

Antrag auf Ausstellung eines qualifizierten Zertifikates

(Erläuterungen zum Ausfüllen und Nutzungsbestimmungen siehe Folgeseiten)

Zertifikatsangaben

| | |
|---|--|
| Vorname(n) | |
| Nachname | |
| Pseudonym ¹ | |
| Titel (Dr./Prof.) ¹ | |
| e-Mail Adresse | |
| Transaktionslimite CHF ¹ | |
| Geburtsdatum | |
| Geburts- oder Bürgerort | |
| Staatszugehörigkeit | |
| Niederlassungsstaat | |
| Firma/Organisation und Ort ² | |
| Organisationseinheit ² | |

1) optionale Zertifikatsanträge 2) Zertifikat mit Firmeneintrag (optional)

Zusätzliche Angaben

| | | | | | |
|--|--|----------------------|-----------------|--------|-----------------|
| Private Adresse (Strasse, PLZ, Ort) | | | | | |
| Tel. Privat | | | | | |
| Tel. Privat Mobile | | | | | |
| Firmenadresse (Strasse, PLZ, Ort) ² | | | | | |
| Tel. Firma ² | | | | | |
| Firmenvertreter (Zeichnungsberechtigte/r) ² | | | | | |
| Erkennungspasswort (mind. 8 Zeichen) | | | | | |
| Gewünschte Laufzeit | <table border="1"> <tr> <td>3 Jahre (Standard)</td> <td>2 Jahre</td> <td>1 Jahr</td> <td>Test (3 Monate)</td> </tr> </table> | 3 Jahre (Standard) | 2 Jahre | 1 Jahr | Test (3 Monate) |
| 3 Jahre (Standard) | 2 Jahre | 1 Jahr | Test (3 Monate) | | |
| Gewünschter Datenträger | <table border="1"> <tr> <td>USB Token (Standard)</td> <td>Smartcard</td> <td>HSM</td> </tr> </table> | USB Token (Standard) | Smartcard | HSM | |
| USB Token (Standard) | Smartcard | HSM | | | |

Notwendige Ausweisdokumente/Beilagen

| | |
|--|--|
| Pass/ID Nr. (Antragsteller) | |
| Pass/ID Nr. (Firmenvertreter) ² | |
| HR-Auszug vom ² | |

Alle Zertifikatsangaben werden zur Zertifikatserzeugung an das QuoVadis Trust Center in Hamilton BM übermittelt. Bei Anwendung des Zertifikates werden diese Daten mit der Signatur mitgegeben, können jedoch nicht über Web-Zugriff von der QuoVadis Datenbank abgefragt werden. Alle anderen Daten werden unter Anwendung des Datenschutzgesetzes streng vertraulich, unter Verschluss und nur innerhalb von QuoVadis Trustlink Schweiz AG aufbewahrt.

Mit der Annahme des Zertifikates bestätige ich, dass

- sämtliche Angaben und Erklärungen in Bezug auf die im Zertifikat enthaltenen Informationen der Wahrheit entsprechen
- ich keine persönlichen Daten für die Kreierung des PIN-Codes oder des Passwortes benutze
- der private Schlüssel von mir geschützt und getrennt vom zugehörigen PIN Code aufbewahrt wird
- ich keiner unbefugten Person Zugang zu meinem Signaturschlüssel gewähre
- ich das Zertifikat ausschliesslich in Übereinstimmung mit der aktuellen Certificate Policy (CP/CPS) einsetzen werde
- das Zertifikat unverzüglich von mir ungültig erklärt wird, wenn die Angaben des Zertifikates nicht mehr stimmen oder der Signaturschlüssel abhanden gekommen, gestohlen oder möglicherweise kompromittiert wurde
- ich mit der Veröffentlichung des Zertifikates einverstanden bin
- ich die nachfolgenden Nutzungsbestimmungen vollständig akzeptiere und einhalten werde.

| | |
|---|---|
| Der Antragsteller | |
| Ort, Datum | Unterschrift Antragsteller |
| Die Firmenvertretung² | |
| 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:

Für Zertifikate mit Firmeneintrag oder bei Verwendung der E-Mail-Adresse der Firma

- Kopie Pass oder ID des Antragstellers
- Beglaubigung des Zertifikatsantrages (Seite 5)
- Kopie Pass oder ID der zeichnungsberechtigten Person(en)
- Kopie eines beglaubigten Handelsregisterauszuges

Für Privatpersonen (ohne Firmeneintrag)

- Kopie Pass oder ID des Antragstellers
 - Beglaubigung des Zertifikatsantrages (Seite 5)
-

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.

Bei der Vergabe von Namen für Pseudonyme muss eine Verwechslung mit natürlichen und juristischen Personen oder Bezeichnungen von Organisationseinheiten ausgeschlossen werden können.

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

Namenskonventionen für natürliche Personen

Namenszusätze (Titel) können nur verwendet werden, wenn diese in einem amtlichen Ausweispapier mit Lichtbild enthalten sind (z.B.: „Dr. Peter R. Mueller“).

