Einbindung von D-Trust in NoSpamProxy Encryption

Version 14

Net at Work
Building IT-Excellence.

Rechtliche Hinweise

Alle Rechte vorbehalten. Dieses Dokument und die darin beschriebenen Programme sind urheberrechtlich geschützte Erzeugnisse der Net at Work GmbH, Paderborn, Bundesrepublik Deutschland. Änderungen vorbehalten. Die in diesem Dokument enthaltenen Informationen begründen keine Gewährleistungs- und Haftungsübernahme seitens der Net at Work GmbH. Die teilweise oder vollständige Vervielfältigung ist nur mit schriftlicher Genehmigung der Net at Work GmbH zulässig.

Copyright © 2023 Net at Work GmbH

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

Microsoft®, Windows®, Microsoft Exchange®, SQL Server®, SQL Server Express®, Windows Server 2008®, Windows Server 2012®, Windows Server 2012 R2®, Windows Server 2016®, Microsoft .NET Framework®, Microsoft Report Viewer®, Microsoft Office®, Microsoft 365®, Office 365®, Microsoft Outlook®, Microsoft Visual Studio® und Azure® sind eingetragene Handelsmarken der Microsoft Corporation. NoSpamProxy® und 32Guards® sind eingetragene Handelsmarken der Net at Work GmbH. Alle anderen verwendeten Handelsmarken gehören den jeweiligen Herstellern beziehungsweise Inhabern.

DIESES DOKUMENT WURDE ZULETZT AM 27. NOVEMBER 2023 ÜBERARBEITET.

Inhalt

Hinweise und Voraussetzungen 1

Browser-Einstellungen (Firefox) 2

Systemzertifikat erstellen 4

Systemzertifikat an D-Trust senden 6

Erstellen des Schlüsselmaterials 9

D-Trust in NoSpamProxy einbinden 10

Hilfe und Unterstützung 11

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**.

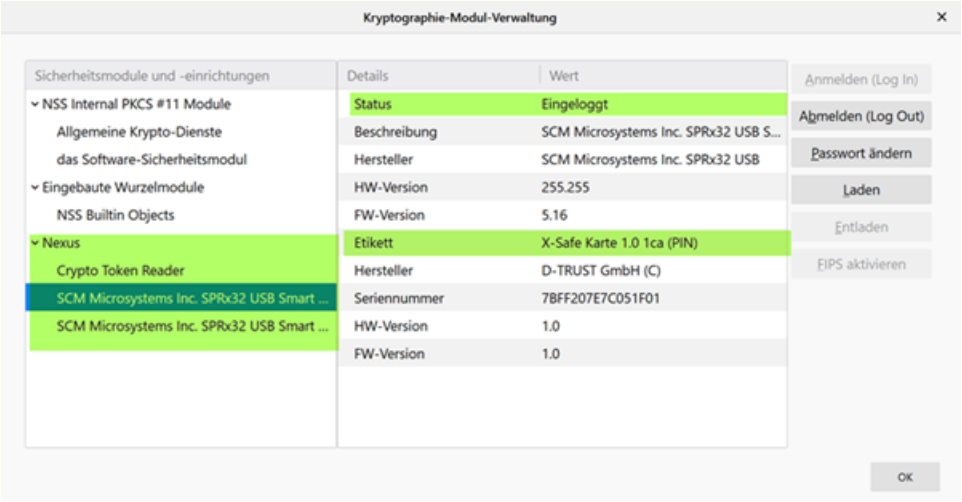
Browser-Einstellungen (Firefox)

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:



D-Trust in NoSpamProxy einbinden

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`

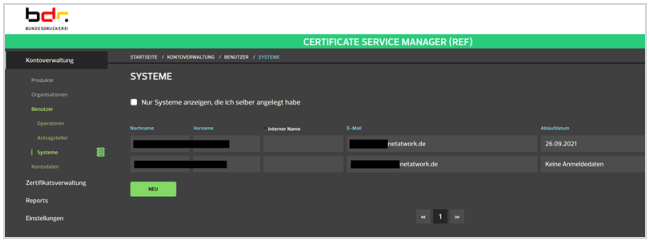
6. Öffnen Sie die Datei **request.csr** und kopieren Sie den Inhalt in die Zwischenablage.

```
-----BEGIN CERTIFICATE REQUEST-----
MIICpjCCAY4CAQAwYTELMAkGA1UEBhMCREUxDDAKBgNVBAgMA05SVzESMBAGA1
BwwJUGFkZXJib3JuMRcwFQYDVQQKDA5OZXRhdHdvcmsgR2liSDEXMBUGA1UECw
TmV0YXR3b3JrIEdtYkgwggEiMA0GCSqGSIb3DQEBAQUAA4IBDWAwggEKAoIBAQ
ON12XIhHU/3BOe+Zsb4woS6w21eHVc66Mee9iONygsOMPOeBGS+zT7DVKVqKjF
zjKdjO3p9CzxOqIRz3HH5MU37yRU4/MF8orfhwJfd1vWuqRHuy2GEpHLWDOXTa
EuMArKURV2Vit1FKbpC56xqd4BB1XidJgE8hShBwsq3pmLo5w3MJcwcD9hIzPm
/Jv5dt7tdbQftl96Fp+JhElvmaZWTpInwfyePTrQHifU16fknHLS6qe63EhwVC
P9yufSe8jAhZCu9kOf+TZ4OZ1pTOdMkYGxUUxcdWKO6TJkMMzJZmgX/q6yDvtB
l6JcxDKACA99gMRyCQMbAgMBAAGgADANBgkqhkiG9w0BAQsFAAOCAQEAq2voeB
U9EiAX2df9TOsKi+QLsiof7rPcu8KDvjaldDpNDw6vHO4667MGucxZJrk4rrWq
Zwq96BQXXnVppTTf9A1kSWV5gSMyz8eOXESOBmrmnsPbpOQJJgYVGzZ+aGoPN8
+UXEe2tLtGMp3lm/uRZFDgAlxVqlFne/kmHmwFkDyWApiBqin2nl3GCWGtaZnN
LkJ34EGEGaSeV8ho/Y5cPVtE64uneCmfPiel7Dg+LaT29H3HOdN05zwOOkhwvM
Mw4VSXtC7NtCH33r+vQf9zsZyX+pHeanYWI2s+5us4YtkFGJDLOcRUdpQEDD/i
1aFrNyZPR+NQTw==
-----END CERTIFICATE REQUEST-----
```

D-Trust in NoSpamProxy einbinden

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 im NoSpamProxy Command Center zu **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 im NoSpamProxy Command Center zu **Identitäten > Anforderung kryptographischer Schlüssel > Anbieter für Schlüsselanforderungen**.
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 falls gefordert 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

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.

NoSpamProxy-Forum

Das **NoSpamProxy-Forum** gibt Ihnen die Gelegenheit, sich mit anderen NoSpamProxy-Anwendern auszutauschen, sich zu informieren sowie Tipps und Tricks zu erhalten und diese mit anderen zu teilen.

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 des NoSpamProxy Command Center angezeigt.

YouTube

In unserem **YouTube-Kanal** finden Sie Tutorials, How-tos und andere Produktinformationen, die Ihnen das Arbeiten mit NoSpamProxy erleichtern.

NoSpamProxy-Support

Unser Support-Team erreichen Sie

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