Factsheet
Extended Validation (EV) SSL Zertifikate

Version 1.1
30. April 2007

QuoVadis Trustlink Schweiz AG
Teufenerstrasse 11
9000 St. Gallen

Phone +41 71 272 60 60
Fax +41 71 272 60 61
www.quovadis.ch

Was ist ein EV SSL Zertifikat?

SSL (Secure Socket Layer) ist ein Verschlüsselungsprotokoll für die sichere Datenübertragung im Internet.

Ein Extended Validation (EV) Zertifikat ist eine neue Kategorie von SSL Zertifikaten, welches vom **Industriekonsortium CA/Forum** ins Leben gerufen wurde.

Veränderungen beim Prüfungsablauf unterschiedlicher Zertifizierungsstellen (engl. Certificate Authority, kurz CA) bewirkten, dass Unsicherheiten bei den Internetbenutzern in Bezug auf die Vertrauenswürdigkeit der aufgerufenen Internetseiten aufkamen.

Im Gegensatz dazu verpflichtet EV zu einheitlichen und konsistenten Abläufen unter allen beteiligten CAs und zur stringenteren Prüfung und Identifikation eines EV SSL Besitzers/Betreibers.

Klassische SSL Zertifikate sind domänengeprüfte, das heisst, wenn das Zertifikat den korrekten Domänennamen (z.B. *www.quovadis.ch*) beinhaltet, so wird das SSL Schloss geschlossen. Weiter können diese SSL Zertifikate auch organisationsgeprüft sein. Dies ist dann der Fall, wenn neben dem Domänennamen auch die Firma entsprechend geprüft wurde. Sämtliche von QuoVadis Trustlink Schweiz AG ausgegebenen klassischen SSL Zertifikate sind organisationsgeprüfte Zertifikate.

Wer steht hinter CA/Forum?

Das Certification Authority Browser Forum (CA/Browser Forum – *www.cabforum.org*) ist eine Organisation von führenden Zertifizierungsstellen, Anbietern von Internet Browsern und anderen Teilnehmern (z.B. Rechtspersonen).

Die Mitglieder des CA/Browser Forums erarbeiteten in enger Zusammenarbeit Richtlinien und Einsatzmöglichkeiten eines Extended Validation (EV) SSL Zertifikatsstandard, der zur Erhöhung der Sicherheit bei Internet Transaktionen beiträgt und zu einer intuitiveren Methode dem Internetbenutzer sichere Internetseiten anzuzeigen.

Die folgenden CAs haben EV OIDs (Object Identifier) mit den Browser-Herstellern registriert und haben sich dem zwingenden EV Audit unterzogen (respektive sind gerade im Auditprozess) – Stand: Januar 2007:

1. Comodo
2. Cybertrust
3. Digicert
4. DigiNotar (Holland)
5. Entrust
6. GeoTrust
7. GlobalSign
8. GoDaddy / Starfield
9. Network Solutions
10. QuoVadis
11. TDC (Denmark)
12. Thawte
13. Trustis (UK)
14. Verisign
15. Wells Fargo
16. Xramp / SecureTrust

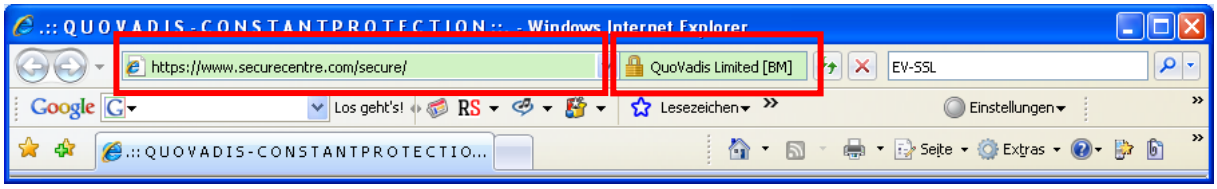
Internet Browser Anbieter sind zurzeit:

