Digitale Signatur

Durch Zuhilfenahme der Digitalen Signatur im E-Mailverkehr werden folgende 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.

Die Pädagogische Hochschule Freiburg ist als Mitglied des Deutschen Forschungsnetzes e.V. somit auch Mitglied im GÉANT, dem pan-europäische Internet-Verbindungsnetzwerk. Darüber dürfen wir den Dienstleister Sectigo zum Beantragen und Ausstellen von Digitale Signaturen in Anspruch nehmen.

Für die Beantragung eines persönlichen Zertifikats (Voraussetzung Beschäftigt an der PH Freiburg und Inhaber eines PH Accounts) besuchen Sie bitte die unten stehende Webseite und melden Sie sich mit Ihrem PH Account an. Beachten Sie bitte:

- Ihr im Zertifikat verwendeter Name ist voreingestellt und nicht änderbar.
- Nur für die an der PH-Freiburg für Sie als primär hinterlegte Mailadresse wird das Zertifikat ausgestellt.

Wird ein Zertifikat für eine andere Mailadresse (Funktionsadresse, Gruppenmailbox o.a.) benötigt, dann nehmen Sie bitte per E-Mail Kontakt mit dem ZIK-Support auf.

Sollten Sie den Verdacht haben, dass Ihr Zertifikat in fremde Hände gelangt ist, muss das Zertifikat umgehend gesperrt werden. Bitte setzen Sie sich aber in jedem Fall mit dem ZIK-Helpdesk in Verbindung.

Beantragen einer digitalen Signatur

Adresse zur Beantragung: Sectigo Certificate Manager

Wichtig: Im Folgenden müssen Sie ein Passwort setzen. Dies darf keine Umlaute und Sonderzeichen aus dem erweiterten ASCI Raum haben, also z.B. kein ö, ä, ü, ß oder € (u.a.).

- Die Webseite ist in englischer Sprache, ebenso die Lizenzvereinbarung (dort „Eula“ genannt). Wir können dies nicht ändern.
- Als „Certificale Profile“ wählen Sie „GÉANT Personal email signing and encryption“ aus.
- Bei „Term“ kann die maximale Laufzeit gewählt werden.
- Als „Enrollment Method“ wählen Sie bitte „Key Generation“ aus.
- Bei „Key Type“ empfehlen wir „RSA - 4096“.
- Mit dem anzugebenden Passwort schützen Sie die dann im folgenden angebotene Datei mit

„.p12“ Endung. In dieser Datei ist auch ihr privater, schützenswerter Key. Obigen Hinweis zu Sonderzeichen beachten!
- Unter „Choose key protection algorithm“ wird „Secure AES256-SHA256“ empfohlen.

Die Zertifikatsdatei (.p12) wird standardmäßig unter „Downloads“ gespeichert. Sie sollten Ihr Zertifikat noch in die PH-Zertifikatsdatenbank im ZIK-Portal importieren. Ihr Zertifikat wird dadurch an zentraler Stelle gespeichert und Sie benötigen keine weitere Sicherungskopie mehr.

Zertifikat mit privatem Schlüssel sichern

Gehen Sie dabei wie folgt vor:

1. Melden Sie sich im Portal mit Ihrem PH-Account an. Wählen Sie unter den angezeigten Services die „Zertifikatsdatenbank“ aus. Über „PKCS#12-Datei importieren“ öffnet sich das unten angezeigte Fenster. Über „Datei wählen“ wählen Sie bitte die Zertifikats-Datei aus, die Sie auf das (z.B.) persönliche Homelaufwerk gesichert/gespeichert haben. Verwenden Sie unter „Zertifikatsdatei-Passwort“ das Kennwort, welches Sie bei der Beantragung verwendet haben. Wenn Sie kein Import Passwort angeben, wird das Zertifikatsdatei-Passwort auch für den Import des Zertifikats in die Datenbank verwendet.
   Drücken Sie dann „Importieren“.

Wichtig: Merken Sie sich dieses Passwort gut, schreiben Sie es auf und verwahren Sie es an einem sicheren Ort. Sollten Sie es vergessen, muss ein neues Zertifikat beantragt werden.

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

Durch Zuhilfenahme der Digitalen Signatur im E-Mailverkehr werden folgende 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.

Die Pädagogische Hochschule Freiburg ist als Mitglied des Deutschen Forschungsnetzes e.V. somit auch Mitglied im GÉANT, dem pan-europäische Internet-Verbindungsnetzwerk. Darüber dürfen wir den Dienstleister Sectigo zum Beantragen und Ausstellen von Digitale Signaturen in Anspruch nehmen.

Für die Beantragung eines persönlichen Zertifikats (Voraussetzung Beschäftigt an der PH Freiburg und Inhaber eines PH Accounts) besuchen Sie bitte die unten stehende Webseite und melden Sie sich mit Ihrem PH Account an. Beachten Sie bitte:

- Ihr im Zertifikat verwendeter Name ist voreingestellt und nicht änderbar.
- Nur für die an der PH-Freiburg für Sie als primär hinterlegte Mailadresse wird das Zertifikat ausgestellt.

Wird ein Zertifikat für eine andere Mailadresse (Funktionsadresse, Gruppenmailbox o.a.) benötigt, dann nehmen Sie bitte per E-Mail Kontakt mit dem ZIK-Support auf.

