Krypto-Schutz für Ihre digitale Sicherheit

OpenPGP + S/MIME
End-2-End-Encryption

www.gnupg.com

Die sicherste Art der Nachrichtenübertragung


```
-----BEGIN PGP MESSAGE-----

kA0DAAgW4/3/IY5FtysBy11iAF9Q3S8KCkdudVBHIC0gZGllIHNpY2hlcnN0ZSBB
cnQgZGVyIE5hY2hyaWNodGVuw7xiZXJ0cmFndW5nCgpXZWl0ZXJlIGluZm9zOiB3
d3cuZ251cGcuY29tCgqJAfUEABYIAZ0WIQTB00tpIZ5K7sC6HCHj/f8hjkW3KwUC
X1DdL8C+JgCYMwRU5NYCFgkrBgEEAdpHDwEBB0D16DIBI1sikMsiN5rSt/gjzms6
ZT7KU25dh0+e5wn8zbQnV2VybmVyIEtvY2ggKHdoZWF0c3RvbmUgY29tbWl0IHNp
Z25pbmcpiH8EExYIACcFAlTk1gICGwMFCRLMAwAFCwkIBwIGFQgJCgsCBBYCAwEC
HgECF4AACgkQ4/3/IY5FtytAcgD/TaGyWy+kCd2A3s6/wew9LQx1fcEejlHQrkYS
MC6RrN4BAJdNgnoEqIdiGZIgf5TsGl+wj9Qhycrrn0ljrSBfxEkAuDgEVsB9QhIK
KwYBBAGXVQEFAQEHQLKYNXqUd9d/MQYvfGMO+EBndtcW6lYBAtD0sFMkq9JdAwEI
B4hhBBgWCAAJBQJWwH1CAhsMAAoJEOP9/yGORbcrP9AA/0Rbr/THO9LVhqiOk/RI
6vYRd6N5yWINECw5vnTXTZkiAP9m2/gdOTSRvVjSNaIRAMXU1ggrSEGt1l730gJq
auNdCAAKCRDj/f8hjkW3K0A8AP4r+D4pM/YTX74/b7OOmr2oz/xvXBaXgKFnjiUf
hPS3lQEA9t3o0N1TAeTdC1A6pKRxgriCM1Bfu2KSTOi6qlXS5Ao=
-----END PGP MESSAGE-----
```


Bewährt und Sicher

Seit 1997 funktioniert der GnuPG-Verschlüsselungscode und bietet einen unerreichten Schutz vor Nachrichtenüberwachung und unberechtigter Datenspeicherung durch Dritte. Ein Code von dem es heißt, dass es selbst der National Security Agency (NSA) bis heute nicht gelungen ist, diesen zu entschlüsseln.

Ihr Schutzschild bei der Mail- und Datenübertragung

Flexibel
Vereinheitlicht OpenPGP und S/MIME

Universell
Unterstützt Windows, Linux und macOS

Intuitiv
Integriert E2EE in Ihr gewohntes Arbeitsumfeld

Langlebig
Garantiert Sicherheitsupdates und Support

Sicher
Bietet zugelassenen Schutz für VS-NfD

Transparent
Überzeugt durch Open Source

Unabhängig
Entbindet Sie von Vendor-Lock-In

Digitaler Werterhalt

Die Idee der freien Verschlüsselung wurde vom FSFE[1]-Mitgründer und Geschäftsführer der g10 Code GmbH Werner Koch begonnen. Der Firmenname nimmt Bezug auf Artikel 10 Grundgesetz[2].

