

SSL TOOL 1.2 V6.1.0

Stand 18.03.2024



unicreditgroup.eu/clientsolutions

UC eBanking prime (Cash Management	Payments	Orders			_	_	ö
								· · · ·
Payments								
Options •								
I > 3 Page(s), 158 Records						+ 3	0 12 a Y	Σ Q ≡
				· · Bestatest		0		. Data
bank	Account	67.90			25.000.00	EUD	Type	27.02.2012
Hypovereinsbank	122456789.0	07.09		SPIELZEUGLAND ASIA	25.000,00	EUR	A70((G)	27.02.2013
HypoVereinsbank	12345645776	89.001		Susan Parker	12 987 45	FUR	RET	05.03.2013
HypoVereinsbank	123456789.0	11		Roger Donaldson	1 376 38	FUR	FSU	05.03.2013
HypoVereinsbank	123456789.0	01		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	123456789.0	01		Susan Parker	1.376.38	EUR	RFT	05.03.2013
HypoVereinsbank	9865456789	001		Roger Donaldson	234.50	EUR	ESU	05.03.2013
HypoVereinsbank	544445566-0	01		John O'Connor	12.987,45	EUR	IZV	28.05.2013
HypoVereinsbank	12345623453	89 001		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 0	D1		Roger Donaldson	12.987,45	EUR	ESU	02.07.2013
HypoVereinsbank	543256789 0	D4		John O'Connor	1.376,38	EUR	IZV	05.03.2013
HypoVereinsbank	123456789 0	01		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 0	01		Roger Donaldson	345.992.779,00	EUR	ESU	15.09.2013
HypoVereinsbank	560.3463-11	0		John O'Connor	234,50	EUR	ESU	05.03.2013
HypoVereinsbank	123456789 0	D1		XY Company	12.987,45	EUR	IZV	05.03.2013
							Create assignm	tent Sign
© UniCredit Bank GmbH UC eBanking prime. License Information								
							ø	
							<u> </u>	
antenn veloeband ar eer en de konstant I	et anezőlősése jevél a jöltős ö						randa de desta (Ganta	

SSL Tool 1.2

Inhaltsverzeichnis

1. ALLGEMEINE INFORMATIONEN

1.1 STOP UC eBANKING PRIME SERVICES

2. SSL TOOL OPTIONEN

3. EINSTELLUNGEN

- 3.1 BESTEHENDES ZERTIFIKAT KONFIGURIEREN
- 3.2 NEUES ZERTIFIKAT ERSTELLEN UND KONFIGURIEREN (SELF-SIGN)
- 3.3 ZERTIFIKAT EXPORTIEREN
- 3.4 ZERTIFIKAT (SELF-SIGN) VERLÄNGERN
- 3.5 ZERTIFIKAT (SIGNIERT) VERLÄNGERN
- 3.6 KEYSTORE ALIAS AUSLESEN
- 3.7 KEYSTORE UND CSR ERSTELLEN
- 3.8 SIGNIERTES ZERTIFIKAT IN KEYSTORE IMPORTIEREN
- 3.9 BESTEHENDE SSL-KONFIGURATION LÖSCHEN

4. START UC eBANKING PRIME (CLIENT)

- 4.1 SSL UC eBANKING PRIME OTC KONFIGURATION
- 4.2 BROWSER-KONFIGURATION BEI VERWENDUNG EINES SELFSIGNED ZERTIFIKATES (OPTIONAL)

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 Banking 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 f
 ür die Verwendung in UC eBanking prime konfiguriert werden.
- Neues Zertifikat erstellen und konfigurieren (self-sign)
 Mit dieser Option kann ein selbstsigniertes Zertifikat f
 ür die Anwendung in UC ebanking prime erstellt und konfiguriert werden.
- Zertifikat exportieren
 Mit dieser Option kann ein Client-Zertifikat f
 ür 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.



