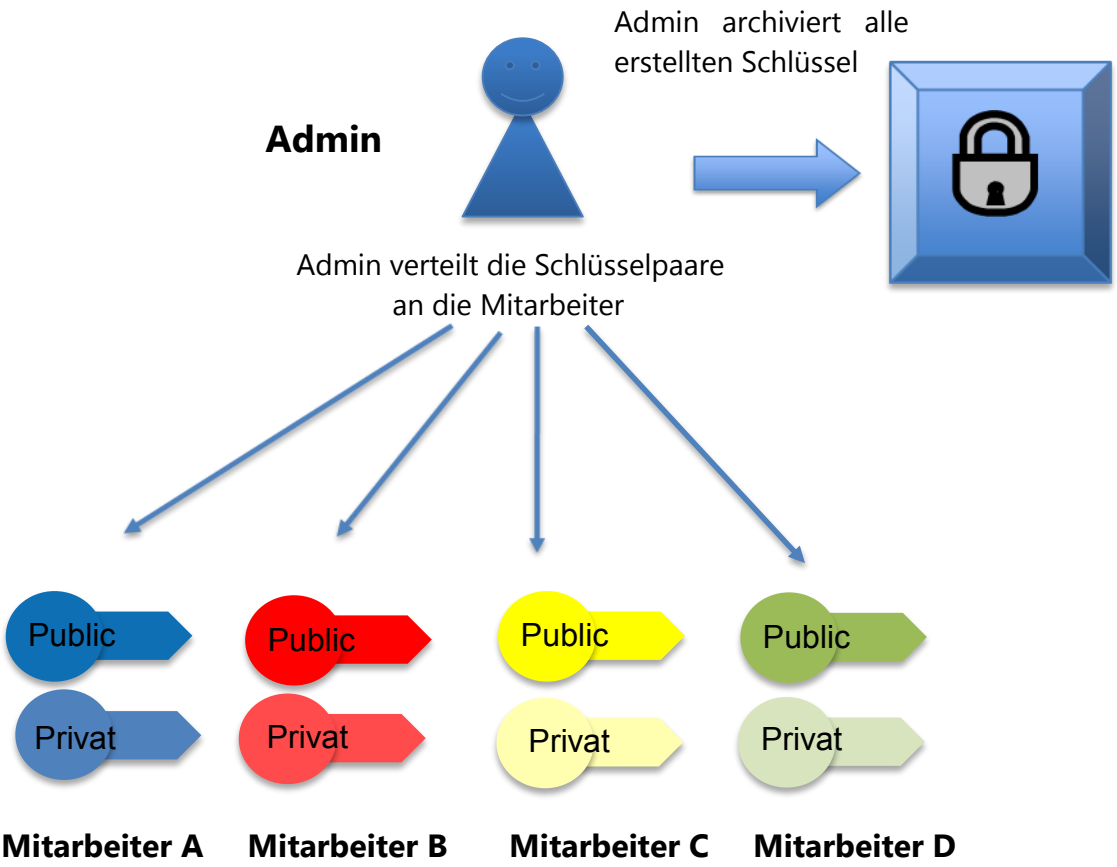
4 Verteilung vorgegebener Schlüsselpaare

4.1 Einordnung

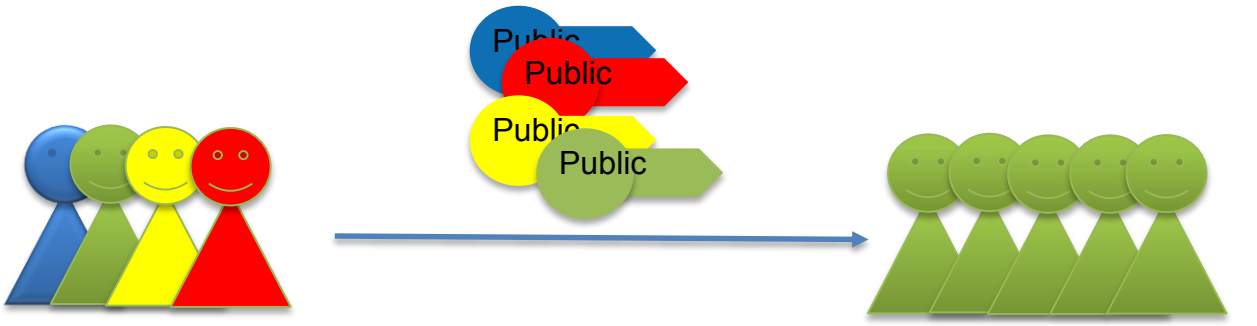
Aufwand Administration:	Mäßig
Aufwand Anwender:	Gering
Sicherheitsniveau:	Hoch
Nutzen für E-Mail Signaturen:	Hoch
Geeignet für:	Alle Unternehmen

