E-Mail

- E-Mail-Verschlüsselung
  - Empfang verschlüsselter E-Mails
  - Empfang verschlüsselter E-Mails - bereits vergebenes Passwort vergessen
  - Versand verschlüsselter E-Mails mit Outlook
  - E-Mails mit DATEV SmartCard signieren, verschlüsseln und entschlüsseln
- Mozilla Thunderbird
  - Prüfen, ob Thunderbird Standardprogramm ist / Scan2Mail
  - Microsoft 365 mit Thunderbird nutzen
- Eigene E-Mail-Domain im Geschäftsbetrieb: Vorteile, rechtliche Anforderungen und Archivierungspflichten (Deutschland)

E-Mail-Verschlüsselung

E-Mail-Verschlüsselung

Empfang verschlüsselter E-Mails

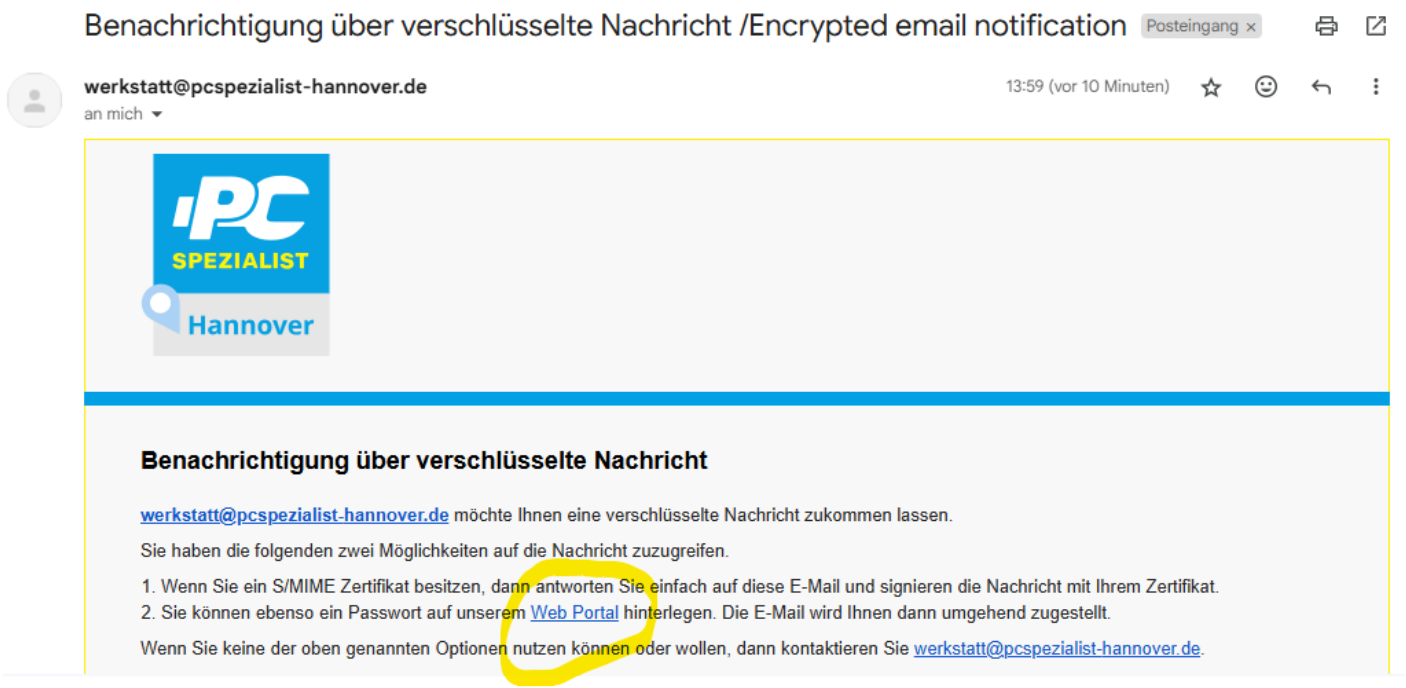
Wir senden sensible Informationen in einer E-Mail ausschließlich verschlüsselt.
Wenn Sie selbst verschlüsselte E-Mail-Kommunikation benutzen, erhalten Sie unsere E-Mail wie gewohnt.
Es besteht kein weiterer Handlungsbedarf.

Nutzen Sie ausschließlich unverschlüsselte Kommunikation, benötigen Sie ein Passwort, um unsere verschlüsselte E-Mail zu lesen.

