E-Mail

Verbindung mit mobilen Geräten

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

Mailinglisten

Als Hochschulmitglied kann man beim ZIK Mailinglisten beantragen und dann selbst verwalten. Die datenschutzrechtlichen Belange sind vom Antragsteller (Betreiber) zu berücksichtigen.

Mailinglisten können sehr unterschiedlich eingestellt werden. Besonders die Fragen, wer Post darüber verschicken darf und wer sich auf die Liste setzten darf, muss geklärt und vom Antragsteller eingestellt werden.

Die Mailadressen der Listen enden auf **@lists.ph-freiburg.de**. Unter dem **Name einer Mailingliste** wird das verstanden, **was vor dem @ steht**.

Zur Verwaltung der der Listen existiert eine Webseite. Darüber kann ein Betreiber einer Liste Einstellungen vornehmen, aber auch Besucher können sich informieren, welche Listen es gibt und Aktionen tätigen (vornehmlich abbestellen oder abonnieren, sowie Besuch des Listenarchivs).

Im Jahr 2023 erfolgt eine Umstellung der Mailinglistensoftware. Die Mailadressen und Namen der Listen bleiben erhalten. Alte und neue Software werden parallel betrieben.

Mailinglisten mit Mailman3

Unter listen.ph-freiburg.de ist die neue Software Mailman3 zu erreichen.

Mailman3 hat Benutzerprofile eingeführt.

Man kann auf einer Liste stehen, auch ohne dass man einen Login/Konto/Profil in Mailman3 angelegt hat. Diese Aktion kann man jederzeit nachholen.

Das Nutzerprofil in Mailman3 wird nach einem Login via DFN Shibboleht automatisch erstellt, oder nach manueller Registrierung selbst angelegt. Mailman3 ordnet dann automatisch diesem Profil etwaige Mailinglisten zu (sei es als Nutzer oder Admin) zu, auf welchen eine der Mailadresse(n) dieses Profils zu finden sind. Nach Anmeldung wird u.a. eine schöne Übersicht über die eigenen Abos angezeigt.

Hat man sich schon am Browser via Shibboleth für einen Dienst (Zoom, Bibliothekdienste u.v.a) bereits authentifiziert und besucht dann unsere Mailman3 Installation, ist man automatisch in Mailman3 auch eingeloggt (Grundfunktionalität der auf Shibboleth basierenden Diensten).

Die meisten Funktionen aus Mailman2 sind auch in Mailman3 zu finden, nur an etwas anderen Stellen. Das Archiv ist deutlich moderner und Leistungsfähiger. Die Übersicht zu den Listen lässt sich nach

dem Einloggen umschalten (siehe „Rolle“).

Zentral gepflegte Mailinglisten

Informationen über die von der Hochschule zentral gepflegten Mailinglisten für Rundschreiben an Personal oder Studierende finden Sie hier.

Webschnittstelle Horde

Bei der Webschnittstelle Horde handelt es sich um sog. Groupware; das Programm bietet außer dem Zugriff auf den E-Mail-Dienst die Nutzung von Kalendern, Adressbüchern und Aufgabenlisten sowie den Zugriff auf Dateiressourcen (Home- und Gruppenlaufwerke) der PH Freiburg.

Der Zugriff auf das Programm erfolgt mit einem Webbrowser über diese Adressen:

- Personal der PH-Freiburg: https://pmail.phfr.de
- Studierende der PH-Freiburg:https://smail.phfr.de

Module von Horde

Webmail

- Empfangen und Schreiben von E-Mails
- Anzeige von digital signierten E-Mails
- Einrichtung von Abwesenheitsmeldung („Filter“)
- Ordner teilen und freigeben
- Automatisches Einsortieren eingehender Post in Ordner („Filter“)
- Suchlisten erstellen / speichern oder und als Virtuelle Ordner festlegen.
- Synchronisation von E-Mails mit iPhone, Smartphone u.a.

Kalender

- Einrichten eines oder mehrerer Kalender
- Vergabe von Freigaben (teilen) einzelner Kalender (Gruppenkalender)
- Synchronisation von Kalender mit iPhone, Smartphone u.a.

