

E-Mail

Verbindung mit mobilen Geräten

umgezogen nach <https://wiki.ph-freiburg.de/!service/email:mobilgeraet>

Mailinglisten

umgezogen nach <https://wiki.ph-freiburg.de/!service/email:mailinglisten>

Webschnittstelle Horde

umgezogen nach <https://wiki.ph-freiburg.de/!service/email:horde>

E-Mail-Client einrichten

Thunderbird-Anleitung

umgezogen nach <https://wiki.ph-freiburg.de/!service/email:thunderbird>

Sicherheit bei der Nutzung von E-Mail

umgezogen nach <https://wiki.ph-freiburg.de/!service/email:sicherheit>

Zertifikat in E-Mailprogramm einrichten

Beschreibung für Horde: umgezogen nach
https://wiki.ph-freiburg.de/!service/email:horde#s_mime_zertifikat

Thunderbird

Um das Zertifikat einzurichten, muss dieses importiert werden. Dabei gehen Sie wie folgt vor:

- In Thunderbird klicken Sie auf Extras → Konten-Einstellungen → Ende-zu-Ende-Verschlüsselung.
- Nun auf „S/MIME-Zertifikate verwalten“ klicken.
- Im geöffneten Fenster „Zertifikatverwaltung“ kann das Zertifikat importiert werden. Dabei wird nach einem Kennwort gefragt. Hierfür verwenden Sie bitte das gleiche Kennwort welches Sie

beim Sichern der Zertifikatsdatei genutzt haben.

- Nach dem das Zertifikat importiert wurde, kann dieses über den „Auswählen...“-Button ausgewählt werden.
- Danach werden Sie gefragt, ob das Zertifikat auch zum Ver- und Entschlüsseln verwendet werden soll. Hier wählen Sie bitte „Nein“ aus.
- Nach diesem Schritt noch den Haken bei „Eigene digitale Unterschrift standardmäßig hinzufügen“ setzen



IMAP/SMTP Daten PH-Freiburg

umgezogen nach <https://wiki.ph-freiburg.de/!service/email:zugangsdaten>

IMAP-Ordner freigeben






umgezogen nach <https://wiki.ph-freiburg.de/!service/email:horde#mailordner>

Funktionsadresse, kooperatives Arbeiten





„Zusätzliche Mailadressen“ umgezogen nach <https://wiki.ph-freiburg.de/!service/email:adressen>

Gruppenmailbox

Da es sich bei der Gruppenmailbox auch um eine Hordeinstanz handelt, welche im Browser geöffnet wird, gibt es einen kleinen Workaround, falls schon eine Hordeinstanz (über pmail / smail) geöffnet wurde. (Ist dies nicht der Fall, können Sie ab Punkt 3 beginnen)

1. Firefox öffnen und oben rechts auf  (Menü öffnen) klicken
2. „Neues privates Fenster“ auswählen

3. Horde (<https://pmail.phfr.de>) in einem (neuen, privaten) Fenster öffnen
Auf „LogIn Gruppenmailbox“ klicken

4. Anmelden (Benutzername + Kennwort des zugeordneten Accounts)

5. Falls mehrere Gruppenmailboxes vorhanden sein sollen, wählen die entsprechende Gruppenmailbox aus.


Sind Sie der erste Nutzer, der sich an der Gruppenmailbox anmeldet, gehen Sie bitte wie folgt vor:

1. Einstellungen (Zahnrad) → Benutzereinstellungen → Webmail anklicken

2. Persönliche Angaben anklicken
3. Unter Standardidentität Namen, Standard-E-Mail (optional: Signatur) einpflegen

4. Speichern
5. Nun erhalten Sie eine E-Mail, in der Sie Ihre Identität bestätigen müssen (Link anklicken)

6. Daten kontrollieren und „Speichern“

7. Die Ersteinrichtung ist nun abgeschlossen

Falls Sie ein Gruppenmailzertifikat benötigen, können Sie sich gerne an support@ph-freiburg.de wenden.

Per Alias Mail verschicken

Nachdem für Sie beim Helpdesk ein Alias eingerichtet wurde, empfangen Sie die Mails der Aliasadresse.

Um unter der neuen Alias schreiben zu können, erstellt man im Mailclient ein weiteres Profil.

Dabei geht man folgendermaßen vor:

1. In Horde auf Zahnrad\Benutzereinstellungen\Webmail\Persönliche Angaben klicken
2. Unter „Wählen Sie eine Identität“ „Neue Identität anlegen“
3. Entsprechende Angaben tätigen. Wichtig ist, unter „Die Standard-E-Mail-Adresse für diese Identität:“ Ihren (neuen) Alias einzutragen
4. Speichern
5. Sie bekommen eine E-Mail, die bestätigt werden muss. (evtl. im SPAM-Ordner nach der Bestätigungs-Mail nachschauen)
6. Danach können Sie in Horde bei „Neue Nachricht“ unter „Von“ die zweite Identität auswählen

Falls Sie Thunderbird verwenden, finden Sie unter folgendem Link eine Anleitung:

<https://support.mozilla.org/de/kb/identitaeten-verwenden>

Abwesenheitsnachricht per Horde

umgezogen nach <https://wiki.ph-freiburg.de/!service/email:horde#abwesenheitsnotiz>

Gemeinsam genutzter Horde-Kalender oder Mailordner erstellen

umgezogen nach https://wiki.ph-freiburg.de/!service/email:horde#gemeinsame_nutzung

Dienstliche Daten und persönliche Schlüssel/Zertifikate

Wenn Sie dienstliche Daten verschlüsseln und dabei Ihr persönliches Zertifikat verwenden, können nur Sie und nicht Ihr Dienstherr auf die Daten zugreifen. Bei Verlust des Schlüssels, bei Todesfall, wenn Sie sich weigern oder nicht verfügbar sind o.a., kann der Dienstherr nicht mehr auf die dienstlichen Daten zugreifen.

