GoCrypt

Hochsichere Dateiverschlüsselung und einfacher Versand, großer Bedienkomfort für die Nutzer

Für die Dateiverschlüsselung und den digitalen Transport von Daten gibt es viele Möglichkeiten, sei es die E-Mail-Verschlüsselung mit PGP oder mit S/MIME oder eigene Cloud-Anwendungen. Die meisten dieser Angebote haben einen großen Nachteil: sie sind nutzerunfreundlich in der Bedienung, Nutzer sehen sich mit privaten / öffentlichen Schlüssel, Signierung, Zertifikaten... konfrontiert. Die technische Einrichtung ist aufwendig und kompliziert, ob die Empfängerseite auch alle notwendigen Sicherheitsschritte realisiert hat, ist nicht bekannt. Hinzu kommt, dass es nicht bekannt ist, über welche Server, Länder die E-Mails transportiert werden. Die Akzeptanz bei Nutzern ist aufgrund der zusätzlichen Arbeit nicht sonderlich hoch.

Alternative Methode zur Verschlüsselung von E-Mails

Hybride Verschlüsselungstechnik

Das haben wir, als Entwickler von GoCrypt, zum Anlass genommen eine lokale Datei- und oder Textnachrichtverschlüsselung mit anschließendem Datentransport zu entwickeln, für den Nutzer intuitiv und einfach zu bedienen, auf der Ebene der Datenschutz-Grundverordnung (DSGVO). Mit dem Programm GoCrypt für Windows muss der Nutzer selbst keine Schlüsselpaar Generierung und Verteilung des öffentlichen Schlüssels vornehmen, das erledigt GoCrypt mit der einmaligen Registrierung.

Der Nutzer wählt den Empfänger und die zu verschlüsselten Dateien aus (Drag & Drop) und klickt auf den Go Knopf. Das ist alles!

GoCrypt hat keinesfalls die Sicherheit der Daten aufgrund des Komforts vernachlässigt. GoCrypt arbeitet mit der **hybriden Verschlüsselungstechnik** und benutzt dabei die weltweit anerkannten Techniken wie symmetrische AES 256 Bit Dateiverschlüsselung, die asymmetrische RSA 2048 Bit Schlüsselgenerierung, das Signieren, die Integritätsprüfung sowie die Authentifizierung. Darüber hinaus hat GoCrypt mit der Einbindung von FIDO Token auch einen noch höheren Sicherheitslevel im Angebot, um auch eine mobile Nutzung (Home, Office, Notebook) erreichen zu können. Zur FIDO Alliance gehören die größten Tech-Konzerne, wie zum Beispiel Microsoft, Google, Intel, Apple und viele mehr. Unser FIDO Token unterstützt nicht nur Fido2 oder Fido U2F sondern hat auch noch die Applets Open PGP, Smart Card (PIV), HOPT integriert. Damit kann der Fido Token nicht nur die GoCrypt Verschlüsselung bedienen, sondern ist auch noch zum Anmelden / Authentifizieren an vielen Webseiten (Google, usw) oder zum passwortlosen Anmelden am Computer einsetzbar.

Für Anwender die keinen FIDO Token einsetzen wollen, bietet GoCrypt eine Version ohne FIDO an, natürlich lassen sich die beiden Versionen miteinander kombinieren.

GoCrypt ist einfach zu bedienen, der Schlüsselaustausch erfolgt automatisch.

„Zero-Knowledge" Prinzip. Niemand, außer dem Empfänger hat Einblick in die verschlüsselten Dateien – nicht einmal GoCrypt!

DSGVO-konform, entsprechend geltender Gesetze in Deutschland und EU.

