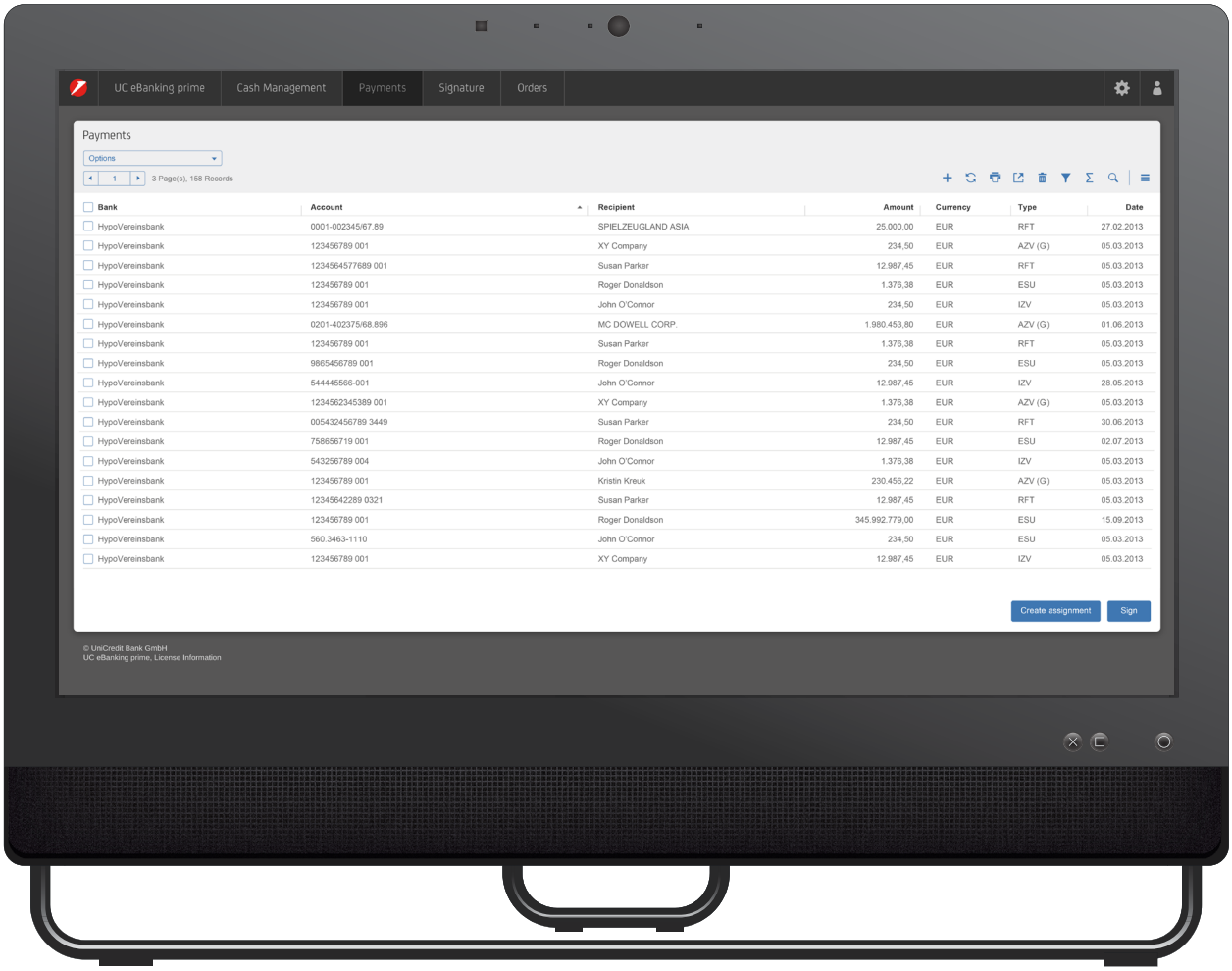
SSL TOOL 1.2
V6.1.0

Stand 18.03.2024

unicreditgroup.eu/clientsolutions

UniCredit


UC eBanking prime
Cash Management
Payments
Signature
Orders
Payments
Options
1
3 Page(s), 158 Records
Bank
Account
Recipient
Amount
Currency
Type
Date
HypoVereinsbank 0001-002345/67.89 SPIELZEUGLAND ASIA 25.000,00 EUR RFT 27.02.2013
HypoVereinsbank 123456789 001 XY Company 234,50 EUR AZV (G) 05.03.2013
HypoVereinsbank 1234564577689 001 Susan Parker 12.987,45 EUR RFT 05.03.2013
HypoVereinsbank 123456789 001 Roger Donaldson 1.376,38 EUR ESU 05.03.2013
HypoVereinsbank 123456789 001 John O'Connor 234,50 EUR IZV 05.03.2013
HypoVereinsbank 0201-402375/68.896 MC DOWELL CORP. 1.980.453,80 EUR AZV (G) 01.06.2013
HypoVereinsbank 123456789 001 Susan Parker 1.376,38 EUR RFT 05.03.2013
HypoVereinsbank 9865456789 001 Roger Donaldson 234,50 EUR ESU 05.03.2013
HypoVereinsbank 544445566-001 John O'Connor 12.987,45 EUR IZV 28.05.2013
HypoVereinsbank 1234562345389 001 XY Company 1.376,38 EUR AZV (G) 05.03.2013
HypoVereinsbank 00543245678 9 3449 Susan Parker 234,50 EUR RFT 30.06.2013
HypoVereinsbank 758656719 001 Roger Donaldson 12.987,45 EUR ESU 02.07.2013
HypoVereinsbank 543256789 004 John O'Connor 1.376,38 EUR IZV 05.03.2013
HypoVereinsbank 123456789 001 Kristin Kreuk 230.456,22 EUR AZV (G) 05.03.2013
HypoVereinsbank 12345642289 0321 Susan Parker 12.987,45 EUR RFT 05.03.2013
HypoVereinsbank 123456789 001 Roger Donaldson 345.992.779,00 EUR ESU 15.09.2013
HypoVereinsbank 560.3463-1110 John O'Connor 234,50 EUR ESU 05.03.2013
HypoVereinsbank 123456789 001 XY Company 12.987,45 EUR IZV 05.03.2013
Create assignment
Sign
© UniCredit Bank GmbH
UC eBanking prime, License Information

SSL Tool 1.2

Inhaltsverzeichnis

1. ALLGEMEINE INFORMATIONEN

Dieses Dokument beschreibt die Konfiguration eines SSL-Zertifikats zur Verwendung in UC eBanking prime.

Voraussetzungen für die Ausführung des UC eBanking prime SSL-Tools:

- Administratorrechte auf Betriebssystemebene zur Ausführung des SSL-Tools.
- UC eBanking prime ist installiert.
- UC eBanking prime Dienste sollten gestoppt sein.
- Der Keystore-Ordner ist vorhanden.

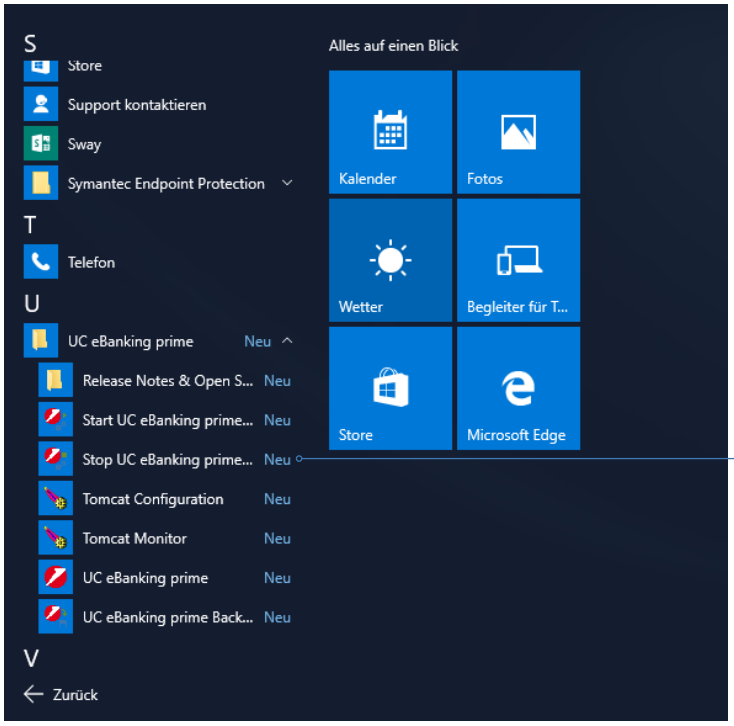
Diese Anleitung wurde am Beispiel des Betriebssystems Microsoft Windows 10 erstellt.

1.1 STOP UC eBANKING PRIME SERVICES

⚠ Wenn das UC eBanking prime SSL Tool als eigenständiges Tool ausgeführt wird, müssen vor der SSL-Konfiguration alle UC eBanking prime Dienste manuell gestoppt werden.

Im Vorfeld muss dafür über das Windows „Start Menü“ das Verzeichnis „Alle Apps › UC eBanking prime“ aufgerufen, und durch Anklicken von "Stop UC eBanking prime Services" gestoppt werden.

Nach erfolgreicher SSL-Konfiguration können die Dienste über den darüberliegenden Punkt „Start UC eBanking prime Services“ wieder gestartet werden.



Bitte stoppen Sie die Services der Anwendung UC eBanking prime durch Klicken auf „Stop UC eBanking prime Services“.

Nach erfolgreicher Einrichtung der SSL-Konfiguration können Sie die Dienste über „Start UC eBanking prime Services“ wieder starten.

2. SSL TOOL OPTIONEN

Das UC eBanking prime SSL-Tool bietet die folgenden Optionen.

- Bestehendes Zertifikat konfigurieren
  Mit dieser Option kann ein vorhandenes Zertifikat für die Verwendung in UC eBanking prime konfiguriert werden.

- Neues Zertifikat erstellen und konfigurieren (self-sign)
  Mit dieser Option kann ein selbstsigniertes Zertifikat für die Anwendung in UC ebanking prime erstellt und konfiguriert werden.

- Zertifikat exportieren
  Mit dieser Option kann ein Client-Zertifikat für die Verbindung des OTC-Clients mit UC eBanking prime exportiert werden.

- Zertifikat (self-sign) verlängern
  Diese Option kann verwendet werden, um die Gültigkeit eines bestehenden selbstsignierten Zertifikats für die Verwendung in UC eBanking prime zu verlängern.

- Zertifikat (signiert) verlängern
  Mit dieser Option können Sie die Gültigkeit eines bestehenden signierten Zertifikats für die Verwendung in UC eBanking prime verlängern.

- Keystore Alias auslesen
  Diese Option wird verwendet, um einen Keystore-Alias zu holen.

- Keystore und CSR erstellen
  Diese Option wird verwendet, um einen Schlüsselspeicher zu erstellen und eine CSR zu erzeugen.

- Signiertes Zertifikat in Keystore importieren
  Diese Option wird verwendet, um ein signiertes Zertifikat in den Keystore zu importieren.

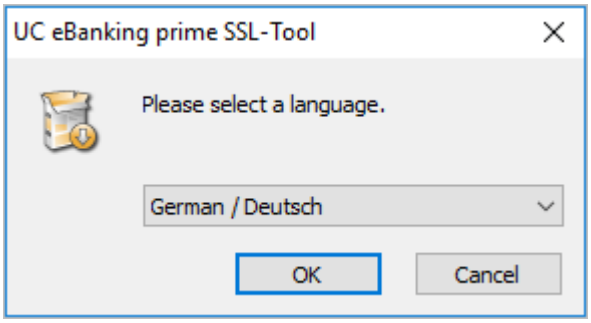
- Bestehende SSL-Konfiguration löschen
  Diese Option wird verwendet, um eine bestehende SSL-Konfiguration zu löschen.

3. EINSTELLUNGEN

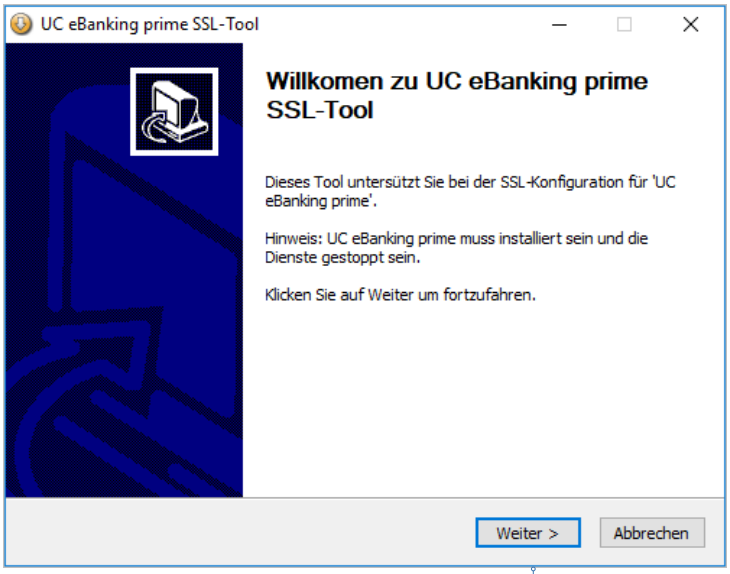
Um das UC eBanking SSL Tool zu starten, doppelklicken Sie auf die Datei "SSL-Tool-nnn.exe".

Bei Windows-Systemen mit aktiver Benutzerkontensteuerung muss der Start über die Option: „Ausführen als Administrator“ erfolgen.

Das UC eBanking prime SSL Tool führt Sie durch die Konfigurationsschritte, beginnend mit der Sprachauswahl.



Wählen Sie im ersten Schritt die gewünschte Sprache für das SSL Tool (deutsch/englisch) aus. Per default ist die Sprache des Betriebssystems voreingestellt. Bestätigen Sie den Vorgang mit „OK".



Klicken Sie auf “Weiter“ um fortzufahren.