Adressbuch

- Einrichten von einem oder mehreren Adressbüchern
- Vergabe von Freigaben (teilen) einzelner Adressbücher (Gruppenadressbuch)
- Synchronisation von Adressbuch mit iPhone, Smartphone u.a.

Zugriff auf Netzlaufwerke

- Unter dem Menüpunkt „Weitere\Dateimanager“ wird der Zugriff auf das Homelaufwerk und das Gruppenlaufwerk nur ggf. nach Antrag genehmigt.

Lesezeichen speichern

- Unter dem Menüpunkt „Weitere\Lesezeichen“ können Lesezeichen angelegt und verwaltet werden.

Abwesenheitsnotiz in Horde

Um eine automatisierte Abwesenheitsnotiz in Horde WebGroupware zu erstellen, gehen Sie folgendermaßen vor:

1. Im Menü öffnen Sie bitte „Webmail“ und klicken auf „Filter“
2. Wählen Sie nun „Abwesenheit“, um den Filter zu bearbeiten
3. Unter „Einfache Einstellungen“ geben Sie nun den Beginn und das Ende, sowie den Betreff und den Text Ihrer Abwesenheitsnachricht ein
4. Unter „Erweiterte Einstellungen“ können Sie weitere E-Mail-Adressen* angeben (voreingestellt ist Ihre „E-Mail-Adresse„). Nur noch die Anzahl der Tage festlegen, wie lange die Abwesenheitsnachricht verschickt werden soll.
5. Mit „Speichern“ wird die Vorlage Ihrer Abwesenheitsnachricht gespeichert. (mit „Speichern und Aktivieren“ wird die Abwesenheitsnachricht sofort aktiviert/gültig)

Falls Sie für Ihre Alias-Adresse(n) ebenfalls automatisch eine Antwortmail senden möchten, tragen Sie diese im oberen Feld **Meine E-Mail-Adressen** in jeweils eine neue Zeile zusätzlich ein **Wichtig:** Der Filter „Abwesenheit“ muss **UNBEDINGT** an letzter Stelle der Filterregeln stehen. Falls dies bei Ihnen nicht der Fall sein sollte, so bewegen Sie den Abwesenheitsfilter bitte (mit den Pfeilen rechts) an die letzte Stelle. Tun Sie das nicht, werden Spam-Mails von Ihnen automatisch beantwortet, sodass die PH-Freiburg auf die Blocklisten kommt!!!

E-Mail-Client einrichten

Thunderbird-Anleitung

1. Thunderbird starten und später als Standard festlegen.

2. Geben Sie nun unter „Bestehende E-Mail-Adresse einrichten“ folgendes ein:

- Ihr vollständiger Name (Nur, wenn nicht bereits vorhanden)
- Ihre E-Mail-Adresse
- Ihr Passwort, danach klicken Sie auf „Manuell einrichten“.

3. Geben Sie nun unter „Manuelle Einrichtung“ folgendes ein:

- Im Post**ein**gangsserver:
  - Protokoll: IMAP
  - Hostname: imap.ph-freiburg.de
  - Port: 993
  - Verbindungssicherheit: SSL/TLS (wird automatisch ausgefüllt)
  - Authentifizierungsmethode: Passwort, normal
  - **Benutzername:** abc123 (**Wichtig:** Hier müssen Sie Ihre eigene Benutzerkennung bzw. LogIn Kürzel eintragen)

- Im Post**aus**gangsserver:
  - Hostname: smtp.ph-freiburg.de
  - Port: 465
  - Verbindungssicherheit: SSL/TLS (wird automatisch ausgefüllt)
  - Authentifizierungsmethode: Passwort, normal
  - **Benutzername:** abc123 (**Wichtig:** Hier müssen Sie Ihre eigene Benutzerkennung bzw. LogIn Kürzel eintragen)

4. Als nächsten Schritt muss überprüft werden, ob die Einstellungen korrekt sind und der Server gefunden wird:
5. Klicken Sie dazu auf „Erneut testen“

- Wenn nun der folgende Hinweis auftaucht, können Sie auf „Fertig“ klicken.