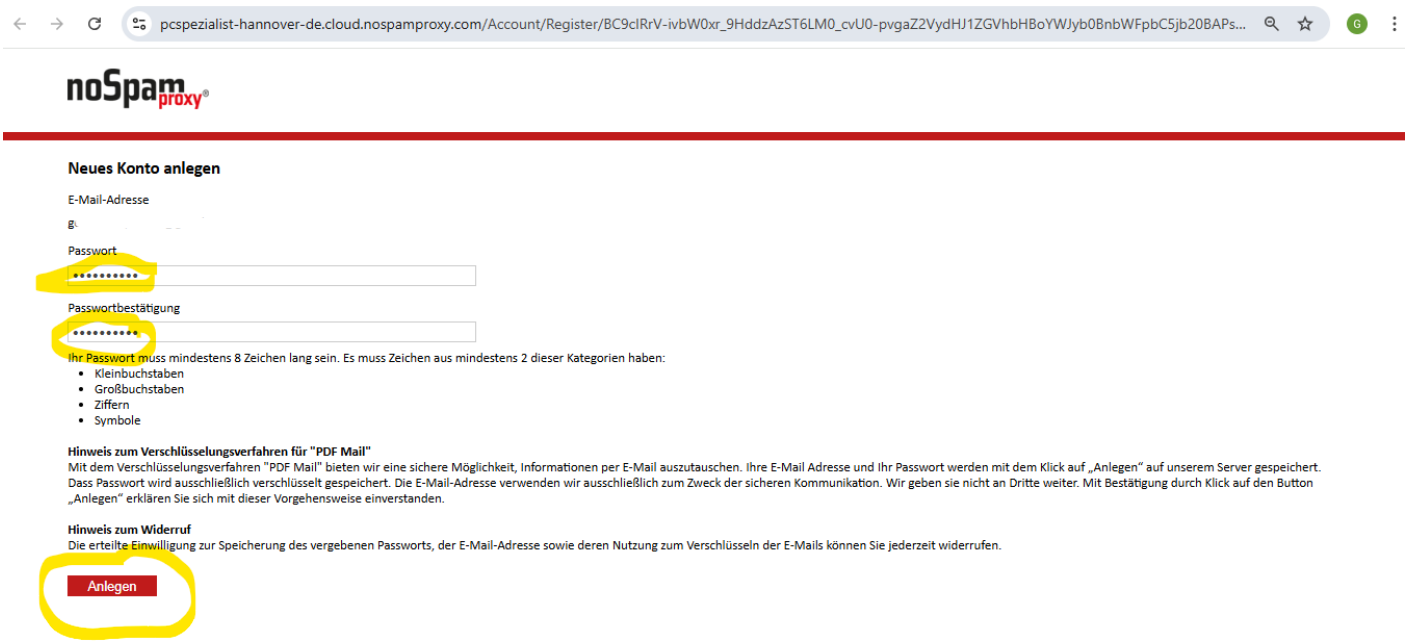
So funktioniert es:

1.) Sie erhalten eine E-Mail mit dem Betreff **Benachrichtigung über verschlüsselte Nachricht / Encrypted email notification**, die einen Link zum Web Portal enthält. Öffnen Sie das **Web Portal** mit einem Klick darauf.

Hier ein Beispiel für den Inhalt der E-Mail, welche Ihnen zugestellt wird:



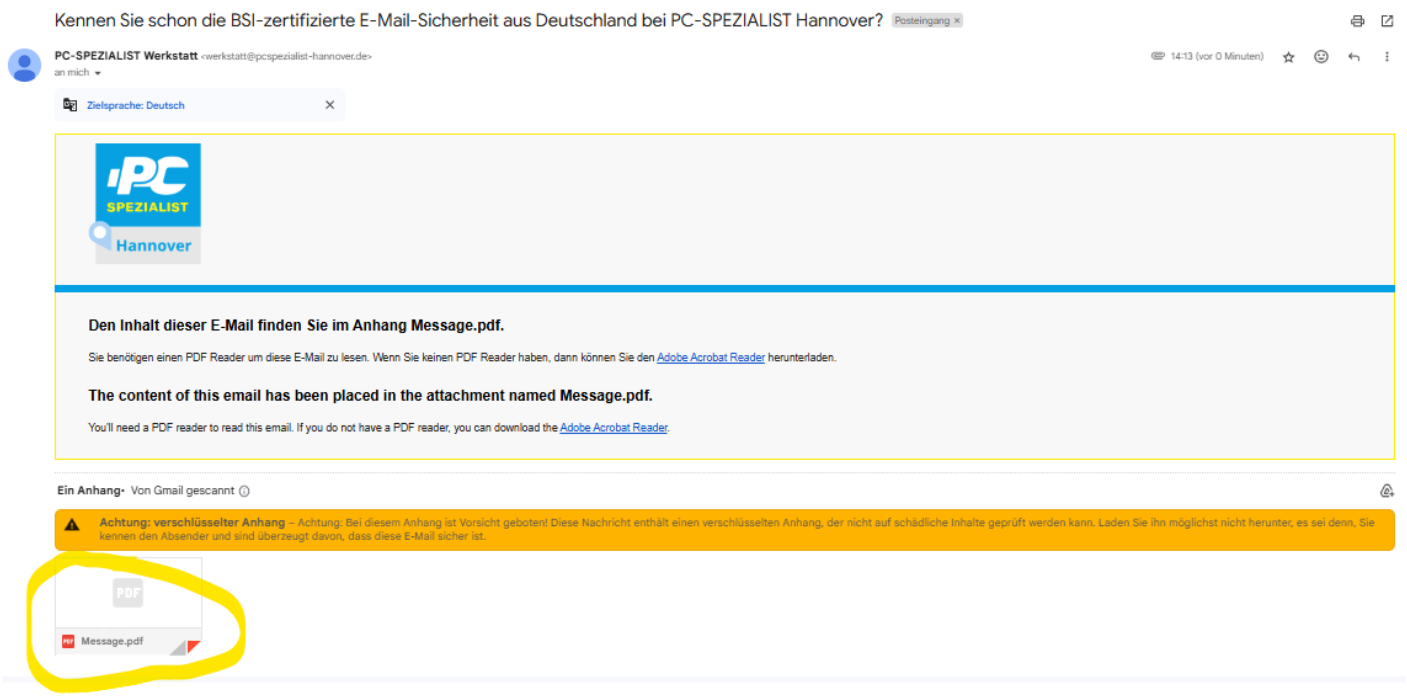
2.) Im Web Portal können Sie nun ein neues Konto **anlegen**. Tragen Sie Ihre E-Mail-Adresse und ein selbst gewähltes Passwort ein. Wir empfehlen das Hinterlegen des Passworts in Ihrem Passwortmanager.



