



Version 13

Einbindung von D-Trust in NoSpamProxy Encryption



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 © 2019 Net at Work GmbH

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

Microsoft®, Windows®, Windows Server 2008®, Windows Server 2012®, Windows Server 2012 R2®, Windows Server 2016®, Microsoft Office®, Office 365® und Azure® sind eingetragene Handelsmarken der Microsoft Corporation. NoSpamProxy® ist eine eingetragene Handelsmarke der Net at Work GmbH. Alle anderen verwendeten Handelsmarken gehören den jeweiligen Herstellern beziehungsweise Inhabern.

Dieses Dokument wurde zuletzt am 03. September 2019 überarbeitet.

Inhalt

Hinweise und Voraussetzungen	1
Browser-Einstellungen (Firefox)	2
Systemzertifikat erstellen	3
Systemzertifikat an D-Trust senden	5
Erstellen des Schlüsselmaterials	8
D-Trust in NoSpamProxy einbinden	9
Hilfe und Unterstützung	10

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.



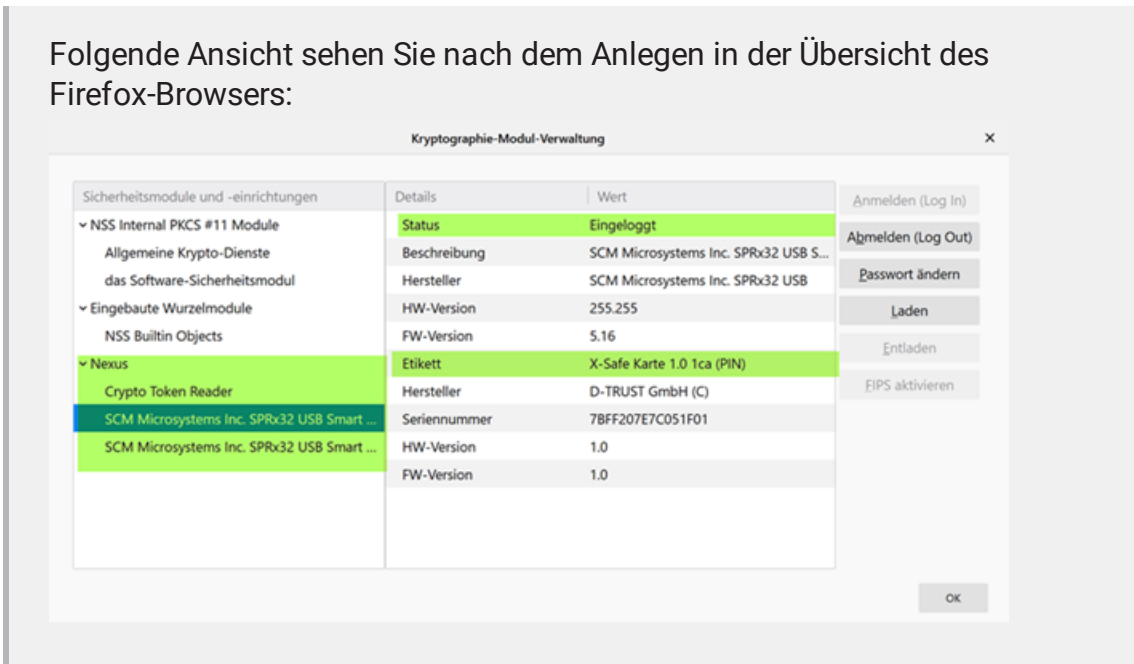
HINWEIS: OpenSSL ist standardmäßig in Linux-Betriebssystemen enthalten. Eine Installer-Datei zur kostenfreien Installation von OpenSSL unter Windows finden Sie unter <http://slproweb.com/products/Win32OpenSSL.html>.

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.

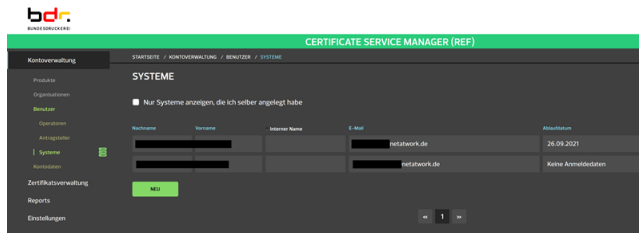
3. Geben Sie Ihre PIN ein.
4. Erstellen Sie über OpenSSL einen Schlüssel, indem Sie folgendes in die Kommandozeile eingeben:
`openssl genrsa -out private.key 2048`
5. Erstellen Sie über OpenSSL mit Hilfe des Schlüssels einen Certificate Signing Request (CSR):
`openssl req -new -key private.key -out request.csr`