[1] Free Software Foundation Europe, gegründet im März 2001

[2] Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich

Werner Koch
Geschäftsführer
GnuPG-Maintainer

+49 2104 493 879 2
werner.koch@gnupg.com

Universell in der Anwendung – flexibel im Einsatz

Warum GnuPG

Wir schützen Ihre Daten indem wir eine programmübergreifende Ende-zu-Ende-Verschlüsselung ermöglichen, mit der Sie sowohl Mails, Nachrichten, Dokumente etc. ver- und entschlüsseln, als auch digitale Signaturen erzeugen und prüfen können. Die Endpunkte der Kommunikation können dabei je nach Einsatz Einzelpersonen, Gruppen, Meeting- oder Cloud-Teilnehmer sein.

Mails / Anhänge

Handhaben Sie Krypto-Mails so unkompliziert wie Standard-Mails

Daten / Ordner

Verschlüsseln Sie Ordner jeder Datengröße und Dokumente jeden Formats

Chat- / Messenger-Dienste

Kommunizieren Sie sicher über alle etablierten Messenger- und Meeting-Dienste

Cloud- / Filesharing-Dienste

Archivieren, transferieren oder hosten Sie große Datenmengen im Krypto-Format

Zertifikatsverwaltung

Nutzen Sie die vielfältigen Möglichkeiten der automatisierten Zertifikatsverwaltung

Der Krypto-Alleskönner

Wir vereinheitlichen OpenPGP und S/MIME zu einer flexiblen Lösung. Im Gegensatz zu einer Transportverschlüsselung oder einer Gateway-Lösung ist es mit uns nicht möglich, Mails auf dem Transportweg zu entschlüsseln – auch außerhalb Ihres geschützten Netzwerks und ohne VPN kommunizieren Sie mit GnuPG stets sicher.

Intuitive Benutzerführung durch Systemintegration

Desktop-PlugIn

Unsere Sicherheits-Software unterstützt alle gängigen Betriebssysteme. Sie erweitert Ihre gewohnte Desktop-Umgebung um die Möglichkeit, Dateien jeden Formats mit nur wenigen Klicks zu ver- und entschlüsseln. Sie ist so entworfen, dass sie sowohl in Ihrem Arbeitsumfeld, als auch in etablierten Web- und Meeting-Applikationen jeglicher Art Anwendung findet. Durch die intuitive Handhabung ist sie für Einsteiger sowie für erfahrene Nutzer multifunktional anwendbar.

Maximale Usability

Unser Hauptziel ist, dass sich verschlüsselte Kommunikation so anfühlt, wie über den herkömmlichen Weg. Dafür arbeiten wir täglich mit großer Freude an Lösungen, die in Ihren Arbeitsalltag einfließen und Sie unterstützen.

Andre Heinecke
Leitender Produktentwickler
GnuPG-Engineer

+49 2104 493 879 4
andre.heinecke@gnupg.com

Outlook-PlugIn

Die Programmerweiterung fügt sich nahtlos in Ihr Outlook-Menü und ermöglicht einen benutzerfreundlichen Umgang mit Krypto-Mails innerhalb Ihrer vertrauten Groupware.

Wir geben unberechtigter Datenspeicherung keine Chance

Ende-zu-Ende Verschlüsselung

Jede Nachricht durchläuft bei der Übermittlung viele Computer und landet oftmals in fremden Datenbanken. Die E2EE-Kommunikation verhindert dabei das Mitlesen durch Andere, einschließlich Telekommunikationsanbieter, Internetprovider und Kommunikationsdienstleister. Selbst wenn Ihre verschlüsselten Mails abgefangen werden sollten, sind diese für Dritte unmöglich zu entschlüsseln.

Vorteile

- Die Nachrichten können nur von den Endpunkten gelesen werden (Vertrauen)
- Die Echtheit des Senders kann stets gewährleistet werden (Authentizität)
- Der Inhalt kann nicht unbemerkt verändert werden (Integrität)

Funktionsprinzip

Der Sender verschlüsselt seine digitalen Informationen mit dem öffentlichen Schlüssel der Person, die sich am Endpunkt der Kommunikation befindet. Diesen hat er entweder direkt vom Empfänger, oder über öffentliche Schlüssel- bzw. Zertifikatsserver erhalten. Der Empfänger ist als Einziger in der Lage, die erhaltenen Informationen mittels seines dazugehörigen privaten Schlüssels zu lesen.