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

	UC eBanking prime SSL- Port- und Zertifikatsopti Tomcat https- und Zertifika	-Tool — — X ionen atskonfiguration	
Wählen Sie diese Option, um den http-Port auf den	SSL-Port	443 ∘	Geben Sie die SSL- Portnummer ein
https-Port umzuleiten	Zertifikatsoptionen	Bestehendes Zertifikat konfigurieren	
Wählen Sie eine der Optionen		Zertifikat exportieren Zertifikat (self-sign) verlängern Zertifikat (self-sign) verlängern Keystore Alias auslesen Keystore und CSR erstellen Signiertes Zertifikat in Keystore importieren Bestehende SSL-Konfiguration löschen.	
	UniCredit ———	< Zurück Weiter > Abbrechen	
		l Nach Eingabe der Port-Informationen und Auswahl der Option zur Zertifikatskonfiguration Klicken Sie auf "Weiter", um fortzufahren.	

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.

UC eBanking prime SSL-Tool Bestehendes Zertifikat konfigurieren Details des bestehenden Keystore	- • ×
Keystores mit den Erweiterungen ".keystore, .jks, .p12, .pfx" werder Keystore Keystore-Passwort	n unterstützt.
UniCredit	Klicken Sie auf "Weiter", um zur nächsten Maske zu gelangen. iter > Abbrechen
UC eBanking prime SSL-Tool Bestehendes Zertifikat konfigurieren List of alias names from keystore	- • ×
Alias list primejks	
Keypair-Passwort	
UniCredit	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.

🕘 UC eBanking prir	ne SSL-Tool	_		×
Bestehendes Zert	ifikat konfigurieren			
List of alias names	rom keystore			5
Alias list	primejks		~	
	🔕 UC eBanking prime SSL-Tool	×		
			~	
Keypair-Passwort	SSL Connector erfolgreich angelegt.			
	-			
	OK			
	UK .			
UniCredit				
	Zurick Weite		Abbr	ochon
	< zuruck Weite		ADDr	echen

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.

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.

🕘 UC eBanking prime SS	L-Tool	_		×
Port- und Zertifikatsop Tomcat https- und Zertifi	tionen katskonfiguration			
SSL-Port	443			
Zertifikatsoptionen	Neues Zertifikat erstellen und	l konfigurieren (\sim	
UniCredit				
	< Zurück	Weiter >	Abbr	echen
	Kli ur zu	icken Sie auf n zur nächste gelangen.	"Weiter", en Maske	

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.

🔕 UC eBanking prime SSL-Tool	– 🗆 X
Neues Zertifikat erstellen und Keystore-Details	konfigurieren (self-sign)
Keystore-Type	JKS ~
Keystore-Erweiterungen	.jks 🗸
Verschlüsselungsalgorithmus	RSA V
Schlüssellänge	2048 ~
Gültigkeitsdauer	365 (in Tagen)
UniCredit	
	< Zurück Weiter > Abbrechen
	Klicken Sie auf "Weiter", um zur nächsten Maske zu gelangen.

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.

🔕 UC eBanking prime SSL-Too	I			_			×
Neues Zertifikat erstellen ur Zertifikat-Details	nd konfiguriere	n (self-sign))				
Common Name (CN) Organization Unit (OU) Organization Name (O) Locality (L) State (ST) Country (C) Alternative name (SAN)	UCeBanking						
UniCredit	[< Zurück	W	/eiter >		Abbre	echen
		Klio Um ZU	cken : n zur i gelar	i Sie auf nächste igen.	"Wei n M	iter", aske	

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.

UC eBanking prime SSL-Tool	-	_	×	
Neues Zertifikat erstellen und ku Keystore- und Schlüsselpaar-Passwö	o nfigurieren (self-sign) rter			
Keystore-Name	UCeBanking			
Alias	UCeBanking			
Keystore-Passwort	•••••			
Bestätigung Keystore-Passwort	•••••			
Keypair-Passwort	•••••			
Bestätigung Keypair-Passwort	•••••			
UniCredit ————	< Zurück Weiter >	Abbr	echen	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.

Keystore-Mame				
Reystore-walle	UCeBanking			
Alias	UCeBanking			
Keystore-Passwort 🕓	JC eBanking prime SSL-Tool 🛛 🛛 🗙			
Bestätigung Keystore- Keypair-Passwort Bestätigung Keypair-P	j Keystore erfolgreich angelegt			
	ОК			
UniCredit				
	< Zurück Weite	er >	Abbr	echen

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".