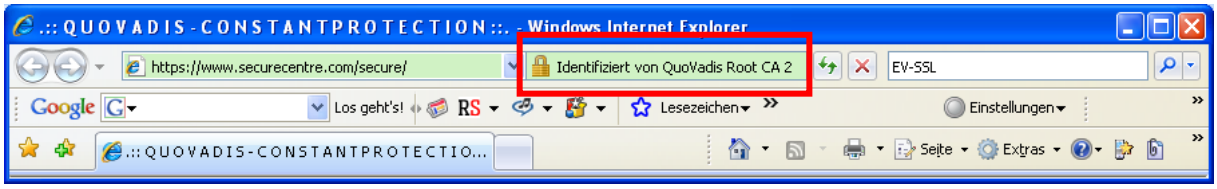
1. Microsoft Corporation
2. The Mozilla Foundation
3. Opera Software ASA
4. KDE

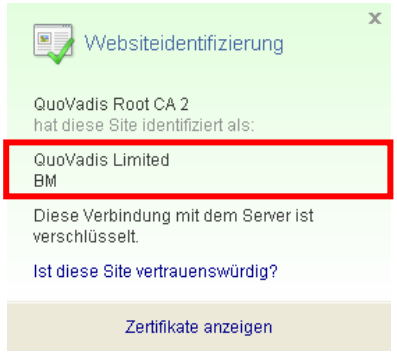
Was sind die Vorteile von EV SSL?

Wenn eine Website für e-Commerce oder e-Banking betrieben wird respektive sensitive oder private Daten gesammelt oder angezeigt werden, dann sollten EV SSL Zertifikate einsetzt werden. Mit dem verbesserten Prüfprozedere und der Sicherheitsanzeige helfen EV SSL Zertifikate den Benutzern und Kunden die Internettransaktionen verschlüsselt und vertrauensvoll durchzuführen während gleichzeitig ein effektiver Schutz gegen den Internet-Betrug, wie zum Beispiel Phishing[1] und Pharming[2], besteht.

Benutzer sehen bei Einsatz eines EV SSL bereiten Browsers einige Veränderungen gegenüber den traditionellen SSL Zertifikaten. Wenn eine EV gesicherte Website mit Microsofts Internet Explorer 7 (IE7) besucht wird, erscheint nach wie vor das SSL Schloss. Zusätzlich färbt sich die Adressleiste grün und die Sicherheitsanzeige wechselt zwischen der Identität der Website und der Zertifizierungsstelle, die das erweiterte Prüfverfahren durchgeführt hat.







Die grüne Adressleiste zeigt die CA und den geprüften Betreiber/Besitzer. Ein Mausklick auf das Schloss zeigt den erweiterten Sicherheitsbericht.

Diese EV Anzeige bestätigt, dass der Betreiber und der Inhaber der Website geprüft wurden, was dem Benutzer Sicherheit und Vertrauen in Bezug auf die Nutzung des Internetdienstes vermittelt.

Benutzer erkennen aus der Bescheinigung ebenfalls, in welchem Land die Website registriert wurde.

[1] Phishing (nach engl. fishing, „Angeln“, „Fischen“, evtl. in Anlehnung an Phreaking nach password fishing, bildlich das „Angeln nach Passwörtern mit Ködern“) ist eine kriminelle Handlung, die Techniken des Social Engineering verwendet. Phisher geben sich als vertrauenswürdige Personen aus und versuchen, durch gefälschte elektronische Nachrichten an sensible Daten wie Benutzernamen und Passwörter für Online-Banking oder Kreditkarteninformationen zu gelangen. Phishing-Nachrichten werden meist per E-Mail oder Instant Messaging versandt und fordern den Empfänger auf, auf einer präparierten Webseite oder am Telefon geheime Zugangsdaten preiszugeben. Versuche, der wachsenden Anzahl an Phishing-Versuchen Herr zu werden, setzen unter anderem auf geänderte Rechtsprechung, Anwendertraining und technische Hilfsmittel. (Quelle: Wikipedia)

[2] Pharming ist eine Betrugsmethode, die durch das Internet verbreitet wird. Sie basiert auf einer Manipulation der DNS-Anfragen von Webbrowsern (beispielsweise durch DNS-Spoofing), um den Benutzer auf gefälschte Webseiten umzuleiten. Es ist eine Weiterentwicklung des klassischen Phishings. Der Begriff "Pharming" rührt von dem Umstand her, dass die Pharming-Betrüger eigene grosse Server-Farmen unterhalten, auf denen gefälschte Webseiten abgelegt sind. (Quelle: Wikipedia)

Was wird für eine korrekte Anzeige benötigt?