- Zum Abschluss erscheint die Information, dass Ihr Konto erfolgreich hinzugefügt wurde. Sie können nun auf „Beenden“ klicken.

Sicherheit bei der Nutzung von E-Mail

HTML-Format

Dienstliche E-Mails sind grundsätzlich nur im reinen Text-Format zu verfassen (Kanzlerrundschreiben 10 vom 07.01.2016).
Hintergrund: HTML-Mails können einerseits Schadcode aus dem Netz nachladen und andererseits die Leser der E-Mail ausspionieren.

Umgang mit Anhängen

Lassen Sie beim Öffnen von Anhängen äußerste Vorsicht walten.
E-Mails mit schädlichem Anhang sind inzwischen auf einem hohen sprachlichen Niveau und können durchaus Bezug nehmen auf reale Prozesse wie z. B. Bewerbungen und Bestellungen.
Vergewissern Sie sich beim geringsten Zweifel beim Absender auf einem alternativen Kanal (Telefon) von der Echtheit der E-Mail.

Lokale Speicherung von E-Mails

Wenn Sie auf einem mobilen Gerät ein E-Mail-Programm verwenden, welches die E-Mails auf einem lokalen Datenträger speichert (z. B. Thunderbird), muss dieser unbedingt verschlüsselt werden für den Fall, dass das Gerät gestohlen wird oder verloren geht.
Besser: auf mobilen Geräten nur das Webmailprogramm Horde verwenden.

Digitale Signatur

Durch Zuhilfenahme der Digitalen Signatur im E-Mailverkehr werden folgende (Ende-zu Ende) Verbesserungen eingeführt:

1. Die wahre Identität einer Person hinter einer E-Mailadresse wird erkennbar.
2. Der Inhalt einer E-Mail wurde auf ihrem Weg vom Absender zum Empfänger nicht manipuliert.
3. Bei Bedarf lässt sich auch der Inhalt einer E-Mail durch Verschlüsselung schützen.

Um selbst digital signierte E-Mails lesen und überprüfen zu können, benötigt man in aller Regel keine weiteren Hilfsmittel. Viele Mailprogramme beherrschen diese Funktionalität von Haus aus. Will man hingegen signierte E-Mails selbst verschicken können, muss man bei einer speziellen Organisation seine Identität und E-Mailadresse überprüfen lassen. Bei diesem Vorgang wird ein elektronisches Zertifikat erstellt, welches Sie dann in Ihrem Mailprogramm verwenden können.

Infos zur Beantragung eines S/MIME Zertifikats finden Sie hier ...

Besitzen Sie bereits ein Zertifikat, können Sie dieses auch im E-Mailprogramm einrichten (s.u.).

Zertifikat in E-Mailprogramm einrichten

Horde Webgroupware

Melden Sie sich in der Horde Webgroupware an (https://pmail.phfr.de).

Öffnen Sie die Benutzereinstellungen (unterhalb des „Rädchens“) von Webmail. Im „S/MIME“- Bereich unter „Ihr persönliches S/MIME Zertifikat“ wird gegebenenfalls Ihr altes Zertifikat angezeigt.

Dieses können Sie durch einen Klick auf „Persönliches …“ löschen. Nur dann können Sie das neue Zertifikat importieren!

Die Standardeinstellungen sehen wie folgt aus:

Klicken Sie hier auf „Persönliches Zertifikat importieren“ und wählen die zuvor gesicherte Zertifikatsdatei aus.

Im ersten der zwei Passwortfelder geben Sie das Zertifikatsdatei-Passwort ein (beim Sichern aus Firefox festgelegt worden), im zweiten Feld setzen Sie ein Kennwort, mit welchem der Zugriff auf die Zertifikatsdaten geschützt werden soll. Dieses zweite Kennwort wird einmalig pro Sitzung in Horde verlangt. Klicken Sie danach auf „Importieren“.