UC eBanking prime SSL-Tool Nouse Zettifikat orstellen un	d konfiguriaren (oolf sign)	— [×	
Client-Zertifikat des erzeugten :	Gchlüsselpaares (Keystore)		I	
Formattyp des Zertifikates Dateiname des Zertifikates Export der Datei	UCeBanking D:\Trivium eSolutions\UCeBanking	Prime Anzeige	n	
UniCredit	< Zurück We	iter >	bbrechen	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.

UC eBanking prime SSL-Tool — X Neues Zertifikat erstellen und konfigurieren (self-sign)
Client-Zertifikat des erzeugten Schlüsselpaares (Keystore)
Formattyp des Zertifikates .cert ~
Dateiname des Zertifikates UCeBanking
Export der Datei UC eBanking prime SSL-Tool X Zertifikat erfolgreich erzeugt/exportiert. SSL-Konfiguration in server.xml angelegt.
ОК
UniCredit

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 "Zertifikat herunterladen" können Sie das Zertifikat in Ihrem persönlicne Verzeichnis der OTC-Anwendung speichern.

Weitere Informationen entnehmen Sie dem Dokument "UC eBanking prime OTC".

UC eBanking prime SSL-Too	l	_		\times
Port- und Zertifikatsoptione Tomcat https- und Zertifikatsko	n Dnfiguration			
SSL-Port	443 Http-Port-Weiterleitung			
Zertifikatsoptionen	Zertifikat exportieren	~	•	
uses a				
UniCredit	< Zurück Weite	r >	Abbr	echen
	Klicken Si	e auf "	Weiter'	4

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.

Zertifikat exportieren	1	
Details des Keystores zum Export de	s Client-Zertifikates	5
Keystore	C:\Program Files\UniCredit Bank AC Anzeigen	
Speicherort für Client-Zertifikat	:\Program Files\UniCredit Bank AC Anzeigen	
Dateiname des Zertifikates	UCeBanking	
Formattyp des Zertifikates	.cert 🗸	
Alias	UCeBanking	
Keystore-Passwort		
		Klicken Sie auf Weiter"
		um zur nächsten Maske
JniCredit		zu gelangen.

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

🚯 UC eBanking	g prime SSL-Tool		_		
Zertifikat exp List of alias na	portieren ames from keystore				
Alias list	primejks		< v		
UniCredit ———		< Zurück	Veiter >	Abbrechen	 Klicken Sie auf "Weiter" um zur nächsten Maske zu gelangen.

3.3 ZERTIFIKAT EXPORTIEREN

 WC eBanking prime SSL-Tool
 —
 ×

 Zertifikat exportieren
 Image: Comparison of the systeme
 Image: Comparison of the systeme

 Alias list
 Image: Comparison of the systeme
 Image: Comparison of the systeme
 Image: Comparison of the systeme

 Alias list
 Image: Comparison of the systeme
 Image: Comparison of the systeme
 Image: Comparison of the systeme

 Alias list
 Image: Comparison of the systeme
 Image: Comparison of the systeme
 Image: Comparison of the systeme

 Alias list
 Image: Comparison of the systeme
 Image: Comparison of the systeme
 Image: Comparison of the systeme

 Alias list
 Image: Comparison of the systeme
 Image: Comparison of the systeme
 Image: Comparison of the systeme

 Alias list
 Image: Comparison of the systeme
 Image: Comparison of the systeme
 Image: Comparison of the systeme

 Alias list
 Image: Comparison of the systeme
 Image: Comparison of the systeme
 Image: Comparison of the systeme

 Image: Comparison of the systeme
 Image: Comparison of the systeme
 Image: Comparison of the systeme
 Image: Comparison of the systeme

 Image: Comparison of the systeme
 Image: Comparison of the systeme
 Image: Comparison of the systeme
 Image: Comparison of the systeme
 Image: Comparison of the systeme

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.



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.

🕓 UC eBanking prime S	SL-Tool	_		×	
Port- und Zertifikatsop Tomcat https- und Zertif	stionen ikatskonfiguration				
SSL-Port	443 Http-Port-Weiterleitung				
Zertifikatsoptionen	Zertifikat (self-sign) verlängern		~		
UniCredit	z Zuräck Wa	iter >	Abbre	chen	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.