3. EINSTELLUNGEN

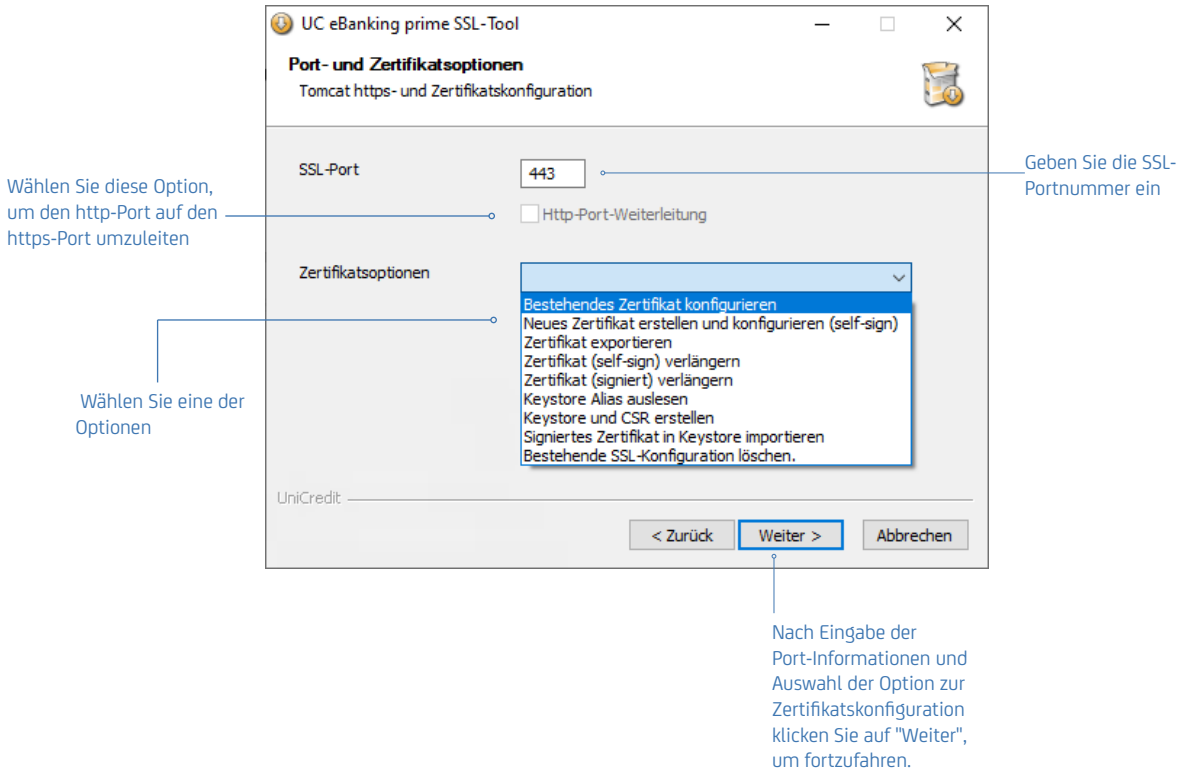
Hier wird die zu verwendende https-Portnummer des UC eBanking prime-Servers eingegeben und die Zertifikatskonfiguration ausgewählt.

SSL Port:
Als Voreinstellung ist der Port 443 eingetragen.

Http-Port-Weiterleitung:
Ermöglicht die automatische Umleitung des http-Ports auf den konfigurierten https-Port, um die Verwendung von TLS sicherzustellen.
Hinweis: Eine Verbindung mit UC eBanking prime ist dadurch nur noch verschlüsselt möglich.

Die folgenden Zertifikats-Konfigurationsoptionen sind im UC eBanking prime SSL Tool verfügbar:

- Bestehendes Zertifikat konfigurieren
- Neues Zertifikat erstellen und konfigurieren (self-sign)
- Zertifikat exportieren
- Zertifikat (self-sign) verlängern
- Zertifikat (signiert) verlängern
- Keystore Alias auslesen
- Keystore und CSR erstellen
- Signiertes Zertifikat in Keystore importieren
- Bestehende SSL-Konfiguration löschen



3.1 BESTEHENDES ZERTIFIKAT KONFIGURIEREN

Diese Option wird verwendet, um ein vorhandenes Zertifikat für den UC eBanking-Prime-Server zu konfigurieren.
Aktuell werden Keystores in den Formaten
.keystore,.jks, .p12 und .pfx unterstützt.

Einzelheiten über den vorhandenen Keystore, in dem das Zertifikat vorhanden ist, müssen zusammen mit Keystore, Schlüsselpasswort und Alias angegeben werden. Wobei der Alias das im Keystore befindliche Zertifikat identifiziert.

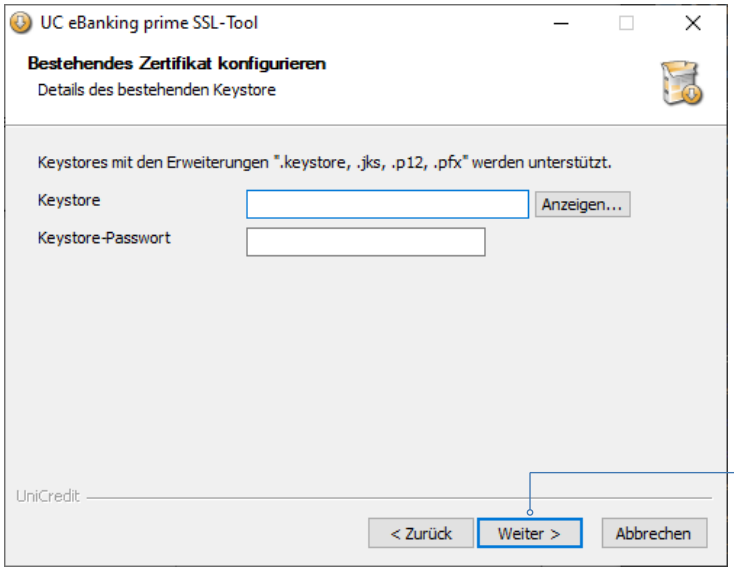
Keystore:
Enthält Schlüssel und Zertifikate.

Keystore-Passwort:
Passwort des Keystores.

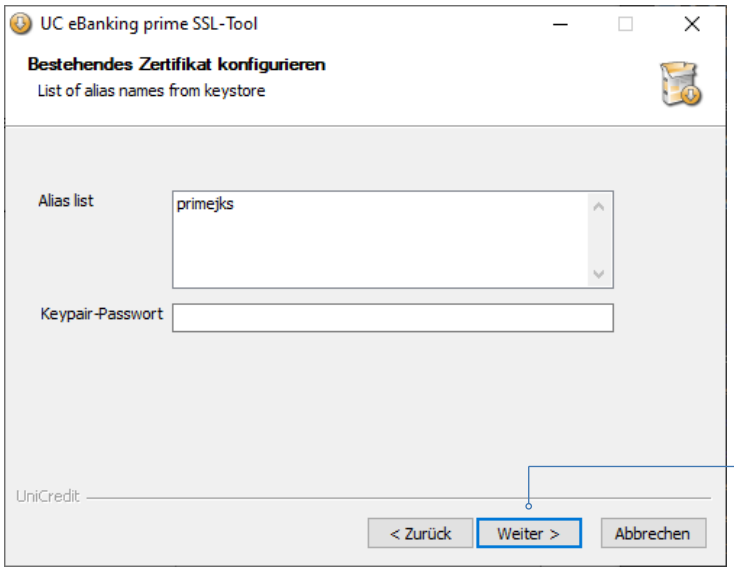
Schlüsselpasswort:
Passwort des Schlüssels (keypass).

Alias:
Name eines im Schlüsselspeicher befindlichen Zertifikates.

Wenn das Zertifikat erfolgreich konfiguriert ist, werden Meldungen angezeigt, die darüber informieren, dass die Konfiguration erfolgreich durchgeführt wurde.



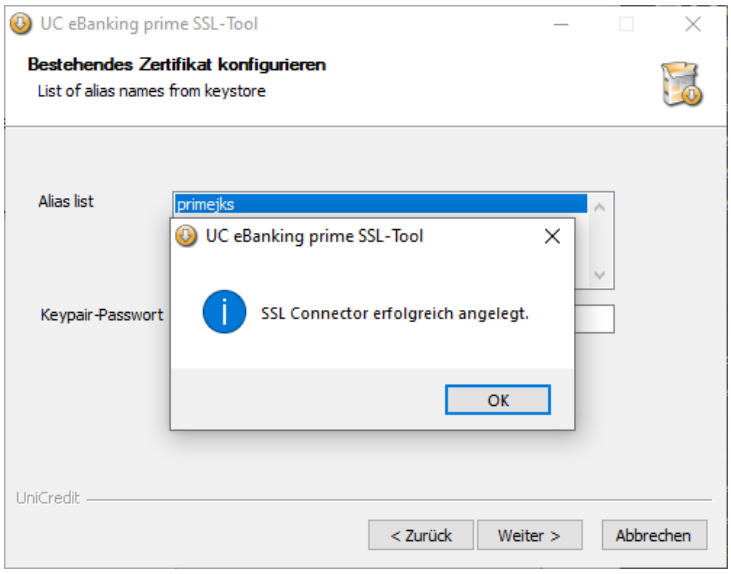
Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.



Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.

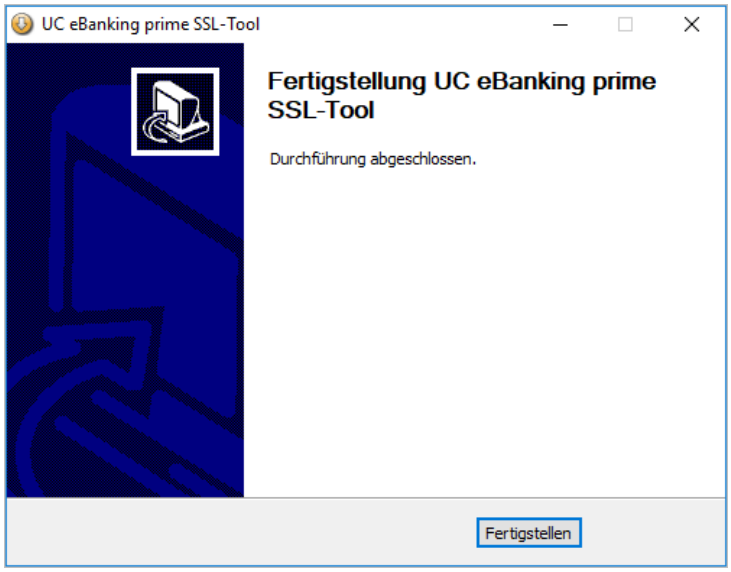
3.1 BESTEHENDES ZERTIFIKAT KONFIGURIEREN

Wenn das Zertifikat erfolgreich konfiguriert wurde, wird eine Meldung angezeigt, die angibt, dass die Konfiguration erfolgreich war.



Dieser Bildschirm zeigt die erfolgreiche Einrichtung eines bestehenden SSL-Zertifikats im UC eBanking-Prime-Server.

Mit Klick auf den Button „Fertig stellen“ wird das UC eBanking prime SSL Tool beendet.



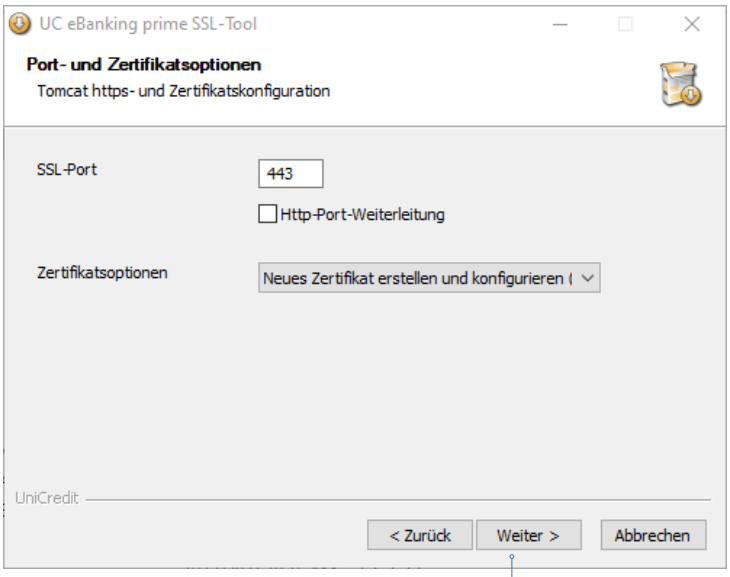
Start UC eBanking prime Services

Nach erfolgreicher SSL-Konfiguration starten Sie die Dienste neu, indem Sie im Windows-Startmenü im Verzeichnis "Programm" auf "UC eBanking prime Services starten" klicken.

3.2 NEUES ZERTIFIKAT ERSTELLEN UND KONFIGURIEREN (SELF-SIGN)

Diese Option hilft bei der Erstellung eines neuen selbstsignierten Zertifikats und dessen Konfiguration im UC eBanking-Prime-Server.

Bei dieser Option werden die Details des neuen Keystore und des neuen Zertifikats zusammen mit den Keystore- und Schlüsselpaar-Passwörtern erfasst, die dann dazu verwendet werden, einen Keystore mit einem Zertifikat zu erstellen und zu konfigurieren.



Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.
.

3.2 NEUES ZERTIFIKAT ERSTELLEN UND KONFIGURIEREN (SELF-SIGN)

In dieser Maske werden Details für einen neuen Keystore zur Speicherung von Zertifikat und Schlüssel erfasst.

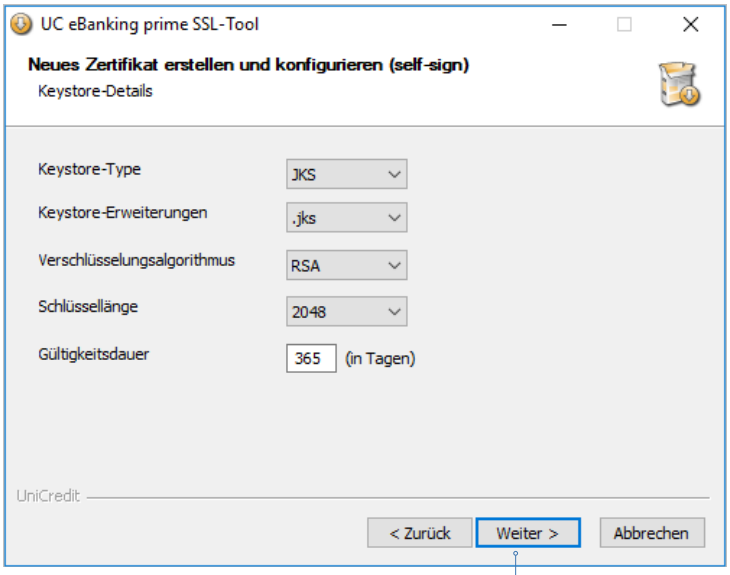
Keystore-Type:
Speicherformat für die Zertifikate und Schlüssel.
(Voreinstellung JKS)

Keystore-Erweiterungen:
Dateierweiterung der Keystore-Datei, dies hilft auch bei der Identifizierung des Keystore-Typs. (Voreinstellung .jks).

Verschlüsselungsalgorithmus:
Algorithmus, welcher zum Schutz der Integrität des Schlüsselpaares verwendet wird. (Voreinstellung RSA).

Schlüssellänge:
Die Schlüssellänge ist die Anzahl der Bits in einem Schlüssel, der von einem kryptographischen Algorithmus verwendet wird.
(Voreinstellung 2048).