4.2 Durchführung

1. Ein autorisierter Mitarbeiter im Unternehmen („Admin“) erstellt für jeden Mitarbeiter ein Schlüsselpaar mit einer sicheren Paarphrase.
2. Das Schlüsselpaar wird mit der neuen Passphrase archiviert.
3. Das Schlüsselpaar wird an den Mitarbeiter ausgegeben.
4. Der Mitarbeiter soll die vorgegebene Passphrase ändern.



Mitarbeiter verteilen Ihren Öffentlichen Schlüssel



Mitarbeiter A - D

Kommunikationspartner

Die Mitarbeiter dürfen bei diesem Konzept keine eigenen Schlüssel erstellen und verwenden.

5 Sichern bereits vorhandener Schlüsselpaare

5.1 Einordnung

Aufwand Administration:	Hoch
Aufwand Anwender:	Gering
Sicherheitsniveau:	Hoch
Nutzen für E-Mail Signaturen:	Hoch
Geeignet für:	Unternehmen mit vorhanden Schlüsseln

Insoweit im Unternehmen bereits Schlüsselpaare vorhanden sind, die weiter verwendet oder ggf. im Rahmen einer Informationssicherheitsstrategie eingebaut oder gar zurückgezogen werden sollen, muss die erste Maßnahme sein, diese zentral einzusammeln und zu sichern. Nur so kann der in Abschnitt 1 aufgezeigten Motivationslage umfänglich Rechnung getragen werden.

