

Erstellen von Zertifikaten

Inhalt

Tools	1
Erstellen einer CA mit XCA	1
Vorlagen	1
Vorlage für Root CA	2
Vorlage für die Applikation	5
Vorlage für die Clients	9
Erstellen der Zertifikate	13
Zertifikat der Root CA	13
Zertifikat der Applikation	16
Zertifikat eines Clients	18
Erstellen des Keystores	20
Erstellen des Truststores	20
Erstellen einer p12 Datei für einen Client	21

Tools

Für die einfache Erstellung der Privaten Schlüssel, der Zertifikate und der Zertifikatspeicher können folgende Tools verwendet werden.

- [XCA](#)
- [KeyStore Explorer](#)

Wer mit OpenSSL und dem Java Keytool vertraut ist, kann auch diese Programme für die Erzeugung der benötigten Dateien verwenden. Im folgenden ist die Erstellung mit den oben genannten Tools beschrieben.

Erstellen einer CA mit XCA

Das XCA Programm öffnen und eine neue Datenbank erstellen (Menü → Datei → Neue Datenbank).

Vorlagen

Damit nicht bei jedem Zertifikat erneut die richtigen Einstellungen getroffen und alle benötigten Felder ausgefüllt werden müssen können Vorlagen angelegt werden. Wir legen

uns für die Root CA, für die Applikation (Server) und für die Clients Vorlagen an.

Vorlage für Root CA

Im Tab Vorlagen den Button "Neue Vorlagen" wählen. Im Auswahldialog "[default] CA" wählen.

Die Vorlage entsprechend der Screenshots ausfüllen.

Tab Inhaber

The screenshot shows the 'XCA Vorlage ändern' (Change XCA Template) dialog box. The title bar reads 'X Certificate and Key management'. The dialog has several tabs: 'Inhaber' (selected), 'Erweiterungen', 'Schlüsselverwendung', 'Netscape', 'Erweitert', and 'Kommentar'. The 'Inhaber' tab contains the following fields:

- Interner Name:** Root CA
- Distinguished name:**
 - countryName:** DE
 - stateOrProvinceName:** Berlin
 - localityName:** Berlin
 - organizationName:** Nortel AG
 - organizationalUnitName:** Financial Solutions
 - commonName:** XTA Tester Root CA
 - emailAddress:** [redacted]
- Privater Schlüssel:** A dropdown menu with a downward arrow, followed by a checkbox labeled 'auch verwendete Schlüssel' and a button labeled 'Erstelle einen neuen Schlüssel'.

At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Help'. On the right side of the 'Distinguished name' section, there are two buttons: 'Hinzufügen' and 'Löschen'.