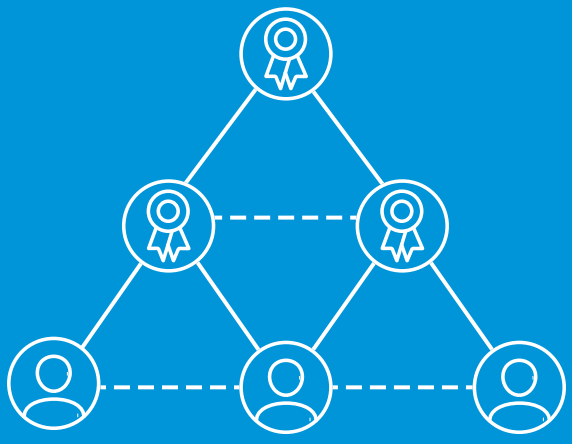
Zertifikatsverwaltung mit S/MIME und OpenPGP

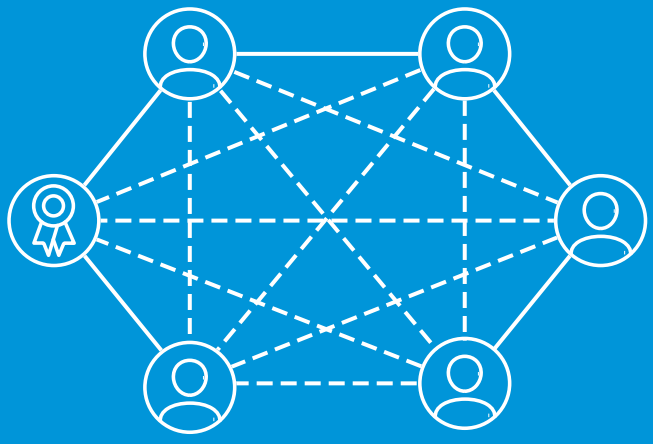
Identitätsmanagement

Kryptographisches Material ist stets mit einer Identität verbunden. Die Kombination aus Schlüssel- und Identitätsinformation wird als öffentlicher Schlüssel bzw. Zertifikat bezeichnet. GnuPG bietet Ihnen viele benutzerfreundliche Möglichkeiten diese, für die Kommunikation notwendigen Zertifikate, auch automatisiert auszutauschen.

Vorteile

- Bei Enterprise-Lösungen konfigurieren wir Ihnen ein passendes und individuell auf die Bedürfnisse Ihrer Organisation zugeschnittenes Lösungspaket für S/MIME oder OpenPGP.





S/MIME

Vertrauenswürdige Wurzelzertifikate werden hierarchisch konfiguriert. In Kombination mit einem Zertifikatsserver sucht und aktualisiert unser Outlook-PlugIn für Sie ganz automatisch das passende Zertifikat.

OpenPGP

Die Zertifikatsverwaltung erfolgt hierbei über zentrale und dezentrale Wege. Mit der richtigen Konfiguration erreichen Sie hierbei ein weitaus höheres Sicherheitsniveau, da ausschließlich legitimierten Zertifikaten vertraut werden kann.

Unser Komplettpaket zum Schutz Ihrer Daten

Viel erwarten – mehr bekommen

Bei Enterprise-Einsätzen haben Sie mit uns die Möglichkeit, sich von GnuPG zu überzeugen, indem Sie unser Software- und Dienstleistungsangebot im Probebetrieb vollumfänglich testen. Nachfolgend finden Sie unser komplettes Leistungsspektrum für sichere Kommunikation:

Open Source Software

Bestehend aus Kryptosoftware, Zertifikatsmanager und PlugIns

Initial-Workshop

E2EE-Einstiegskurs für den sicheren Umgang mit GnuPG

Support

Telefonische Unterstützung mit Direktzugriff auf unsere Entwickler

Consulting

Beratungs- und Lösungskonzepte zur Unterstützung Ihrer Organisation

Maintenance

Sicherheitsupdates und Long-Term-Support

Schulung

Individuell auf Ihre Organisation angepasste Weiterbildungsseminare

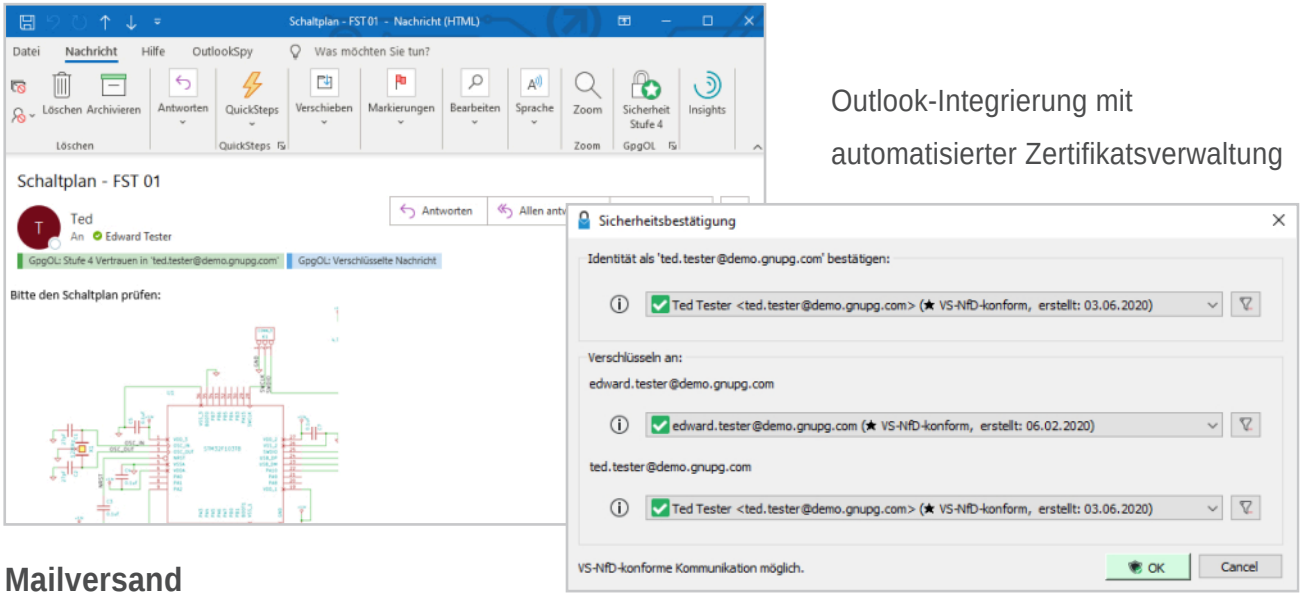
Know-How

Professionelle Beratung rund um das Thema E2EE – direkt vom Hersteller

Development

In Ihrem Auftrag entwickeln und programmieren wir neue, individuelle Features

