noSpamProxy®

Version 13

Einbindung von D-Trust in NoSpamProxy Encryption

ENCRYPTION PROTECTION LARGE FILES DISCLAIMER

Net at Work
Building IT-Excellence.

Rechtliche Hinweise

Net at Work GmbH
Am Hoppenhof 32a
D-33104 Paderborn
Deutschland

Dieses Dokument wurde zuletzt am 03. September 2019 überarbeitet.

Inhalt

Hinweise und Voraussetzungen

Die folgende Hardware und Software ist für die Nutzung von D-Trust-Zertifikaten in NoSpamProxy Encryption erforderlich:

- Smartcard
- Kartenlesegerät
- PIN
- **neXus Personal Desktop**
- OpenSSL

HINWEIS: Das Zertifikat, das auf der Smartcard hinterlegt ist, kann nicht exportiert oder direkt in NoSpamProxy benutzt werden. Es dient lediglich der Authentifizierung als Operator an der Weboberfläche. Mit Hilfe des Zertifikats erzeugen Sie dann ein Systemzertifikat, das in NoSpamProxy zur Nutzung des Konnektors hinterlegt wird.

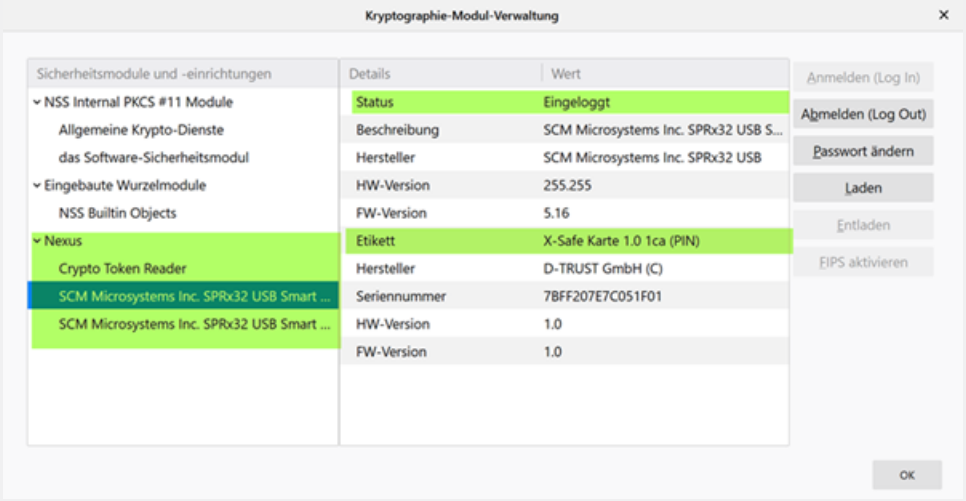
HINWEIS: OpenSSL ist standardmäßig in Linux-Betriebssystemen enthalten. Eine Installer-Datei zur kostenfreien Installation von OpenSSL unter Windows finden Sie unter **http://slproweb.com/products/Win32OpenSSL.html**.

Browser-Einstellungen (Firefox)

Um die Kommunikation Ihres Kartenlesegeräts durch nexXus Personal mit der SmartCard zu ermöglichen, müssen Sie die folgenden Einstellungen in Ihrem Firefox-Browser vornehmen:

1. Starten Sie Firefox und gehen Sie zu **Firefox-Einstellungen**.
2. Gehen Sie zu **Datenschutz & Sicherheit** und scrollen Sie zu **Zertifikate**.
3. Klicken Sie **Kryptographie-Module...** und dann **Laden**.
4. Vergeben Sie einen beliebigen Modulnamen und klicken Sie **Durchsuchen...**.
5. Navigieren Sie in das Nexus-Programmverzeichnis:
   - 32-Bit OS: **C:\Program Files\Personal\bin**
   - 64-Bit OS: **C:\Program Files (x86)\Personal\bin**
   - 64-Bit OS und Firefox 64-Bit: **C:\Program Files (x86)\Personal\bin64**
6. Wählen Sie die Programmbibliothek **personal.dll** (Firefox 64-Bit: **personal64.dll**).
7. Klicken Sie **Öffnen**.