Höchste Sicherheit, Option zwischen verschiedene Sicherheitsstufen (FIDO)

Made in Germany, hostet auf deutschem Server

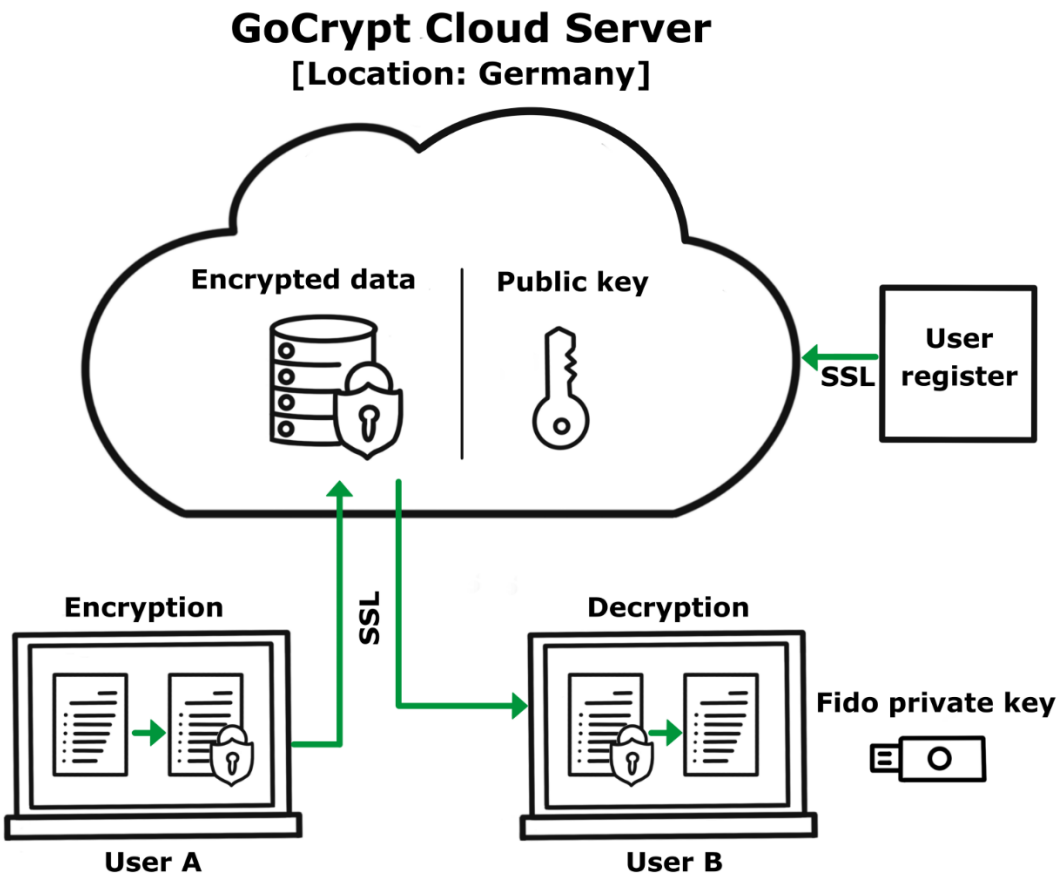
Wie es funktioniert:

1. Datei senden: Benutzer A möchte eine Datei über das Internet an Benutzer B übermitteln.

2. Verschlüsseln & Übertragen: Benutzer A verschlüsselt die Datei lokal auf seinem Computer mit GoCrypt und sendet diese an den GoCrypt-Server. Die Originaldatei verbleibt auf dem Rechner.

3. Benachrichtigung: Benutzer B erhält sofort eine Benachrichtigung über die bereitgestellte Datei.

4. Herunterladen und Entschlüsselung: Benutzer B lädt die verschlüsselten Dateien herunter. Nach dem Herunterladen werden diese automatisch lokal auf seinem Computer mit GoCrypt entschlüsselt.



Neben der Verschlüsselung steht die Benutzerfreundlichkeit im Vordergrund:
Mit GoCrypt ist alles mit nur wenigen Klicks erledigt:

- Sie wählen Ihre Dateien und oder Textnachricht aus.
- Sie bestimmen den Empfänger.
- Sie klicken auf "GO" und GoCrypt erledigt den Rest.

Sofortige Benachrichtigungen:
Der Empfänger wird sofort benachrichtigt, wenn eine Datei / Nachricht für ihn bereitsteht. Ein Klick, und die verschlüsselte Datei / Nachricht wird heruntergeladen und anschließend automatisch auf seinem Computer entschlüsselt.