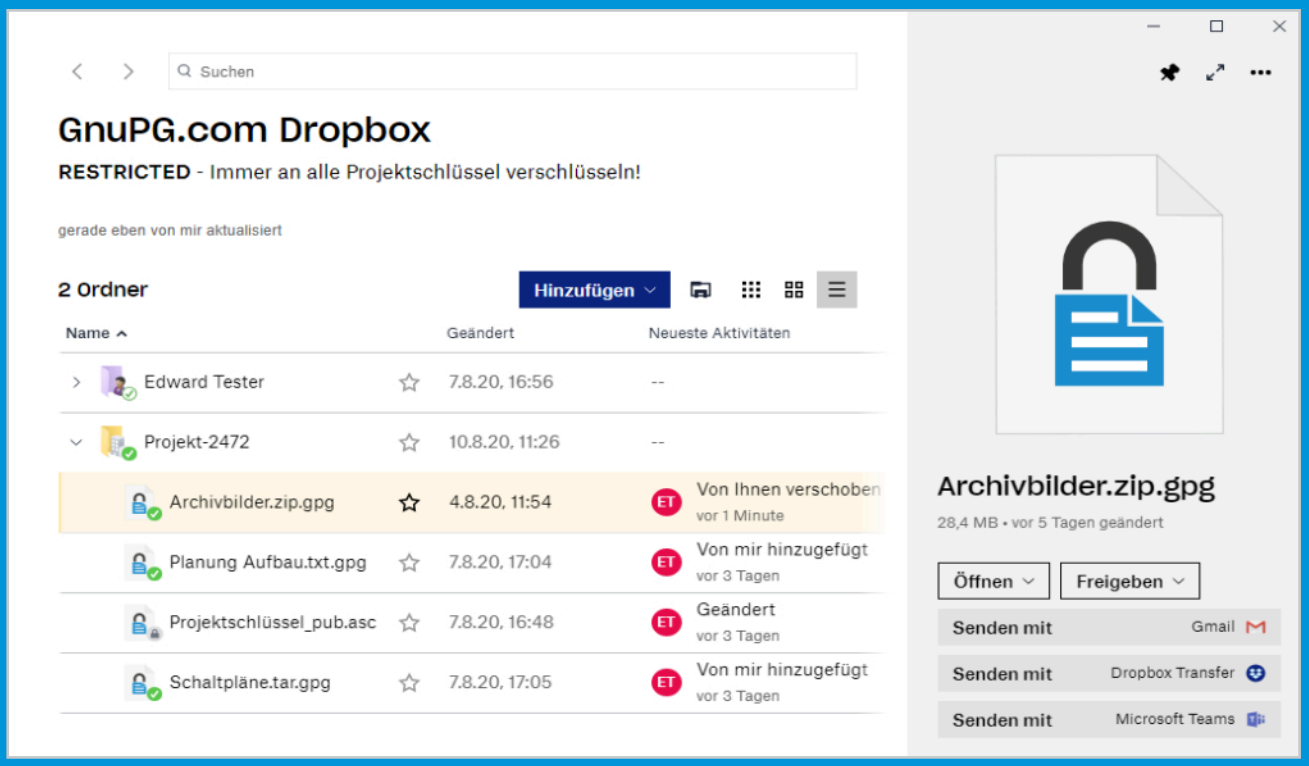
Anwendungsbeispiele



Outlook-Integrierung mit automatisierter Zertifikatsverwaltung

Mailversand

Datentransfer



Übertragung und Verarbeitung geheimgehaltener Daten

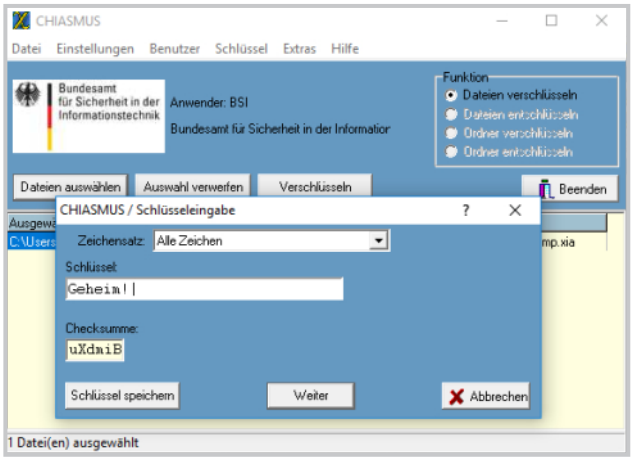
IT-Sicherheit mit VS-NfD Freigabe

2019 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) unsere Krypto-Komplettlösung für die Übertragung von vertraulichen Dokumenten der Geheimhaltungsstufe „Verschlusssache – nur für den Dienstgebrauch“ (VS-NfD) zugelassen. Diese gilt sowohl für das OpenPGP- als auch für das S/MIME-Protokoll und sieht vor, dass Langzeit-Geheimnisse u.a. auch auf der Festplatte gespeichert werden können.