Folgende Ansicht sehen Sie nach dem Anlegen in der Übersicht des Firefox-Browsers:



Systemzertifikat erstellen

1. Melden Sie sich am Certificate Service Manager an (CSM).

   - Testzugang zum CSM: **https://staging.d-trust.net/csm**
   - Reguläres CSM: **https://my.d-trust.net/csm/**
2. Klicken Sie **Login mit Operatorkarte**.

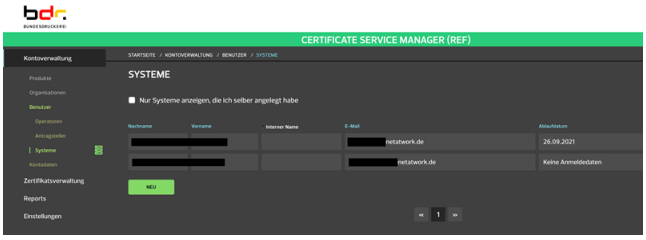
   > Es öffnet sich ein Fenster der Software neXus Personal.

3. Geben Sie Ihre PIN ein.
4. Erstellen Sie über OpenSSL einen Schlüssel, indem Sie folgendes in die Kommandozeile eingeben:
   `openssl genrsa -out private.key 2048`
5. Erstellen Sie über OpenSSL mit Hilfe des Schlüssels einen Certificate Signing Request (CSR):
   `openssl req -new -key private.key -out request.csr`

6. Öffnen Sie die Datei **request.csr** und kopieren Sie den Inhalt in die Zwischenablage.

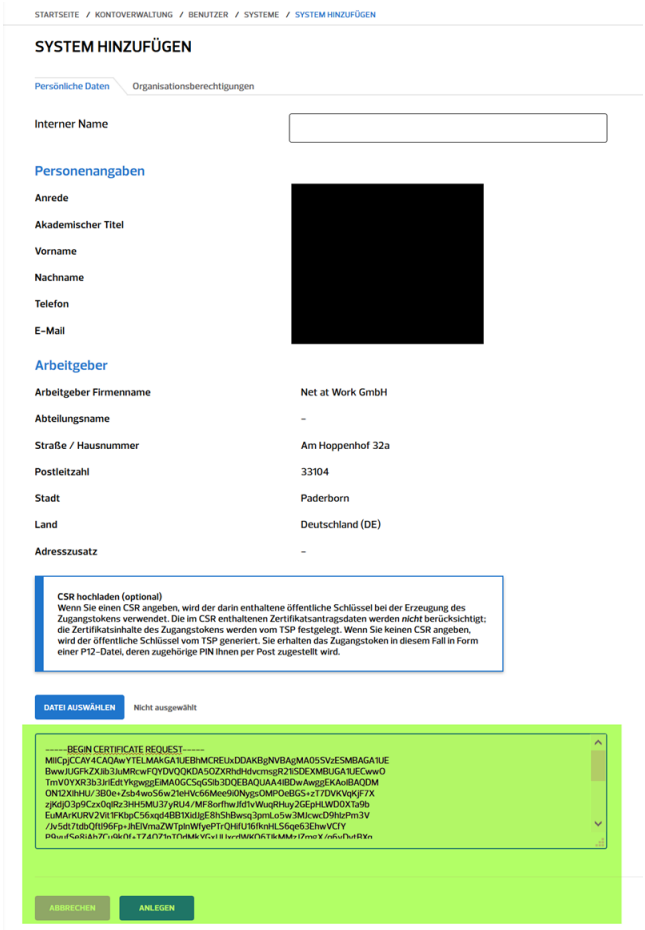
Systemzertifikat an D-Trust senden

1. Öffnen Sie den Certificate Service Manager.
2. Gehen Sie zu **Startseite > Kontoverwaltung > Benutzer > Systeme**.



