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.

Die europäische eIDAS-Verordnung gibt den Rahmen unserer gesetzingen Grundlagen dieser Signaturen (siehe auch Signaturgesetz) vor. Drei Arten, frei gesprochen „Qualitätsstufen“ gibt es, siehe hierzu auch DFN-PKI FAQ, oder auch die gute Zusammenfassung der Bundesdruckerei. Wir bieten hier die Fortgeschrittene elektronische Signatur (FES) an. Diese genügt **nicht**, um eine gesetzlich vorgeschriebenen Schriftformerfordernis, also unsere Unterschrift, zu ersetzten. Allerdings können Vertragspartner, Einrichtungen natürlich definieren und festlegen, was sie alles mit dieser Forgeschrittenen Signatur anerkennen.

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.

Verwendung des S/MIME Zertifikats in Anwendungen

Im Wiki zu E-Mail und auch bei anderen Anwendungen finden Sie Hinweise zur Integration und Verwendung Ihres S/MIME Zertifikats.