

Themen:

- Übersicht PKI-Services der LUH
- Nutzerzertifikate unter TCS/Sectigo
- Persönliche Identifizierungen
- SAP-Smartcard

Übersicht über die PKI-Services der LUH

- Browser-verankerte Zertifikate über:
 - GÉANT "Trusted Certificate Service" (GÉANT TCS)
 - Nutzer- und Serverzertifikate
- Nicht browserverankerte Zertifikate
 - DFN-PKI Community PKI
 - Verschiedene mögliche Szenarien
 - z.B. SAP-Smartcard
 - Geeignet für hochschulübergreifende Zusammenarbeit.
- Übersicht:
<https://www.luis.uni-hannover.de/de/services/it-sicherheit/zertifikate-der-luh-ca/zertifikatshierarchie-und-ras>

Themen:

- Übersicht PKI-Services der LUH
- Nutzerzertifikate unter TCS/Sectigo
- Persönliche Identifizierungen
- SAP-Smartcard

Nutzerzertifikate unter TCS/Sectigo: Allgemeines

- TSC-Sectigo-Zertifikate haben eine Laufzeit von 2 Jahren.
- Beantragung erfolgt über ein Webformular.
- Identifizierung über
 - signierte Mail
 - Postident
 - Neu: Im Institut durch akkreditierte Person
- Zertifikatabholung nach Erhalt eines Einladungslinkes.
- Mails von Sectigo werden unsigniert verschickt.

Nutzerzertifikate unter TCS/Sectigo: Zertifikatstypen

- Persönliche Zertifikate
 - Profil: GÉANT Personal signing and encryption
 - Common Name: Vorname Nachname
 -
- Gruppenzertifikate (für Funktions-Mailadressen)
 - Profil: GÉANT Organisation email signing
 - Common Name: Mailadresse
- Schritt-für-Schritt-Anleitung zur Beantragung auf der Webseite
<https://www.luis.uni-hannover.de/de/services/it-sicherheit/zertifikate-der-luh-ca/nutzerzertifikate>

Nutzerzertifikate unter TCS/Sectigo: Anleitungen

- Einbinden der Zertifikate:
 - Menüpunkt „Anleitungen“ auf der Zertifikate-Webseite
 - Schritt-für-Schritt-Anleitung für einzelne Mailclients
 - Dokumentation von Problemen:
 - Entweder innerhalb der Anleitung .
 - Unterhalb der jeweiligen Anleitung:
 - Probleme / Troubleshooting
 - Häufiger Problemfall: Veralteter Hash-Algorithmus in Outlook
- Signieren von PDF-Dokumenten: Schritt-für-Schritt-Anleitung für
 - Acrobat (Windows)
 - Okular (Linux)
 - Libre Office

Themen:

- Übersicht PKI-Services der LUH
- Nutzerzertifikate unter TCS/Sectigo
- Persönliche Identifizierungen
- SAP-Smartcard

Persönliche Identifizierungen:

- Standard:
 - Postident für Erstbeantragungen und Sonderfälle.
 - Signierte Mail für Wiederholungsbeantragungen.
 - Passwortübermittlung z.B. bei zweiter Mailadresse
- Nur im Ausnahmefall:
 - Terminvergabe für Einzel-Identifikationen im LUIS
- Hinweise:
 - Die Identifizierung muss vorliegen bevor das Zertifikat ausgestellt werden kann.
 - Postident vor der Beantragung durchführen.
 - Eine Identifizierung gilt für eine Person, nicht für einen bestimmten Zweck.

Persönliche Identifizierungen: Vor Ort im Institut (1):

Voraussetzungen:

- Eine von der Institutsleitung zur Ausführung dieser Tätigkeit akkreditierte Person.
- Die Akkreditierung erfolgt über ein Akkreditierungsformular.
- Teil des Akkreditierungsformulars ist ein Aufklärungsblatt.
- Das Akkreditierungsformular wird digital signiert von
 - Akkreditierter Person
 - Institutsleitung
 - Anschließend von der akkreditierten Person per signierter Mail eingesandt an:
 - akkreditierung@ca.uni-hannover.de

Persönliche Identifizierungen: Vor Ort im Institut (2) :

Geplanter Ablauf nach erfolgreicher Akkreditierung:

- Die Dokumentation jeder Identifizierung erfolgt einzeln.
 - Mail an eine dedizierte Mailadresse im LUIS.
 - Mail signiert mit persönlichem Zertifikat.
- Nachdem diese Dokumentationsmails im LUIS eingegangen sind, können die Zertifikate beantragt werden.

Bei Interesse: Bitte beim Zertifikatsteam melden.

- Keine ausführliche Dokumentation online, Hinweis geplant. Unterlagen werden auf Anfrage versendet.
- Neu eingeführt, deshalb: Abläufe und Regelungen können sich unter Umständen noch ändern.

Themen:

- Übersicht PKI-Services der LUH
- Nutzerzertifikate unter TCS/Sectigo
- Persönliche Identifizierungen
- SAP-Smartcard

SAP-Smartcard: Neue Beantragungssoftware

- Beantragung über eine Portallösung (noch Pilotbetrieb)
 - SAP-Zertifikat auf der Leibniz-Card
 - Leibnizcard muss mit einem Smartcard-HSM versehen werden
 - Die Leibniz-Card muss im Portal einer Person zugeordnet werden.
 - Erfolgt in Absprache mit SAP-Support in der ZUV
 - SAP-SUPPORT@zuv.uni-hannover.de
- Identifizierung
 - Standard: Signierte Mail
 - Postident bei Neueinstellungen und Namensänderungen.

- SAP-Smartcard: Software-Voraussetzungen
 - Aktuelles OpenSC
 - Aktuelle Treibersoftware für Reader
 - Bei Fragen: Kontakt zur SAP-Basis
 - sapbasis@luis.uni-hannover.de
 - Java-Applikation namens ocf_cc.jar
 - Für Smartcard-Anmeldung am Portal über Browser
 - Erste Dokumentationen zu Beantragung und Hilfe für KeyUser/administrierende Personen:
 - [Link zur noch provisorischen Dokumentationsseite](#)
 - Bei Fragen zur Zertifikatbeantragung: Kontakt zum SAP-Support der ZUV oder zum SAP-Zertifikatsteam:
 - zertifikatsteam@luis.uni-hannover.de

Haben Sie Fragen?

Für Fragen, die Ihnen später noch einfallen:

zertifikatsteam@luis.uni-hannover.de