

Antrag auf Ausstellung eines SSL Zertifikates (Business SSL, SSL UCC, SSL Wildcard)

(Erläuterungen zum Ausfüllen und Nutzungsbestimmungen siehe Folgeseiten)

Zertifikatsangaben

Firmenname/Organisation	
Organisationseinheit	
Firmenadresse (Strasse, PLZ, Ort)	
Land	

Gewünschte Funktion

SSL	URL			
SSL UCC (1 - 8 Webadressen)	URL		URL	
	URL		URL	
	URL		URL	
	URL		URL	
SSL Wildcard	URL			
	Anzahl Domains			
Gewünschte Laufzeit	3 Jahre (Standard)	2 Jahre	1 Jahr	Test (1 Monat)
Web-Server (Angabe für SSL Zertifikate)	IIS	Apache		

Zusätzliche Angaben

Firmenvertreter (Zeichnungsberechtigte/r)	
- Tel. Nr. Geschäft	
- e-Mail Adresse	
- Funktion, Abteilung	
Techn. Ansprechpartner	
- Tel. Nr. Geschäft	
- Tel. Nr. Mobile	
- e-Mail Adresse	

Notwendige Ausweisdokumente/Beilagen

Pass/ID Nr. (Firmenvertreter)	
HR-Auszug vom	

Alle Daten werden unter Anwendung des Datenschutzgesetzes streng vertraulich und unter Verschluss aufbewahrt.

Mit der Annahme des Zertifikates bestätigen wir, dass

- sämtliche Angaben und Erklärungen in Bezug auf die im Zertifikat enthaltenen Informationen der Wahrheit entsprechen
- der Signaturschlüssel von uns geschützt aufbewahrt wird
- wir keiner unbefugten Person Zugang zum Signaturschlüssel gewähren
- wir das Zertifikat ausschliesslich in Übereinstimmung mit der Certificate Policy (CP/CPS) einsetzen werden
- das Zertifikat unverzüglich von uns ungültig erklärt wird, wenn die Angaben des Zertifikates nicht mehr stimmen oder der Signaturschlüssel abhanden gekommen, gestohlen oder möglicherweise kompromittiert wurde
- wir die nachfolgenden Nutzungsbestimmungen vollständig akzeptieren und einhalten werden.

Der Antragsteller	
Ort, Datum	Unterschrift(en) Zeichnungsberechtigte(r)
QuoVadis Trustlink Schweiz AG	
Ort, Datum	Unterschrift Mitarbeiter der Registrierungsstelle

Notwendige amtliche Ausweisdokumente

Die folgenden zusätzlichen Dokumente sind mit dem unterschriebenen Antrag einzureichen:

- Kopie Pass oder ID der zeichnungsberechtigten Person(en)
- Kopie eines beglaubigten Handelsregisterauszuges

Zur Ausstellung eines SSL Zertifikates benötigen wir die elektronische Zertifikatssignierungsanfrage (Certificate Signing Request CSR) vom betreffenden Webserver (senden an register.ch@quovadisglobal.com).

Generelle Namensformen

Der Name muss den Zertifikatsinhaber eindeutig identifizieren und in einer für Menschen verständliche Form vorliegen. Zertifikate dürfen nur auf einen zulässigen Namen des Zertifikatsinhabers ausgestellt werden. Anonyme Zertifikate sind nicht möglich.

Der Namenseintrag des Zertifikatsinhabers muss eindeutig sein. Nur wenn ein Zertifikatsinhaber mehrere Zertifikate mit unterschiedlicher Schlüsselnutzung besitzt, kann ein Name mehrmals vorkommen.

Erlaubte Zeichen sind: a-z A-Z 0-9 / Leerzeichen. Umlaute werden in zwei Buchstaben dargestellt (z.B. Ä = Ae).

Identitätsüberprüfungen bei Neuantrag

Für alle im Zertifikat vermerkten Attribute hat ein Nachweis und eine Bestätigung anhand eines amtlichen Dokumentes zu erfolgen. Bezieht sich ein Eintrag auf den Handelsregisterauszug, so ist nebst dem aktuellen Handelsregisterauszug auch eine Zustimmungserklärung der handelsrechtlich eingetragenen Geschäftsleitung oder der Inhaber beizubringen.

Annahme des Zertifikates

Ein Zertifikat wird durch den Zertifikatsinhaber akzeptiert, wenn das Zertifikat verwendet wird oder innerhalb von 10 Tagen nach Erhalt kein Widerspruch erfolgt. Fehlerhaft ausgestellte Zertifikate sind QuoVadis unverzüglich zu melden.

Ungültigerklärung

Die Ungültigerklärung eines Zertifikats kann telefonisch, per E-Mail oder handschriftlich an QuoVadis erfolgen. Eine Suspendierung (zeitliche Aussetzung) von Zertifikaten wird nicht vorgenommen. Einmal ungültig erklärte Zertifikate können nicht erneuert oder verlängert werden.

