



STRATEGIEPAPIER

---

## Maximierung des Vertrauens der Website-Besucher mit Extended Validation SSL





**INHALT**

+ Die Erosion der SSL-Identitätsversicherung	3
+ Einführung einer Identität, die Vertrauen schafft	4
Internet Explorer 7: Grün wie Grünes Licht	4
+ Funktionsweise von Extended Validation	7
+ EV Upgrader erweitert den Schutz für Windows XP Clients	8



Internetunternehmen befinden sich in einer Vertrauenskrise. Das Vertrauen in die Sicherheit von Websites sinkt und immer mehr Verbraucher schränken ihre Online-Transaktionen ein oder stellen sie komplett ein. Laut einer Studie von Forrester Research vom 8. Dezember 2005 gaben erstaunliche 24 Prozent der Internetbenutzer an, ihre Weihnachtseinkäufe aufgrund von Sicherheitsbedenken in diesem Jahr nicht online zu tätigen. Und ganze 61 Prozent gaben an, sie hätten ihre Online-Einkäufe aus demselben Grund zumindest eingeschränkt. Obwohl dieses Phänomen wegen der Gesamtzunahme der Online-Aktivitäten wie Online-Banking, Online-Broking und Online-Steuererklärungen nicht ganz so deutlich ausgeprägt ist, bleibt dennoch die Tatsache, dass viele Online-Einzelhandelsunternehmen weniger effektiv arbeiten als sie könnten, was sich in finanziellen Verlusten ausdrückt.

Seit Anfang 2007 können Online-Unternehmen Kunden ihre Identität definitiv versichern und Kunden diese Identität überprüfen, bevor sie Websites ihr Vertrauen schenken. Diese Möglichkeit eröffnet sich durch die bahnbrechendste Entwicklung in der Sicherheitsstruktur des Internets: Zum ersten Mal seit den Anfängen der Technologie vor über zehn Jahren wird eine neue Art von SSL-Zertifikat eingeführt.

Diese so genannten Extended Validation (EV)-SSL-Zertifikate sind das Ergebnis eines Jahres voller Arbeit des CA/Browser Forums, eines Branchenkonsortiums führender Webbrowser-Anbieter und SSL-Zertifizierungsstellen (Certification Authorities, CAs) wie VeriSign. Seit Ende 2006 sind diese neuen Zertifikate bei den Mitgliedern des CA/Browser Forums erhältlich. Internetunternehmen und Website-Besucher profitieren gleichermaßen. Die Zertifikate erleichtern den Online-Handel in all seinen Facetten, da sie das Vertrauen der Besucher in legitime Websites stärken und die Effektivität von Phishing-Angriffen empfindlich schwächen.

## Die Erosion der SSL-Identitätsversicherung

Fragen Sie einen durchschnittlichen Online-Einkäufer, was das kleine Schlosssymbol im Internetbrowser bedeutet und er oder sie wird antworten, es bedeutet, dass die Transaktionen verschlüsselt werden und daher vor unliebsamen Gästen geschützt sind. Technisch gesehen, ist das zwar korrekt, doch das war noch nicht alles, was die Pioniere des Internethandels damit ausdrücken wollten.

Der ursprüngliche Zweck von SSL-Zertifikaten lag darin, die Identität einer Website zu bestätigen, wenn ein Benutzer sie anzeigt. Es ist nämlich schwer, ein Unternehmen physisch vorzutäuschen, online ist es hingegen eine Kleinigkeit. Die Branche hat dieses Prinzip bereits 1995 erkannt und daraufhin die SSL-Zertifikate entwickelt. Die Zertifikate sollten im Sinne der Erfinder die Identität einer Website belegen und Online-Einkäufer vor Betrügereien schützen. Anfangs reichte die Identitätsversicherung eines Standard-SSL-Zertifikats aus. Heute ist das jedoch nicht mehr der Fall. Die verbreitete Nutzung des Internets durch Laien ohne spezielle Computerkenntnisse in Kombination mit der geringen Auffälligkeit des Schlosssymbols in den gängigen Internetbrowsern, haben Phishing zu seiner Erfolgssträhne verholfen.

Herkömmliche SSL-Zertifikate sind also nicht das Ei des Kolumbus. Obwohl einige CAs bei der Authentifizierung der Identität hervorragende Arbeit leisten, engagieren sich andere nur in geringem Maße oder verwenden Verfahren, die sehr leicht umgangen werden können. Es gibt sogar Websites mit selbstsignierten SSL-Zertifikaten, die keinerlei Identitätsprüfung bieten. In der zweiten Hälfte des Jahres 2005 kamen es zu groß angelegten Phishing-Angriffen, für die SSL-Zertifikate mit schwacher Authentifizierung leichte Beute für die Vortäuschung von Legitimität waren.