Tab Erweiterungen

X Certificate and Key management

XCA Vorlage ändern

Inhaber Erweiterungen **Schlüsselverwendung** Netscape Erweitert Kommentar

X509v3 Basic Constraints

Typ **Zertifikats Autorität** ▼

Pfadlänge ☐ Critical

Key identifier

☒ X509v3 Subject Key Identifier

☐ X509v3 Authority Key Identifier

Darf nicht aktiv sein

Gültigkeit

Nicht vor dem ▼

Nicht nach dem ▼

Zeitspanne

Jahre ▼

☐ Mitternacht ☐ Ortszeit ☐ Undefiniertes Ablaufdatum

X509v3 Subject Alternative Name

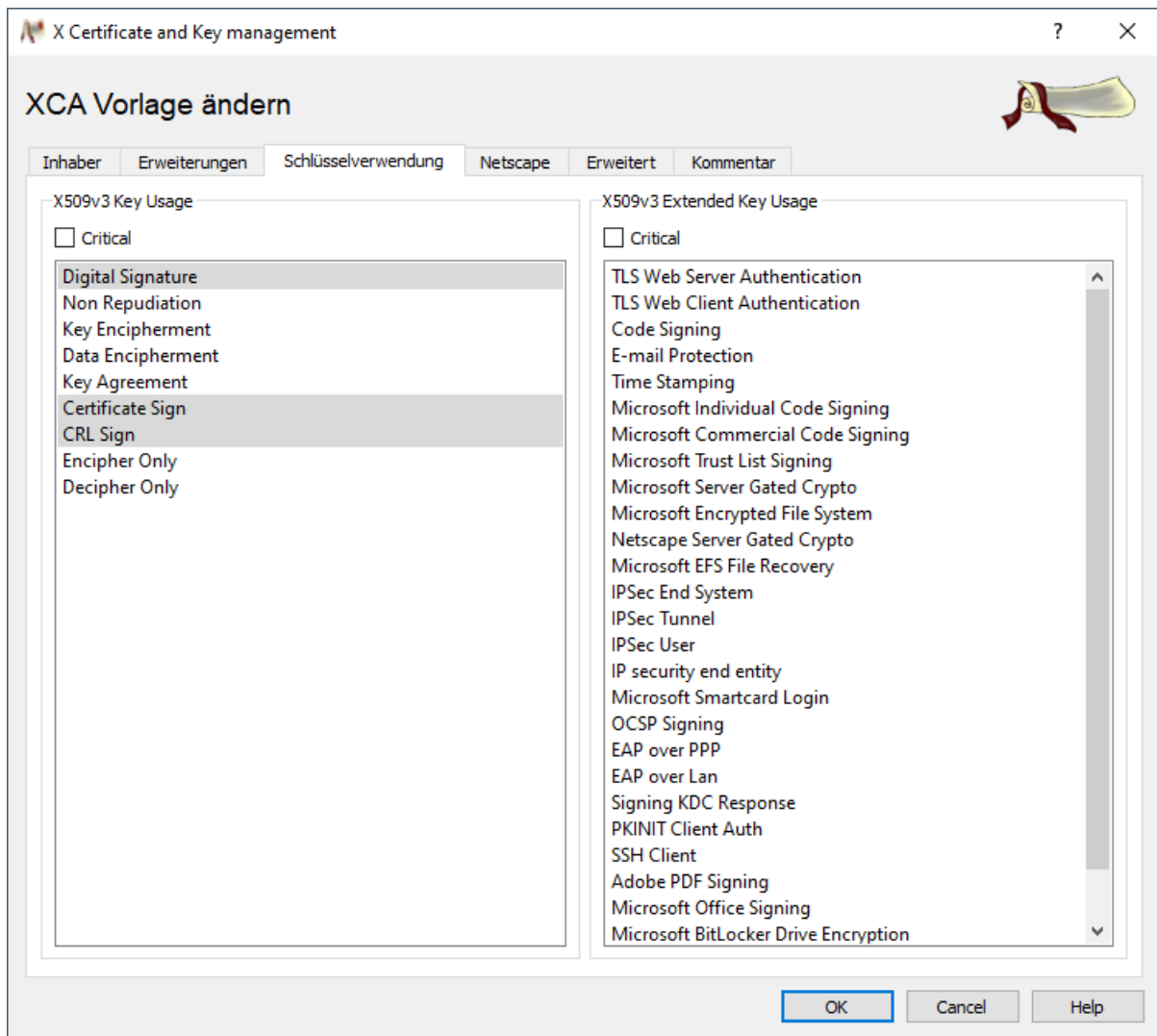
X509v3 Issuer Alternative Name

X509v3 CRL Distribution Points

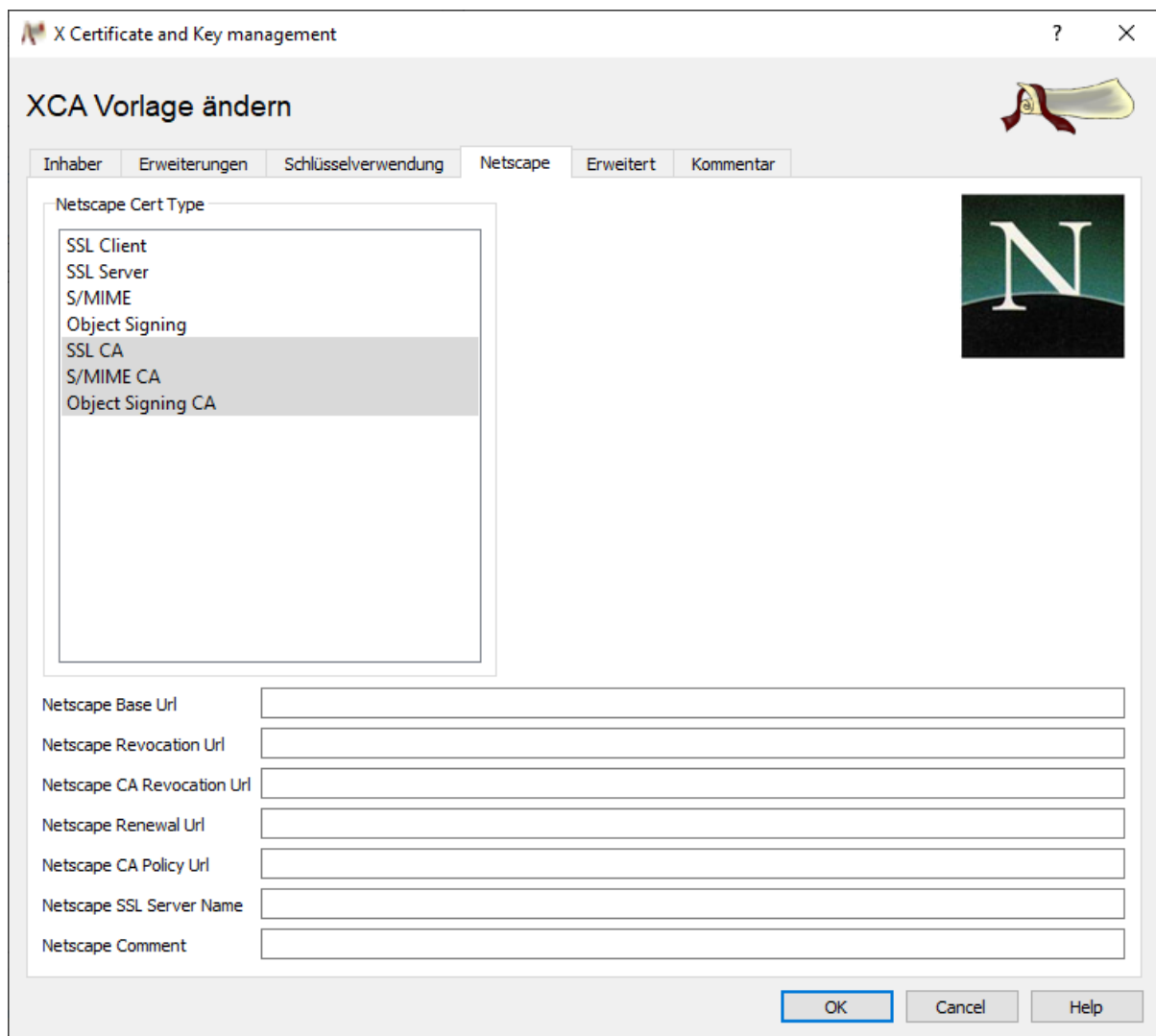
Authority Information Access

☐ OCSP Must Staple

Tab Schlüsselverwendung



Tab Netscape



Tab Erweitert

Hier sollte kein Text in rot enthalten sein.