Gültigkeitsdauer:
Gültigskeitsdauer des Zertifikates in Tagen.



Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.
.

3.2 NEUES ZERTIFIKAT ERSTELLEN UND KONFIGURIEREN (SELF-SIGN)

In dieser Maske werden die Details des zu erstellenden Zertifikats erfasst.

Common name (CN):
Enthält den zu identifizierenden Namen – Hier ist der Rechnername einzutragen über den die Clients die Verbindung zum UC eBanking prime-Server herstellen.

Organization Unit (OU):
Name der organisatorischen Einheit, z.B. Abteilungsname

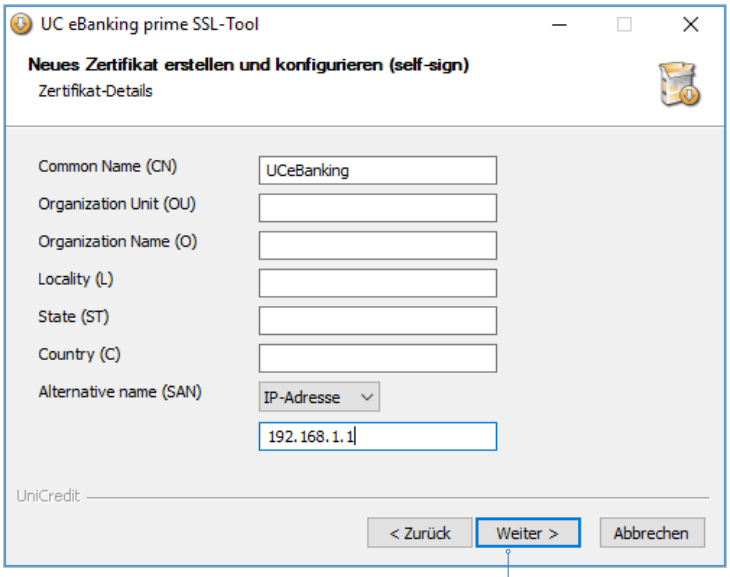
Organization Name (O):
Name der Organisation bzw. des Unternehmens.

Locality (L):
Name der Stadt der Organisation bzw. des Unternehmens.

State (ST):
Name des Bundeslandes der Organisation bzw. des Unternehmens.

Country (C):
ISO-Ländercode (z.B. „DE“ für Deutschland) der Organisation bzw. des Unternehmens.

Alternative name (SAN):
Alternativer Servername. Hier kann eine alternative IP-Adresse oder DNS-Name, über den der UC eBanking prime Server erreicht werden kann, eingetragen werden.

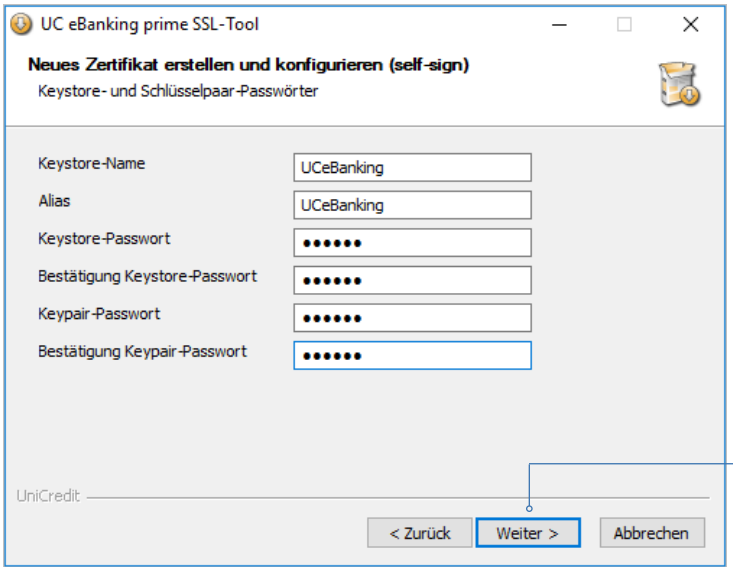


Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.

3.2 NEUES ZERTIFIKAT ERSTELLEN UND KONFIGURIEREN (SELF-SIGN)

In diesem Bildschirm werden die Keystore- und Schlüsselpaar-Passwörter erfasst.

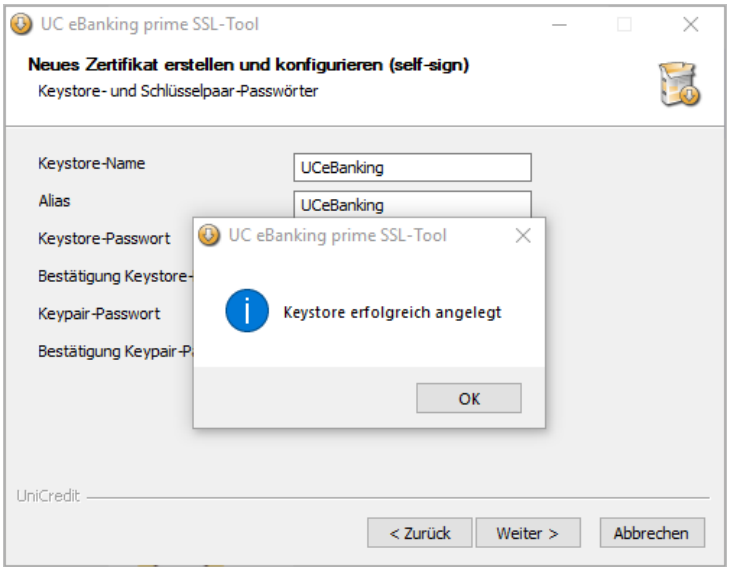
Sie benötigen die von Ihnen gewählten Passwörter für die Konfiguration auf dem Tomcat-Server. Es wird empfohlen, im Falle des Typs JKS-Keystore keine identischen Passwörter zu verwenden, während für den Typ PKCS12 Keystore nur ein identisches Passwort möglich ist.



Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.

Sobald der Keystore erfolgreich generiert wurde, wird eine Meldung angezeigt.

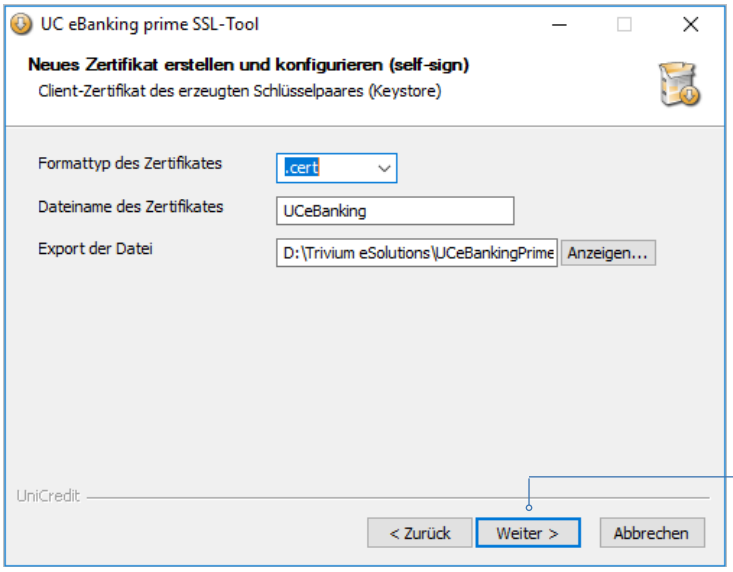
Die Keystore-Datei wurde nun im Verzeichnis "[LW]:[Installationsverzeichnis UC eBanking prime]\Keystore" erstellt.



3.2 NEUES ZERTIFIKAT ERSTELLEN UND KONFIGURIEREN (SELF-SIGN)

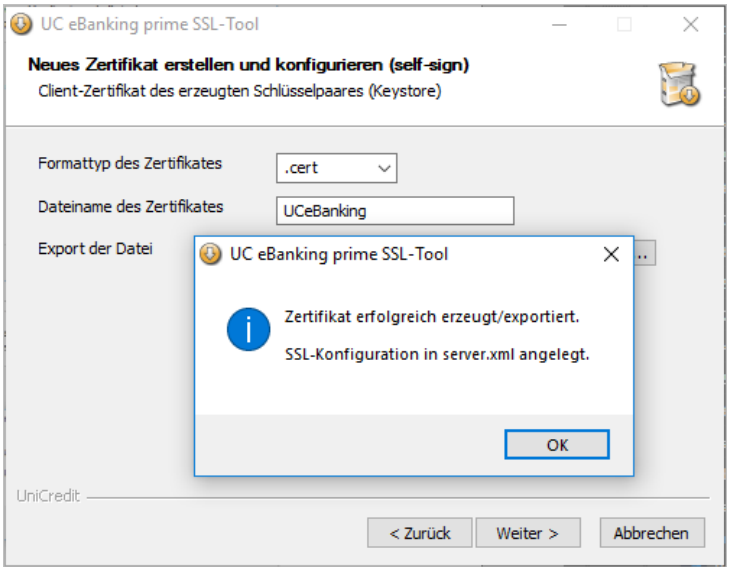
Sobald das selbstsignierte Zertifikat generiert wurde, sollte es exportiert werden, damit es für die Verbindung von Clients zum UC eBanking-Prime-Server verwendet werden kann.

Der Standard-Exportpfad ist das Verzeichnis "[LW]:[Installationsverzeichnis UC eBanking prime]\keystore".



Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.

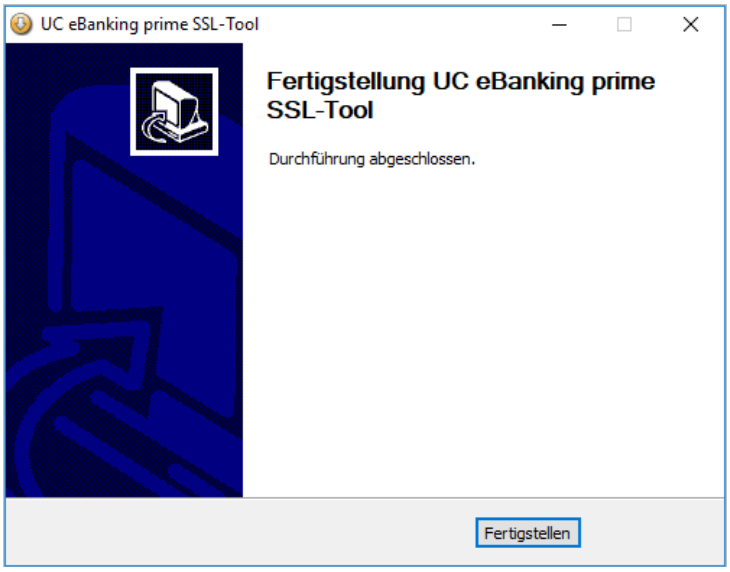
Sobald das Zertifikat erfolgreich erzeugt oder exportiert wurde, wird eine Meldung angezeigt. Die Datei "server.xml" wird mit den SSL-Konfigurationsdetails aktualisiert.



3.2 NEUES ZERTIFIKAT ERSTELLEN UND KONFIGURIEREN (SELF-SIGN)

Dieser Bildschirm zeigt die erfolgreiche Einrichtung des selbstsignierten Zertifikats nach der Erstellung eines neuen Schlüsselspeichers im UC eBanking-Prime- Server.

Mit Klick auf den Button „Fertig stellen“ wird das UC eBanking prime SSL Tool beendet.



Start UC eBanking prime Services

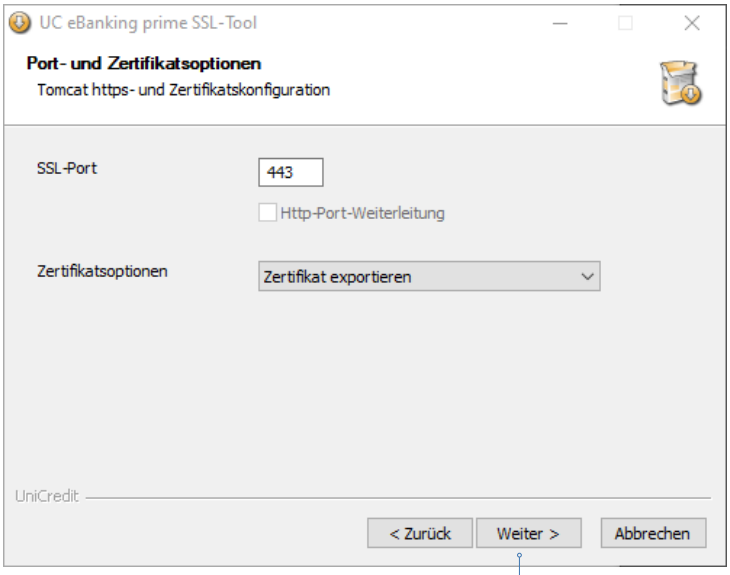
Nach erfolgreicher SSL-Konfiguration starten Sie die Dienste neu, indem Sie im Windows-Startmenü im Verzeichnis "Programm" auf "UC eBanking prime Services starten" klicken. .

3.3 ZERTIFIKAT EXPORTIEREN

Mit dieser Option können Client-Zertifikate für die Clients des UC eBanking Prime-Servers exportiert werden.

Hinweis: Um die SSL-Kommunikation für UC eBanking prime OTC zu aktivieren, geben Sie die entsprechende Server-URL (z.B. https://localhost:443) unter dem OTC Menü Einstellungen ein. Aktivieren Sie "Custom Zertifikat" und wählen Sie den Speicherort des Zertifikats. Mit „Zertifkat herunterladen“ können Sie das Zertifikat in Ihrem persönlicne Verzeichnis der OTC-Anwendung speichern.

Weitere Informationen entnehmen Sie dem Dokument „UC eBanking prime OTC“.



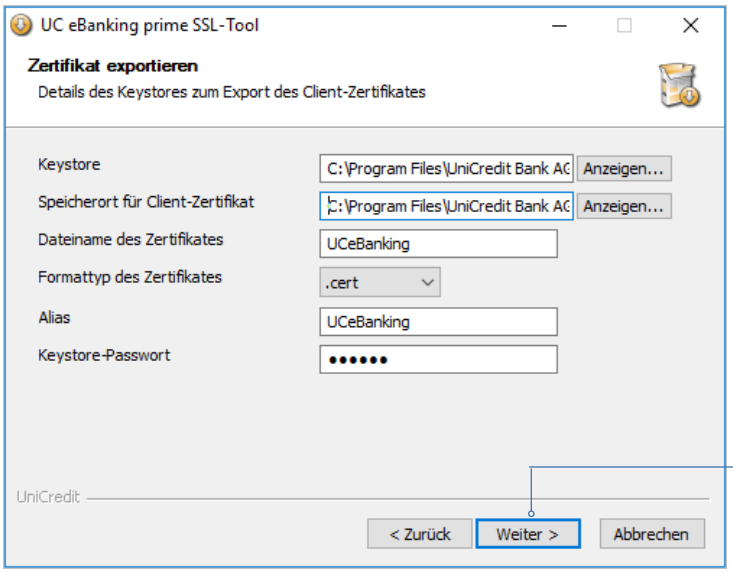
Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.

