Nutzerzertifikate

Hochschulmitglieder - mit Ausnahme der Studierenden - können mit Hilfe der DFN-PKI digitale Nutzerzertifikate nach dem X.509 Standard erhalten, die nach einer Identitätsfeststellung zur Signierung und Verschlüsselung von Dateien/Dokumenten und E-Mails geeignet sind. Bitte beantragen Sie Nutzerzertifikate nur nach Rücksprache mit dem HRZ.

Beantragung

Bei der Beantragung eines Nutzerzertifikats wird auf Ihrem PC und unter Ihrer Benutzerkennung in dem von Ihnen verwendeten Webbrowser ein Schlüsselpaar generiert, welches im weiteren Verlauf von der DFN-PKI signiert wird.

Bitte beantragen Sie Ihr Nutzerzertifikat auf der folgenden Webseite unter dem Punkt Zertifikate / Nutzerzertifikat:

- HS-WOE CA - G2

WICHTIG: Führen Sie diesen Vorgang nicht in einem öffentlichen Poolraum aus.

Folgen Sie den Hinweisen auf der Webseite. Am Ende der Beantragung werden Sie aufgefordert, den Zertifikatsantrag auszudrucken. **Hier bitten wir darauf zu achten, dass Sie den Antrag auf einem (!) doppelseitig bedruckten Blatt drucken.** Bringen Sie bitte diesen Zertifikatsantrag eigenhändig unterschrieben unter Vorlage eines gültigen, amtlichen Ausweisdokumentes in das Hochschulrechenzentrum.

Ausstellung

Nach erfolgter Prüfung erhalten Sie von der DFN-PKI eine E-Mail, in der das weitere Vorgehen beschrieben ist. Folgen Sie hier bitte den Anweisungen in der E-Mail.

WICHTIG: Führen Sie diesen Vorgang an demselben PC, unter derselben Benutzerkennung und im selben Webbrowser aus, den Sie bei der Beantragung des Nutzerzertifikates verwendet haben.

Am Ende der Prozedur liegt ein gültiges Nutzerzertifikat zur Benutzung vor. Das Zertifikat befindet sich je nach benutztem Webbrowser bei der Antragstellung an unterschiedlichen Orten:

- Microsoft Internet Explorer: Extras / Internetoptionen / Inhalte / Zertifikate: Karte „Eigene Zertifikate“
- Mozilla Firefox: Einstellungen / Erweitert / Zertifikate / Zertifikate anzeigen / Ihre Zertifikate

Sicherung

Sofort nach der Ausstellung sollten Sie Ihr Nutzerzertifikat in eine Datei sichern. Der Export ist wichtig für folgende Funktionen:

- Import des Nutzerzertifikates in den Windows Zertifikatsspeicher Windows Cryptographic Service Provider (CSP)
- Import des Nutzerzertifikates in andere Softwareprodukte (z.B. Mozilla Firefox und Thunderbird)
- Import des Nutzerzertifikates in ein Security-Token (Smartcard)

Die Prozedur unterscheidet sich etwas je nach verwendetem Webbrowser bei der Beantragung:

Microsoft Internet Explorer: Einstellungen / Internetoptionen / Inhalte / Zertifikate: Karte „Eigene Zertifikate“ Doppelklicken Sie Ihr Nutzerzertifikat und notieren Sie sich das beginnende Gültigkeitsdatum (Gültig ab) in der folgenden Form: JJJJ-MM-TT. Schließen Sie das Fenster mit „OK“. Markieren Sie Ihr Nutzerzertifikat und klicken Sie auf „Exportieren“. Folgen Sie den Anweisungen und exportieren Sie hierbei unbedingt den privaten Schlüssel mit und vergeben Sie ein starkes Kennwort mit mindestens 8 Zeichen. Als Dateiname sollten Sie folgende Notation verwenden:

- <JJJJ-MM-TT>_DFN-Verein_Global_Issuing_CA_<Vorname_Nachname>.pfx

Mit Hilfe des Buttons „Durchsuchen“ wählen Sie einen geeigneten Speicherort außerhalb Ihres PCs (z.B. Laufwerk Z:\Zertifikate) aus. Merken Sie sich das dazugehörige Kennwort, um das Nutzerzertifikat im Bedarfsfall wiederherstellen zu können.

Mozilla Firefox: Einstellungen / Datenschutz & Sicherheit / Bereich Zertifikate: Zertifikate anzeigen / Ihre Zertifikate Doppelklicken Sie Ihr Zertifikat und notieren sich das Datum unter Gültigkeitsdauer / Beginnt mit in der folgenden Form: JJJJ-MM-TT. Schließen Sie das Fenster mit „Schließen“. Klicken Sie auf „Sichern“. Als Dateinamen sollten Sie folgende Notation verwenden:

- <JJJJ-MM-TT>_DFN-Verein_Global_Issuing_CA_<Vorname_Nachname>.p12

Vergeben Sie ein starkes Kennwort mit mindestens 8 Zeichen. Speichern Sie diese Datei außerhalb Ihres PCs (z.B. Laufwerk Z:\Zertifikate). Merken Sie sich das dazugehörige Kennwort, um das Nutzerzertifikat im Bedarfsfall wiederherstellen zu können.

Wichtig: Bitte bewahren Sie Ihre abgelaufenen Nutzerzertifikate ebenfalls auf. Sie benötigen diese zur Kontrolle von Signaturen und zur Entschlüsselung von E-Mails.