Tab Kommentar

Ein ggf. enthaltener Kommentar kann entfernt werden.

Vorlage für die Applikation

Im Tab Vorlagen den Button "Neue Vorlagen" wählen. Im Auswahldialog "[default] TLS_server" wählen.

Die Vorlage entsprechend der Screenshots ausfüllen.

Tab Inhaber

X Certificate and Key management

XCA Vorlage ändern

Inhaber Erweiterungen Schlüsselverwendung Netscape Erweitert Kommentar

Interner Name XTA Tester Application

Distinguished name

countryName	DE	organizationalUnitName	Financial Solutions
stateOrProvinceName	Berlin	commonName	XTA Tester Application
localityName	Berlin	emailAddress	
organizationName	Nortal AG		

Typ	Inhalt

Hinzufügen
Löschen

Privater Schlüssel

☐ auch verwendete Schlüssel [Erstelle einen neuen Schlüssel](#)

OK Cancel Help

Tab Erweiterungen

Unter "X509v3 Subject Alternative Name" alle alternativen DNS Namen eintragen (inkl. IPs). Wurde ein gültiger Domainname als "commonName" eingetragen, dann kann dieser mit "DNS:copycn" übernommen werden.

X Certificate and Key management

XCA Vorlage ändern

Inhaber Erweiterungen **Schlüsselverwendung** Netscape Erweitert Kommentar

