WITTEWELLER
PATENTANWÄLTE

Verschlüsselte Kommunikation mit uns — How-to für externe Sender

Wir unterstützen die zwei verbreiteten Standards für E-Mail-Verschlüsselung:

VERFAHREN	SIE AN UNS	WIR AN SIE
OpenPGP / GPG	✓	✓
S/MIME (X.509)	✓	✓

Verschlüsselte Eingangsnachrichten werden bei uns automatisch erkannt und entschlüsselt. Ausgehende Nachrichten an Sie werden automatisch verschlüsselt, sobald Ihr öffentlicher Schlüssel oder Ihr Zertifikat bei uns bekannt ist.

---

1. Was wir von Ihnen benötigen

Für jede Verschlüsselungsrichtung benötigen wir ausschließlich den **öffentlichen** Teil Ihres Schlüssels bzw. Zertifikats:

- OpenPGP / GPG: Ihren **OpenPGP-Public-Key** (`.asc` oder `.gpg`).
- **S/MIME:** Ihr **X.509-Zertifikat** (`.pem` oder `.cer`), idealerweise einschließlich der ausstellenden CA-Zertifikatskette.

> **Wichtig:** Senden Sie uns **niemals** Ihren privaten Schlüssel oder Ihre Passphrase. Diese gehören ausschließlich auf Ihre eigenen Geräte.

2. Wie wir Ihren Public-Key oder Ihr Zertifikat erhalten

Wir versuchen zunächst, Ihren Public-Key bzw. Ihr Zertifikat automatisch abzurufen. In vielen Fällen müssen Sie daher nichts aktiv tun, wenn Ihre Schlüssel- oder Zertifikatsinformationen an einer Standardstelle veröffentlicht sind.

2a. Automatischer Lookup (bevorzugt)

Wenn wir Ihnen schreiben und noch keinen Public-Key bzw. kein Zertifikat von Ihnen kennen, prüfen wir die folgenden Quellen:

WKD (Web Key Directory) — für OpenPGP / GPG

- Standardpfad: `https://openpgpkey.<ihre-domain>/.well-known/openpgpkey/<ihre-domain>/hu/<hash(localpart)>`
- Falls Ihr E-Mail-Provider WKD unterstützt, müssen Sie nichts weiter tun. Dies gilt beispielsweise für viele Provider mit WKD-Unterstützung sowie für eigene Domains mit entsprechend konfiguriertem WKD.

LDAP-Server — für S/MIME-Zertifikate

- **Auto-Discovery über DNS-SRV:** Wir prüfen `_ldap._tcp.<ihre-domain>` und `_ldaps._tcp.<ihre-domain>` gemäß RFC 2782 und fragen den dort angegebenen Public-Certificate-LDAP automatisch ab.
- Wenn Ihre Organisation einen öffentlich erreichbaren LDAP-Dienst für S/MIME-Zertifikate betreibt und ein passender SRV-Record vorhanden ist, müssen Sie nichts weiter tun.
- Der Abruf erfolgt per Anonymous Bind über das Attribut `userCertificate;binary`.
- Falls Ihr LDAP-Server auf andere Weise erreichbar ist, kontaktieren Sie uns bitte per E-Mail; siehe Kontakt.

2b. Automatischer Import aus eingehenden E-Mails (beide Verfahren)

- Wenn Sie uns eine **signierte** E-Mail senden (PGP/MIME oder S/MIME), wird der enthaltene Public-Key bzw. das enthaltene Zertifikat bei uns automatisch importiert. Ab unserer nächsten Antwort können wir verschlüsselt an Sie senden.
- Der Import funktioniert auch, wenn Sie Ihren Public-Key oder Ihr Zertifikat als **Anhang** mitsenden, beispielsweise als `.asc`-, `.pem`- oder `.cer`-Datei.

---

3. Wie Sie unsere Public-Keys und Zertifikate erhalten

3a. WKD (für OpenPGP / GPG, automatisch)

Der bevorzugte Weg für OpenPGP / GPG ist der automatische Abruf über WKD. Moderne E-Mail-Clients — beispielsweise Thunderbird mit integriertem OpenPGP, Outlook mit GpgOL/Gpg4win, Apple Mail mit GPG Suite, Evolution oder KMail — können den Public-Key automatisch über WKD abrufen.

Sobald Sie eine E-Mail an eine unserer Adressen verfassen, fragt Ihr Client unser WKD ab und importiert den passenden Public-Key automatisch, sofern Ihr Client diese Funktion unterstützt.

3b. LDAP (für S/MIME, automatisch via DNS-SRV oder manuell)

Wir betreiben einen anonymous-readable LDAP-Server mit `userCertificate;binary`-Attribut.