🕓 UC eBanking prime SSL-Tool		_		×	
Bestehendes Zertifikat verlär Details des bestehenden Keysto	the set				
Keystores mit den Erweiterungen Keystore Keystore-Passwort	1 ".keystore, .jks, .p12, .pfx" werd	en unterstützt. Anzeigen	1		
UniCredit	< Zurück V	/eiter >	Abbrech	ien	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.

🕓 UC eBanking pri	me SSL-Tool	_		
Bestehendes Zer Liste der Aliase im	tifikat verlängern Keystore			
Alias	gtb.unicredit.eu		х ,	
Keypair-Passwort Gültigkeitsdauer			(in Tagen)	
UniCredit		< Zurück Weiter >	Abbrechen	Klicken Sie auf "Weiter", um zur nächsten Maske zu gelangen.

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

🚯 UC eBanking prime SSL-To	bl	_		×	
Bestehendes Zertifikat ver Zertifikat-Details	āngem				
Alias Common Name (CN) Organization Unit (OU) Organization Name (O) Locality (L) State (ST) Country (C) Alternative name (SAN)	gtb.unicredit.eu gtb.unicredit.eu Applicativi UniCredit Milano IT DNS-Name gtb.unicredit.eu				Klicken Sie auf "Weiter",
UniCredit	< Zurück	Weiter >	Abbre	echen	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.

UC eBanking prime SSL-To Bestehendes Zertifikat ver	ool	_		×
Zertifikat-Details				5
Alias	gtb.unicredit.eu			
Common Name (CN)	gtb.unicredit.eu			
Organi 🕓 UC eBanking p	rime SSL-Tool		×	
Organi:				
Locality Neues Z	ertifikat mit bestehendem Schlüsse	el und neuer		
State (ensuader wurde enorgreich eizeug			
Countr				
Alterna		ОК		
	gtb.unicredit.eu			
UniCredit				
	< Zurück	Weiter >	Abbr	echen

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.

🕓 UC eBanking prime SSL-Tool		_		×	
Bestehendes Zertifikat verlä Client-Zertifikat des erzeugten S	n gern chlüsselpaares (Keystore)				
Formattyp des Zertifikates Dateiname des Zertifikates Export der Datei	.cert unicredit C:\Trivium eSolutions\JC eBanking	prim An	zeigen]	
UniCredit	< Zurück Wei	ter >	Abbre	echen	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.

🔕 UC eBanking prime SSL-Tool	_		\times
Bestehendes Zertifikat verlängern Client-Zertifikat des erzeugten Schlüsselpaares (Keystore)			
Formattyp des Zertifikates .cert 🗸			
Dateiname des Z 🕔 UC eBanking prime SSL-Tool	×		
Export der Datei		nzeigen	
ОК			
UniCredit	r >	Abbro	echen

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

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



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.

🕘 UC eBanking prime SSI	-Tool	- 🗆	×	
Port- und Zertifikatsop Tomcat https- und Zertifi				
SSL-Port	443 Http-Port-Weiterleitung			
Zertifikatsoptionen	Zertifikat (signiert) verlängern		~	
UniCredit	< Zurück We	iter > Ab	brechen	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.

OC eBanking prime SSL-To	ol	_	×	
Zertifikat (signiert) verläng	em			
Details des bestehenden Key	store		5	
Keystores mit den Erweiterun	gen ".keystore, .jks, .p12, .pfx" werd	en unterstützt.		
Keystore		Anzeigen		
Keystore-Passwort				
				Klicken Sie auf "Weiter",
UniCredit				zu gelangen.
	< Zurück W	Veiter > At	obrechen	

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.

🕘 UC eBanking pri	me SSL-Tool			×	
Zertifikat (signie Liste der Aliase im	r t) verlängern Keystore				
Alias	gtb.unicredit.eu		<		
Keypair-Passwort Gültigkeitsdauer			(in T	agen)	
UniCredit		< Zurück Weit	er > Abbr	rechen	Klicken Sie auf "Weiter", um zur nächsten Maske zu gelangen.