3.3 ZERTIFIKAT EXPORTIEREN

Dieser Bildschirm erfasst die Keystore-Details, die für den Export des Client-Zertifikats benötigt werden.

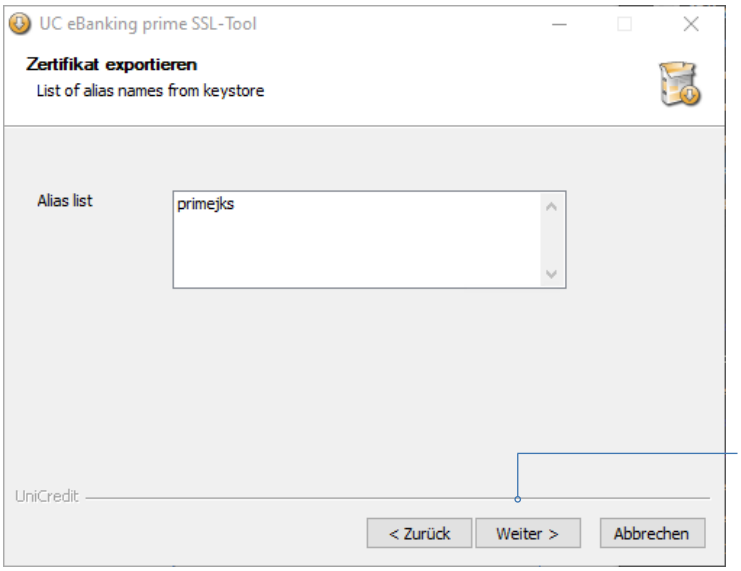
Wählen Sie den Pfad des vorhandenen Schlüsselspeichers und den Pfad, in dem das exportierte Zertifikat gespeichert werden soll.

Sobald das Zertifikat erfolgreich exportiert wurde, wird eine Meldung angezeigt.



Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.

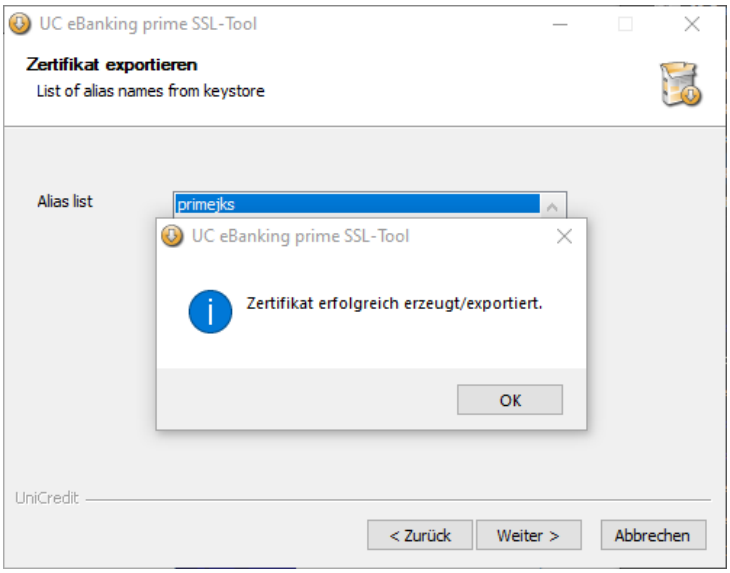
Wählen Sie den Alias für den Keystore aus der angezeigten Liste.



Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.

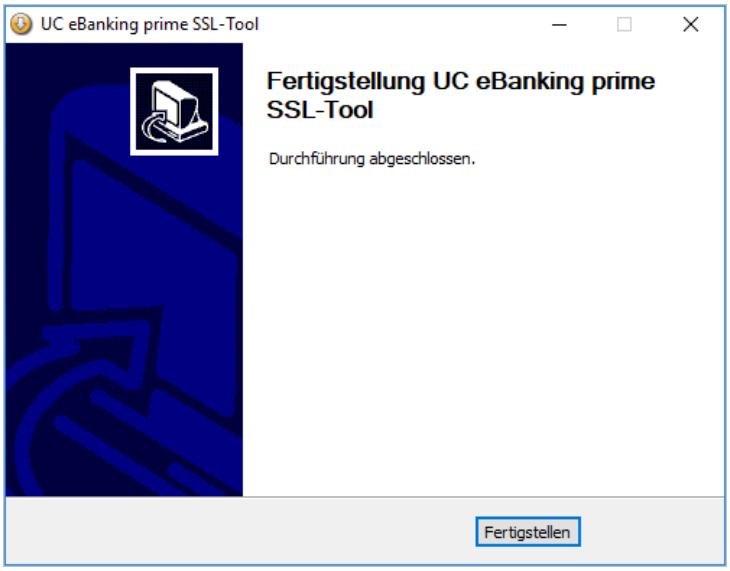
3.3 ZERTIFIKAT EXPORTIEREN

Sobald das Zertifikat erfolgreich exportiert wurde, wird eine Meldung angezeigt.



Dieser Bildschirm zeigt den erfolgreichen Export des Client-Zertifikats an.

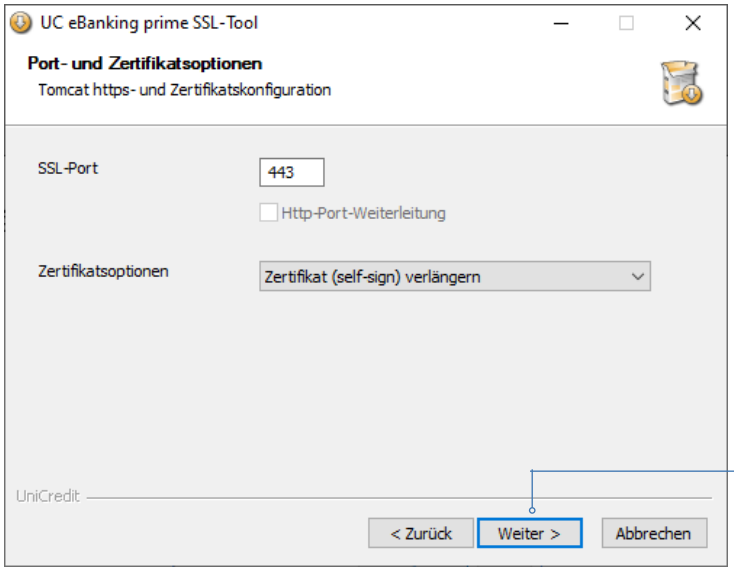
Mit Klick auf den Button „Fertig stellen“ wird das UC eBanking prime SSL Tool beendet.



3.4 ZERTIFIKAT (SELF-SIGN) VERLÄNGERN

Diese Option wird verwendet, um die Gültigkeit eines bestehenden selbstsignierten Zertifikats zu verlängern.

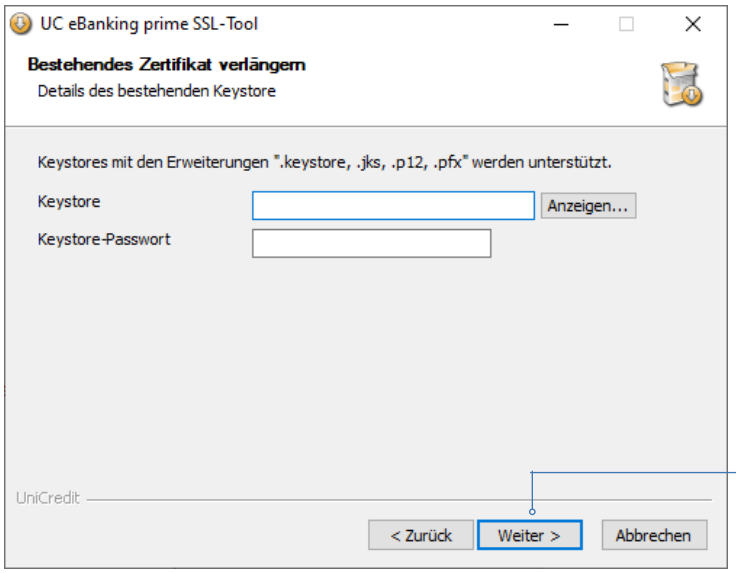
In diesem Bildschirm werden die Details des vorhandenen Schlüsselspeichers und Zertifikat zusammen mit den Passwörtern für den Schlüsselspeicher und Schlüsselpaar-Passwörter erfasst, um dann die Gültigkeit des Zertifikats zu verlängern.



Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.

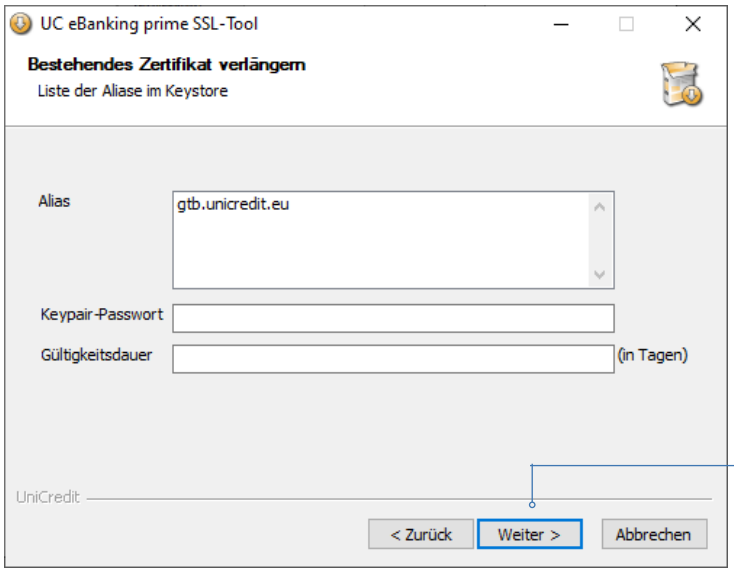
3.4 ZERTIFIKAT (SELF-SIGN) VERLÄNGERN

In diesem Bildschirm müssen die Details des vorhandenen Schlüsselspeichers, in dem sich das Zertifikat befindet, zusammen mit dem Passwort angegeben werden.



Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.

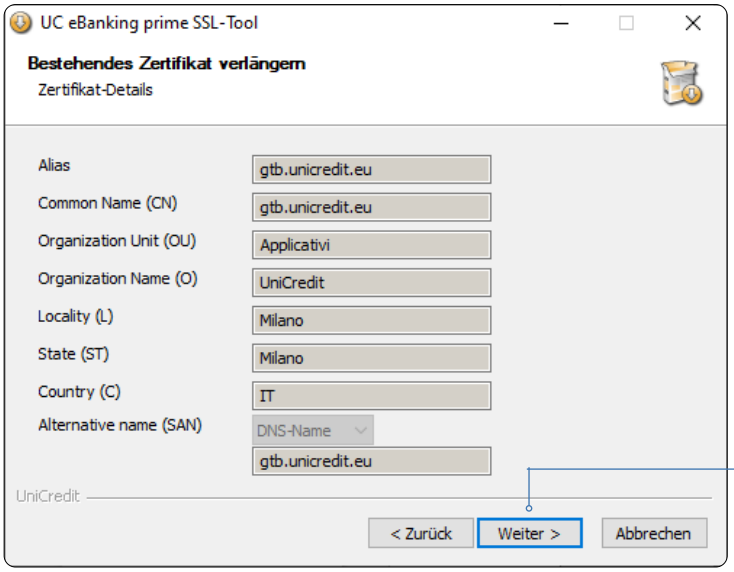
In diesem Bildschirm wählen Sie einen Alias aus der angezeigten Liste und geben Sie das Kennwort für das Schlüsselpaar ein. Geben Sie die Anzahl der Tage ein, um die die Gültigkeit des Zertifikats ab dem aktuellen Tag verlängert werden soll.



Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.

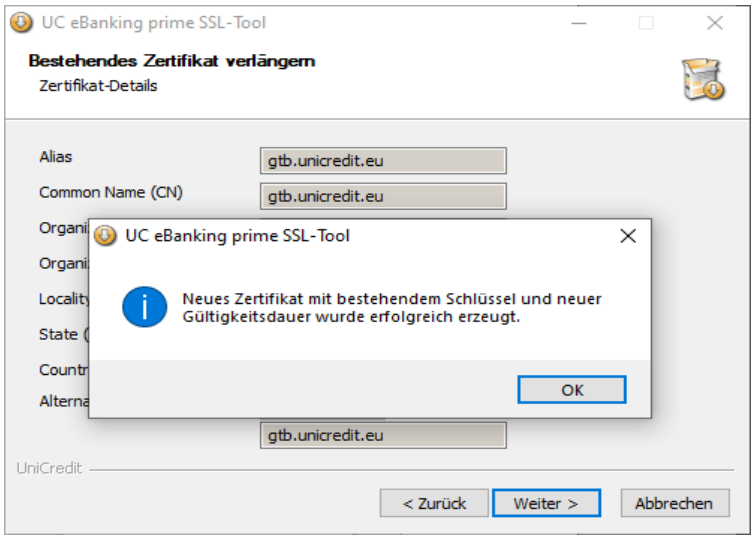
3.4 ZERTIFIKAT (SELF-SIGN) VERLÄNGERN

In diesem Bildschirm werden die Details des zu erstellenden Zertifikats angezeigt.



Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.

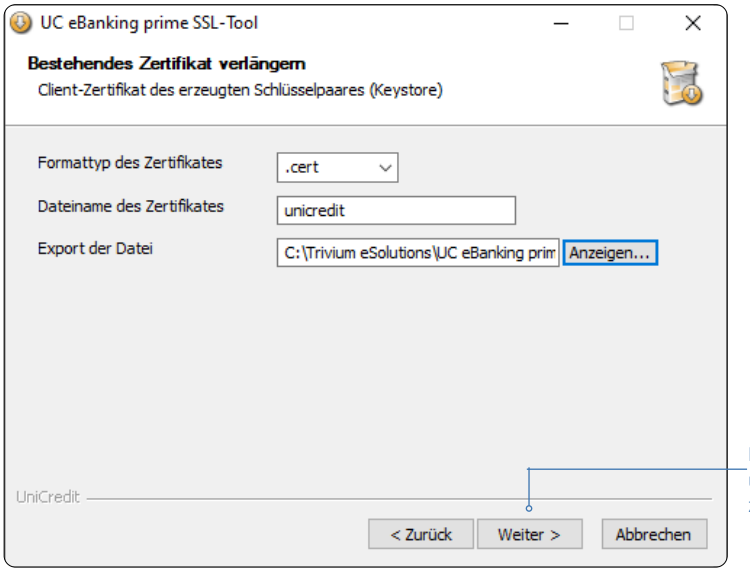
Sobald das neue Zertifikat erfolgreich generiert wurde, wird eine Meldung über die neue Gültigkeit angezeigt.
Die Keystore-Datei wurde nun im Verzeichnis "[LW]:[Installationsverzeichnis UC eBanking prime]\Keystore" erstellt.