1. *Die Aktualisierung der vertrauenswürdigen Stammzertifikate muss über den Windows Update vorgenommen werden:*

   Rufen Sie folgenden Link in einem Internet Browser auf, um sich das Aktualisierungsprogramm von Microsoft herunterzuladen:

   http://download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/rootsupd.exe

   Hinweis: Dieser Link ist auch unter http://www.quovadis.bm/root ersichtlich.

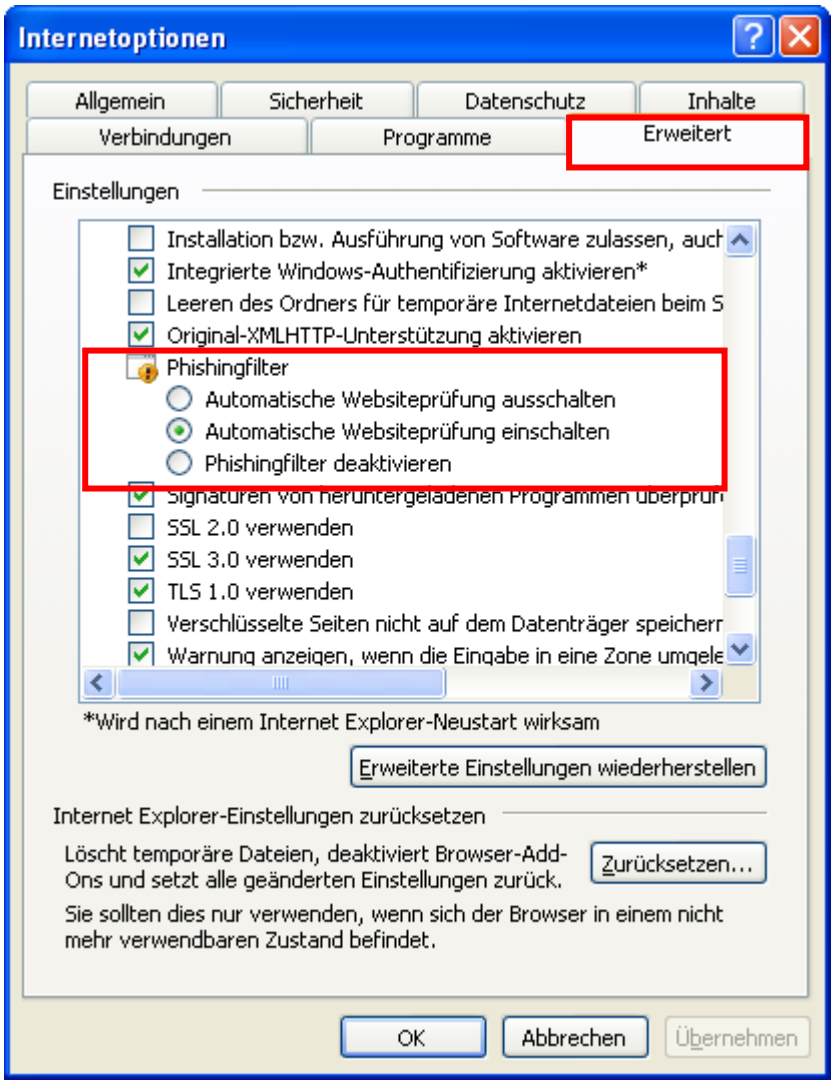
   Beantworten Sie den nachfolgenden Dialog mit Klicken auf die Schaltfläche „Ausführen“

   Anschliessend starten Sie die Ausführung mit Klicken auf die Schaltfläche „Ausführen“

   Hinweis: Die Ausführung des Programms wird beendet ohne einen Hinweisdialog.