3. Klicken Sie **Neu**.

4. Scrollen Sie an das Ende der Seite.



5. Geben Sie einen internen Namen für das System ein.
6. Führen Sie einen der beiden folgenden Schritte durch:
   - Klicken Sie **Datei auswählen** und laden Sie die Datei **request.csr** hoch.
   - Kopieren Sie den Inhalt der Datei **request.csr** aus der Zwischenablage in das grüne Eingabefeld.
7. Klicken Sie **Anlegen**.

HINWEIS: Das Zertifikat wird nun verarbeitet. Der zugehörige PIN wird Ihnen über den Postweg zugestellt.

TIPP: Den Status Ihres Zugangstokens können Sie unter **Startseite > Einstellungen > Meine Zugangstoken** überprüfen.

Erstellen des Schlüsselmaterials

Nach Durchführung der vorangegangenen Schritte bekommen Sie von D-Trust eine E-Mail, die den öffentlichen Schlüssel als Anhang beinhaltet. Mit Hilfe dieses öffentlichen Schlüssels sowie des privaten Schlüssels erstellen Sie nun das benötigte Schlüsselmaterial/Schlüsselpaar.

1. Geben Sie Folgendes in die Kommandozeile ein:
   `openssl pkcs12 -export -inkey Pfad/des/privaten/Schlüssels.key -in Pfad/des/öffentlichen/Schlüssels.pem -name mail -out NameDesSchlüsselpaars.pfx`

   > **HINWEIS:** Geben Sie hierbei die entsprechenden Pfade der Schlüssel und den Namen für das Schlüsselpaar an.

2. Gehen Sie in der NoSpamProxy-Konsole zu **Menschen und Identitäten > Zertifikate > Zertifikatsverwaltung**.
3. Klicken Sie **Importieren** und dann **Zertifikate wählen**.
4. Wählen Sie das erstellte Zertifikat und klicken Sie **Weiter**.
5. Klicken Sie **Fertigstellen**.

D-Trust in NoSpamProxy einbinden

1. Gehen Sie in der NoSpamProxy-Konsole zu **Menschen und Identitäten > Anforderung kryptographischer Schlüssel > Anbieter für die Anforderung von kryptographischen Schlüsseln**.
2. Klicken Sie **Hinzufügen**.
3. Wählen Sie als Typ **D-Trust** aus und klicken Sie **Weiter**.
4. Geben Sie einen Anbieternamen an und wählen Sie das Operator-Zertifikat aus.
5. Geben Sie den Namen der Zertifikatsvorlage und die Operator-Adresse an.

   > **HINWEIS:** Den Namen der Zertifikatsvorlage finden Sie im Certificate Service Manager von D-Trust unter **Kontoverwaltung > Produkte > Produktdetails**.

6. Klicken Sie **Weiter** und dann **Fertigstellen**.

Hilfe und Unterstützung

Wir freuen uns, dass Sie sich für NoSpamProxy® entschieden haben!

Bei Fragen zu NoSpamProxy oder diesem Dokument stehen Ihnen folgende Ressourcen zur Verfügung:

KNOWLEDGE BASE

Die **Knowledge Base** enthält weiterführende technische Informationen zu unterschiedlichen Problemstellungen.

WEBSITE

Auf der **NoSpamProxy-Website** finden Sie Handbücher, Whitepaper, Broschüren und weitere Informationen zu NoSpamProxy.

BLOG

Das **Blog** bietet technische Unterstützung, Hinweise auf neue Produktversionen, Änderungsvorschläge für Ihre Konfiguration, Warnungen vor Kompatibilitätsproblemen und vieles mehr. Die neuesten Nachrichten aus dem Blog werden auch auf der Startseite der NoSpamProxy-Managementkonsole angezeigt.

NOSPAMPROXY-SUPPORT

Unser Support-Team erreichen Sie

- per Telefon unter **+49 5251304-636**
- per E-Mail unter **support@nospamproxy.de**.

Wir wünschen Ihnen viel Erfolg und Spaß mit NoSpamProxy®.