Daher sollten dienstliche Daten, welche zu einem späteren Zeitpunkt nochmals verwendet werden sollen, nicht mit einem persönlichen Zertifikat verschlüsselt werden.

Als Alternative kann sich unter Umständen ein Gruppenzertifikate anbieten, doch auch hier gibt es Risiken: Scheiden Personen aus der Gruppe aus und hatten direkten Zugriff auf die Zertifikatsdaten mit dem privaten Schlüsseln, muss ein neues Zertifikat mit neuem Schlüsseln für diese Gruppe erstellt werden. Die alten Dokumente können aber nur mit altem Schlüssel gelesen werden. Das Schlüsselmanagement muss diesen Anforderungen gerecht werden können.

Verschlüsselung nur für eingeschränkten Nutzerkreis möglich

Bei der Verschlüsselung wird durch das Mailprogramm der Nachrichtentext zweimal, mit zwei verschiedenen, öffentlichen Schlüsseln verschlüsselt. Einmal mit dem eigenen Public Key, damit man die Korrespondenz selbst noch lesen kann und einmal mit dem Public Key des Empfängers. Daher gilt:

Nur wenn der Public Key des Empfängers vorliegt, wenn der Empfänger also selbst ein S/MIME Zertifikat hat, kann dieser die verschlüsselte Nachricht entschlüsseln und lesen.

Schlüsselverwaltung mehrerer Generationen, Verlust des Schlüssels

Prüfen und klären Sie vorab, ob und wie Ihr verwendetes Mailprogramm mit mehreren, oder alten, abgelaufenen Zertifikaten/Schlüsseln umgehen kann. Denn ein Zertifikat ist nur für eine begrenzte Zeit gültig. Danach muss es erneuert werden. Oft werden hierbei ebenso die Schlüsselpaare erneuert. Sie können auf alte, verschlüsselte Daten nur zugreifen, wenn Ihr Mailprogramm die passenden, alten Schlüssel vorhalten kann und installiert hat. Wird der Schlüssel verloren (z.B. durch Schaden o. Verlust des PCs) und ist keine Sicherung vorhanden, oder wird das Passwort zum Schutz des Schlüssels vergessen, sind die verschlüsselten Daten unwiederbringlich verloren.

Betrug, fälschliche Sicherheit und Virens Scanner

Ein Angreifer, ein Betrüger ein „Spammer“ kann Ihnen eine verschlüsselte und signierte E-Mail zuschicken. Er könnte hierfür mit einem gestohlenen Zertifikat unterschreiben, bzw. sich an verschiedenen Stellen selbst eines besorgt, erstellt haben. Signierte und verschlüsselte E-Mails können ebenso SPAM und Viren beinhalten!

Wenn Sie eine verschlüsselte E-Mail empfangen haben, kann kein Virens Scanner zuvor einen etwaigen Virus in dieser E-Mail erkennen. Bis zum Zeitpunkt der Entschlüsselung bleibt völlig unklar, was für Daten in der E-Mail enthalten sind. Sie sollten sich deshalb nicht in fälschlicher Sicherheit wiegen, wenn Sie eine signierte und auch noch verschlüsselte E-Mail erhalten. Es gilt hier besonders, die E-

Mail auf Plausibilität, auf ein gültiges Zertifikat hin zu prüfen und Dateianhänge nicht blind links zu öffnen.

Prüfen Sie genau den Absender, das dort verwendete Zertifikat. Trauen Sie nicht „blind“ signierten, besonders nicht noch verschlüsselten, E-Mails.

Inkompatibilitäten von Mailprogrammen

Die Entwicklung der Mailprogramme durch die verschiedenen Hersteller gewährt nicht immer, dass Technologien in allen Programmen gleich, bzw. überhaupt, vorhanden sind. Bevor ein Prozess auf verschlüsselte Mailkommunikation zwischen zwei Stellen festgelegt wird, ist zu prüfen und zu testen, ob die Gegenstellen problemlos Ihre Daten lesen und verarbeiten können. Bedauerlicherweise ist die Technologie S/MIME nicht in allen Mailprogrammen realisiert. Es sind auch Probleme zwischen unterschiedlichen Mailprogrammen mit S/MIME Unterstützung bekannt. Die Probleme könnten in zukünftigen Versionen behoben sein, aber auch erst noch auftauchen.

From:

<https://wiki.ph-freiburg.de/!zik/> - **HelpDesk Wiki**

Permanent link:

<https://wiki.ph-freiburg.de/!zik/email?rev=1727865836>

Last update: **2024/10/02 12:43**