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

UC eBanking prime SSL-1	lool	_		×	
Zertifikat (signiert) verlār Zertifikat-Details	igem				
Alias Common Name (CN) Organization Unit (OU)	gtb.unicredit.eu gtb.unicredit.eu Applicativi				
Organization Name (O) Locality (L) State (ST)	UniCredit Milano Milano				
Country (C) Alternative name (SAN)	IT DNS-Name gtb.unicredit.eu				Klicken Sie auf "Weiter", um zur nächsten Maske
UniCredit ———	< Zurück We	eiter >	Abbro	echen	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.

🔞 UC eBanking prime SSL-Tool	_		×
Zertifikat (signiert) verlängern Zertifikat-Details			
Alias gtb.unicredit.eu Common Name (CN) otb.unicredit.eu			
Organiza Organiza Locality State (S	d neuer	×	
Country Alternation of the province of the pro	OK		_
< Zurück Weite	r >	Abbr	echen

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.
---	--

1	🔕 UC eBanking prime	SSL-Tool	_		×	
	Zertifikat (signiert) Details der CSR Datei	verlängern				
	Alias File name File Path	gtb.unicredit.eu prime.csr C:\Trivium eSolutions\UC eBanking prim	Anzeig	jen		
	UniCredit	 Zurück 	· >	Abbr	echen	Klicken Sie auf "Weiter", um zur nächsten Maske zu gelangen.

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

\mathrm UC eBanking pr	ime SSL-Tool — 🗆 🗙
Zertifikat (signie	rt) verlängern
Details der CSR D	atei
Alias	gtb.unicredit.eu
File name	UC eBanking prime SSL-Tool X
File Path	CSR Datei erfolgreich erstellt
UniCredit	OK < Zurück Weiter > Abbrechen

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.

UC eBanking prime SSL-Too	bl	_		×	
Port- und Zertifikatsoptione Tomcat https- und Zertifikatsk	:n onfiguration				
SSL-Port	443 Http-Port-Weiterleitung				
Zertifikatsoptionen	Keystore Alias auslesen		~		
UniCredit	< Zurück	Weiter >	Abbre	echen	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.

OC eBanking prime SSL-	Tool	_	×	
Alias auslesen Keystore wählen				
Keystores mit den Erweiter	ungen ".keystore, .jks, .p12, .pfx" werd	en unterstützt.		
Keystore		Anzeigen		
Keystore-Passwort				
				Klicken Sie auf "Weit
UniCredit				zu gelangen.
	< Zurück V	Veiter > Abb	orechen	_

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.

🚯 UC eBanking	prime SSL-Tool – 🗆 🗙	
Alias auslesen Liste der Aliase	i im Keystore	
Alias	gtb.unicredit.eu	
Dateiname Verzeichnis auswählen	prime.txt C:\Trivium eSolutions\UC eBanking prime\Keystore Anzeigen	
UniCredit	< Zurück Weiter > Abbrechen	Klicken Sie auf "Weiter", um zur nächsten Maske zu gelangen.

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

🕓 UC eBanking	orime SSL-Tool — 🗆 🗙
Alias auslesen Liste der Aliase	im Keystore
Alias	gtb.unicredit.eu
Dateiname Verzeichnis auswählen	prie Export des Alias erfolgreich C: Anzeigen
UniCredit	< Zurück Weiter > Abbrechen

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.



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

🕘 UC eBanking prime SSI	-Tool	_	Х	
Port- und Zertifikatsopt Tomcat https- und Zertifik	i onen (atskonfiguration			
SSL-Port	443 Http-Port-Weiterleitung			
Zertifikatsoptionen	Keystore und CSR erstellen	~		
				Vlickop Sig ouf Weiter"
UniCredit	< Zurück	Weiter > Abbre	echen	um zur nächsten Maske zu gelangen.