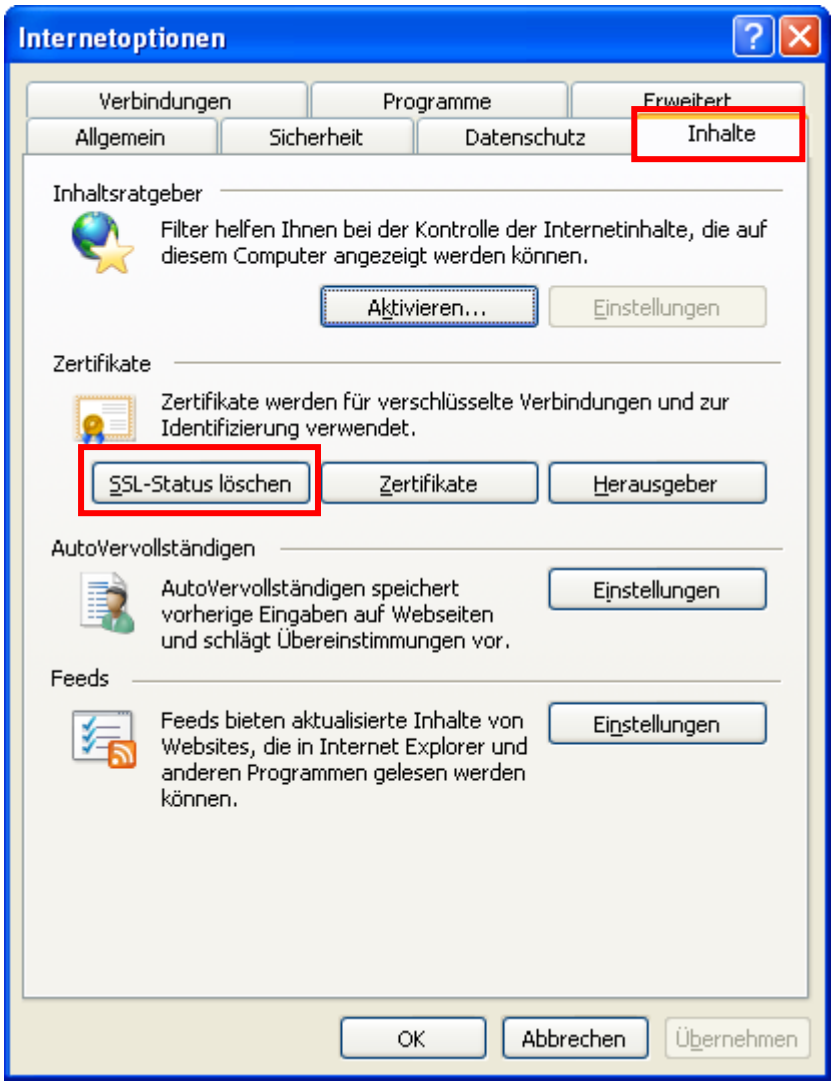
2. *Schalten Sie in den erweiterten Optionen des Internet Explorers (oder in einem anderen Internet Browser) den Phishing-Filter, also die automatische Websiteprüfung, ein:*

   Unter Extras | Internetoptionen das Register „Erweitert“ aufrufen und die Einstellung gemäss Screenshot vornehmen:



3. In den Internetoptionen den SSL-Status löschen:

Unter Extras | Internetoptionen das Register „Inhalte“ aufrufen und die Schaltfläche „SSL-Status löschen“ betätigen:



Wie lange ist ein EV SSL Zertifikat gültig?

Die Laufzeit eines EV SSL Zertifikats kann **12 oder maximal 24 Monate** betragen.

Wo liegt der Unterschied zum normalen SSL Zertifikat?