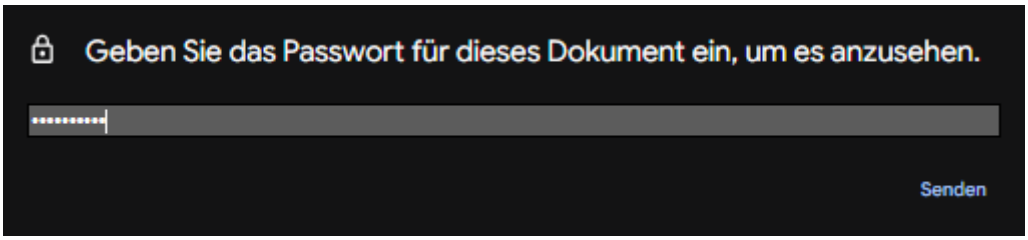
Hinweis: Es werden nicht alle Sonderzeichen akzeptiert.

3.) Sie erhalten dann eine weitere E-Mail von uns, in der Ihnen Mittgeteilt wird, dass das Passwort gespeichert wurde.

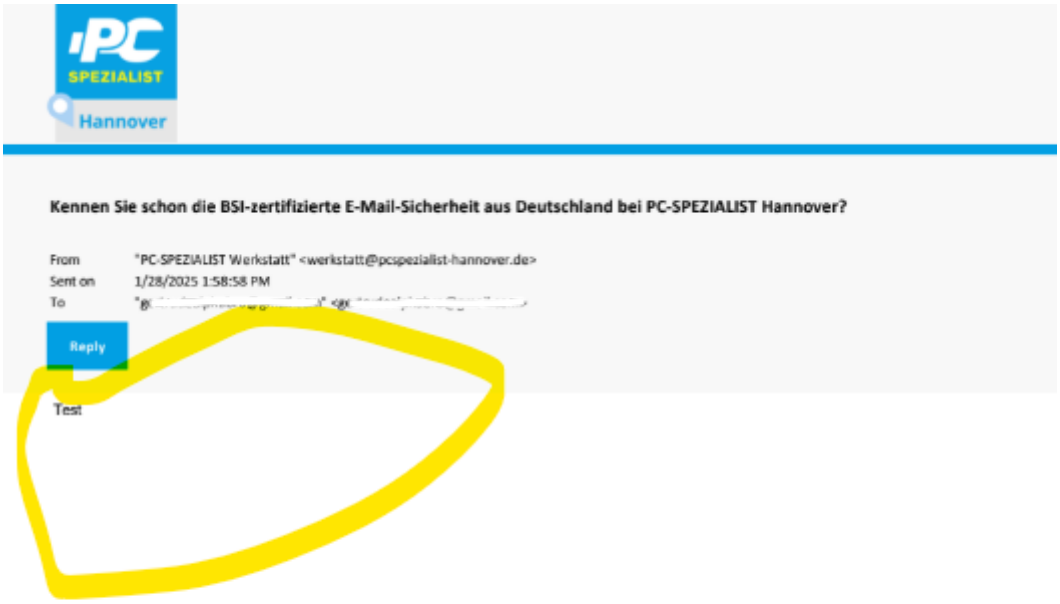
4.) Sie erhalten nun die eigentliche E-Mail mit dem Inhalt in einem verschlüsselten PDF-Dokument namens **Message.pdf**.



5.) Entsperren Sie jetzt diese Datei mit dem zuvor vergebenen Passwort.



6.) Nun sehen Sie unsere Nachricht in Ihrem PDF-Anzeigeprogramm. Geschafft. □□



Hinweis: Falls Sie ein bereits vergebenes Passwort vergessen haben, können Sie es so zurücksetzen: https://wiki.pcspezialist-hannover.de/books/e-mail/page/empfang-verschlusselter-e-mails-bereits-vergebenes-passwort-vergessen.