Sicherheit bei jedem Schritt:
Während der Registrierung generiert GoCrypt ein einzigartiges Schlüsselpaar für jeden Benutzer:

- **Öffentlicher Schlüssel:** Wird auf dem GoCrypt Server gespeichert.
- **Privater Schlüssel:** Wird sicher lokal auf Ihrem Computer gespeichert. Für Professional- / Premium-Nutzer kann der private Schlüssel mit der dazugehörigen E-Mail Adresse im Fido Token gespeichert werden.

- Die Ver- und Entschlüsselung der Dateien findet **nur** auf dem lokalen Computer statt. Die Originaldateien werden **nicht** unverschlüsselt über das Netzwerk / Internet gesendet/empfangen, sondern nur verschlüsselt. Es gibt keine Möglichkeit, unsere Server oder unser Netzwerk anzugreifen (z. B. mit Traffic Sniffers), um an die Originaldateien zu gelangen. Auch öffentliche Netze bieten keine Schwachstellen für gesendete/empfangene Dateien.

- Gesendete Dateien können nur vom Empfänger in den Originalzustand zurückversetzt werden. Auch der Absender kann die Datei nach der Verschlüsselung **nicht mehr entschlüsseln**. Die Verschlüsselungstechnik ist so ausgelegt, dass niemand sonst die Datei entschlüsseln kann.

- Die Dateien werden mit dem AES-Algorithmus (256 Bit) ver- und entschlüsselt. Der symmetrische Schlüssel für den AES-Algorithmus wird dann mit einem 2048-Bit-RSA-Schlüssel verschlüsselt.

- Ein theoretischer Brute-Force-Angriff auf einen 2048-Bit-RSA-Schlüssel würde beim heutigen Stand der Computertechnik bis zu 300 Billionen Jahre dauern.

- Die Verwendung eines Fido-Schlüssels erhöht die Sicherheit zusätzlich:

- Schutz vor Phishing
- Keine gemeinsamen Geheimnisse, der private Schlüssel verlässt nie den Fido-Key
- Man-in-the-Middle-Angriffe werden mit dem Fido Key erschwert.
- Physische Sicherheit mit dem Fido Key im Vergleich zu nur Passwörtern
- Authentifizierung und Integritätsprüfung mit dem Fido Key