Die EV Richtlinien zeigen ausführliche Verfahren auf, denen QuoVadis und andere CAs folgen müssen, um die Existenz und die Identität des Antragstellers sowie die exklusive Verwendung des Domainnamens zu prüfen und die Ermächtigung der Nutzung des SSL Zertifikats zu erteilen.

Wegen der zusätzlichen Schritte im Überprüfungsprozess kann der Antrag für ein EV SSL Zertifikat länger dauern. Sobald jedoch erfolgreich geprüft wurde, ist der Antragsteller in der Lage, zusätzliche SSL Zertifikate in einem beschleunigten Verfahren von QuoVadis zu erhalten.

QuoVadis bietet spezielle Angebote für bestehende SSL Kunden an, die einen Wechsel auf EV SSL vollziehen möchten. EV SSL Zertifikate beinhaltet unter anderem zusätzliche Informationen, wie zum Beispiel Vollmachten oder Registernummern, im Gegensatz zu klassischen SSL Zertifikaten.

Technischer Hinweis
Es sind **keine Wildcard Zertifikate** (z.B. *.quovadisglobal.com) erlaubt.

Welche Browser unterstützen bereits EV SSL Zertifikate?

Momentan unterstützt nur Microsofts Internet Explorer 7 die neuen EV SSL Zertifikate. Das aktive Handeln von Microsoft veranlasst auch die anderen Browserhersteller zum Handeln. Es wird erwartet, dass im Verlaufe von 2007 auch Mozilla, Opera und Safari nachziehen werden.

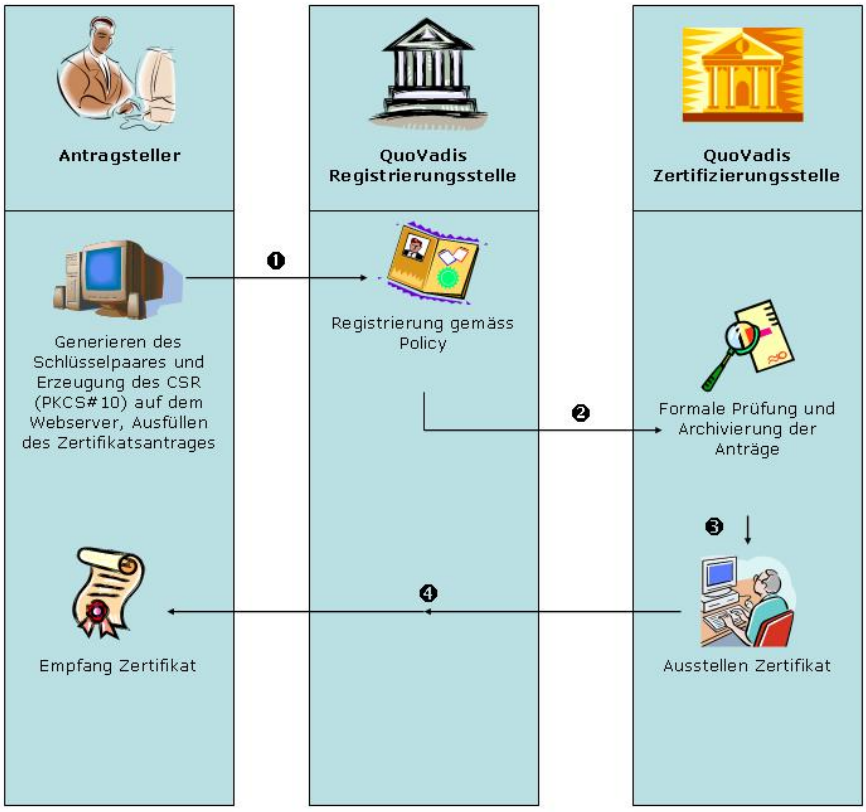
Technischer Hinweis
EV SSL Zertifikate sind rückwärts kompatibel mit älteren Browsern. EV SSL bereite Browser erkennen die klassischen SSL Zertifikate weiterhin. Solange das Zertifikat von einer vom Browser als vertrauenswürdig eingestufte CA ausgestellt wurde, schliesst das SSL Schloss im Browser wie erwartet.