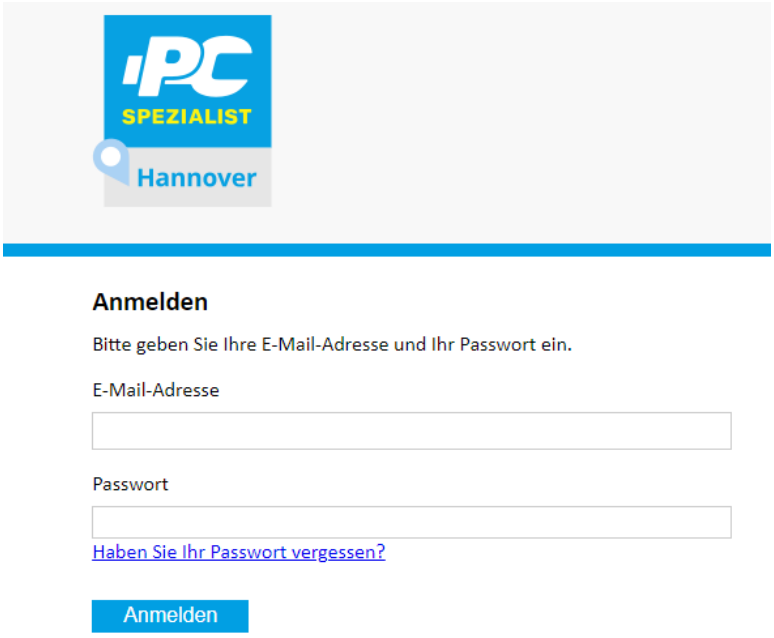
E-Mail-Verschlüsselung

Empfang verschlüsselter E-Mails - bereits vergebenes Passwort vergessen

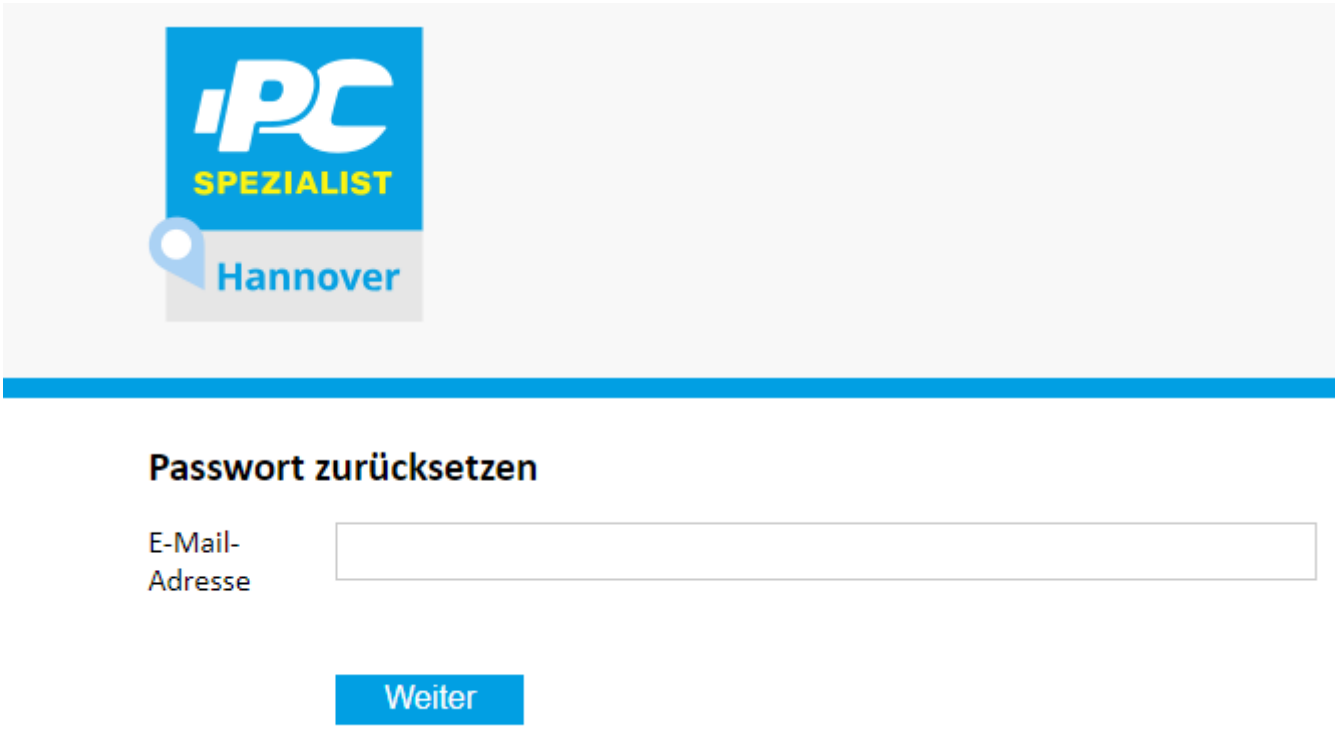
Sollten Sie eine verschlüsselte Mail empfangen haben, aber sich nicht mehr an das bereits vergebene Passwort erinnern können, so müssen Sie dies zurücksetzen.

Klicken Sie bitte auf diesen Link: Anmelden (pcspezialist-hannover-de.cloud.nospamproxy.com)

Es erscheint diese Eingabemaske



Klicken Sie auf "Haben Sie Ihr Passwort vergessen?"

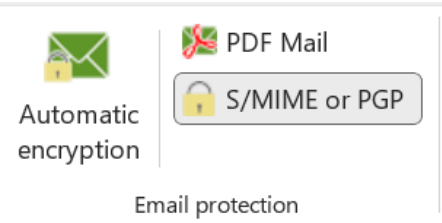


Geben Sie Ihre Mailadresse ein und Klicken auf "Weiter"

E-Mail-Verschlüsselung

Versand verschlüsselter E-Mails mit Outlook

Um verschlüsselte E-Mails versenden zu können, muss in Outlook ein Plug-In installiert sein.
Sie erkennen diese, wenn Sie auf "Neue E-Mail" klicken in der Menuleiste



Fehlt dies? Sprechen Sie uns an.
Sie dürfen selbst Programme installieren? Hier ist der Link:

https://service.nospamproxy.de/file/OutlookAddinSetup

Klicken Sie auf "Automatic encryption" und schreiben danach Ihre E-Mail wie gewohnt.

Wenn Ihr Empfänger ebenfalls verschlüsselte E-Mails senden und empfangen kann, ist nichts weiter zu tun.

Ist Ihr Empfänger nicht in der Lage verschlüsselt zu kommunizieren, senden Sie ihm zur Sicherheit eine separate E-Mail mit unserer Anleitung, wie mit verschlüsselten E-Mails umzugehen ist:

Empfang verschlüsselte... | PC-SPEZIALIST Wiki (pcspezialist-hannover.de)