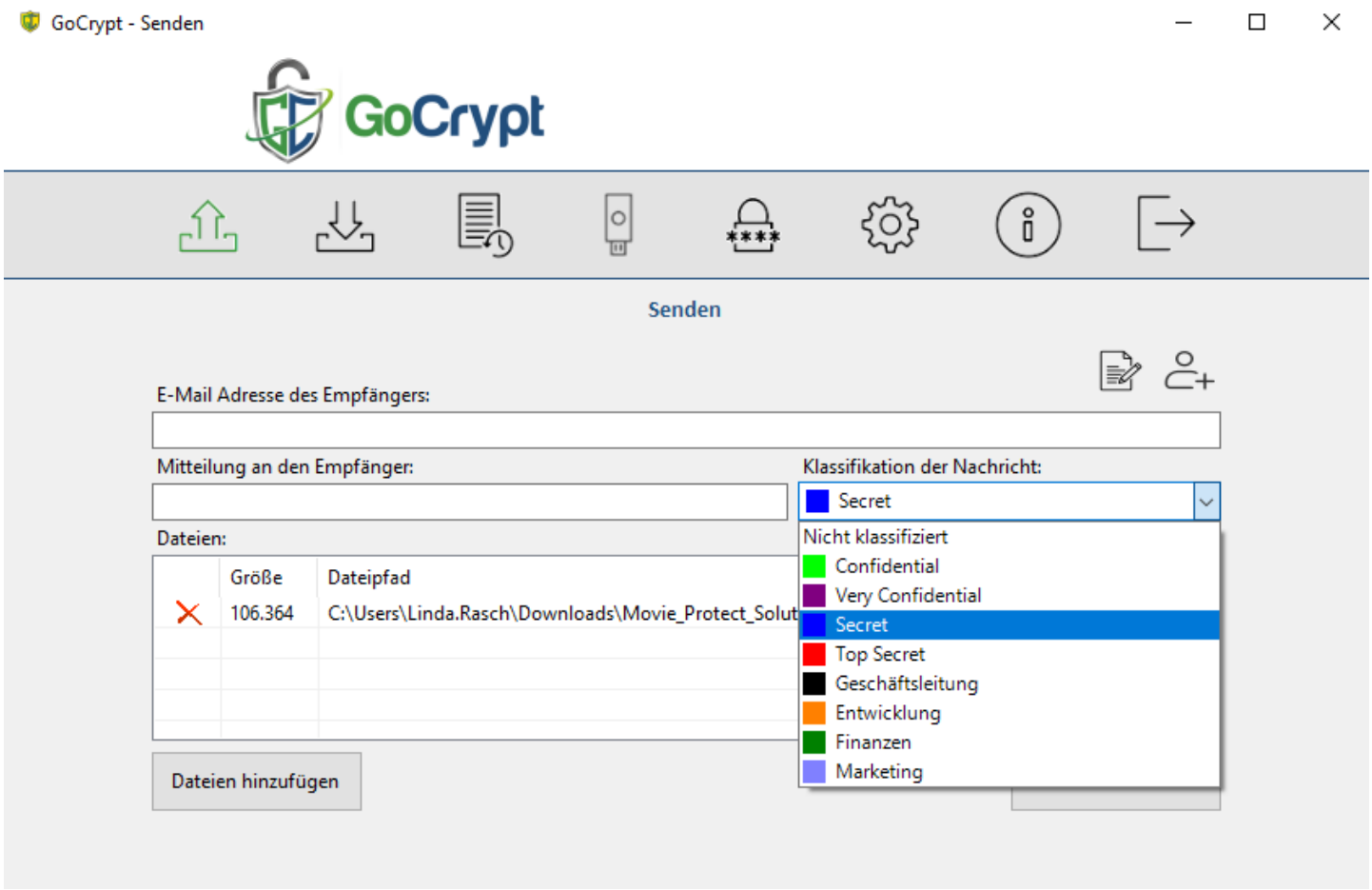
GoCrypt unterstützt die Datenklassifikation beim Teilen von Dateien

Die Datenklassifikation spielt eine entscheidende Rolle in der Zugriffssteuerung, da sie dabei hilft, sicherzustellen, dass nur autorisierte Benutzer Zugang zu bestimmten Daten basierend auf ihrer Klassifizierung haben.

Oftmals wird Datenklassifizierung nachträglich auf bereits bestehende Dokumente angewendet. Die GoCrypt Klassifizierung von bestehenden Dateien ermöglicht es Organisationen, das Teilen von sensiblen Dateien zu definieren, die auf den Sensibilitätsgrad der Daten abgestimmt sind. Daten werden typischerweise in Kategorien wie öffentlich, intern, vertraulich und streng vertraulich eingeteilt. Basierend auf diesen Klassifikationen können beim Teilen von Dateien entsprechende Zugriffsrechte zugewiesen werden, sodass beispielsweise nur Mitarbeiter mit der notwendigen Berechtigung auf vertrauliche oder streng vertrauliche Informationen zugreifen können.

Durch die Einschränkung des Zugriffs auf sensible Daten gemäß ihrer Klassifikation können Organisationen das Risiko von Datenverletzungen und unerlaubtem Zugriff reduzieren. Dies ist besonders wichtig für Daten, die personenbezogene Informationen, Geschäftsgeheimnisse oder andere Arten von sensiblen Informationen enthalten.

Viele Datenschutzvorschriften fordern, dass Unternehmen angemessene Maßnahmen ergreifen, um sensible Informationen zu schützen. Durch die Anwendung von Datenklassifikation in der Zugriffssteuerung können Organisationen nachweisen, dass sie proaktive Schritte unternommen haben, um die Sicherheit und Vertraulichkeit von Daten zu gewährleisten, was zur Einhaltung von gesetzlichen und branchenspezifischen Anforderungen beiträgt.



Textnachricht

Schreibe Textnachrichten, füge Tabellen, Bilder, Videos dort ein. Drücke auf Speichern und die Mitteilung wird automatich an das Sende-Fenster weitergeleitet.