Leibniz Universität IT Services

Leibniz Universität Hannover

Zertifikatsbetrieb an der LUH

LUIS Sicherheitstage 27. und 28. 02.2024

Webseite Zertifikate:
https://www.luis.uni-hannover.de/de/services/it-sicherheit/zertifikate-der-luh-ca/

Themen:

- Übersicht PKI-Services der LUH
- Nutzerzertifikate unter TCS/Sectigo
  - Allgemeines
  - Auftretende Probleme und Lösungen
- Persönliche Identifizierungen

Übersicht über die PKI-Services der LUH

- Browser-verankerte Zertifikate über:
  - GÉANT "Trusted Certificate Service" (GÉANT TCS)
    - Derzeitiger PKI-Dienstleister Sectigo
      - Sectigo Certificate Manager (SCM)
- Nicht browserverankerte Zertifikate
  - DFN-PKI Community PKI
    - Verschiedene mögliche Szenarien.
    - Auch für hochschulübergreifende Zusammenarbeit.
- Übersicht sowie Links zu Wurzel- und Intermediate-Zertifikaten

  https://www.luis.uni-hannover.de/de/services/it-sicherheit/zertifikate-der-luh-ca/zertifikatshierarchie-und-ras

- DFN-PKI Global 2 (noch aufgeführt, aber auslaufend).

DFN Community-PKI

- Wurzelzertifikat der Community PKI CA muss auf allen Systemen installiert sein.
- Längere Laufzeiten sind möglich
- Alle für Serverzertifikate akkreditierten Personen können über die Community-CA Zertifikate beantragen.
- Beantragung:

  https://pki.pca.dfn.de/dfn-pki/dfn-verein-community-ca/3990/
- Quittungs-PDF als Anhang einer digital signierten Mail einsenden.
  - antrag@ca.uni-hannover.de
  - Betreff: Community CA: <Dateiname Quittungs-PDF>

https://www.luis.uni-hannover.de/de/services/it-sicherheit/zertifikate-der-luh-ca/zertifikate-community-ca

Themen:

- Übersicht PKI-Services der LUH
- Nutzerzertifikate unter TCS/Sectigo
  - Allgemeines
  - Auftretende Probleme und Lösungen
- Persönliche Identifizierungen

Nutzerzertifikate unter TCS/Sectigo: Allgemeines 1

- Umstellung von DFN-PKI zu TCS-Sectigo zum 30.08.2023
- Unter der DFN-PKI ausgestellte Zertifikate bleiben bis zum Ende ihrer Laufzeit weiterhin gültig.
- TSC-Sectigo-Zertifikate haben eine Laufzeit von 2 Jahren.
- Kein Einsenden von Papieranträgen notwendig.
- Beantragung erfolgt über ein Webformular.
- Identifizierung über signierte Mail oder Postident.
- Zertifikatabholung nach Erhalt eines Einladungslinkes.
- Mails von Sectigo werden unsigniert verschickt.

Nutzerzertifikate unter TCS/Sectigo: Allgemeines 2

- Persönliche Zertifikate
  - Profil: GÉANT Personal signing and encryption
  - Common Name: Vorname Nachname
- Gruppenzertifikate (für Funktions-Mailadressen)
  - Profil: GÉANT Organisaton email signing
  - Common Name: Mailadresse
  - Auch für ein Gruppenzertifikat wird ein Personen-Datensatz für die beantragende Person im SCM angelegt
- Schritt-für-Schritt-Anleitung auf der Webseite

  https://www.luis.uni-hannover.de/de/services/it-sicherheit/zertifikate-der-luh-ca/nutzerzertifikate

Nutzerzertifikate unter TCS/Sectigo: Allgemeines 3

- Hinweise
  - Signiertes Mail senden über Listserv:
    - Nicht über Listserv direkt möglich.
    - Mails signiert aus dem Mailclient an die Liste senden.
    - Listserv darf an dieser Mail keine Änderungen mehr vornehmen.
      - Die Liste muss entsprechend umkonfiguriert werden.
      - Wichtige Informationen (z.B. Abmeldelink) direkt in die Mail eintragen.

https://www.luis.uni-hannover.de/de/services/it-sicherheit/zertifikate-der-luh-ca/anleitungen/listserv

  - Generell: Git Commits können auch mit Nutzerzertifikaten signiert werden.