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

```
-----BEGIN CERTIFICATE REQUEST-----  
MIICpjcCAy4CAQAwYTELMAkGA1UEBhMCREUxDDAKBgNVBAGMA05SVZESMBAGA1  
BwwJUGFKZjZj1b3JUMRcwFQYDVQQKDA50ZXRhHdvcmsgR211SDEXMBUGA1UECM  
TmV0YXR3b3JrIEEdYkkgwggE1MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAAIBAQ  
ON12XIhHU/3B0e+Zsb4woS6w21eHvc66Mee9i0NygS0MP0eBGS+zT7DVkVqKjF  
zjKdj03p9Czx0qIRz3HH5MU37yRU4/MF8orFhwJfd1vwuqRHuy2GEpHLWd0XTa  
EuMarKURV2Vi1t1FKbpC56xqd4BB1Xi1dJgE8hShBwsq3pmLo5w3MJcwcD9hIzPm  
/Jv5dt7tdbqft196Fp+JhE1VmaZWtpInwFyePTrQH1fU16fknHLS6qe63EhwvC  
P9yufSe8jAhZcu9k0f+Tz40Z1pTodMkYgXUuxcdwK06TJkMMzJZmqX/q6yDvtB  
161cxDKACA99gMRyCMBAgMBAAGgADANBgkqhkiG9w0BAQsFAAOCQAQEAQ2voeB  
U9EjAX2df9T0sk1+QLs1of7rPcu8KDVja1dDpNDw6vH04667MGucxZJrK4rRwC  
Zwq96BQXnVppTTf9A1kSWV5gSMyz8eOXES0BmrMnsPbp0QJjgYVGZz+aGoPN8  
+UXEe2tLtgMp31m/URZFDgA1xVq1Fne/kmHmwFkDyWAp1Bqin2n13GCWgtaznN  
LkJ34EGEGaseV8ho/Y5cPVtE64uneCmfPie17Dg+LaT29H3H0dN05zw00khwvM  
Mw4VSxtc7NtCH33r+vQF9zszYx+pHeanYWI2s+5us4YtkFGJDL0cRUdpQEDD/i  
1aFrNyZPR+NQTW==  
-----END CERTIFICATE REQUEST-----
```

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.

STARTSEITE / KONTOVERWALTUNG / BENUTZER / SYSTEME / SYSTEM HINZUFÜGEN

SYSTEM HINZUFÜGEN

[Persönliche Daten](#) / [Organisationsberechtigungen](#)

Interner Name

Personenangaben

Anrede

Akademischer Titel

Vorname

Nachname

Telefon

E-Mail

Arbeitgeber

Arbeitgeber Firmenname	Net at Work GmbH
Abteilungsname	-
Straße / Hausnummer	Am Hoppenhof 32a
Postleitzahl	33104
Stadt	Paderborn
Land	Deutschland (DE)
Adresszusatz	-

CSR hochladen (optional)
Wenn Sie einen CSR angeben, wird der darin enthaltene öffentliche Schlüssel bei der Erzeugung des Zugangstokens verwendet. Die im CSR enthaltenen Zertifikatsantragsdaten werden nicht berücksichtigt; die Zertifikatsinhalte des Zugangstokens werden vom TSP festgelegt. Wenn Sie keinen CSR angeben, wird der öffentliche Schlüssel vom TSP generiert. Sie erhalten das Zugangstoken in diesem Fall in Form einer P12-Datei, deren zugehörige PIN Ihnen per Post zugestellt wird.

DATEI AUSWÄHLEN Nicht ausgewählt

```
-----BEGIN CERTIFICATE REQUEST-----
MIICpCCAY4CAQAwYTELMAkGA1UEBhMCDEuDDAKBgNVBAgMA055vzESMBAGA1UE
BwwUGFRZAb3J3MmRwYQYDVO0KDA5OZkxhbnRhdmVzZm91ZDZlZS5SRDAMBgA1UECwwO
TmV0YXR3b3J3eHJlYkpwZzEMADGC5q5b3DQEBAAUAA4BDwAwggEKAnIBAQDM
ONTXhHhLJ/3BD0e-Zsb4wo56w2teHvc96Mee9l0Nyp5OMP0eBG5+2TDVKqKj7X
z9693pCz2q823HSHML37yRlU4/MF5ierfwaJHvWuq9HszZGepHLD0X39b
EuMAKURVZVilTEKbpC56xq44BtXqjg8HSHBwq3pmLo5w3McowD9NzPm3V
/v5dt7dbQH96Fp-jHElVmsZWtpmWfyPTrQHfU16RkHLSq663EhwVCTY
RQw4Cw8h37F-d8hN-774777bT5MAKVCx1k1v4H4K1616M4vDp4eK7e8uTh8Dkx
```

ABRECHEN **ANLEGEN**

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®.