## Einführung einer Identität, die Vertrauen schafft

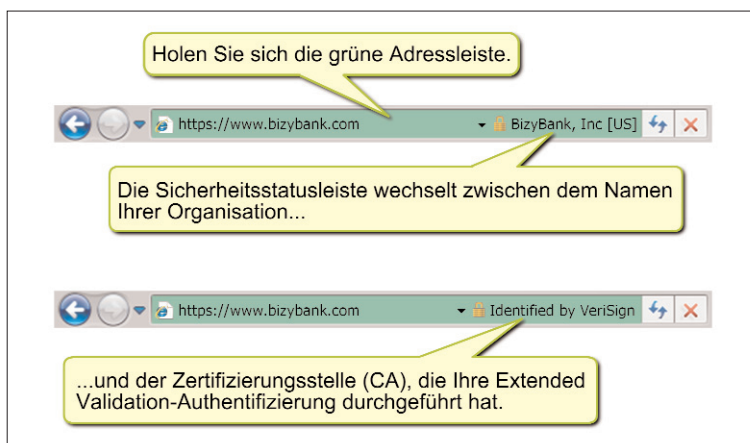
Um die Autorität von SSL-Zertifikaten als Quelle der Information über die Identität einer Website wiederherzustellen, mussten die Branchenführer zwei Schwächen des bestehenden Systems beseitigen. Zunächst musste eine neue Kategorie von SSL-Zertifikaten entwickelt werden, die ein höheres Maß an Sicherheit hinsichtlich der Identität des Website-Inhabers bietet. Dann musste eine Browser-Schnittstelle geschaffen werden, die klar erkenntlich anzeigt, ob eine Identität bekannt oder unbekannt ist. Bei diesen neuen Zertifikaten handelt es sich um die oben genannten EV-SSL-Zertifikate. Einige Benutzer verwenden auch den Arbeitstitel „High Assurance (HA)-SSL-Zertifikate“. Sie unterscheiden sich von den herkömmlichen Zertifikaten mit hoher Zusicherung, da sie keinen EV-Status implizieren.

Das CA/Browser Forum setzt sich aus über 20 der führenden Webbrowser-Hersteller, Anbieter von SSL-Zertifikaten und WebTrust-Prüfer zusammen. Es arbeitete über ein Jahr lang mit dem American Bar Association Information Security Committee (ABA-ISC) zusammen an der Entwicklung eines standardisierten Authentifizierungsverfahrens, das jede CA bei der Ausstellung von EV-Zertifikaten einhalten muss. Derartige CAs müssen sich durch unabhängige Prüfer die Einhaltung des erwähnten Prozesses bestätigen lassen. Das CA/Browser Forum hat dieses Verfahren auf bestehenden Verfahrensweisen für die Bestätigung von Unternehmensidentitäten aufgebaut, die sich über die Jahre bei der Authentifizierung mehrerer Millionen SSL-Zertifikate als erfolgreich erwiesen haben.

Führt eine CA die Authentifizierung nach diesem Verfahren aus, kann sie Zertifikate mit EV-Status ausstellen. Dieses Zertifikat funktioniert genau wie ein herkömmliches SSL-Zertifikat. Browser, die nicht auf die Erkennung von EV-Zertifikaten ausgelegt sind (wie Windows® Internet Explorer® 6, Mozilla® Firefox® 2.0 und deren vorherige Versionen) verhalten sich genauso wie bei Zertifikaten ohne EV-Status. Neue EV-kompatible Browser zeigen diese Zertifikate jedoch auffälliger und mit mehr Informationsgehalt an. Der erste dieser Browser ist Internet Explorer 7 (IE7).

### + Internet Explorer 7: Grün wie Grünes Licht

IE7 hat einige Optimierungen an der Benutzeroberfläche vorgenommen, um die Identifizierung des Website-Inhabers zu erleichtern. Am offensichtlichsten ist die „grüne Adressleiste“. Wenn ein IE7-Browser auf eine Website mit gültigem EV-Zertifikat zugreift, wird die Adressleiste grün hinterlegt. Diese einfache Veränderung zeigt sehr deutlich an, dass eine Website einem strengen Identitätsprüfungsverfahren unterzogen wurde. Die Wahl der Farbe ist konform mit den etablierten Konventionen für Benutzeroberflächen. Grün symbolisiert auf Benutzeroberflächen, dass der Vorgang sicher fortgesetzt werden kann, während rot für Gefahr oder Warnung steht.