X509v3 Basic Constraints

Typ **End Instanz** Pfadlänge ☐ Critical

Key identifier

☒ X509v3 Subject Key Identifier

☐ X509v3 Authority Key Identifier

Gültigkeit

Nicht vor dem 30.11.2021 07:49 GMT

Nicht nach dem 30.11.2026 07:49 GMT

Zeitspanne

5 Jahre Übernehmen

☐ Mitternacht ☐ Ortszeit ☐ Undefiniertes Ablaufdatum

X509v3 Subject Alternative Name ✓ **DNS:localhost, IP:127.0.0.1** Bearbeiten

X509v3 Issuer Alternative Name Bearbeiten

X509v3 CRL Distribution Points Bearbeiten

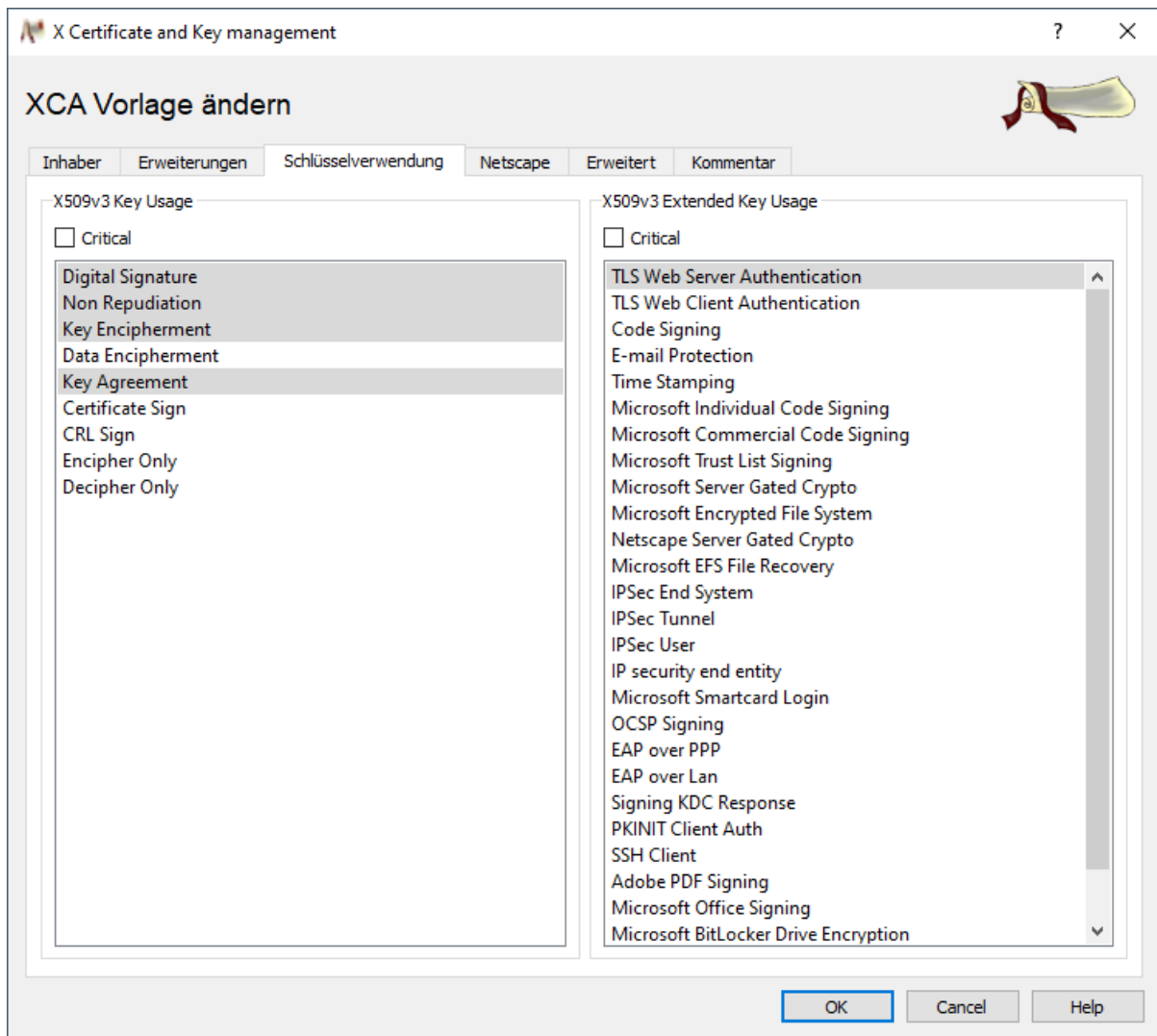
Authority Information Access Bearbeiten

☐ OCSP Must Staple

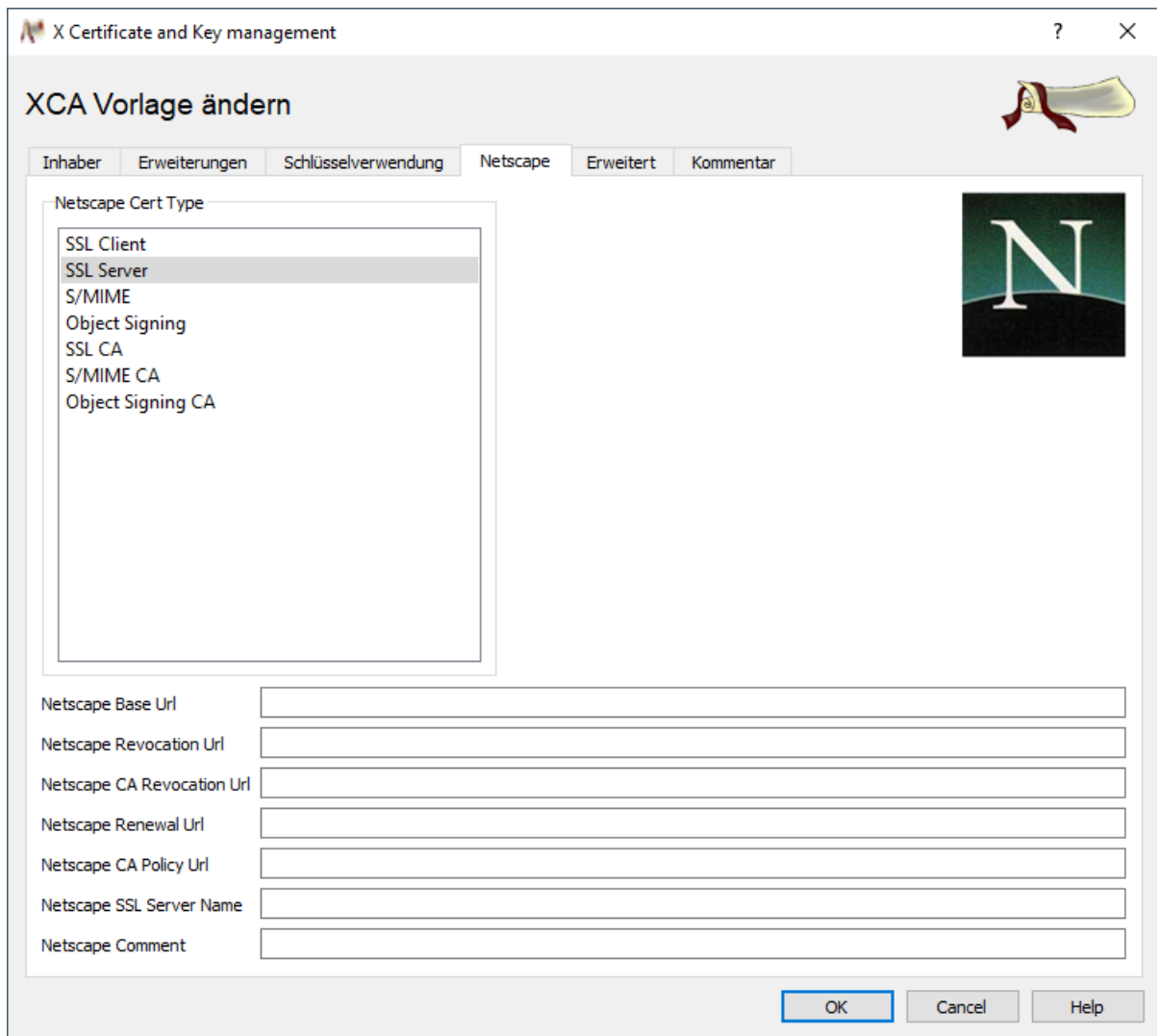
OK Cancel Help

Darf nicht aktiv sein

Tab Schlüsselverwendung



Tab Netscape



Tab Erweitert

Hier sollte kein Text in rot enthalten sein.

Tab Kommentar

Ein ggf. enthaltener Kommentar kann entfernt werden.

Vorlage für die Clients

Im Tab Vorlagen den Button "Neue Vorlagen" wählen. Im Auswahldialog "[default] TLS_client" wählen.

Die Vorlage entsprechend der Screenshots ausfüllen.

Tab Inhaber

Im Feld "commonName" den Benutzernamen und in das Feld "emailAddress" dessen Email Adresse eintragen.