Zertifikaterneuerung unter Verwendung eines neuen Schlüssels

Bei einer Zertifikaterneuerung hat der Zertifikatsinhaber zu bestätigen, dass die im Zertifikat enthaltenen Informationen unverändert bleiben und die anlässlich der Zertifikatsausstellung vorgelegten Ausweise und Dokumente noch gültig sind. Das alte Zertifikat wird nach Ausstellung des neuen Zertifikats nicht ungültig erklärt und bleibt bis zum Ablauf der Gültigkeitsdauer gültig.

Pflichten des Zertifikatsinhabers

Der Benutzer verpflichtet sich:

- a) seinen Signaturschlüssel zu sichern und alle angemessenen und notwendigen Vorsichtsmassnahmen gegen Diebstahl, unberechtigte Sichtung, Manipulation, Gefährdung, Verlust, Beschädigung, Störung, Freigabe, Änderung oder unberechtigten Gebrauch seines Signaturschlüssels zu treffen (inkl. Passwort, Token oder Smartcard und Aktivierungsdaten)
- b) die alleinige und vollständige Kontrolle über den Gebrauch des Signaturschlüssels auszuüben
- c) QuoVadis im Falle einer Gefährdung oder eines anderen Vorfalles, wie unter (a) festgehalten, sowie wie in Fällen, in denen der Zertifikatsinhaber glaubt oder annimmt, dass dies der Fall ist, umgehend davon in Kenntnis zu setzen
- d) sein Zertifikat zu jeder Zeit nach allen anwendbaren Gesetzen und Richtlinien zu verwenden
- e) unverzüglich nach Beendigung, Widerruf oder Ablauf des Benutzervertrages (aus welchen Gründen auch immer), den Gebrauch des Zertifikats vollständig einzustellen
- f) alle angemessenen Massnahmen zu treffen, um die Sicherheit oder die Integrität der QuoVadis PKI nicht zu gefährden
- g) bei Verlust oder Missbrauch des Signaturschlüssels umgehend eine Revozierung zu veranlassen
- h) QuoVadis innerhalb eines Monats jede Änderung der Zertifikatsinhaberdaten, insbesondere Wohn- und E-Mail-Adresse, unverzüglich schriftlich oder mittels signiertem E-Mail zu melden
- i) die vereinbarten Preise fristgerecht zu zahlen

Verletzt der Zertifikatsinhaber die ihm obliegenden Pflichten erheblich oder nachhaltig, so kann QuoVadis das Zertifikat auf Kosten des Kunden revozieren.

Haftung des Zertifikatsinhabers

Der Inhaber eines Signaturschlüssels haftet Drittpersonen für Schäden, die diese erleiden, weil sie sich auf das gültige Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten verlassen haben. Die Haftung entfällt, wenn der Inhaber des Signaturschlüssels glaubhaft darlegen kann, dass er die nach den Umständen notwendigen und zumutbaren Sicherheitsvorkehrungen getroffen hat, um den Missbrauch des Signaturschlüssels zu verhindern.

Vertragsdauer und Kündigungsfristen

Die Mindestvertragsdauer ergibt sich aus der im Zertifikat angegebenen Gültigkeitsdauer.

Das Vertragsverhältnis ist für beide Vertragspartner mit einer Frist von drei Monaten zum Ablauf der Mindestvertragslaufzeit kündbar. Die Kündigung muss QuoVadis mindestens drei Monate vor dem Tag, an dem sie wirksam werden soll, schriftlich oder per signiertem E-Mail zugehen.

Die Vertragslaufzeit verlängert sich jeweils um die Gültigkeitsdauer des Zertifikates, wenn nicht spätestens drei Monate vor ihrem Ablauf schriftlich oder per signiertem E-Mail gekündigt wird.

Rechte und Pflichten nach Vertragsbeendigung

Die Beendigung des Vertragsverhältnisses wirkt sich nicht auf Handlungen aus, die vor der Beendigung unternommen wurden. Alle Rechte und Pflichten bleiben intakt und überdauern diese Beendigung. Die Aufbewahrungsdauer von Dokumenten und Zertifikaten entspricht den Vorgaben des ZertES von 11 Jahren.

Weitere Informationen

Die Homepage von QuoVadis (www.quovadis.ch) informiert Sie über die Ihrem Vertragsverhältnis zu Grunde liegenden Dokumente:

- QuoVadis Certification Policy CP/CPS
- QuoVadis Relying Party Agreement
- QuoVadis Terms and Conditions of Use
- QuoVadis User Agreement

Änderungen werden laufend über die Homepage publiziert.

Kontaktangaben, Revozierungsdienst (7x24x365), Support (Bürozeiten)

QuoVadis Trustlink Schweiz AG, Teufenerstrasse 11, 9000 St. Gallen

Tel. +41 71 272 60 60, Fax +41 71 272 60 61, info.ch@quovadisglobal.com, www.quovadis.ch

Revozierungsdienst: www.quovadis.ch

Support (während Bürozeiten): Tel. +41 71 272 60 60, support.ch@quovadisglobal.com