WITTEWELLER
PATENTANWÄLTE

Encrypted communication with us — How-to for external sender

We support the two common standards for email encryption:

METHOD	YOU TO US	WE TO YOU
OpenPGP / GPG	✓	✓
S/MIME (X.509)	✓	✓

Inbound encrypted emails are automatically detected and decrypted by our systems. Outbound emails to you are automatically encrypted as soon as your public key or certificate is known to us.

---

1. What We Require from You

For each encryption direction, we only need the **public** part:

- **OpenPGP / GPG**: Your **OpenPGP public key** (`.asc` / `.gpg`).
- **S/MIME:** Your **X.509 certificate** (`.pem` / `.cer`), ideally including the issuing CA chain.

> **Important: Never** send us your private key or your passphrase.
> These belong exclusively on your own devices.

2. How We Obtain Your Public Keys / Certificates

We try the following methods automatically — in many cases, you do not need to take any active steps if your keys are published at one of the standard locations.

2a. Automatic Lookup (preferred)

If we write to you and do not yet know your key or certificate, we look up the following sources:

WKD (Web Key Directory) — for OpenPGP / GPG

Standard path:

`https://openpgpkey.<ihre-domain>/.well-known/openpgpkey/<ihre-domain>/hu/<hash(localpart)>`

If your email provider supports WKD, you do not need to do anything else. This applies, for example, to many providers with WKD support as well as to custom domains with a correspondingly configured WKD.

LDAP Server for S/MIME Certificates

Auto-Discovery via DNS-SRV: We check `_ldap._tcp.` and `_ldaps._tcp.` in accordance with RFC 2782 and automatically query the public certificate LDAP specified there.

If your organization operates a publicly accessible LDAP service for S/MIME certificates and a matching SRV record is available, you do not need to do anything else.

The retrieval is performed via Anonymous Bind using the attribute `userCertificate;binary`.

If your LDAP server is accessible in a different way, please contact us via email; see Contact.

2b. Automatic Import from Inbound Mail (Both Methods)

- If you send us a **signed** email (PGP/MIME or S/MIME), the contained public key or certificate is automatically imported on our end. Starting with our next reply, we can send encrypted emails to you.

- The import also works if you send your public key or certificate as an **attachment**, for example as an `.asc`, `.pem`, or `.cer` file.

---

3. How You Can Obtain Our Public Keys and Certificates

3a. WKD (for OpenPGP / GPG, Automatic)

The preferred method for OpenPGP / GPG is automatic retrieval via WKD. Modern email clients—for example Thunderbird with integrated OpenPGP, Outlook with GpgOL/Gpg4win, Apple Mail with GPG Suite, Evolution, or KMail—can retrieve the public key automatically via WKD.

As soon as you compose an email to one of our addresses, your client queries our WKD and automatically imports the matching public key, provided your client supports this feature.

3b. LDAP (for S/MIME, Automatic via DNS-SRV or Manual)

We operate an anonymous-readable LDAP server with the `userCertificate;binary` attribute.

- **Connection:** `ldaps://ldap.wwp.de` (Port 636, TLS) or `ldap://ldap.wwp.de` (Port 389, optional StartTLS)
- **Base DN:** `dc=wwp,dc=de` or `''`
- **Bind:** anonymous
- **Filter:** (`mail=<address>`)
- **Cert Attribute:** `userCertificate;binary`

Outlook, Apple Mail, and Thunderbird automatically query the LDAP as soon as you write an email to one of our recipients. For inbound signed emails from us, many clients also automatically fetch the certificate via LDAP and use it when replying.

Our CA Trust Chain via LDAP (for S/MIME Validation): If your client does not yet trust our signatures (our CA is self-signed), you can retrieve the complete chain (Root + Issuing CA) in a standard-compliant manner from the same LDAP as pkiCA entries (RFC 4523). The connection and bind are identical to the details above, only the filter and attribute differ:

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

After importing these CA certs as trusted root certificates, our S/MIME signatures will be recognized as valid in your client.

If your client does not support auto-discovery, you can manually integrate the LDAP as an address book / certificate directory in your client—the connection data above is all you need.

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

If neither WKD nor LDAP works, for example because your client does not support these methods or a firewall blocks access, you can manually download our public keys and certificates from the following website:

`https://pki.wwp.de`

Enter the recipient's email address or name there. You will then receive:

- **OpenPGP public key** (`.asc`),
- **S/MIME certificate** (`.pem`),
- **Trust Chain Bundle** (Root CA and Issuing CA as `.pem`), which is important for S/MIME validation in your email client.

3d. Request via Subject Line (If Your Gateway Only Imports from Inbound Mail)

Some encryption gateways can only import certificates/keys from inbound mail and cannot query WKD, LDAP, or the website. For this scenario, you can request our certificates/keys via email:

Write an email to the desired recipient address(es) (e.g., `person@wwp.de`) with **exactly one** of these subject lines, **without any additional** text:

- To request the **S/MIME certificate** for this address(es):
  `SMIME Request`
- To request the **OpenPGP public key** for this address(es):
  `GPG Request`

Shortly afterwards, you will receive a reply **from that exact address** containing the material as an attachment (`.pem` or `.asc`). For S/MIME, the reply is additionally signed, meaning the certificate can also be imported directly from the signature. Your gateway will then automatically import it from this inbound email.

Notes:

- **Multiple addresses at once:** If you direct the request to several of our recipients at the same time, you will receive a separate reply for each address.
- **Two-way exchange:** If you sign your request (or attach your own public key), we will import your certificate/key at the same time—the exchange is then completed in both directions.
- **No material available:** If no certificate/key exists (yet) for the address, you will receive a short notification instead of an attachment.

---

4. Configuration in Your Email Client

Encryption typically takes place via one of the following components:

- A **plugin** for your email client, such as Gpg4win/GpgOL for Outlook, GPG Suite for Apple Mail, or the integrated OpenPGP support in Thunderbird starting from version 78, or
- An **encryption gateway** in your organization that encrypts emails transparently.

In both cases, you import our public key or certificate once, or let them be retrieved automatically via WKD or LDAP. After that, your plugin or gateway will automatically encrypt outbound emails to us, provided the respective solution is configured accordingly.

---

5. Contact

If you have any questions or encounter issues during the setup, please contact:

Email: support@wwp.de