Wer kann EV SSL Zertifikate einsetzen?

Die EV Richtlinien beschränkten den Einsatz von EV SSL Zertifikaten auf öffentlich oder privatrechtliche Institutionen. Letztere müssen im Handelsregister/Öffentlichkeitsregister eingetragen sein. Für öffentlich rechtliche Einrichtungen bedarf es einer Kopie der Wahlverfügung respektive einer Bestätigung der zuständigen kantonalen Behörde.

Das CA/B Forum arbeitet zurzeit an einer Definition des Prüfverfahrens für weitere Konstellationen (z.B. allgemeine Teilhaberschaften, nicht eingetragene Firmen, Eigentümer oder Einzelpersonen).

Wie läuft die Registrierung für EV SSL Zertifikate ab?



1. Der Antragsteller füllt den entsprechenden Zertifikatsantrag, erhältlich unter *https://www.quovadis.ch/page.asp?contentid=20*, aus und erzeugt ein neues Schlüsselpaar auf dem Webserver. Dies wird in vielen Fällen gleichzeitig mit der Erstellung des so genannten Certificate Signing Requests (kurz CSR oder PKCS#10 Request) vorgenommen. Nähere Informationen und Instruktionen zu den diversen Webservern erhalten Sie unter dem Link: *https://www.quovadis.bm/ssl/generaterequest.asp*.
2. Der unterzeichnete Antrag wird per Post an QuoVadis Trustlink Schweiz AG versandt. Damit ein beschleunigtes Verfahren stattfinden kann, wird auch der elektronische Versand (per e-Mail) eines gescannten Dokuments akzeptiert, sofern der Originalantrag anschliessend per Post nachgesandt wird. Neben dem Antrag sind die folgenden Unterlagen zwingend einzureichen:
    a. Handelsregisterauszug (nicht älter als 3 Monate) bei privatrechtlichen Organisation; Kopie der Wahlverfügung respektive einer Bestätigung der zuständigen kantonalen Behörde bei öffentlichen Organisationen
    b. Pass- oder ID-Kopie der unterzeichnungsberechtigten Person(en)
    c. Nachweis, dass sich die qualifizierte URL im Besitze des Antragstellers befindet (kann auch ein Ausdruck der URL-Registrierung beim Web-Hosting-Unternehmen sein). Ist der Antragsteller nicht im direkten Besitz der Web-Adresse (URL) benötigt dieser das schriftliche Einverständnis des effektiven Eigners.

3. QuoVadis überprüft die Angaben des Antrags unter Zuhilfenahme der Ausweiskopie, des Handelsregisterauszugs sowie weiteren Online-Verzeichnissen. Sind alle Angaben in Ordnung werden die eingereichten Dokumente archiviert, das Zertifikat ausgestellt und dem Antragsteller zugestellt.