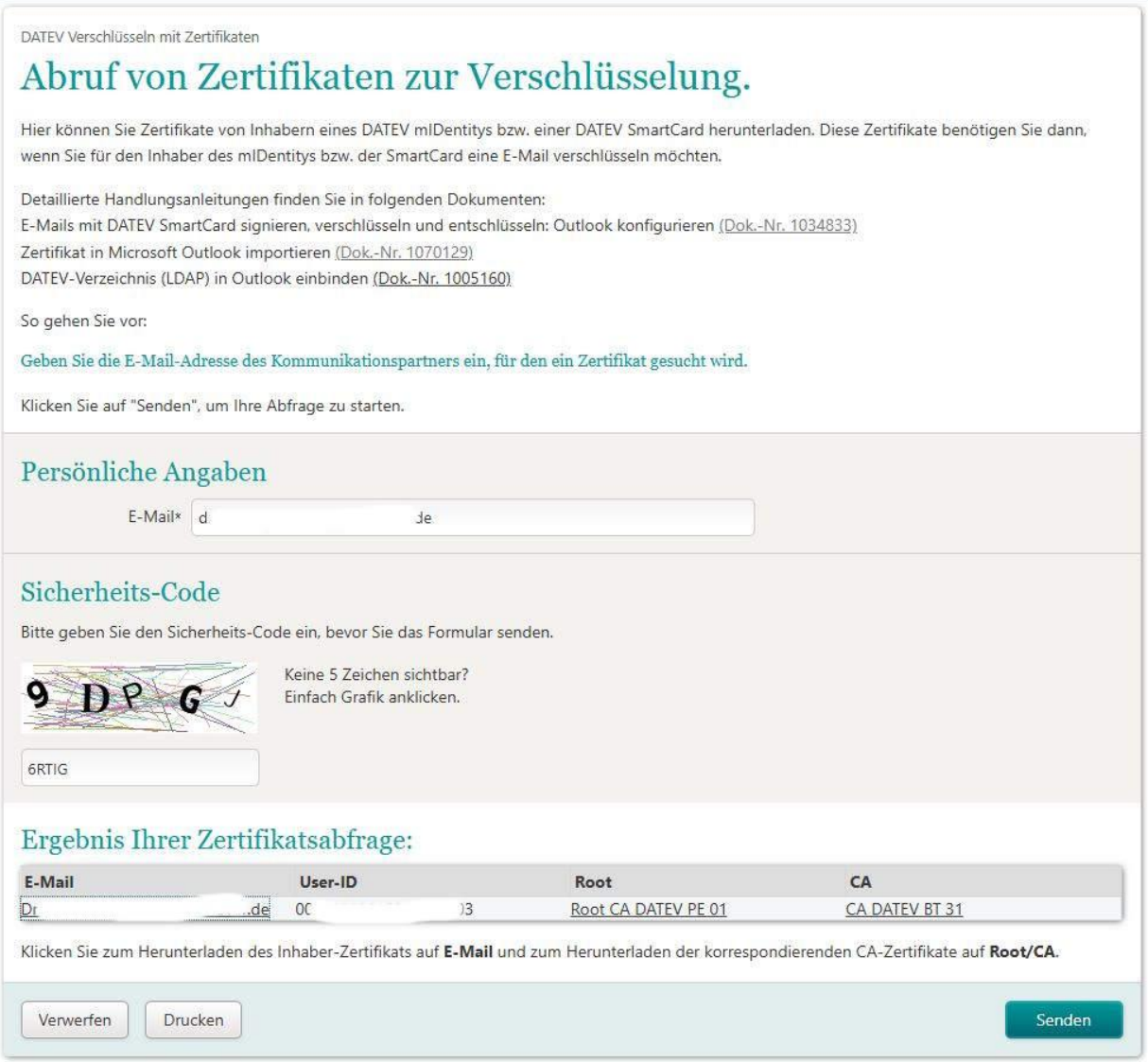
E-Mail-Verschlüsselung

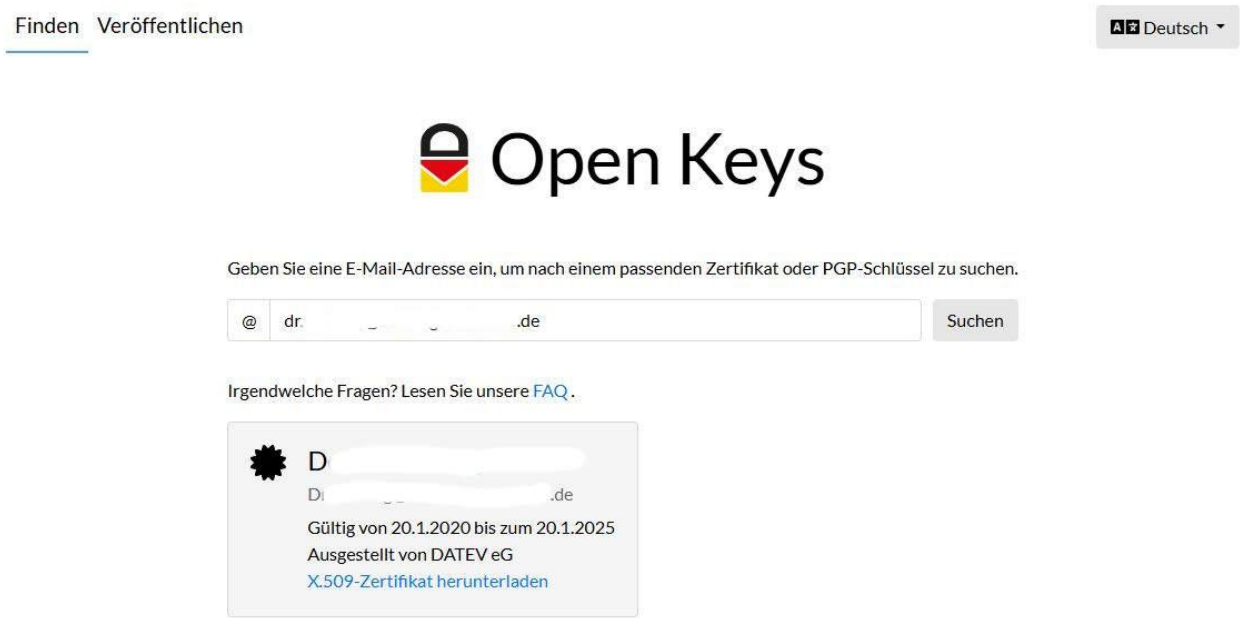
E-Mails mit DATEV SmartCard signieren, verschlüsseln und entschlüsseln

Uns ist aufgefallen, dass Nutzer einer DATEV SmartCard manchmal verschlüsselte E-Mails erhalten und nicht wissen, warum dem so ist.