3.4 ZERTIFIKAT (SELF-SIGN) VERLÄNGERN

Sobald das selbstsignierte Zertifikat erstellt ist, sollte es exportiert werden, damit es für die Verbindung von Clients zum UC eBanking prime Server verwendet werden kann.

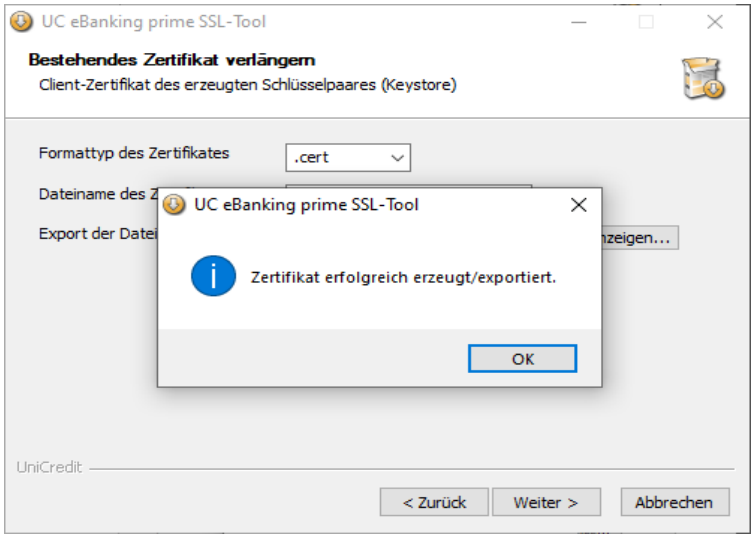
In diesem Bildschirm werden die Exportdetails für das Zertifikat abgefragt.



Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.

Der Standard-Exportpfad ist "[LW]:[InstallationsVerzeichnis UC eBanking prime]\keystore" Verzeichnis.

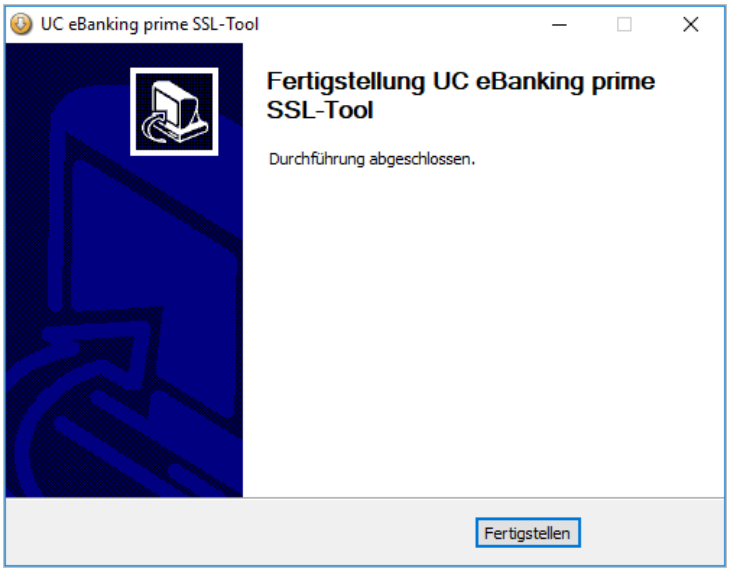
Sobald das Zertifikat erfolgreich generiert oder exportiert wurde wird eine Meldung angezeigt. Die Datei "server.xml" wird mit den SSL Konfigurationsdetails aktualisiert.



3.4 ZERTIFIKAT (SELF-SIGN) VERLÄNGERN

Dieser Bildschirm zeigt die erfolgreiche Verlängerung des selbstsignierten Client-Zertifikats.

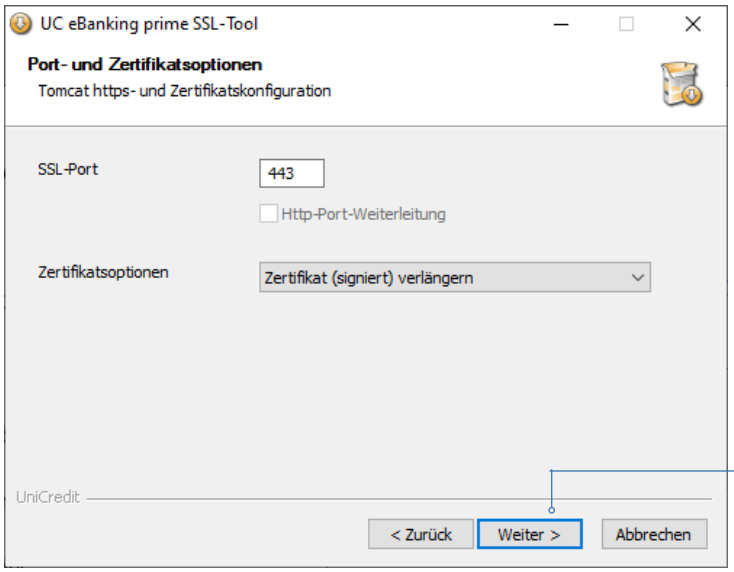
Mit Klick auf den Button „Fertigstellen“ wird das UC eBanking prime SSL Tool beendet.



3.5 ZERTIFIKAT (SIGNIERT) VERLÄNGERN

Diese Option wird verwendet, um die Gültigkeit eines bestehenden signierten Zertifikats zu verlängern.

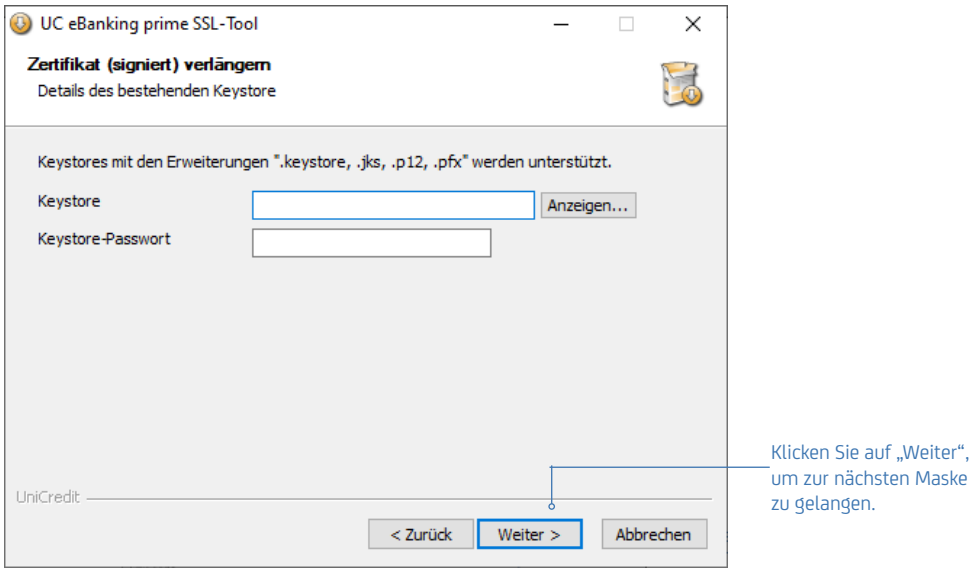
In diesem Bildschirm werden die Details des vorhandenen Schlüsselspeichers und Zertifikats zusammen mit den Passwörtern für den Schlüsselspeicher und die Schlüsselpaare erfasst, die dann zur Verlängerung der Gültigkeit des Zertifikats verwendet werden.



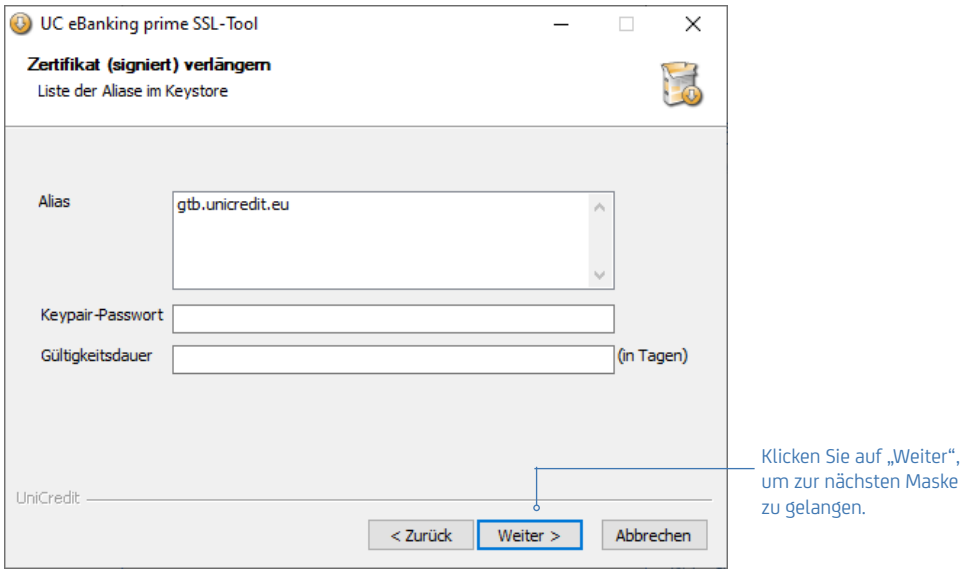
Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.

3.5 ZERTIFIKAT (SIGNIERT) VERLÄNGERN

In diesem Bildschirm müssen die Details des vorhandenen Schlüsselspeichers in dem sich das Zertifikat befindet, zusammen mit dem Passwort angegeben werden.

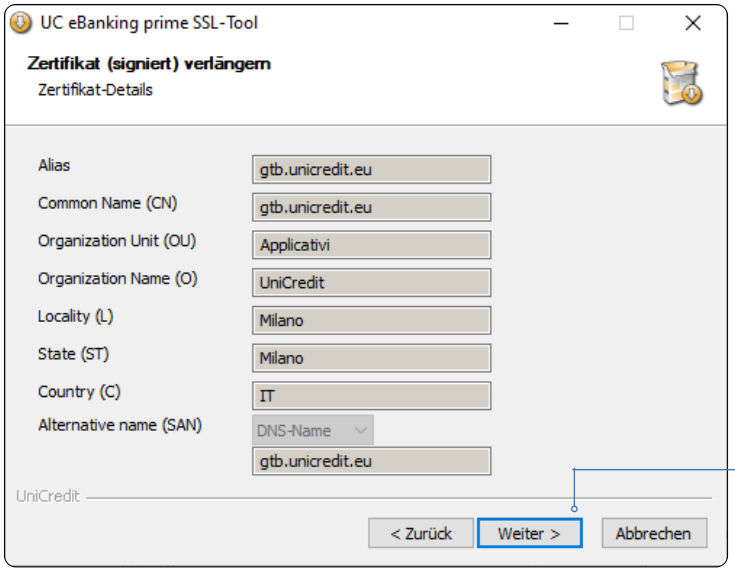


In diesem Bildschirm wählen Sie einen Alias aus der angezeigten Liste und geben Sie das Kennwort für das Schlüsselpaar ein. Geben Sie die Anzahl der Tage ein, um die die Gültigkeit des Zertifikats ab dem aktuellen Tag verlängert werden soll.



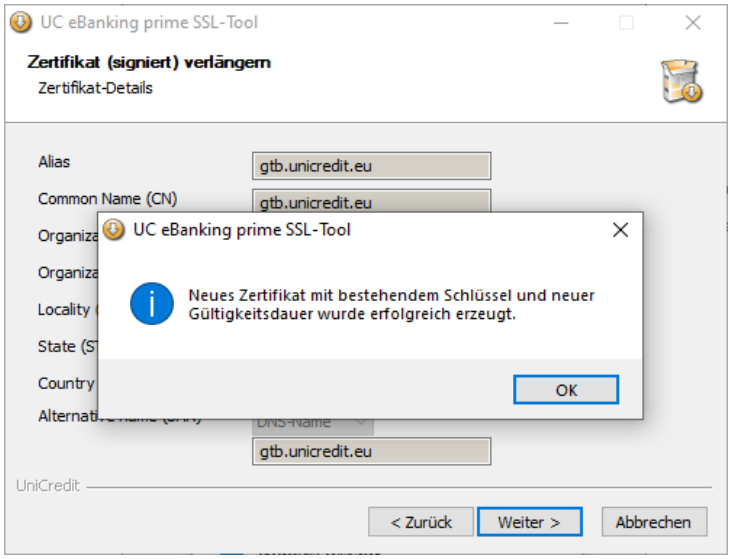
3.5 ZERTIFIKAT (SIGNIERT) VERLÄNGERN

In diesem Bildschirm werden die Details des zu erstellenden Zertifikats angezeigt.



Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen..

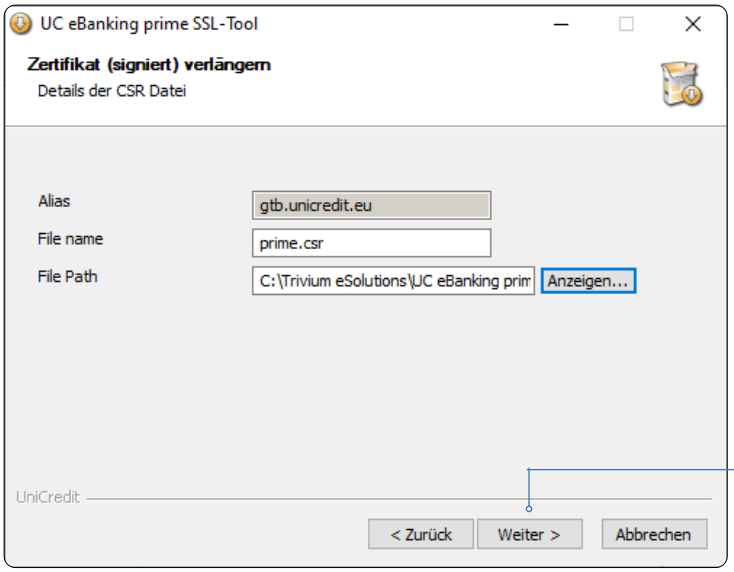
Sobald das neue Zertifikat erfolgreich generiert wurde, wird eine Meldung über die neue Gültigkeit angezeigt.
Die Keystore-Datei wurde nun im Verzeichnis "[LW]:[Installationsverzeichnis UC eBanking prime]\Keystore" erstellt.