X Certificate and Key management

XCA Vorlage ändern

Inhaber Erweiterungen Schlüsselverwendung Netscape Erweitert Kommentar

Interner Name XTA Tester Client

Distinguished name

countryName	DE	organizationalUnitName	Financial Solutions
stateOrProvinceName	Berlin	commonName	
localityName	Berlin	emailAddress	
organizationName	Nortal AG		

Typ	Inhalt
-----	--------

Hinzufügen
Löschen

Privater Schlüssel

☐ auch verwendete Schlüssel [Erstelle einen neuen Schlüssel](#)

OK Cancel Help

Tab Erweiterungen

X Certificate and Key management

XCA Vorlage ändern

Inhaber Erweiterungen **Schlüsselverwendung** Netscape Erweitert Kommentar

X509v3 Basic Constraints

Typ **End Instanz** ▼

Pfadlänge ☐ Critical

Key identifier

☒ X509v3 Subject Key Identifier

☐ X509v3 Authority Key Identifier

Darf nicht aktiv sein

Gültigkeit

Nicht vor dem ▼

Nicht nach dem ▼

Zeitspanne

Tage

☐ Mitternacht ☐ Ortszeit ☐ Undefiniertes Ablaufdatum

X509v3 Subject Alternative Name

X509v3 Issuer Alternative Name

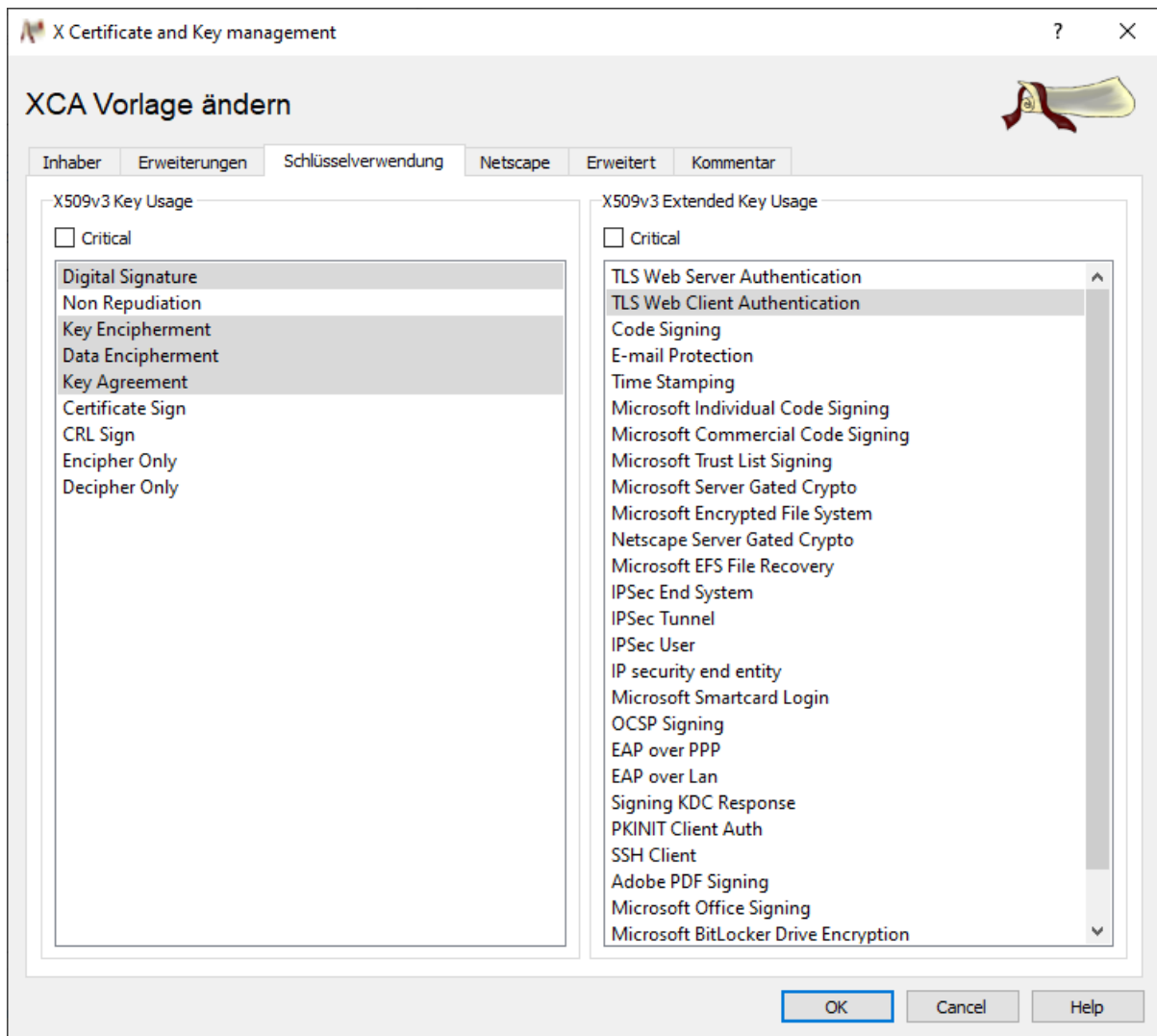
X509v3 CRL Distribution Points

Authority Information Access

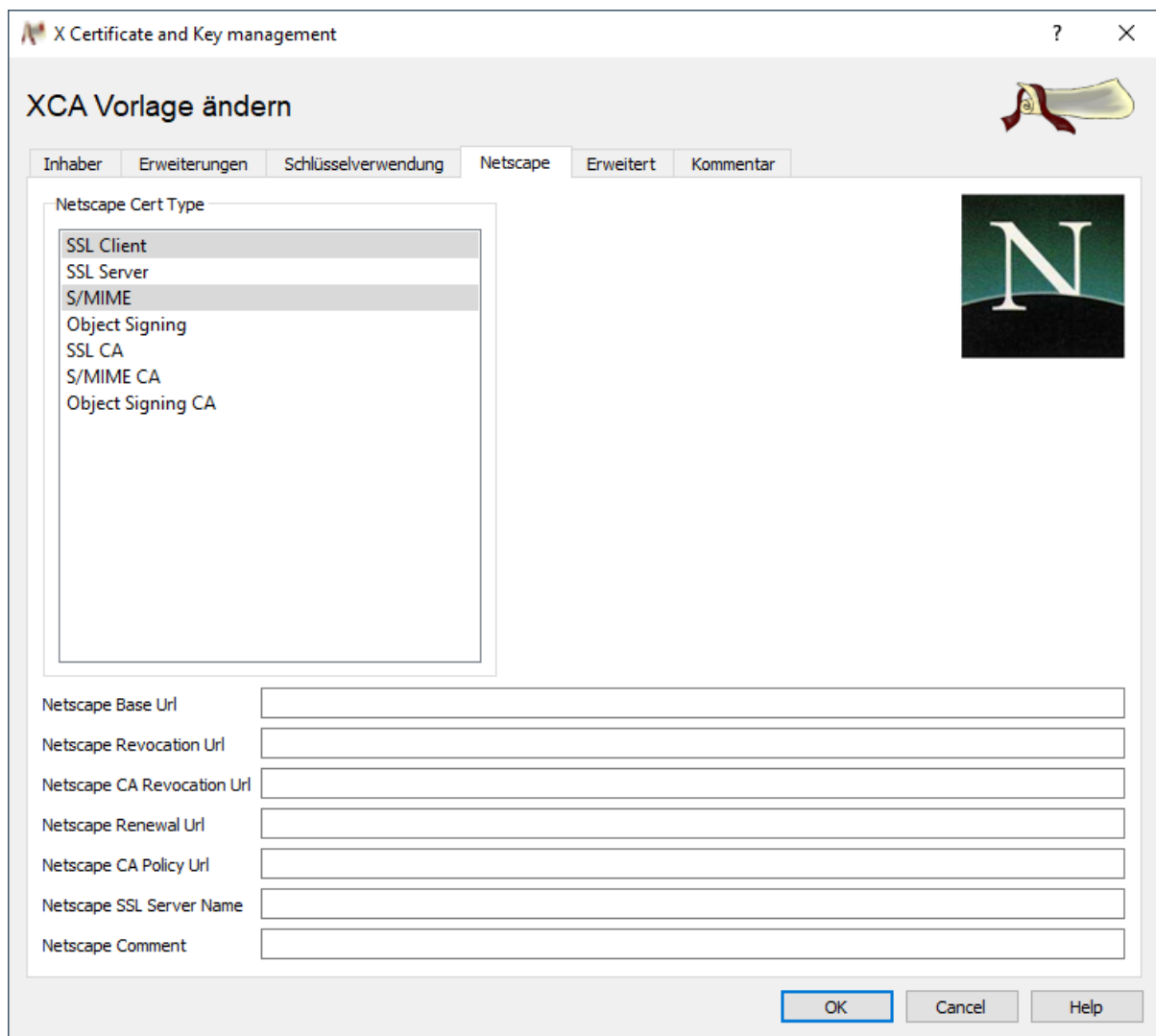
☐ OCSP Must Staple

OK Cancel Help

Tab Schlüsselverwendung



Tab Netscape



Tab Erweitert

Hier sollte kein Text in rot enthalten sein.

Tab Kommentar

Ein ggf. enthaltener Kommentar kann entfernt werden.

Erstellen der Zertifikate

Zertifikat der Root CA

Im Tab "Zertifikate" den Button "Neues Zertifikat" wählen.