Bei Geheimhaltungsgraden die über VS-NfD hinausgehen, kann der Einsatz von GnuPG VS-Desktop direkt mit dem Bundesamt für Sicherheit in der Informationstechnik geklärt werden.

Der neue Weg

Die Zulassung der BSI-Verschlüsselungssoftware Chiasmus läuft am 31.12.2021 endgültig ab. Institutionen die bislang auf diese Sicherheits-Software angewiesen waren und VS-NfD Daten verschlüsselt haben, sind in der Pflicht auf andere zugelassene Lösungen umzustellen. Der Einsatz von GnuPG VS-Desktop bietet Ihnen hierbei weitaus flexiblere Einsatzmöglichkeiten:



- Nutzung aller digitalen Übertragungswege unabhängig von der Transportverschlüsselung
- Automatisierte Schlüsselverwaltung mit Hintergrund-Aktualisierung
- Outlook-Integration

Gerne unterstützen wir Sie rechtzeitig bei der Umstellung von Chiasmus auf GnuPG VS-Desktop.

Bessere Kontrolle durch Security-Token

Digitale Schlüssel zum Anfassen

Security-Token sind Kleinrechner in Form eines USB-Sticks oder einer Chipkarte und ermöglichen eine kennwortlose Benutzeridentifizierung bei der Anmeldung am Arbeitsplatz oder der Nutzung von Webdiensten. Sie erhöhen den Privatsphärenschutz auf ein Maximum, indem Sie Ihnen eine physische Zugriffskontrolle gewährleisten, die Sie wie einen Türschlüssel am Bund bei sich tragen können.

Offene Software – transparente Hardware

Mit dem GnuK USB-Token entwickeln wir gemeinsam mit unseren Partnern weltweit eine Referenzimplementierung für Security-Token und arbeiten an der Spezifikation des OpenPGP Smartcard Standards entsprechend unseren Werten und Prinzipien.

NIIBE Yutaka
Hardware-Anbindung
GnuK-Token

+49 2104 493 879 0
info@gnupg.com

Die richtige Wahl

Bei Enterprise-Einsätzen unterstützen wir Sie beim sicheren Umgang mit Security-Token und ermitteln für Ihre Betriebs-Struktur die bestmögliche Lösung der automatisierten Benutzeridentifizierung und -authentisierung.

GnuPG.com –
eine Marke der g10 Code GmbH

Erfahrung schafft Vertrauen

GnuPG und die g10 Code GmbH stehen für Unabhängigkeit, Souveränität und den Erhalt der digitalen Privatsphäre. Seit über 23 Jahren entsteht unsere Kryptosoftware in einem offenen und transparenten Entwicklungsprozess. Mit viel Herz, großer Leidenschaft, Blut, Schweiß und Tränen arbeiten wir Tag für Tag kontinuierlich für Millionen Nutzer weltweit am max. Privatsphärenschutz bei der Nachrichtenübertragung.

Gemeinsam zum Erfolg

Der GNU Privacy Guard Verschlüsselungscode konnte nur entwickelt und realisiert werden, weil zahlreiche Menschen die Idee der freien und transparenten Software wertschätzen, fördern und finanziell unterstützen.

IT – Sicherheit

Made in Germany

image_gnupg_de.pdf ▪ Rev. 01 ▪ Stand 09/2020
Änderungen, Irrtümer und Druckfehler vorbehalten

g10 Code GmbH
Gutenberg Weg 4
40699 Erkrath / Germany
+49 2104 493 879 0
info@gnupg.com
www.gnupg.com