3.5 ZERTIFIKAT (SIGNIERT) VERLÄNGERN

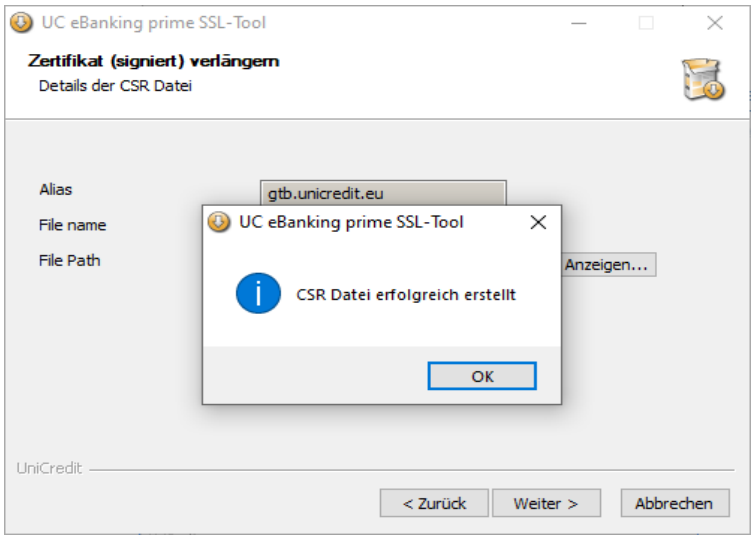
Sobald das selbstsignierte Zertifikat erstellt ist, muss eine Zertifikatssignierungsanforderung (CSR) erstellt und an die Zertifizierungsstelle (CA) gesendet werden. Es wird eine Meldung angezeigt.

In diesem Bildschirm werden die Details der zu erstellenden CSR-Datei angezeigt.



Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.

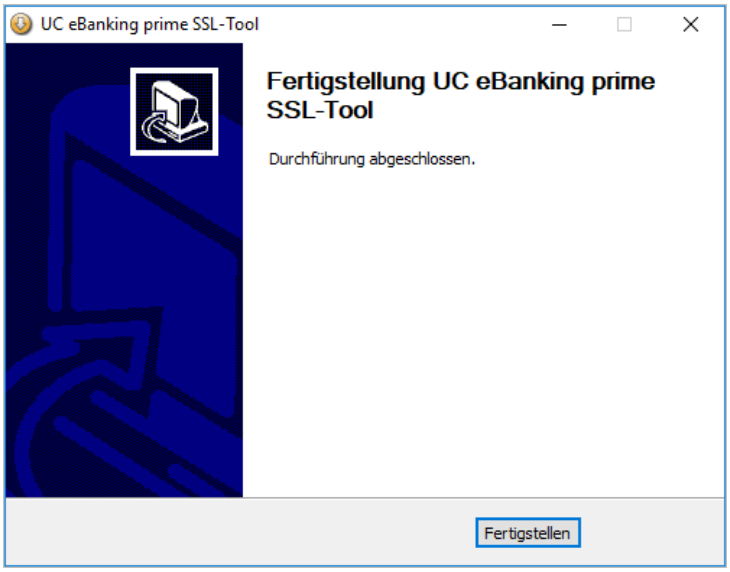
Sobald die CSR-Datei erfolgreich erstellt wurde, wird eine Meldung angezeigt.



3.5 ZERTIFIKAT (SIGNIERT) VERLÄNGERN

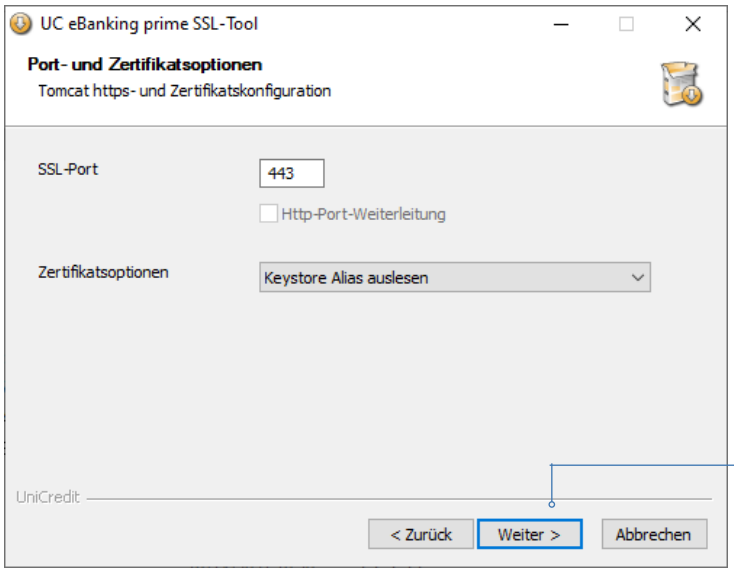
Dieser Bildschirm zeigt die erfolgreiche Verlängerung des signierten Client-Zertifikats.

Mit Klick auf den Button „Fertigstellen“ wird das UC eBanking prime SSL Tool beendet.



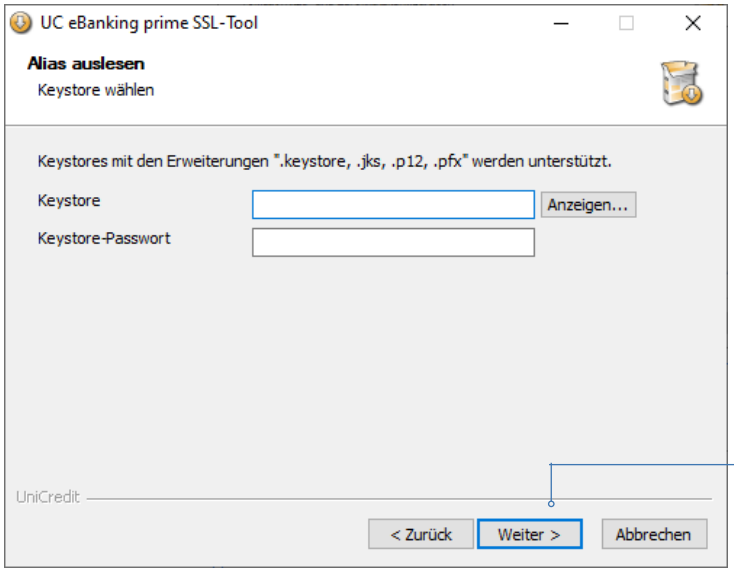
3.6 KEYSTORE ALIAS AUSLESEN

Diese Option wird verwendet, um die Alias-Liste aus einem einem Keystore in einer Textdatei zu speichern.



Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.

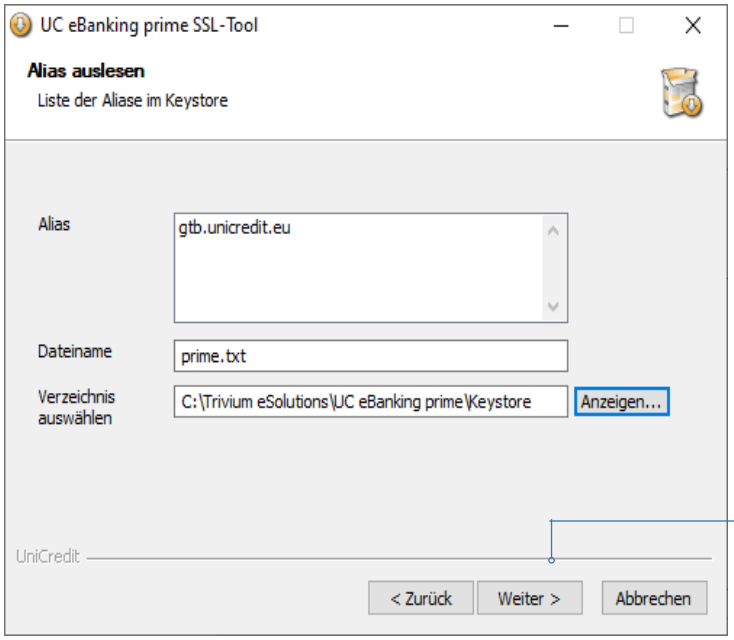
In diesem Bildschirm müssen die Details des vorhandenen Schlüsselspeichers in dem sich das Zertifikat befindet, zusammen mit dem Passwort angegeben werden.



Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.

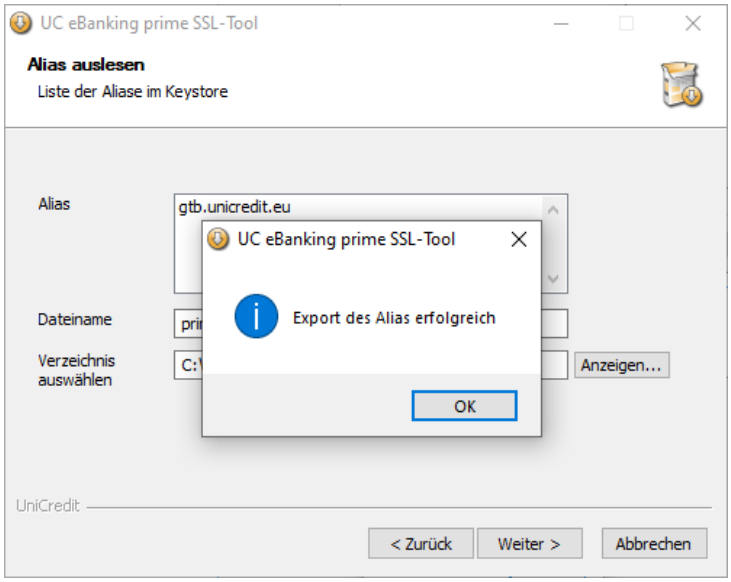
3.6 KEYSTORE ALIAS AUSLESEN

In diesem Bildschirm wird die Liste der im Schlüsselspeicher verfügbaren Aliasnamen angezeigt. Sie sollten einen Dateinamen eingeben und einen Ordner wählen, in den die Alias-Listendatei exportiert werden soll.



Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.

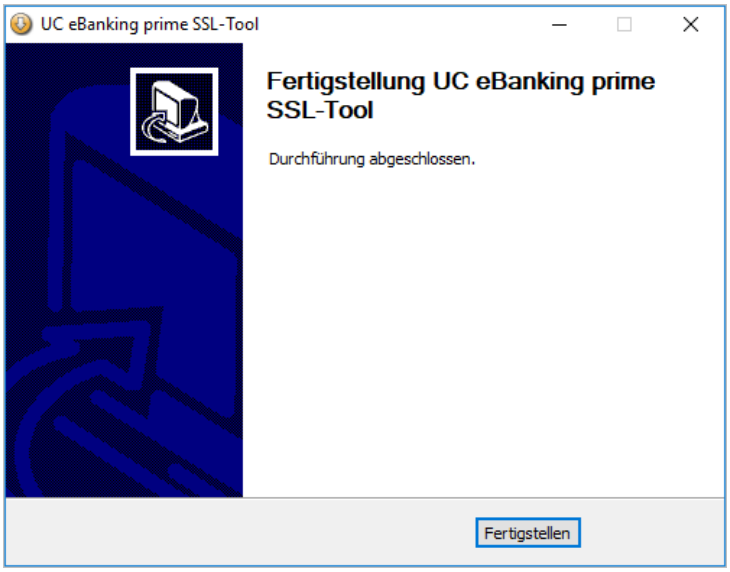
Sobald die Alias-Datei erfolgreich exportiert wurde, wird eine Meldung angezeigt.



3.6 KEYSTORE ALIAS AUSLESEN

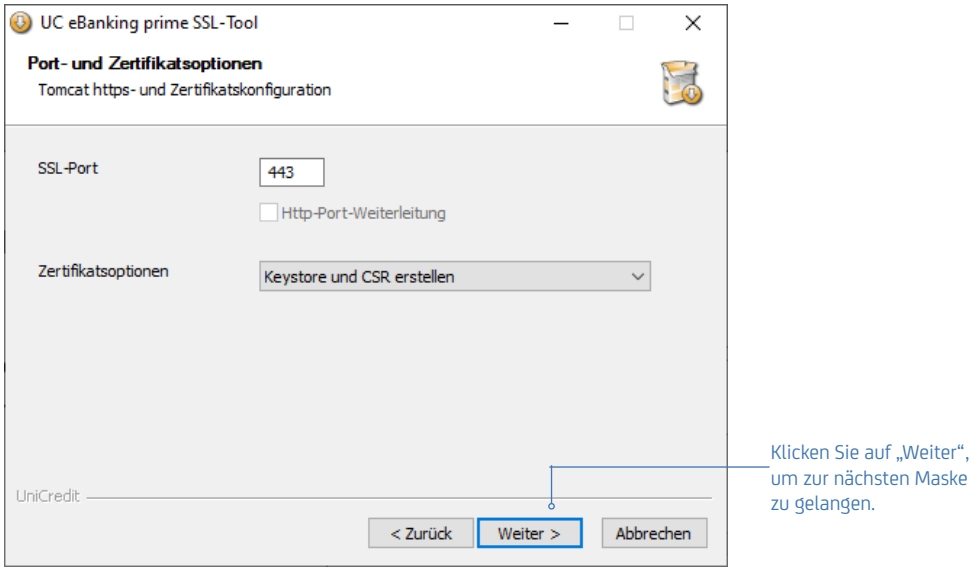
Dieser Bildschirm zeigt den erfolgreichen Export der Alias Liste aus dem Schlüsselspeicher.

Mit Klick auf den Button „Fertigstellen“ wird das UC eBanking prime SSL Tool beendet.

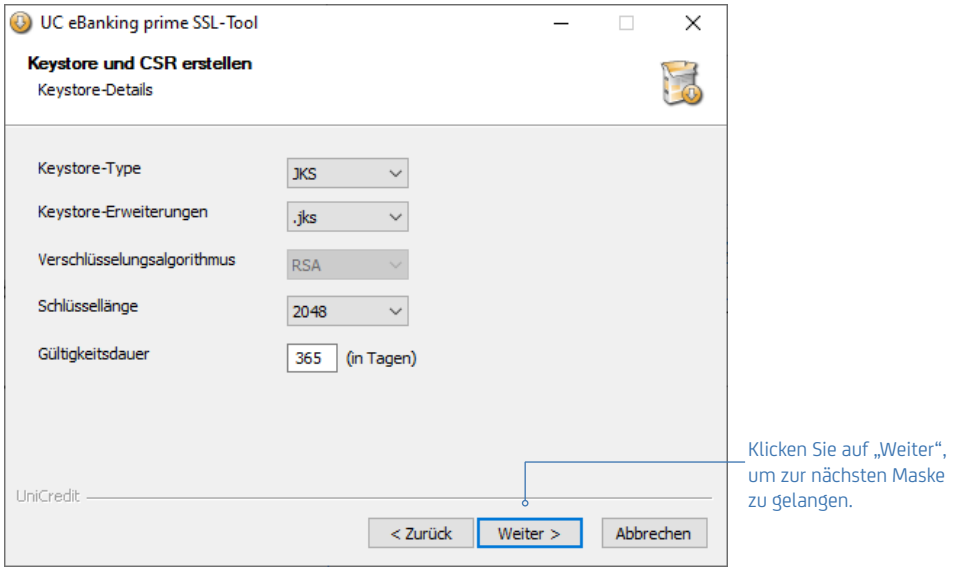


3.7 KEYSTORE UND CSR ERSTELLEN

Diese Option wird verwendet, um einen Schlüsselspeicher zu erstellen und die CSR zu erzeugen.