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

🔕 UC eBanking prime SSL-Tool	- 🗆 X]
Keystore und CSR erstellen Keystore-Details		
Keystore-Type	KS ✓	
Verschlüsselungsalgorithmus	,jks ∨ RSA ∨	
Schlüssellänge Gültigkeitsdauer	2048 V	
UniCredit		Klicken Sie auf "Weiter", um zur nächsten Maske zu gelangen.
	< Zurück Weiter > Abbrechen	

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

🚯 UC eBanking prime SSL-Too	I		-		×
Keystore und CSR erstellen Zertifikat-Details					
Common Name (CN)					
Organization Unit (OU)					
Organization Name (O)					
Locality (L)					
State (ST)					
Country (C)					
Alternative name (SAN)	DNS-Name 🗸				
UniCredit					
	<	K Zurück We	iter >	Abbre	echen

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

UC eBanking prime SSL-Tool		_		\times	
Keystore und CSR erstellen Keystore- und Schlüsselpaar-Passv	/örter				
Keystore-Name Alias Keystore-Passwort Bestätigung Keystore-Passwort Keypair-Passwort Bestätigung Keypair-Passwort	prime				
UniCredit ————————————————————————————————————	< Zurück We	eiter >	Abbr	echen	Klicken Sie auf "Weiter", um zur nächsten Maske zu gelangen.

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

🚯 UC eBanking prime SSL-Tool	_		\times	
Keystore und CSR erstellen Keystore- und Schlüsselpaar-Pass	vörter			
Keystore-Name Alias Keystore-Passwort Bestätigung Keystore-f Keypair-Passwort Bestätigung Keypair-Pa	UCeBanking anking prime SSL-Tool × Keystore erfolgreich angelegt			
UniCredit	< Zurück Weiter >	Abbre	chen	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.

🕓 UC eBanking p	rime SSL-Tool —		
Keystore und C Details der CSR	S R erstellen Datei		
Alias Dateiname Verzeichnis auswählen	prime prime.csr C:\Program Files\UniCredit Bank\UC eBanking prime\kei	Anzeigen	
UniCredit	< Zurück Weiter >	Abbrechen	Klicken Sie auf "Weiter", um zur nächsten Maske zu gelangen

OC eBanking prime SSL-Tool \times Keystore und CSR erstellen Details der CSR Datei Alias UC eBanking prime SSL-Tool \times Dateiname Verzeichnis auswählen g prime Anzeigen... CSR Datei erfolgreich erstellt ОК UniCredit < Zurück Weiter > Abbrechen

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.

🔕 UC eBanking prime SSL-T	iool —		×	
Port- und Zertifikatsoption Tomcat https- und Zertifikat	nen skonfiguration			
SSL-Port	443 Http-Port-Weiterleitung			
Zertifikatsoptionen	Signiertes Zertifikat in Keystore importieren	~]	
UniCredit ————	< Zurück Weiter >	Abbr	echen	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.

🕘 UC eBanking prime SSL-	Tool	- 🗆	Х	
Signiertes Zertifikat in K Keystore- und Zertifikats-I	eystore importieren nformationen			
Keystores mit den Erweiter Keystore Zertifikat wählen Keystore-Passwort	ungen ".keystore, .jks, .p12, .pfx" we	Anzeigen		
UniCredit	< Zurück	Weiter > Abb	rechen	Klicken Sie auf "Weiter" um zur nächsten Maske zu gelangen

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

UC eBanki Signiertes 2 Liste der Ali	ng prime SSL-Tool Zertifikat in Keystore importieren ase im Keystore	-		×	
Alias	gtb.unicredit.eu	< >			
UniCredit	< Zurück W	/eiter >	Abbre	chen	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.

🔕 UC eBanking prime SSL	-Tool —		×	
Port- und Zertifikatsopti Tomcat https- und Zertifik	onen atskonfiguration			
SSL-Port	443 Http-Port-Weiterleitung			
Zertifikatsoptionen	Bestehende SSL-Konfiguration löschen.	~		
UniCredit	< Zurück Weiter >	Abbre	echen	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.

🕓 UC eBanking prime	SSL-Tool —		×	
Bestehende SSL-Konfiguration löschen. Lösche SSL-Konfiguration aus der security.xml und web.xml				
Backupdatei	Delete_backup-2021_11_03-154654.zip			
UniCredit ————	< Zurück Weiter >	Abbr	echen	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.



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



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