Die Ursache ist oft ein von DATEV veröffentlichtes Zertifikat.

Sie können das direkt bei DATEV oder einem anderen Schlüsselserver wie OpenKeys prüfen, indem Sie Ihre E-Mail-Adresse eintragen.





Informationen zur Outlook-Konfiguration gibt es direkt bei DATEV.

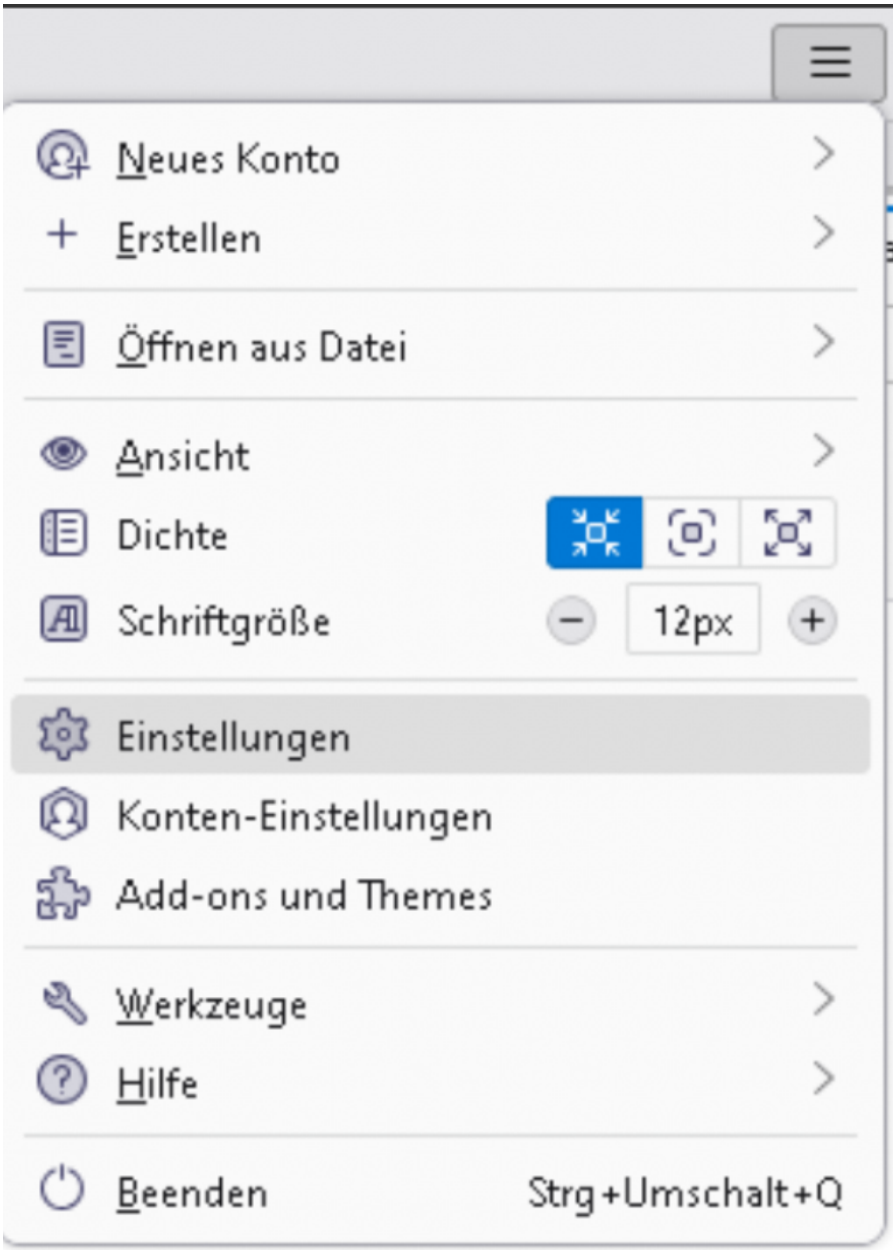
Falls Ihnen das zu umständlich ist, können wir Ihnen gerne unsere Gateway-Lösung anbieten. Diese Lösung hat den Vorteil, dass Sie das Zertifikat nicht für jedes E-Mail-Programm auf jedem Gerät manuell einbinden müssen.

Melden Sie sich bei Interesse einfach über das Taskleisten-Symbol.