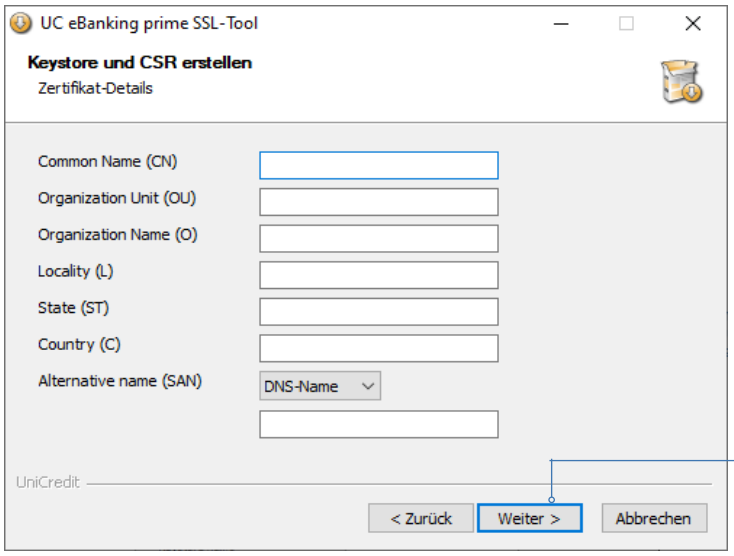


In diesem Bildschirm werden die Details des zu erstellenden Schlüsselspeichers angezeigt.
Die Gültigkeitsdauer kann eingegeben werden.



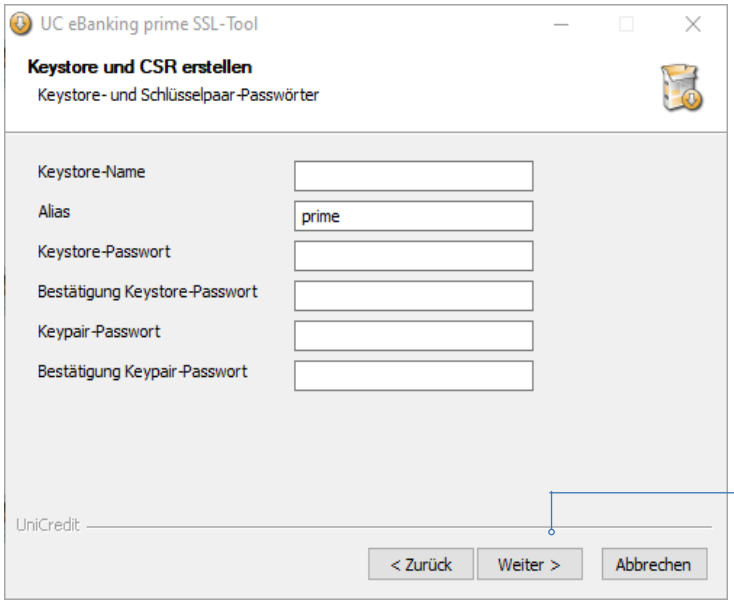
3.7 KEYSTORE UND CSR ERSTELLEN

In diesem Bildschirm werden die Details des zu erstellenden Zertifikats eingegeben.



Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.

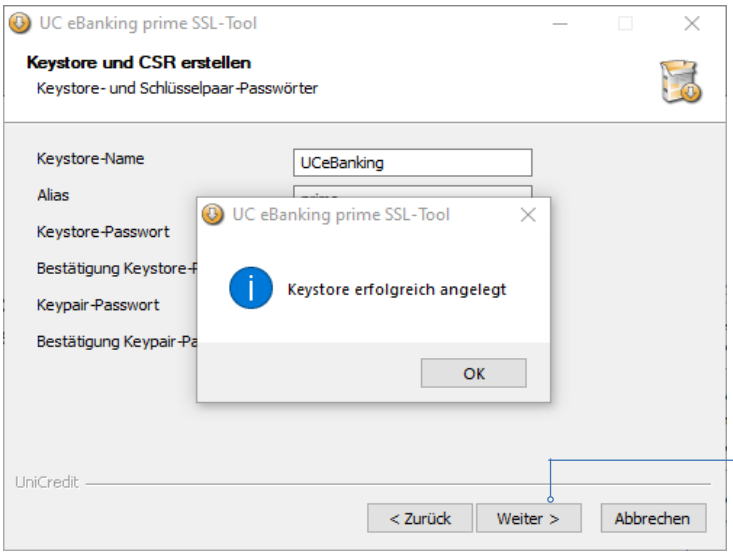
In diesem Bildschirm werden Details zu den Passwörtern von Keystore und Keypair erfasst.



Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.

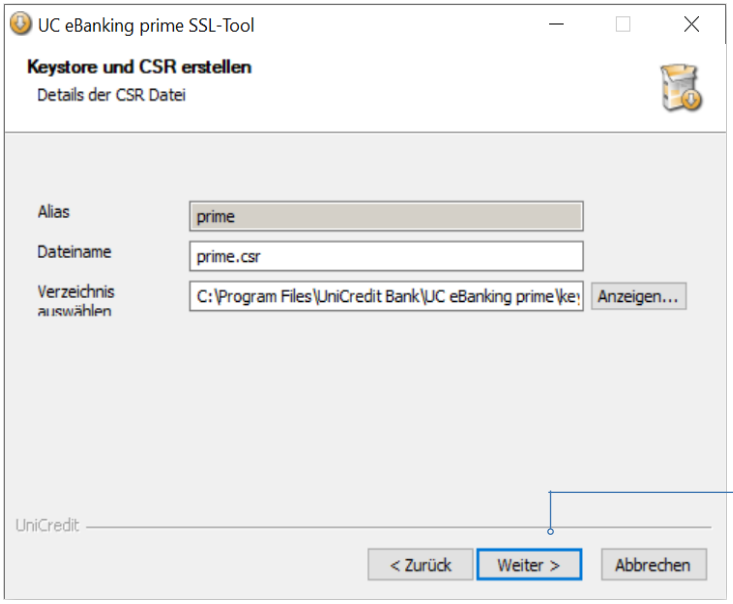
3.7 KEYSTORE UND CSR ERSTELLEN

Sobald der Schlüsselspeicher erfolgreich erzeugt wurde, wird eine Meldung angezeigt.



Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.

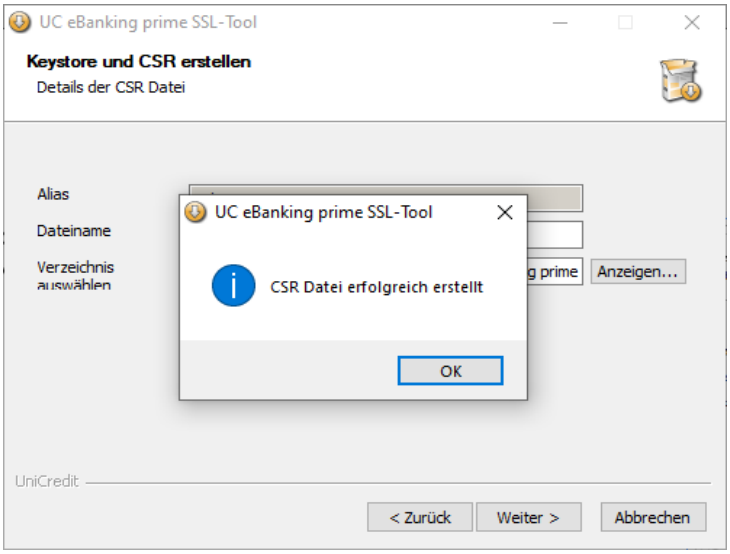
In diesem Bildschirm werden die Details des CSR-Dateinamens und des Ordners in dem sie gespeichert wird, erfasst.



Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen..

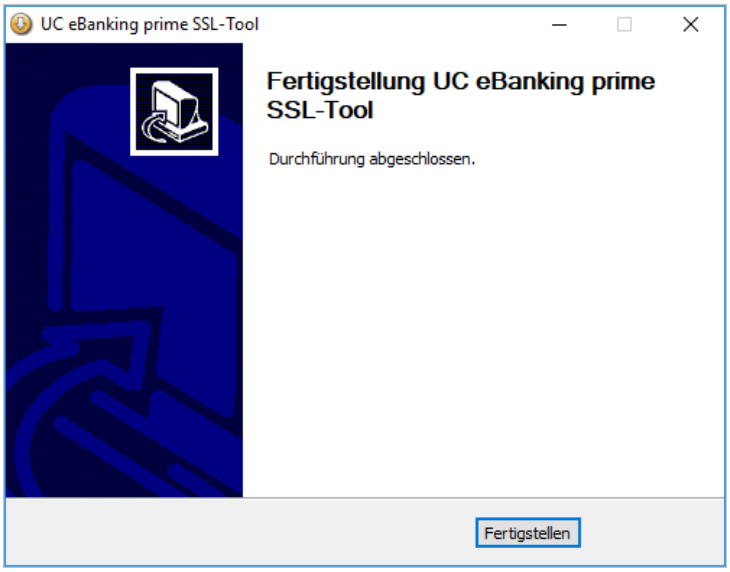
3.7 KEYSTORE UND CSR ERSTELLEN

Sobald die CSR-Datei erfolgreich erstellt wurde, wird eine Meldung angezeigt.



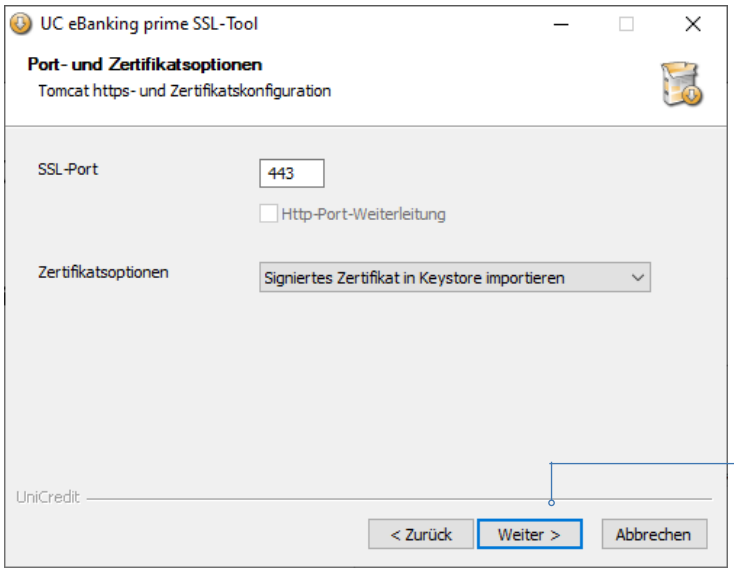
Dieser Bildschirm zeigt die erfolgreiche Erstellung von Keystore und die Erstellung der CSR-Datei.

Mit Klick auf den Button „Fertigstellen“ wird das UC eBanking prime SSL Tool beendet.



3.8 SIGNIERTS ZERTIFIKAT IN KEYSTORE IMPORTIEREN

Diese Option wird verwendet, um ein signiertes Zertifikat in den Keystore zu importieren.

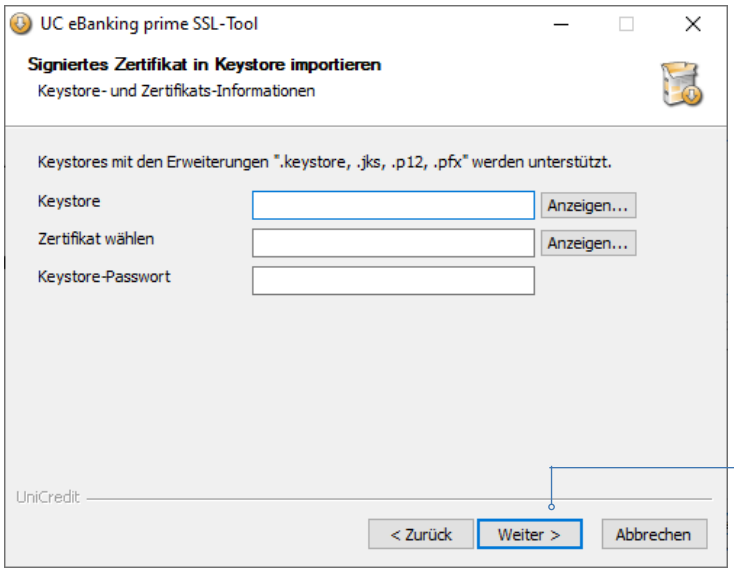


Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.

3.8 SIGNIERTS ZERTIFIKAT IN KEYSTORE IMPORTIEREN

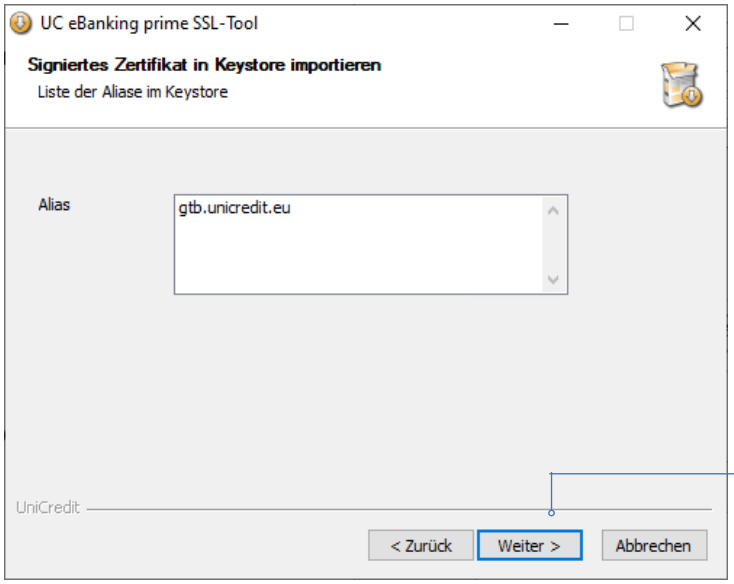
In diesem Bildschirm werden Details zu den
Passwörtern von Keystore und Keypair erfasst.