Das Zertifikat entsprechend der Screenshots ausfüllen.

Tab Herkunft

In der Auswahl "Vorlage für das neue Zertifikat" die Vorlage "Root CA" auswählen und anschließend auf den Button "Alles übernehmen" drücken. Jetzt wurden alle Felder mit den Werten der Vorlage befüllt.

X Certificate and Key management

Erstelle x509 Zertifikat

Herkunft Inhaber Erweiterungen Schlüsselverwendung Netscape Erweitert Kommentar

Zertifikatsantrag

☐ Diesen Zertifikatsantrag unterschreiben

☒ Erweiterungen aus dem Zertifikatsantrag kopieren

☐ Inhaberinformation "subject" des Zertifikatsantrags ändern

Unterschreiben

☒ Selbstsigniertes Zertifikat erstellen

☐ Verwende dieses Zertifikat zum Unterschreiben

Signatur algorithmus: SHA 256

Vorlage für das neue Zertifikat: Root CA

Erweiterungen übernehmen Subject übernehmen **Alles übernehmen**

OK Cancel Help

Tab Inhaber

Zuerst im Feld "Interner Name" "XTA Tester Root CA" eintragen. Anschließend über den Button "Erstelle einen neuen Schlüssel" einen neuen Privaten Schlüssel erzeugen.

X Certificate and Key management

Neuer Schlüssel

Bitte geben Sie dem Schlüssel einen Namen und wählen Sie die gewünschte Schlüssellänge

Schlüsseleigenschaften

Name:

Schlüsseltyp:

Schlüssellänge:

☐ Als Standard speichern

Erstellen **Cancel** **Help**

Nachdem der neue Schlüssel erstellt wurde sollte dieser im Auswahlfeld "Privater Schlüssel" automatisch ausgewählt sein.