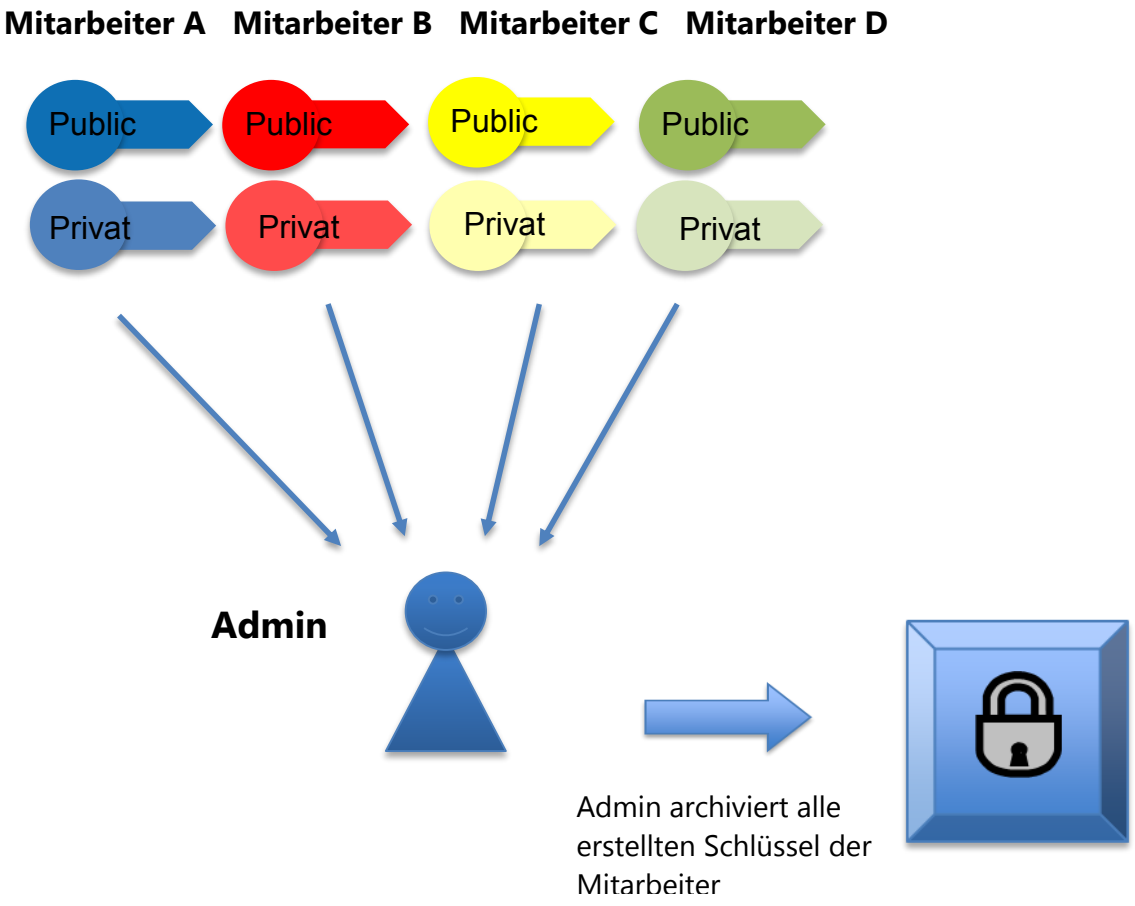
5.2 Durchführung

1. Die Passphrase des Schlüsselpaares wird vom Benutzer auf eine vom Administrator vorgegebene Passphrase geändert.
2. Das Schlüsselpaar wird mit der neuen Passphrase getestet.
3. Das Schlüsselpaar wird exportiert und samt Passphrase archiviert.
4. Nach erfolgter Archivierung wird die Passprase dieses Schlüsselpaares wieder in die gewünschte Passprase des Anwenders geändert.

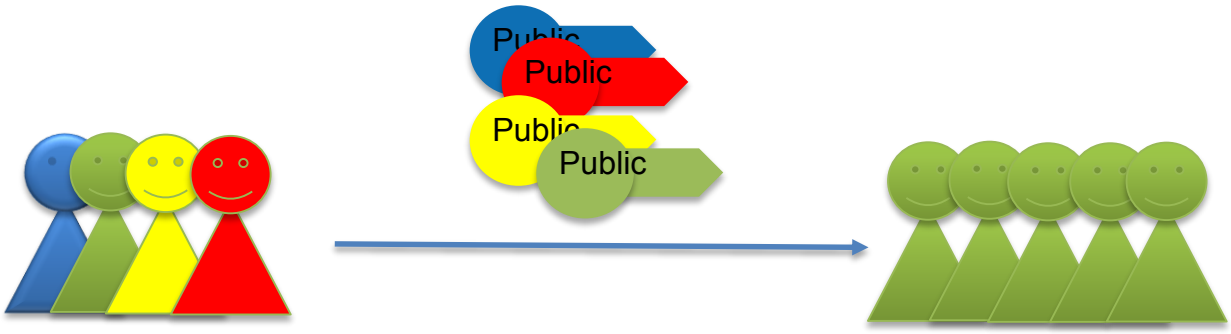
Die einzusammelnden Schlüsselpaare werden so in ein vorher vorbereitetes Archiv samt Passphrase eingepflegt.

Bitte beachten: Die dafür nötigen Prozesse und Werkzeuge im Rahmen einer Gesamtstrategie sind nicht Gegenstand dieses Dokumentes.

Nach der Konsolidierung des vorhandenen Schlüsselmaterials können von zentraler Stelle weitere Schlüssel erstellt und ausgegeben werden. Es kann nicht empfohlen werden, dass Anwender unbeaufsichtigt und eigenmächtig Schlüsselmaterial erstellen und verwenden. So geht dem Unternehmen der Zugriff auf wesentliche, verschlüsselte Informationen eventuell verloren.



Mitarbeiter verteilen Ihren Öffentlichen Schlüssel



Empfehlung: Die Mitarbeiter dürfen nachdem ihr eigener Schlüssel archiviert ist, keine neuen Schlüssel erstellen bzw. verwenden.

6 Kontakt & Info

Der IT-Lösungsanbieter Giegerich & Partner GmbH mit Sitz in Dreieich bei Frankfurt/Main hat sich auf Lösungen für den reibungslosen und sicheren Betrieb von Netzwerken und computergesteuerten Anwendungen spezialisiert. Neben der Beratung und Konzeption übernimmt das Unternehmen die komplette Ausführungen von IT Projekten sowie den Betrieb von IT-Systemen und -Lösungen im Outsourcing. Kundenspezifische Individuallösungen und die Anpassung von IT-Standardprodukten an die Bedürfnisse von Unternehmen gehört zu den Stärken des IT-Spezialisten.

Alles aus einer Hand
Beratung. Konzeption. Ausführung und Support.

Weitere Informationen unter: http://www.giepa.de