- **Verbindung:** `ldaps://ldap.wwp.de` (Port 636, TLS) bzw. `ldap://ldap.wwp.de` (Port 389, optional StartTLS)
- **Base DN:** `dc=wwp,dc=de` oder `''`
- **Bind:** anonymous
- **Filter:** (`mail=<adresse>`)
- **Cert-Attribut:** `userCertificate;binary`

Outlook, Apple Mail und Thunderbird fragen den LDAP automatisch ab, sobald Sie eine Mail an einen unserer Empfänger schreiben. Bei eingehender signierter Mail von uns wird das Zertifikat von vielen Clients ebenfalls automatisch über den LDAP geholt und beim Antworten verwendet.

Unsere CA-Trust-Kette per LDAP (für S/MIME-Validierung): Falls Ihr Client unseren Signaturen noch nicht vertraut (unsere CA ist self-signed), können Sie die komplette Kette (Root- + Issuing-CA) standardkonform aus demselben LDAP ziehen — als `pkiCA`-Einträge (RFC 4523). Verbindung und Bind wie oben, nur Filter und Attribut unterscheiden sich:

- **Filter:** (`objectClass=pkiCA`)
- **CA-Cert-Attribut:** `cACertificate;binary`

Nach Import dieser CA-Certs als vertrauenswürdige Stammzertifikate gelten unsere S/MIME-Signaturen in Ihrem Client als gültig.

Falls Ihr Client kein Auto-Discovery beherrscht, können Sie den LDAP manuell als Adressbuch / Zertifikat-Verzeichnis im Client einbinden — die Verbindungsdaten oben sind alles was Sie brauchen.

3c. Public-Lookup-UI (manueller Fallback)

Wenn weder WKD noch LDAP funktionieren, beispielsweise weil Ihr Client diese Verfahren nicht unterstützt oder eine Firewall den Zugriff blockiert, können Sie unsere Public-Keys und Zertifikate manuell über die folgende Webseite herunterladen:

`https://pki.wwp.de`

Geben Sie dort die Empfänger-E-Mail-Adresse oder den Namen ein. Sie erhalten anschließend:

- **OpenPGP-Public-Key** (`.asc`),
- **S/MIME-Zertifikat** (`.pem`),
- **Trust-Chain-Bundle** (Root-CA und Issuing-CA als `.pem`), wichtig für die S/MIME-Validierung in Ihrem E-Mail-Client.

3d. Anfrage per Betreff (wenn Ihr Gateway nur aus eingehender Mail importiert)

Manche Verschlüsselungs-Gateways können Zertifikate/Keys ausschließlich aus eingehender Mail übernehmen und weder WKD noch LDAP noch die Webseite abfragen. Für diesen Fall können Sie unsere Zertifkate/Keys per E-Mail anfordern:

Schreiben Sie eine E-Mail an die gewünschte Empfänger-Adresse(n) (z.B. `person@wwp.de`) mit **genau einem** dieser Betreffe **ohne weitere Zusätze**:

`SMIME Request`
Sie möchten das **S/MIME-Zertifikat** dieser Adresse(n):

`GPG Request`
Sie möchten den **OpenPGP-Public-Key** dieser Adresse(n):

Sie erhalten kurz darauf eine Antwort **von genau dieser Adresse**, die das Material als Anhang trägt (`.pem` bzw. `.asc`). Bei S/MIME ist die Antwort zusätzlich signiert, sodass das Zertifikat auch direkt aus der Signatur übernommen werden kann. Ihr Gateway importiert es dann automatisch aus dieser eingehenden Mail.

Hinweise:

- **Mehrere Adressen auf einmal:** Richten Sie die Anfrage an mehrere unserer Empfänger gleichzeitig, erhalten Sie je Adresse eine eigene Antwort.
- **Beidseitiger Austausch:** Signieren Sie Ihre Anfrage (bzw. hängen Sie Ihren eigenen Public-Key an), übernehmen wir Ihr Zertifikat/Ihren Key im selben Zug — dann ist der Austausch in beide Richtungen erledigt.
- **Kein Material vorhanden:** Existiert für die Adresse (noch) kein Zertifikat/Key, erhalten Sie einen kurzen Hinweis statt eines Anhangs.

4. Konfiguration in Ihrem E-Mail-Client

Die Verschlüsselung erfolgt in der Regel über eine der folgenden Komponenten:

- ein **Plugin** für Ihren E-Mail-Client, beispielsweise Gpg4win/GpgOL für Outlook, GPG Suite für Apple Mail oder der integrierte OpenPGP-Support in Thunderbird ab Version 78, oder
- ein **Encryption-Gateway** in Ihrer Organisation, das E-Mails transparent verschlüsselt.

In beiden Fällen importieren Sie unseren Public-Key bzw. unser Zertifikat einmalig oder lassen diese automatisch über WKD bzw. LDAP abrufen. Danach verschlüsselt Ihr Plugin oder Gateway ausgehende E-Mails an uns automatisch, soweit die jeweilige Lösung entsprechend konfiguriert ist.

5. Kontakt

Bei Fragen oder Problemen bei der Einrichtung wenden Sie sich bitte an:

E-Mail: support@wwp.de