Öffnen Sie die Benutzereinstellungen (unterhalb des „Rädchens“) von Webmail. Unter „Neue Nachricht“ wählen Sie bitte „Erstellen“ aus. Ändern Sie unter „Ihre Standard-Verschlüsselungsmethode beim Verschicken von Nachrichten:“ den Eintrag auf„Unterzeichnen (S/MIME)“ .

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

- Post**ein**gangsserver: IMAP, Serveradresse: imap.ph-freiburg.de, Port: 993 mit SSL
- Post**aus**gangsserver: SMTP, Serveradresse: smtp.ph-freiburg.de, Port: 465 mit SSL oder Port 587 und 25 mit StartTLS

Es werden nur E-Mails zum Versand angenommen, wenn die darin verwendete Absenderadresse Ihrem Login zugeordnet werden kann.
Sollte ihr Mailprogramm einen Authentifizierungstyp erfragen, so verwenden sie bitte PLAIN.

Als Login/Benutzername ist ihr PH-Login (z.B. muellerfr/xyz123) anzugeben.

Wichtig: Bei SMTP muss ebenfalls Login und Kennwort verwendet werden.
Andernfalls könnten sie nur E-Mails an unsere eigene Maildomain richten (Beispiel: support@ph-freiburg.de klappt, support@gmx.de kommt mit Fehler „relay access denied“ zurück).

IMAP-Ordner freigeben

In der Mail-Komponente von Horde können IMAP-Ordner folgendermaßen für andere Hochschulmitglieder freigegeben werden:
- einen Rechtsklick auf den betreffenden Ordner
- dann auf „ACL bearbeiten“,.
- dann den Login eintragen,
- dann dort im Pulldown wo „Vorlagen:“ steht idR „Alle“ Rechte vergeben und dann
- unten auf „Speichern“ klicken.

Funktionsadresse, kooperatives Arbeiten

Die PH bietet folgende Möglichkeiten des kooperativen Arbeitens über Funktionsadressen an:

1. Alias
Eine Alias-Adresse ist eine (Funktions-) E-Mail Adresse, die Ihrem und ggf. weiteren PH-Accounts zugeordnet werden kann.
E-Mails an diese Adresse werden allen Personen mit dieser Alias-Adresse zugestellt.

2. Gruppenmailbox
Eine Gruppenmailbox ist ein spezielles Postfach mit eigener E-Mail-Adresse, welches mit Ihrem und weiteren PH-Accounts verknüpft werden kann.
Über Horde können zugeordnete Nutzer der Gruppenmailbox auf ein gemeinsames Postfach zugreifen (Einbindung in externes Mailprogramm ist nicht möglich).

Die Nutzer der Gruppenmailbox können von einem Verantworlichen (Moderator) über einen Service im ZIK-Portal verwaltet werden.

3. Mailing-Liste
Eine Mailingliste bietet einem geschlossenen Personenkreis die Möglichkeit des Nachrichtenaustauschs.
Sie besteht aus einer Liste von E-Mail-Adressen, die selbst eine E-Mail-Adresse in der Form [listenname]@lists.ph-freiburg.de hat.
Nachrichten an diese Adresse werden allen Mitgliedern der Mailingliste an die eingetragene E-Mail-Adresse weitergeleitet.
Unsere Mailinglistensoftware (mailman) läßt sich über ein Webinterface dabei so einstellen, dass entweder alle Mitglieder direkt Nachrichten an diese Liste verschicken dürfen,
der Moderator jede Nachricht der Mitglieder an die Liste freigeben muss (moderierte Liste) oder,
dass nur der Moderator der Mailingliste selbst das Recht hat Nachrichten an die Mitglieder der Liste zu versenden (Newsletter).

Falls Sie Bedarf an einer Funktionsadresse / Mailingliste haben und / oder kooperativ mit anderen

Personen arbeiten möchten, schreiben Sie unter Angabe der Wunschadresse und ggf. der beteiligten Personen eine E-Mail an support@ph-freiburg.de, wir finden dann gemeinsame mit Ihnen die beste Lösung.

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 Gruppenmailboxen 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

Am besten können Sie die Abwesenheitsnachricht über Horde einrichten, das geht wie folgt ganz einfach.