Zertifikatsdateien können nur die Endungen ".cer", ".p7b" und ".p7r" haben.



Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen..

In diesem Bildschirm muss der Keystore-Alias aus der Alias-Liste ausgewählt werden.

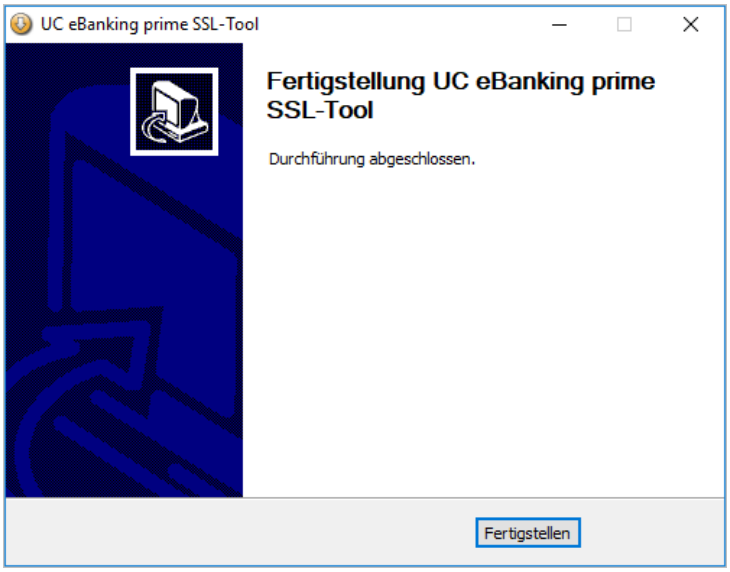


Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.

3.8 SIGNIERTS ZERTIFIKAT IN KEYSTORE IMPORTIEREN

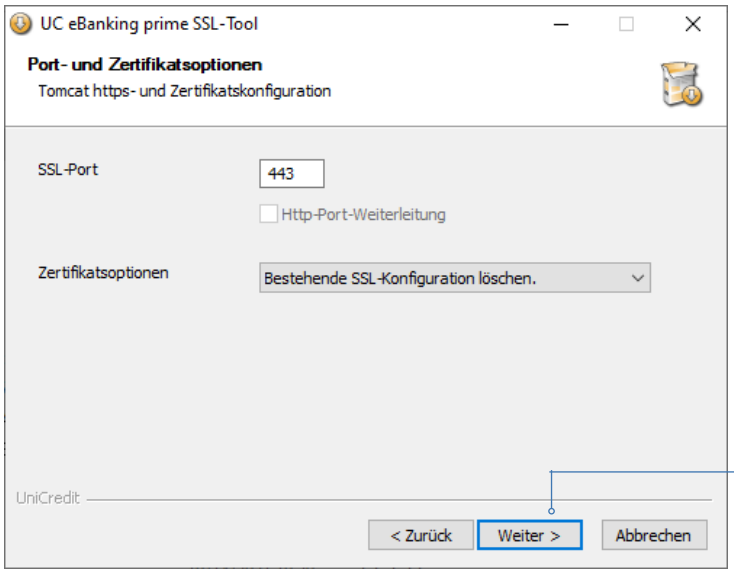
Dieser Bildschirm zeigt den erfolgreichen Import des signierten Zertifikats.

Mit Klick auf den Button „Fertig stellen“ wird das UC eBanking prime SSL Tool beendet.



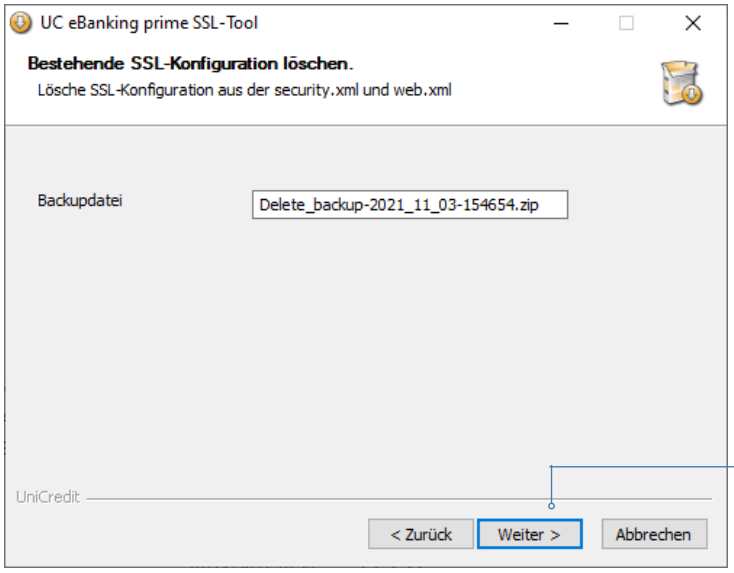
3.9 BESTEHENDE SSL-KONFIGURATION LÖSCHEN

Diese Option wird verwendet, um eine bestehende SSL Konfiguration zu löschen.



Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen

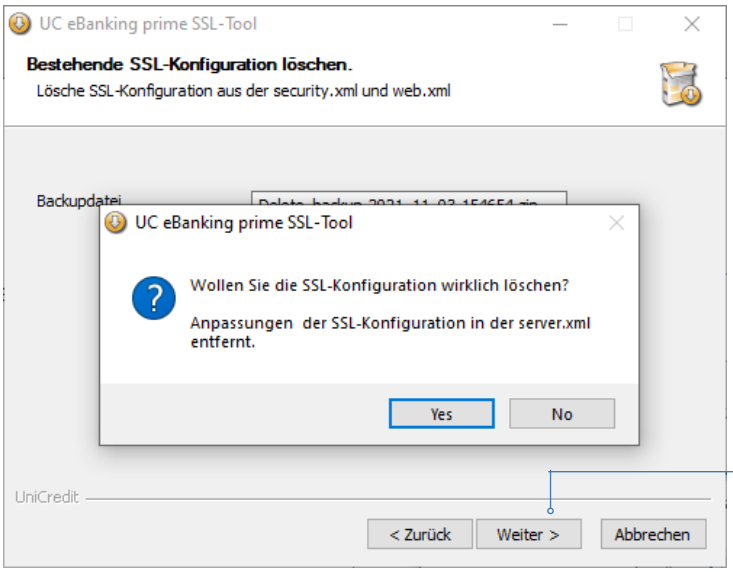
Die bestehende SSL-Konfiguration wird vor dem Löschen aus "server.xml" und "web.xml" gesichert. In diesem Bildschirm wird der Name der Sicherungsdatei festgehalten.



Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.

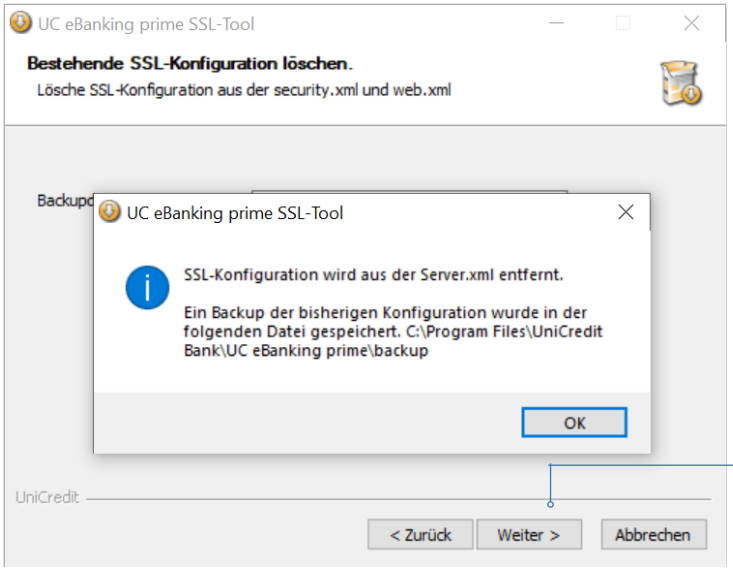
3.9 BESTEHENDE SSL-KONFIGURATION LÖSCHEN

Eine Bestätigungsmeldung wird angezeigt, bevor die SSL Konfiguration gelöscht wird.



Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.

Die bestehende SSL-Konfiguration wird aus "server.xml" gelöscht. Es wird eine Meldung angezeigt.

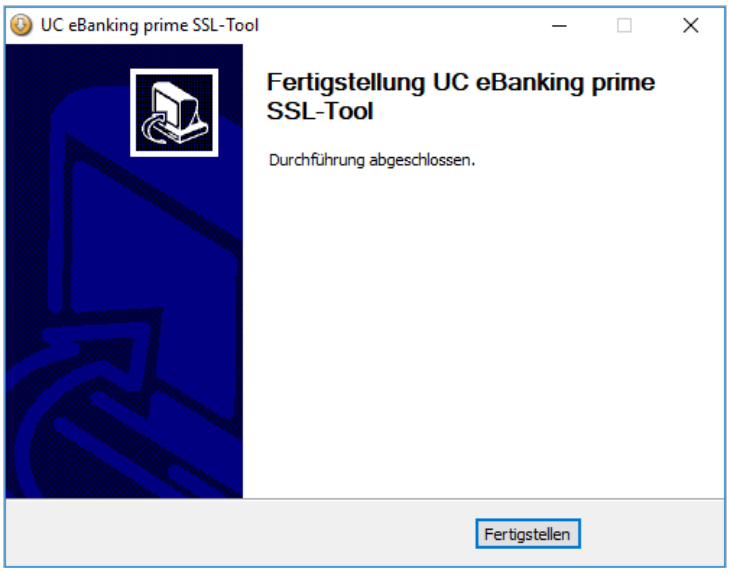


Klicken Sie auf „Weiter“, um zur nächsten Maske zu gelangen.

3.9 BESTEHENDE SSL-KONFIGURATION LÖSCHEN

Dieser Bildschirm zeigt die erfolgreiche Löschung der bestehenden SSL-Konfiguration.

Mit Klick auf den Button „Fertigstellen“ wird das UC eBanking prime SSL Tool beendet.



Start UC eBanking prime Services

Nach erfolgreicher SSL-Konfiguration starten Sie die Dienste neu, indem Sie im Windows-Start menü im Verzeichnis "Programm" auf "UC eBanking prime Services starten" klicken.

4. START UC eBANKING PRIME (CLIENT)

Um UC eBanking prime zu starten, öffnen Sie bitte im Browser die Adresse http://[rechnername]:[port]. Sollte Ihnen die Adresse nicht bekannt sein, wenden Sie sich bitte an Ihren Systemadministrator. Am Server wurde bei der Installation in der Programmgruppe „UC eBanking prime“ eine Verknüpfung „UC eBanking prime“ angelegt, in der die entsprechende Adresse/URL hinterlegt ist.

Die freigegebenen Browser finden Sie in den jeweils gültigen Release Notes.
Je nach verwendetem SSL-Zertifikat können weitere Schritte auf Seiten des Clients (Browser/UC eBanking prime OTC) notwendig sein:

- Browser/UC eBaning prime OTC bei Verwendung eines signierten Zertifikates einer CA (siehe 4.1 SSL UC eBANKING PRIME OTC KONFIGURATION)
- Browser/UC eBanking prime OTC Konfiguration bei Verwendung eines selfsigned Zertifikates (siehe 4.2 Browser-Konfiguration bei Verwendung eines selfsigned Zertifikates (optional))

4.1 SSL UC eBANKING PRIME OTC KONFIGURATION

Der UC eBanking prime OTC Client dient zur Anmeldung und Unterschrift in UC eBanking prime bei Browserverwendung.

Um UC eBanking prime OTC SSL fähig zu machen, tragen Sie unter Einstellungen die entsprechende Server URL (z.B. https://localhost:443) ein. Bitte aktivieren Sie im Anschluss den Punkt „Custom Zertifkat“ und geben Sie den Speicherort des Zertifikates an. Das entsprechende Zertifikat sollte z.B in Ihrem persönlichen Verzeichnis abgespeichert sein. Weitere Informationen entnehmen Sie dem Dokument „UC eBanking prime OTC“.

4.2 BROWSER-KONFIGURATION BEI VERWENDUNG EINES SELFSIGNED ZERTIFIKATES (OPTIONAL)

Ein selfsigned Zertifikat einzubinden ist von der Nutzung des Browsers (z.B. Firefox) abhängig und kann von Browser zu Browser unterschiedlich sein (eine Übersicht der für die Anwendung freigegebenen Browser entnehmen Sie bitte den Release Notes von UC eBanking prime).

Eine HTTPS-Verbindung wird erst dann möglich sein, wenn das Zertifikat manuell dem Browser hinzugefügt wurde.
Beispiel: https://[rechnername]:[port]

4.2.1 SSL UC eBANKING PRIME OTC KONFIGURATION

Der UC eBanking prime OTC Client dient zur Anmeldung und Unterschrift in UC eBanking prime bei Browserverwendung.

Um UC eBanking prime OTC SSL fähig zu machen, tragen Sie unter Einstellungen die entsprechende Server URL (z.B. https://localhost:443) ein. Bitte aktivieren Sie im Anschluss den Punkt „Custom Zertifkat“ und geben Sie den Speicherort des Zertifikates an. Das entsprechende Zertifikat sollte z.B in Ihrem persönlichen Verzeichnis abgespeichert sein.

Zusätzlich bietet der OTC-Client eine Option zum Herunterladen des Client-Zertifikats aus der Maske Einstellungen.

Falls der angegebene Servername nicht mit der tatsächlichen Server-URL übereinstimmt, zeigt der Client eine Zertifikatswarnung an. Weitere Informationen entnehmen Sie dem Dokument „UC eBanking prime OTC“.

Firefox

Wenn Sie die SSL-gesicherte Webseite aufrufen, erhalten Sie eine Warnung über ein nicht vertrauenswürdiges Zertifikat.
Klicken Sie hier auf „Ich kenne das Risiko“ und im Anschluss auf „Ausnahmen hinzufügen…“. Danach erscheint ein Popup, in dem Sie die Ausnahmeregel bestätigen. Das „selfsigned“ Zertifikat ist nun in Ihrem Browser installiert.

Microsoft Edge/Chrome

Beim Zugriff auf die SSL-gesicherte Website erhalten Sie eine Warnung, dass die Verbindung nicht privat ist. Klicken Sie auf "Erweitert" und wählen Sie den Hyperlink aus, mit dem Sie zur unsicheren Website gelangen können.

UniCredit Bank GmbH
Transactions & Payments

Adresse
Arabellastr. 12
D-81925 München

Contact & Service Center UniCredit
Transactions & Payments
gtb-center@unicredit.de

Online
hilfe.hvb.de