X Certificate and Key management

Erstelle x509 Zertifikat

Herkunft Inhaber Erweiterungen Schlüsselverwendung Netscape Erweitert Kommentar

Interner Name:

Distinguished name

countryName: organizationalUnitName:

stateOrProvinceName: commonName:

localityName: emailAddress:

organizationName:

Typ	Inhalt

Hinzufügen **Löschen**

Privater Schlüssel

☐ auch verwendete Schlüssel **Erstelle einen neuen Schlüssel**

OK **Cancel** **Help**

Weitere Anpassungen sind nicht notwendig und das Zertifikat kann erstellt werden.

Zertifikat der Applikation

Im Tab "Zertifikate" den Button "Neues Zertifikat" wählen.

Das Zertifikat entsprechend der Screenshots ausfüllen.

Tab Herkunft

In der Gruppe "Unterschreiben" die Option "Verwende dieses Zertifikat zum Unterschreiben" wählen und die Root CA auswählen. In der Auswahl "Vorlage für das neue Zertifikat" die Vorlage "XTA Tester Application" auswählen und anschließend auf den Button "Alles übernehmen" drücken. Jetzt wurden alle Felder mit den Werten der Vorlage befüllt.

The screenshot shows the 'X Certificate and Key management' window with the 'Erstelle x509 Zertifikat' dialog. The 'Herkunft' tab is selected. The 'Zertifikatsantrag' section has three checkboxes: 'Diesen Zertifikatsantrag unterschreiben' (unchecked), 'Erweiterungen aus dem Zertifikatsantrag kopieren' (checked), and 'Inhaberinformation "subject" des Zertifikatsantrags ändern' (unchecked). The 'Unterschreiben' section has two radio buttons: 'Selbstsigniertes Zertifikat erstellen' (unchecked) and 'Verwende dieses Zertifikat zum Unterschreiben' (checked). A dropdown menu next to the selected radio button shows 'XTA Tester Root CA'. The 'Signatur algorithmus' dropdown shows 'SHA 256'. The 'Vorlage für das neue Zertifikat' dropdown shows 'XTA Tester Application'. Below this dropdown are three buttons: 'Erweiterungen übernehmen', 'Subject übernehmen', and 'Alles übernehmen' (highlighted with a red box). At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Tab Inhaber

Zuerst im Feld "Interner Name" "XTA Tester Application" eintragen. Anschließend über den Button "Erstelle einen neuen Schlüssel" einen neuen Privaten Schlüssel erzeugen.

X Certificate and Key management

Neuer Schlüssel

Bitte geben Sie dem Schlüssel einen Namen und wählen Sie die gewünschte Schlüssellänge

Schlüsseleigenschaften

Name:

Schlüsseltyp:

Schlüssellänge:

☐ Als Standard speichern

Erstellen **Cancel** **Help**

Nachdem der neue Schlüssel erstellt wurde sollte dieser im Auswahlfeld "Privater Schlüssel" automatisch ausgewählt sein.

X Certificate and Key management

Erstelle x509 Zertifikat

Herkunft Inhaber Erweiterungen Schlüsselverwendung Netscape Erweitert Kommentar

Interner Name:

Distinguished name

countryName: organizationalUnitName:

stateOrProvinceName: commonName:

localityName: emailAddress:

organizationName:

Typ	Inhalt

Hinzufügen **Löschen**

Privater Schlüssel

☐ auch verwendete Schlüssel **Erstelle einen neuen Schlüssel**

OK **Cancel** **Help**

Weitere Anpassungen sind nicht notwendig und das Zertifikat kann erstellt werden.

Zertifikat eines Clients

Im Tab "Zertifikate" den Button "Neues Zertifikat" wählen.

Das Zertifikat entsprechend der Screenshots ausfüllen.

Tab Herkunft

In der Gruppe "Unterschreiben" die Option "Verwende dieses Zertifikat zum Unterschreiben" wählen und die Root CA auswählen. In der Auswahl "Vorlage für das neue Zertifikat" die Vorlage "XTA Tester Client" auswählen und anschließend auf den Button "Alles übernehmen" drücken. Jetzt wurden alle Felder mit den Werten der Vorlage befüllt.

The screenshot shows the 'X Certificate and Key management' window with the 'Erstelle x509 Zertifikat' dialog. The 'Herkunft' tab is selected. The 'Zertifikatsantrag' section has three checkboxes: 'Diesen Zertifikatsantrag unterschreiben' (unchecked), 'Erweiterungen aus dem Zertifikatsantrag kopieren' (checked), and 'Inhaberinformation "subject" des Zertifikatsantrags ändern' (unchecked). The 'Unterschreiben' section has two radio buttons: 'Selbstsigniertes Zertifikat erstellen' (unchecked) and 'Verwende dieses Zertifikat zum Unterschreiben' (checked). A dropdown menu next to the checked radio button shows 'XTA Tester Root CA'. The 'Signatur algorithmus' dropdown shows 'SHA 256'. The 'Vorlage für das neue Zertifikat' section has a dropdown menu showing 'XTA Tester Client'. Below this dropdown are three buttons: 'Erweiterungen übernehmen', 'Subject übernehmen', and 'Alles übernehmen' (highlighted with a red box). At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Tab Inhaber

Zuerst im Feld "Interner Name" "XTA Tester Client [NAME]" eintragen und noch commonName und emailAddress ausfüllen. Anschließend über den Button "Erstelle einen neuen Schlüssel" einen neuen Privaten Schlüssel erzeugen.