1. Horde öffnen und anmelden
2. Auf „Webmail“ gehen nun „Filter“ auszuwählen.
3. Dies führt Sie zu den „Filterregeln“
4. Das Wort „Abwesenheit“ anklicken
5. Dort können Sie Beginn und Ende der Nachrichten, denn Betreff der E-Mail und auch den Inhalt (Grund) angeben.
6. Auf „Erweiterte Einstellungen“ klicken (oberhalb des Punktes „Beginn der Abwesenheit“)
7. Dort Ihre Mailadresse (Meine E-Mail-Adresse) angeben
8. Speichern und Aktivieren klicken
9. Nun ist die Abwesenheitsmail für den angegebenen Zeittraum aktiv.

Gemeinsam genutzter Horde-Kalender erstellen

1. In Horde anmelden und zu „Kalender“ navigieren
2. Neben „Meine Kalender“ klicken Sie bitte das Plus-Symbol an, um einen (weiteren) Kalender zu erstellen.
3. Eine aussagekräftigen Kalendernamen verwenden und die gewünschte Farbe auswählen
4. Zu „Teilen“ navigieren
    1. Hier können Sie, durch einen Klick auf „Mit den Benutzern:“, im unteren Feld die Logins der zu berechtigten Personen eintragen.
    (Das Format der Benutzernamen bei alten Logins ist z.B. musterfraufr und bei den Neueren z.B. abc123 / Studierende-Accounts können nicht berechtigt werden)
    Durch eine kommagetrennte Eingabe von Benutzernamen können Sie mehrere Personen berechtigen, wie z.B.: musterfraufr, abc123, xyz789
    2. Im nächsten Schritt vergeben Sie jeweils die Berechtigungen, was eine Person darf. Die Standardeinstellung ist „Termine zu lesen“
    In diesem Fall kann nur der/die Ersteller*in Termine hinzufügen. Bei „Termine zu lesen und zu bearbeiten“ darf jede der oben aufgeführte Benutzer*in Termine lesen/erstellen.
    3. Wenn Sie möchten das die freigegebene Person auch Termine löschen kann. Klicken Sie auf „Erweiterte Rechte-Einstellungen“ und setzen Sie dann den Haken bei Löschen.

5. Nach dem Klick auf „Speichern“ wird der Kalender erstellt
6. Der/Die Ersteller*in sieht nun den neuen Kalender unter „Meine Kalender“. Über das Stiftsymbol kann der Kalender bearbeitet werden.
7. Die berechtigten Benutzer*innen sehen nun den neuen Kalender unter „Gemeinsame Kalender“. Standardmäßig ist dieser eingeklappt und wird über das Dreiecksymbol auf der linken Seite sichtbar.
8. Um den gemeinsamen Kalender in der Ansicht (parallel zum eigenen) anzeigen zu lassen, setzen Sie den den entsprechenden Haken vor den Benutzer*innen.
9. Durch den Klick auf „Neuer Termin“ oder in den Kalender, erstellen Sie einen Termin. Soll dieser nun für alle Benutzer*innen gelten, wählen Sie bei „Termin hinzufügen zu:“ den gemeinsamen Kalender aus.
10. Zuletzt müssen Sie den Termin noch „Speichern“.

Gemeinsam genutzter Horde-Mailordner

1. In Horde anmelden und zu „Webmail“ navigieren
2. Rechtsklick auf den Ordner, den Sie freigeben möchten
3. „ACL bearbeiten“ klicken
4. Nun können Sie bei Benutzer den PH-LogIn der Person eingeben, die die Zugriffsberechtigung erhalten soll
5. Mit der Vorlage können Sie verschiedene Vorlagenmodelle auswählen oder individuell setzen, welche Berechtigungen die Person bekommen sollen.
6. Speichern klicken

Ordner bei Kollege*Innen

1. In Horde unter Webmail „Ordneraktionen“ anklicken
2. „Alle Ordner anzeigen“ auswählen
3. Der freigegebene Ordner wird nun unter „user“ → „LogIn des Besitzers angezeigt

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 Virenscanner

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 Virenscanner 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.