Namenskonventionen für juristische Personen und Organisationen

Juristische Personen oder Organisationen können nur durch eine natürliche Person vertreten werden. Dazu wird ein Zertifikat an eine natürliche Person ausgegeben, wobei in den vorgesehenen Feldern (Organisation und Abteilung) die entsprechenden Namen gemäss dem vorgelegten amtlichen Dokument (aktueller beglaubigter Handelsregisterauszug) eingetragen werden können.

Pseudonyme

Der „common name“ eines Pseudonyms beginnt mit dem Kennzeichen „PSEUDONYM:“, z.B.: „cn=PSEUDONYM: Buchhaltung“.

Transaktionslimite

Optional kann eine Transaktionslimite (in CHF) vom Antragsteller bestimmt werden.

Erkennungs-Passwort

Das Erkennungspasswort (Passphrase) wird bei der Antragstellung vom Zertifikatsinhaber festgelegt. Es ermöglicht QuoVadis, bei telefonischem Kontakt, den Zertifikatsinhaber noch besser zu identifizieren und wird ausschliesslich nur zu diesem Zweck verwendet.

Identitätsüberprüfungen bei Neuantrag und Registrierung

Der Antragsteller eines Zertifikats muss von QuoVadis oder deren Vertragspartner eindeutig anhand eines amtlichen Ausweispapiers mit Lichtbild (Identitätskarte oder Reisepass) identifiziert werden können.

Folgende Registrierungsvarianten sind möglich:

- a) Persönliches Erscheinen auf einer QuoVadis Registrierungsstelle (aktuelle Liste auf www.quovadis.ch)
- b) Registrierung vor Ort beim Antragsteller
- c) Beglaubigung des Zertifikatsantrages durch eine Urkundsperson (Gemeinde, Stadtverwaltung, Notar)

Für alle im Zertifikat vermerkten Attribute hat ein Nachweis und eine Bestätigung anhand eines amtlichen Dokumentes zu erfolgen (Art. 8 ZertES, Art. 5 Abs. 2 VZertES).

Bezieht sich ein Eintrag auf den Handelsregisterauszug (z.B. Funktionsbezeichnung, E-Mail Adresse), so ist nebst dem aktuellen Handelsregisterauszug auch eine Mitunterzeichnung des Antrags durch eine handelsrechtlich eingetragene zeichnungsberechtigte Person erforderlich.

Beantragung weiterer Zertifikate

Verfügt die beantragende Person über ein gültiges Zertifikat, kann die Beantragung weiterer Zertifikate für diese Person auch durch die Übersendung eines verschlüsselten und signierten Antrags erfolgen, sofern sich die Identität der Person nicht geändert hat. Voraussetzung für diese Art der Antragstellung ist, dass seit dem Erstantrag des gültigen Zertifikats nicht mehr als drei Jahre vergangen sind und die bei der Identifizierung vorgelegten Ausweisdokumente noch gültig sind.

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 (ZertES Art. 10). Einmal ungültig erklärte Zertifikate können nicht erneuert oder verlängert werden.

Nutzung des qualifizierten Zertifikates

Qualifizierte digitale Zertifikate können gemäss ZertES nur und ausschliesslich für die elektronische Signatur verwendet werden (non-repudiation und digital signature).

Zertifikaterneuerung unter Verwendung eines neuen Schlüssels

Bei einer Zertifikaterneuerung hat der Zertifikatinhaber 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.

Schlüsselhinterlegung und -wiederherstellung

Schlüsselhinterlegung und -Wiederherstellung ist für qualifizierte Signaturschlüssel gemäss ZertES nicht erlaubt.

Pflichten des Zertifikatsinhabers

Der Benutzer verpflichtet sich:

- a) seinen privaten Schlüssel zu sichern und alle angemessenen und notwendigen Vorsichtsmassnahmen gegen Diebstahl, unberechtigte Sichtung, Manipulation, Gefährdung, Verlust, Beschädigung, Störung, Freigabe, Änderung oder unberechtigten Gebrauch seines privaten Schlüssels zu treffen (inkl. Passwort, Token oder SmartCard und Aktivierungsdaten)
- b) die alleinige und vollständige Kontrolle über den Gebrauch des privaten Schlüssels auszuüben
- c) QuoVadis im Falle einer Gefährdung oder eines anderen Vorfalls, 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 Benutzervertrags (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 privaten Schlüssels umgehend eine Sperrung 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 sperren.

Haftung des Zertifikatsinhabers

Der Inhaber eines Signaturschlüssels haftet Drittpersonen für Schäden, die diese erleiden, weil sie sich auf das qualifizierte gültige Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes vom 19. Dezember 2003 über die elektronische Signatur ZertES verlassen haben (Art. 59a OR). 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

Beglaubigung des Zertifikatsantrages

Die Urkundsperson bescheinigt, dass

- ▶ der Antragsteller für das elektronische Zertifikat persönlich zur Überprüfung seiner Identität erschienen ist
- ▶ die Angaben mit dem vorgelegten amtlichen Ausweis (ID oder Pass) übereinstimmen
- ▶ die beigefügte Kopie des amtlichen Ausweises mit dem Originaldokument übereinstimmt.

Öffentliche Urkundsperson

Datum und Uhrzeit