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 oder manuell)

Wir betreiben einen anonym abfragbaren LDAP-Server mit dem Attribut `userCertificate;binary`.

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

Outlook, Apple Mail und Thunderbird können den LDAP-Dienst automatisch abfragen, sobald Sie eine E-Mail an eine unserer Adressen verfassen. Bei einer von uns eingehenden signierten E-Mail wird das Zertifikat von vielen Clients ebenfalls automatisch abgerufen und anschließend beim Antworten verwendet.

Falls Ihr Client keine Auto-Discovery unterstützt, können Sie den LDAP-Server manuell als Adressbuch oder Zertifikatsverzeichnis im Client einbinden. Die oben genannten Verbindungsdaten reichen hierfür aus.

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:

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

---

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