Themen:

- Übersicht PKI-Services der LUH
- Nutzerzertifikate unter TCS/Sectigo
  - Allgemeines
  - Auftretende Probleme und Lösungen
- Persönliche Identifizierungen

Nutzerzertifikate unter TCS/Sectigo: Probleme und Lösungen 1

- Einbinden der Zertifikate:
  - Menüpunkt „Anleitungen“ auf der Zertifikate-Webseite
  - Abschnitt „E-Mail: Einbinden des Nutzerzertifikats „
  - Schritt-für-Schritt-Anleitung für einzelne Mailclients
  - Dokumentation von Problemen:
    - Auf häufig auftretende Probleme wird direkt innerhalb der Anleitung verwiesen.
    - Seltener auftretende Effekte: Unterhalb der Anleitung der jeweiligen Clients unter der Überschrift:
      - Probleme / Troubleshooting

Nutzerzertifikate unter TCS/Sectigo: Probleme und Lösungen 2

- Beispiele für Probleme bei der Einbindung von Nutzerzertifikaten:
  - Unspezifische Fehlermeldungen wie
    - Aufforderung zum Einstecken einer Smartcard
    - "Das eingegebene Kennwort ist falsch"
    - "Fehler im zugrunde liegenden Sicherheitssystem. Ungültigen Anbietertyp angegeben“
  - Signatur wird nicht als gültig anerkannt
  - Versand leerer E-Mails

Nutzerzertifikate unter TCS/Sectigo: Probleme und Lösungen 3

- Signieren von PDF- Dokumenten
  - Diverse Konfigurationseinstellungen sind notwendig
  - Menüpunkt „Anleitungen“ auf der Zertifikate-Webseite
  - Abschnitt „PDF“
    - Schritt-für-Schritt-Anleitung für
      - Acrobat (Windows)
      - Okular (Linux)

- Trotz allem Probleme? Kontakt zum Zertifikatsteam

Themen:

- Übersicht PKI-Services der LUH
- Nutzerzertifikate unter TCS/Sectigo
  - Allgemeines
  - Auftretende Probleme und Lösungen
- Persönliche Identifizierungen

Persönliche Identifizierungen 1: Aktuelle Möglichkeiten

- Standard:
  - Postident für Erstbeantragungen.
  - Signierte Mail für Wiederholungsbeantragungen.
  - Postident für Sonderfälle
- Nur im Ausnahmefall:
  - Terminvergabe für Einzelidentifikationen im LUIS
- Hinweise:
  - Die Identifizierung muss vorliegen bevor das Zertifikat ausgestellt werden kann.
  - Eine Identifizierung gilt für eine Person, nicht für einen bestimmten Zweck.

Persönliche Identifizierungen 2: Pilot vor Ort im Institut :

Voraussetzungen:

- Eine von der Institutsleitung zur Ausführung dieser Tätigkeit akkreditierte Person.
- Die Akkreditierung erfolgt über ein Akkreditierungsfomular.
- Teil des Akkreditierungsformulares ist ein Aufklärungsblatt mit:
  - Erläuterungen zur Bedeutung der persönlichen Identifizierung.
  - Hinweisen zu unabdingbaren Gegebenheiten, um die Identifizierung vornehmen zu können.
- Das Akkreditierungsfomular wird digital signiert von
  - Akkreditierter Person
  - Institutsleitung

Persönliche Identifizierungen 3: Pilot vor Ort im Institut

- Die Akkreditierte Person bestätigt mit Ihrer Signatur:
  - Sich der Bedeutung der übernommenen Tätigkeit bewusst zu sein.
  - Die übernommene Tätigkeit sorgfältig und unter Einhaltung aller kommunzierten Regelungen auszuführen.
- Die Institutsleitung bestätigt mit Ihrer Signatur:
  - Sich der Bedeutung dieser an eine institutsangehörige Person übertragenen Tätigkeit bewusst zu sein.
  - Die institutsangehörige Person im Bewusstsein der Bedeutung dieser übertragenen Tätigkeit ausgewählt zu haben.

Persönliche Identifizierungen 4: Pilot vor Ort im Institut :

- Akkreditierung und Aufklärungsblatt werden von der akkreditierten Person per signierter Mail eingesandt an: akkreditierung@ca.uni-hannover.de

- Auch diese Mail signiert mit dem persönlichem Zertifikat der akkreditierten Person.

Persönliche Identifizierungen 5: Pilot vor Ort im Institut :

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.

- Es handelt sich vorerst noch um einen „Pilotbetrieb“.
- Abläufe und Regelungen können sich unter Umständen noch ändern.

Haben Sie Fragen?

Für Fragen, die Ihnen später einfallen:

zertifikatsteam@luis.uni-hannover.de