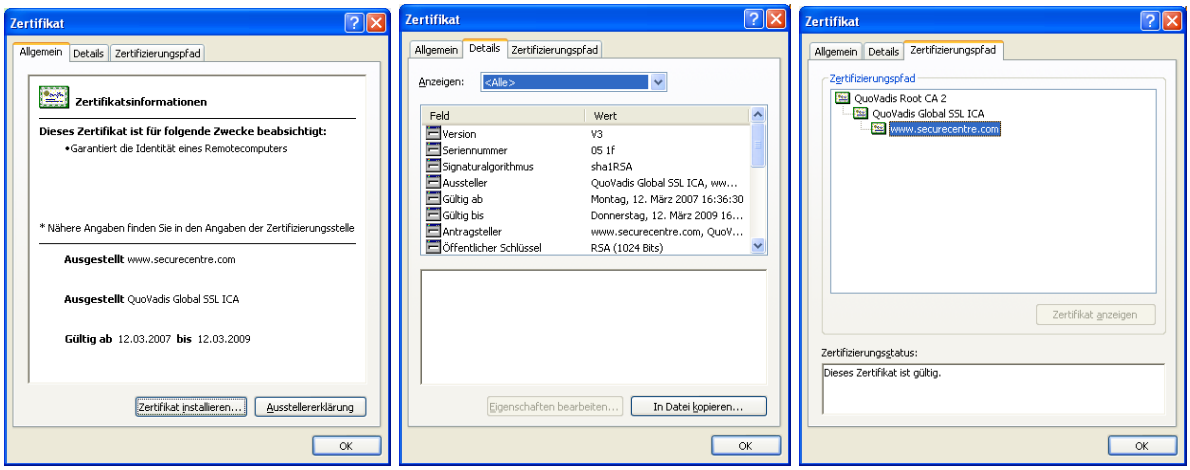
Hinweis: Der so genannte Common Name (CN) im Zertifikat muss auf die qualifizierte URL ausgestellt sein. Zudem muss die „Organization" (kurz „O") als auch der Firmensitz („Locality", kurz „L") den Angaben des Handelsregisterauszuges entsprechen.

Technischer Hinweis: Ein CSR hat normalerweise den folgenden Aufbau:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDVzCCAsACAQAwejELMAkGA1UEBhMCQ0gxCTAHBgNVBAgTADERMA8GA1UEBxMI
TGllc2JlcmcxHDAaBgNVBAoTE0FsdW1pbml1bSBMYXVmZW4gQUcxFDASBgNVBAsT
…
mmUqTjkQ95lp06NON7qcdkrBF+iy0TmOtpGgoS6lCWUMVOshbLGrcBb2hw==
-----END NEW CERTIFICATE REQUEST-----
```

Welche Angaben erscheinen in einem EV SSL Zertifikat?

Klickt man bei der Websiteidentifizierung auf „Zertifikat anzeigen" erscheint folgender Dialog, in dem allgemeine Angaben, Zertifikatsdetails und der Zertifizierungspfad ersichtlich sind:



Die Details beinhalten, unter anderem, folgende (Beispiel-)Angaben:

Attribut	Beispielwert
Version	V3
Seriennummer	05 1f
Signaturalgorithmus	sha1RSA
Aussteller	CN = QuoVadis Global SSL ICA OU = www.quovadisglobal.com O = QuoVadis Limited C = BM
Gültig ab	Montag, 12. März 2007 16:36:30
Gültig bis	Donnerstag, 12. März 2009 16:33:04
Antragsteller	CN = www.securecentre.com OU = QuoVadis EV Demonstration O = QuoVadis Limited L = Hamilton C = BM 1.3.6.1.4.1.311.60.2.1.3 = BM Seriennummer = 28474
Öffentlicher Schlüssel	30 81 89 02 81 81 00 d6 88 76 d2 9e 37 2a 15 ac 1e f6 56 11 16 9d 8f a2 81 72 35 ee 2f 03 77 c7 0d 96 0b a2 c5 13 18 79 3e 3d ad 07 8e 91 4e 8e 2d d9 e3 06 52 8a fb 19 13 ee 77 54 0e b6 70 98 14 cd b4 09 91 15 b6 ee 3e 4e 62 f5 27 1e 65 d3 71 a8 43 81 75 52 5e d6 62 77 a2 9e 95 e4 11 03 ea 3b 82 5f db 65 4d dc 29 48 7b 5d 02 63 f5 20 37 27 40 21 c9 3d 82 27 43 2b a7 a7 2f 56 3a b4 d6 10 47 57 33 d2 43 02 03 01 00 01
Schlüsselverwendung	Digitale Signatur, Schlüsselverschlüsselung
Sperrlisten-Verteilungspunkt	http://crl.quovadisglobal.com/qvsslica.crl
Fingerabdruckalgorithmus	sha1
Fingerabdruck	81 7c c3 23 49 f4 80 7b 65 ab 9f c1 26 5b 1d 0b 7c c5 5c a3