X Certificate and Key management

Neuer Schlüssel

Bitte geben Sie dem Schlüssel einen Namen und wählen Sie die gewünschte Schlüssellänge

Schlüsseleigenschaften

Name:

Schlüsseltyp:

Schlüssellänge:

☐ Als Standard speichern

Erstellen **Cancel** **Help**

Nachdem der neue Schlüssel erstellt wurde sollte dieser im Auswahlfeld "Privater Schlüssel" automatisch ausgewählt sein.

X Certificate and Key management

Erstelle x509 Zertifikat

Herkunft Inhaber Erweiterungen Schlüsselverwendung Netscape Erweitert Kommentar

Interner Name:

Distinguished name

countryName: organizationalUnitName:

stateOrProvinceName: commonName:

localityName: emailAddress:

organizationName:

Typ	Inhalt

Hinzufügen **Löschen**

Privater Schlüssel

☐ auch verwendete Schlüssel **Erstelle einen neuen Schlüssel**

OK **Cancel** **Help**

Weitere Anpassungen sind nicht notwendig und das Zertifikat kann erstellt werden.

Erstellen des Keystores

Privaten Schlüssel der Applikation exportieren

In XCA in den Tab "Private Schlüssel" wechseln und den Schlüssel "XTA Tester Application" wählen. Über den Button "Export" öffnet sich ein Export-Dialog. Den Schlüssel im "PEM" Format unter dem Dateinamen "XTA_Tester_Application.key.pem" exportieren.

Zertifikat der Applikation exportieren

In XCA in den Tab "Zertifikate" wechseln und das Zertifikat "XTA Tester Application" wählen. Über den Button "Export" öffnet sich ein Export-Dialog. Als Exportformat "PEM Kette" wählen und das Zertifikat unter dem Dateinamen "XTA_Tester_Application.pem" exportieren.

Erstellen des Keystores mit dem KeyStore Explorer

Öffnen des **KeyStore Explorers** und einen neuen "PKCS #12" Schlüsselspeicher erzeugen. Anschließend "Schlüsselpaar importieren" wählen. Im sich öffnenden Dialog "OpenSSL" wählen. Im folgenden Dialog die CheckBox "Verschlüsselter privater Schlüssel" deaktivieren und in die entsprechenden Felder den Pfad zum privaten Schlüssel und dem Zertifikat eintragen. Nach dem Import als Alias "xta-tester-application" verwenden. Jetzt muss noch ein Passwort vergeben werden. Zum Abschluss den Keystore noch speichern, auch hier ist ein Passwort anzugeben. Bitte das gleiche Passwort verwenden. Das vergebene Passwort ist später in der application.yml Datei zu konfigurieren.

Erstellen des Truststores

Root CA exportieren

In XCA in den Tab "Zertifikate" wechseln und das Zertifikat "XTA Tester Root CA" wählen. Über den Button "Export" öffnet sich ein Export-Dialog. Als Exportformat "PEM" wählen und das Zertifikat unter dem Dateinamen "XTA_Tester_Root_CA.crt" exportieren.

Erstellen des Truststores mit dem KeyStore Explorer

Öffnen des **KeyStore Explorers** und einen neuen "JKS" Schlüsselspeicher erzeugen. Anschließend "Vertrauenswürdiges Zertifikat importieren" wählen. Im sich öffnenden Dialog das exportierte Zertifikat auswählen und anschließend noch als Alias "XTA Tester Root CA" eintragen. Zum Abschluss den Truststore speichern.

Erstellen einer p12 Datei für einen Client

Es gibt zwei Möglichkeiten. Zum einen kann in XCA im Tab "Zertifikate" das Zertifikat inklusive privatem Schlüssel als p12-Datei exportiert werden. Dabei ist es wichtig den Eintrag mit Zertifizierungskette zu wählen. Die zweite Möglichkeit ist den privaten Schlüssel und das Zertifikat getrennt zu exportieren und anschließend die p12-Datei mit dem KeyStore Explorer zu erzeugen.

Privaten Schlüssel des Clients exportieren

In XCA in den Tab "Private Schlüssel" wechseln und den Schlüssel "XTA Tester Client [Name]" wählen. Über den Button "Export" öffnet sich ein Export-Dialog. Den Schlüssel im "PEM" Format unter dem Dateinamen "XTA_Tester_Client_[NAME].key.pem" exportieren.

Zertifikat des Clients exportieren

In XCA in den Tab "Zertifikate" wechseln und das Zertifikat "XTA Tester Client [Name]" wählen. Über den Button "Export" öffnet sich ein Export-Dialog. Als Exportformat "PEM Kette" wählen und das Zertifikat unter dem Dateinamen "XTA_Tester_Client_[Name].pem" exportieren.

Erstellen der p12 Datei mit dem KeyStore Explorer

Öffnen des **KeyStore Explorers** und einen neuen "PKCS #12" Schlüsselspeicher erzeugen. Anschließend "Schlüsselpaar importieren" wählen. Im sich öffnenden Dialog "OpenSSL" wählen. Im folgenden Dialog die CheckBox "Verschlüsselter privater Schlüssel" deaktivieren und in die entsprechenden Felder den Pfad zum privaten Schlüssel und dem Zertifikat eintragen. Nach dem Import als Alias "[Name] \ (xta tester root ca)" verwenden. Jetzt muss noch ein Passwort vergeben werden. Zum Abschluss den Keystore noch speichern, auch hier ist ein Passwort anzugeben. Bitte das gleiche Passwort verwenden. Das Passwort wird benötigt wenn der Keystore auf dem Client eingespielt wird.