

DFN-Zertifikat

Inhaltsverzeichnis

- 1 Allgemeines
- 2 Zertifikat beantragen
- 3 Zertifikat installieren
- 4 Zertifikat nutzen
- 5 Detaillierte Anleitungen zur Verwendung

Allgemeines

Die Hochschule Mittweida ist Teil der PKI (Public-Key-Infrastruktur) des DFN und Zertifizierungsstelle für die Angehörigen der Hochschule. Damit haben alle Angehörigen der Hochschule die Möglichkeit, ein persönliches Zertifikat beim DFN zu beantragen.

Die Zertifikate werden von der Hochschule nach Prüfung der Identität des Antragstellers freigeschaltet. Zertifikate werden nur an Personen ausgestellt. Das Verfahren zur Beantragung eines persönlichen Zertifikats muss von jeder Person selbst durchgeführt werden. Mit Hilfe eines Zertifikates können E-Mails vom Absender digital signiert werden. Digital signierte E-Mails geben dem Empfänger die Sicherheit, dass

1. Der Absender der Mail verbindlich geprüft werden kann
2. Der Inhalt der Mail während der Übertragung nicht geändert wurde.

An den Inhaber eines Zertifikats können verschlüsselte E-Mails gesendet werden, wenn dieser seinen öffentlichen Schlüssel bereitstellt.

Zertifikat beantragen

Die Beantragung des Zertifikats geschieht auf der Seite <https://pki.pca.dfn.de/hs-mittweida-ca-g2/pub>

Wählen Sie die Registerkarte **Nutzerzertifikat** und folgen Sie den Anweisungen am Bildschirm.

Wenn Sie wollen, dass Ihnen Partner verschlüsselte E-Mails schicken können, müssen Sie einer Veröffentlichung des Zertifikats im Verzeichnisdienst des DFN zustimmen. Das NCC empfiehlt die Veröffentlichung.

Danach erhalten Sie eine E-Mail des DFN mit einem Link zu einem PDF-Dokument, welches sie ausdrucken und unterschreiben müssen. Dieses Dokument und ein amtliches Ausweisdokument muss persönlich zur Verifikation ihren Identität im NCC vorgelegt werden. Berechtigt zur Überprüfung sind an der Hochschule Mittweida Herr Herzberg und Herr Lühr im NCC.

Nach erfolgreicher Identifikations-Prüfung erfolgt die Freischaltung des Zertifikats. Es wird Link zum Zertifikat vom DFN an den Antragssteller gesendet. Über diesen Link können sie das Zertifikat (p12-Datei) herunterladen und anschließend auf ihren Rechner installieren. Sie sollten ihr Zertifikat zudem sichern (bspw. persönlicher Netzwerkspeicher), damit sie bei einer Neuinstallation oder o.ä. wieder darauf zugreifen können.

Zertifikat installieren

Um das Zertifikat mit ihrem Mailprogramm nutzen zu können, muss ihr persönliches Zertifikat im Zertifikatsspeicher der Anwendung oder Zertifikatsspeicher des Betriebssystems hinterlegt werden. Bei der Installation des Zertifikats in den Zertifikatsspeicher müssen sie die Zertifikats-PIN eingeben, welche sie bei der Erstellung angegeben haben.

Zertifikat nutzen

Die Einbindung und Verwendung des Zertifikats gestaltet sich je nach Betriebssystem, Anwendungsprogramm und verwendeten Version sehr unterschiedlich. Generell sollte man auf den Hilfeseiten des jeweiligen Programms unter den Stichworten "Zertifikat", "S/MIME" oder "Signieren/Verschlüsseln" fündig werden. Unter dem nachfolgenden Abschnitt finden sie einige spezielle Anleitungen zu häufig verwendeten Programmen.

Detaillierte Anleitungen zur Verwendung

Die nachfolgenden detaillierten Anleitungen beziehen sich auf die beispielhafte Verwendung von Zertifikaten in den angebenen Programmen:

- [Verwendung von Zertifikaten mit Microsoft Outlook 2016](#)
- [Verwendung von Zertifikaten mit Thunderbird](#)
- [Verwendung unter Apple iOS](#)