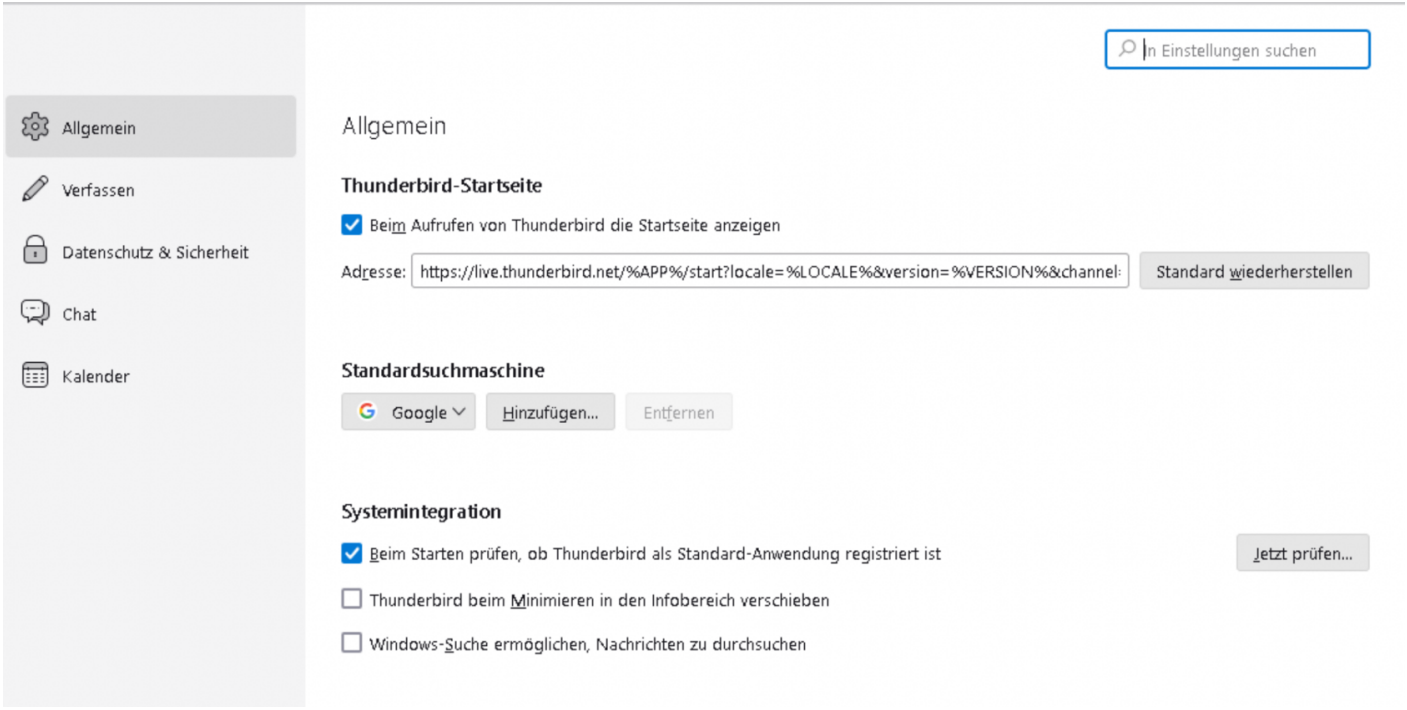
Mozilla Thunderbird

Prüfen, ob Thunderbird Standardprogramm ist / Scan2Mail

Thunderbird öffnen
In der Menuleiste "Extras" und dann "Einstellungen" anklicken
Oder an der rechten Seite auf die 3 Striche



In den Einstellungen unter "Allgemein" den Punkt Systemintegration suchen.
Ist der Haken gesetzt, bei: "Beim Starten prüfen, ob Thunderbird als Standard-Anwendung registriert ist"?



auf "jetzt prüfen" klicken und den alle gewünschten Haken setzen, wenn diese fehlen und bestätigen

Microsoft 365 mit Thunderbird nutzen

Eigene E-Mail-Domain im Geschäftsbetrieb: Vorteile, rechtliche Anforderungen und Archivierungspflichten (Deutschland)

1. Warum eine eigene E-Mail-Domain?

Eine eigene E-Mail-Domain – also eine Adresse wie vorname.nachname@firmenname.de statt @gmail.com oder @t-online.de – ist heute der selbstverständliche Standard im seriösen Geschäftsbetrieb. Sie signalisiert Professionalität, schützt die Marke und schafft technische Unabhängigkeit.

Freemail-Adressen bei Drittanbietern wirken im geschäftlichen Kontext häufig unprofessionell und bringen zusätzliche rechtliche und technische Risiken mit sich – dazu mehr in den folgenden Abschnitten.

---

2. Vorteile einer eigenen Domain

2.1 Professioneller Außenauftritt und Markenstärkung

Jede E-Mail, die Ihr Unternehmen versendet, trägt automatisch den Firmennamen als Absender. Das sorgt für eine einheitliche, wiedererkennbare Kommunikation – bei Angeboten, Rechnungen, Vertragskommunikation und beim Erstkontakt mit Neukunden. Eine Freemail-Adresse hingegen lässt keinen direkten Rückschluss auf Ihr Unternehmen zu und kann das Vertrauen potenzieller Kunden mindern.

2.2 Technische Kontrolle und Sicherheit

Mit einer eigenen Domain können Sie Sicherheitsmechanismen einrichten, die bei Freemail-Anbietern nicht oder nur eingeschränkt verfügbar sind:

- **SPF** (Sender Policy Framework): Legt fest, welche Server in Ihrem Namen E-Mails versenden dürfen
- **DKIM** (DomainKeys Identified Mail): Digitale Signatur zur Echtheitsprüfung
- **DMARC**: Kombiniert SPF und DKIM und schützt aktiv vor Missbrauch Ihrer Domain (Spoofing)

Diese Maßnahmen verbessern die Zustellraten und reduzieren das Risiko, als Spam eingestuft zu werden.

2.3 Unabhängigkeit und Flexibilität

Die Domain gehört Ihrem Unternehmen – nicht dem E-Mail-Anbieter. Sie können den technischen Dienstleister jederzeit wechseln, ohne Ihre E-Mail-Adressen ändern zu müssen. Sie sind damit unabhängig von AGB-Änderungen, Preiserhöhungen oder Abschaltungen einzelner Dienste.

---

3. Rechtliche Grundlagen für geschäftliche E-Mails in Deutschland

3.1 E-Mails als Geschäftsunterlagen

Geschäftliche E-Mails sind in Deutschland rechtlich als **Handels- und Geschäftsbriefe** sowie als **steuerlich relevante Unterlagen** einzustufen. Es gibt kein eigenständiges „E-Mail-Gesetz" – maßgeblich sind folgende Regelwerke:

- **HGB** (Handelsgesetzbuch)
- **AO** (Abgabenordnung)
- **GoBD** (Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff)
- **DSGVO** (Datenschutz-Grundverordnung)

3.2 Welche E-Mails müssen aufbewahrt werden?

Aufbewahrungspflichtig sind alle E-Mails mit Geschäftsbezug, insbesondere:

- Angebote und Auftragsbestätigungen
- Rechnungen und Gutschriften
- Mahnungen und Zahlungsabsprachen
- E-Mails mit steuerlich relevanten Anhängen (z. B. PDF, CSV)

Rein interne Abstimmungen oder private Mitteilungen ohne Geschäftsbezug sind **nicht** aufbewahrungspflichtig.