Sollten Sie den Verdacht haben, dass Ihr Zertifikat in fremde Hände gelangt ist, muss das Zertifikat umgehend gesperrt werden. Bitte setzen Sie sich aber in jedem Fall mit dem ZIK-Helpdesk in Verbindung.

Beantragen und Verwenden einer digitalen Signatur

Weiterleitung zur Info-Seite Digitale Signatur

Beantragen

Adresse zur Beantragung: Sectigo Certificate Manager

Wichtig: Im Folgenden müssen Sie ein Passwort setzen. Dies darf keine Umlaute und Sonderzeichen aus dem erweiterten ASCI Raum haben, also z.B. kein ö, ä, ü, ß oder € (u.a.).

- Die Webseite ist in englischer Sprache, ebenso die Lizenzvereinbarung (dort „Eula“ genannt). Wir können dies nicht ändern.
- Als „Certificale Profile“ wählen Sie „GÉANT Personal email signing and encryption“ aus.
- Bei „Term“ kann die maximale Laufzeit gewählt werden.
- Als „Enrollment Method“ wählen Sie bitte „Key Generation“ aus.
- Bei „Key Type“ empfehlen wir „RSA - 4096“.
- Mit dem anzugebenden Passwort schützen Sie die dann im folgenden angebotene Datei mit „.p12“ Endung. In dieser Datei ist auch ihr privater, schützenswerter Key. Obigen Hinweis zu Sonderzeichen beachten!
- Unter „Choose key protection algorithm“ wird „Secure AES256-SHA256“ empfohlen.

Die Zertifikatsdatei (.p12) wird standardmäßig unter „Downloads“ gespeichert. Sie sollten Ihr Zertifikat noch in die PH-Zertifikatsdatenbank im ZIK-Portal importieren. Ihr Zertifikat wird dadurch an zentraler Stelle gespeichert und Sie benötigen keine weitere Sicherungskopie mehr.

Zertifikat mit privatem Schlüssel sichern

Gehen Sie dabei wie folgt vor:

1. Melden Sie sich im Portal mit Ihrem PH-Account an. Wählen Sie unter den angezeigten Services die „Zertifikatsdatenbank“ aus. Über „PKCS#12-Datei importieren“ öffnet sich das unten angezeigte Fenster. Über „Datei wählen“ wählen Sie bitte die Zertifikats-Datei aus, die Sie auf das (z.B.) persönliche Homelaufwerk gesichert/gespeichert haben. Verwenden Sie unter „Zertifikatsdatei-Passwort“ das Kennwort, welches Sie bei der Beantragung verwendet haben. Wenn Sie kein Import Passwort angeben, wird das Zertifikatsdatei-Passwort auch für den Import

des Zertifikats in die Datenbank verwendet.
Drücken Sie dann „Importieren“.

Wichtig: Merken Sie sich dieses Passwort gut, schreiben Sie es auf und verwahren Sie es an einem sicheren Ort. Sollten Sie es vergessen, muss ein neues Zertifikat beantragt werden.

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

Herunterladen

Über das ZIK Portal kann die Zertifikatsdatei nach dem Sichern beliebig oft auf anderen Geräten heruntergeladen werden.

- ZIK-Portal aufrufen
- Mit PH Account anmelden
- Klicken Sie den Service **Zertifikatdatenbank** an
- Schaltfläche **PKCS#12-Export** beim gewünschten Zertifikat anklicken
- Als Import Passwort das **Zertifikat Passwort** eingeben und den Download mit der Schaltfläche **Exportieren** starten

Zertifikat in Zertifikatspeicher importieren

Um das Zertifikat für das Signieren von PDF Dateien verwenden zu können, muss es zunächst in den Zertifikatspeicher des Betriebssystems importiert werden.

Windows

- Zertifikatdatei öffnen (Doppelklick)
- Dem Assistenten folgen (Voreinstellungen müssen nicht angepasst werden)
- Das beim Beantragen vergebene Zertifikat Passwort eingeben
- Nach Abschluss des Importvorgangs kann das Zertifikat zum Unterschreiben von PDFs mit Foxit PDF Editor verwendet werden

macOS

- Zertifikatdatei öffnen (Doppelklick)
- Das beim Beantragen vergebene Zertifikat Passwort eingeben
- Nach Abschluss des Importvorgangs kann das Zertifikat zum Unterschreiben von PDFs mit Foxit

PDF Editor verwendet werden

Zertifikat verwenden

PDF Dateien digital signieren mit Foxit PDF Editor

Nachdem das Zertifikat in den Zertifikatspeicher des Betriebssystems importiert wurde, kann es zum Signieren von PDFs mit dem Foxit PDF Editor / Adobe Acrobat Reader verwendet werden.

Verfügbare Anleitungen

- PDF Dateien digital signieren mit Foxit PDF Editor (im Reiter „Foxit PDF Editor“)
- Beispiel: EDV Beschaffungsantrag korrekt bearbeiten

Importieren des Zertifikats im Mail Client

Um Mails signieren zu können, muss das Zertifikat zusätzlich im verwendeten Mail Client eingerichtet werden.

Verfügbare Anleitungen

- Horde Webgroupware
- Thunderbird