3.3 Aufbewahrungsfristen

Tabelle

Art der Unterlage	Frist
Handels- und Geschäftsbriefe	6 Jahre
Steuerlich relevante Unterlagen (z. B. Rechnungen)	10 Jahre

> **Hinweis:** Die Frist beginnt jeweils mit dem Ende des Kalenderjahres, in dem die E-Mail entstanden ist. Diese Pflicht gilt für alle Unternehmensgrößen – auch für Einzelunternehmen und Freiberufler.

3.4 Anforderungen an die Archivierung (GoBD)

Eine einfache Ablage in Outlook-Ordnern, PST-Dateien oder ein reguläres Backup reicht **nicht** aus, um die gesetzlichen Anforderungen zu erfüllen. GoBD-konforme Archivierung bedeutet konkret:

- **Vollständigkeit**: Alle relevanten E-Mails müssen erfasst sein
- **Unveränderbarkeit**: Archivierte E-Mails dürfen nachträglich nicht verändert oder gelöscht werden können
- **Originalformat**: E-Mails sind im ursprünglichen Format zu speichern
- **Auffindbarkeit**: Jede E-Mail muss innerhalb angemessener Zeit auffindbar sein
- **Maschinelle Auswertbarkeit**: Die Daten müssen für Prüfungszwecke maschinell lesbar sein

3.5 DSGVO und Aufbewahrungspflicht – kein Widerspruch

Auf den ersten Blick scheinen DSGVO (Datenlöschung) und HGB/AO/GoBD (Aufbewahrung) im Konflikt zu stehen. Die Rechtslage ist jedoch eindeutig: **Gesetzliche Aufbewahrungspflichten haben Vorrang vor datenschutzrechtlichen Löschpflichten.**

Wichtig ist dabei: Dienstliche Postfächer sollten **nicht privat genutzt** werden. Eine klare Trennung zwischen privater und geschäftlicher Kommunikation erleichtert die rechtskonforme Handhabung erheblich.

---

4. Risiken bei der Nutzung von Freemail-Adressen

Tabelle

Risiko	Erläuterung

Keine revisionssichere Archivierung	Freemail-Postfächer bieten keine GoBD-konforme Archivierung
Geringe Sicherheitskontrolle	SPF, DKIM, DMARC oft nicht einstellbar
Drittanbieter-Abhängigkeit	AGB-Änderungen oder Dienstabschaltungen können Ihre Kommunikation betreffen
Unprofessionelle Außenwirkung	Vertrauensverlust bei Kunden und Geschäftspartnern
Erhöhtes Prüfungsrisiko	Bei Betriebsprüfungen kann fehlende Archivierung zu Problemen führen

---

5. Empfohlene Mindeststandards

Für einen rechtssicheren und professionellen E-Mail-Betrieb empfehlen wir:

1. **Eigene E-Mail-Domain** verwenden
2. **Zentrale, automatische Archivierung** einrichten
3. **Löschschutz** für relevante E-Mails aktivieren
4. **Verfahrensdokumentation** erstellen (für Betriebsprüfungen)
5. **Nutzungsrichtlinien** für Mitarbeiter festlegen (insbesondere: keine Privatnutzung dienstlicher Postfächer)

---

6. Optional: Cloud-E-Mail-Plattformen (z. B. Microsoft 365)

> *Dieser Abschnitt ist optional und richtet sich an Unternehmen, die Microsoft 365 oder vergleichbare Cloud-Dienste einsetzen oder planen.*

Cloud-Plattformen wie Microsoft 365 bieten eine leistungsfähige und moderne E-Mail-Infrastruktur – sind aber **nicht automatisch GoBD-konform konfiguriert**. Die bloße Speicherung im Cloud-

Postfach erfüllt die gesetzlichen Archivierungsanforderungen in der Regel nicht, da Nutzer E-Mails löschen oder verändern können und Prozesse häufig nicht dokumentiert sind.

Vorteile bei korrekter Konfiguration:

- Aufbewahrungsrichtlinien und Löschsperren direkt in der Plattform konfigurierbar
- Integrierte eDiscovery-Funktionen für gezielte Suche und Nachweisführung
- Audit-Protokolle für Zugriffs- und Änderungshistorie
- Einfache Integration externer, plattformunabhängiger E-Mail-Archivsysteme
- Datensicherung und E-Mail-Archivierung lassen sich gemeinsam abbilden

Bewährte Praxis: Cloud-E-Mail-Betrieb kombinieren mit einem **separaten, unabhängigen E-Mail-Archiv**, das E-Mails beim Senden und Empfangen automatisch erfasst – unabhängig davon, was im Postfach danach passiert.

---

7. Zusammenfassung

Eine eigene E-Mail-Domain ist heute der Mindeststandard für jedes professionell auftretende Unternehmen. Darüber hinaus ist die rechtskonforme Archivierung geschäftlicher E-Mails in Deutschland gesetzlich vorgeschrieben – unabhängig von Unternehmensgröße oder Branche. Freemail-Adressen sind im Geschäftsbetrieb aus rechtlichen wie aus Reputationsgründen nicht empfehlenswert. Cloud-Dienste können die Anforderungen erfüllen, erfordern aber gezielte Konfiguration und ergänzende Maßnahmen.