Verbraucherumfragen haben ergeben, dass diese Konventionen äußerst effektiv sind. Im Herbst 2006 führte eine Studie zum Benutzerverhalten mit Online-Einkäufern in den USA durch. Dabei kam VeriSign zu folgenden Ergebnissen:

- 100 Prozent der Teilnehmer fiel auf, ob eine grüne Extended Validation-Adressleiste angezeigt wurde.
- 100 Prozent der Teilnehmer gaben ihre Kreditkartendaten eher auf Websites weiter, auf denen die grüne Adressleiste angezeigt wurde.
- 98 Prozent der Teilnehmer kauften lieber auf Websites ein, auf denen die grüne Extended Validation-Adressleiste angezeigt wurde.
- 80 Prozent der Teilnehmer gaben an, dass sie zögern würden einzukaufen, wenn auf einer Website früher eine Extended Validation-Adressleiste grün angezeigt wurde und das jetzt nicht mehr der Fall ist.

Im IE7 wird rechts neben der Adressleiste ein zusätzliches Feld angezeigt – die Sicherheitsstatusleiste. Das Feld wird angezeigt, wenn der Browser über Informationen verfügt, die für die Website-Besucher für die Beurteilung der Website relevant sein könnten. Auf Websites mit EV-SSL-Zertifikaten zeigt die Sicherheitsstatusleiste den Namen der Organisation an. Der Text wird direkt dem Zertifikat der CA entnommen. Da die CA diesen Namen überprüft hat und der Browser den Namen auf seiner eigenen Benutzeroberfläche anzeigt, kann sich der Besucher auf die Zuverlässigkeit dieser Angabe verlassen.

Im Beispiel der hypothetischen Online-Bank „BizyBank“ wird der Name des Geldinstituts direkt auf der Benutzeroberfläche des Browsers angezeigt. Der Endverbraucher kann die Identität der Website überprüfen, indem er nach der grünen Adressleiste und dem Namen „BizyBank“ sucht, die zusammen eine neues und signifikantes Hindernis für Urheber von Phishing-Angriffen darstellen, die danach trachten, ein BizyBank-Konto zu übernehmen. Bisher mussten Angreifer lediglich die Original-Website kopieren und einen überzeugenden URL finden, um im Geschäft zu sein. Wenn die Kunden der BizyBank lernen, nach dem Namen des Unternehmens und der grünen Adressleiste zu suchen, bevor sie vertrauliche Informationen weitergeben, haben potenzielle Angreifer keine Chance, diese Oberfläche nachzuahmen. Auch wenn der Phishing-Angreifer ein bestehendes Unternehmen verwendet, um EV-Zertifikate für die Phishing-Website zu erwerben, würde die Browser-Oberfläche nicht den Namen „BizyBank“ enthalten.

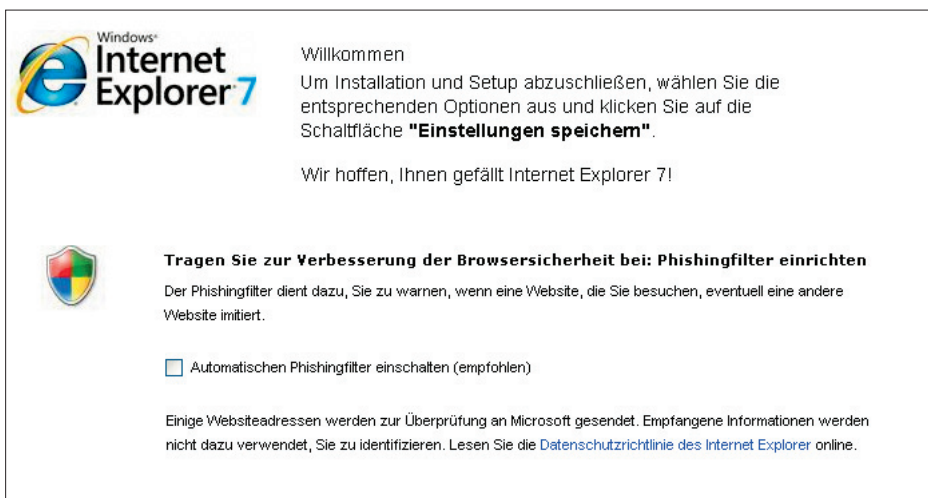
Die Sicherheitsstatusleiste zeigt zudem den Namen der ausstellenden CA an. Auch dadurch kann der Benutzer die Sicherheit der Website beurteilen, bevor er sich dazu entschließt, Geschäfte zu tätigen. Wenn die Website-Besucher dem gewählten SSL-Zertifikatsanbieter kein Vertrauen schenken, können sie ihre Geschäfte an anderer Stelle abwickeln. Ebenso lernt die Öffentlichkeit, keinen Websites zu vertrauen, die SSL-Zertifikate einer CA einsetzen, die nicht vertrauenswürdige EV-Zertifikate ausstellt.

Untersuchungen ergaben, dass die Marke der SSL-Zertifikate erheblichen Einfluss auf die Bereitschaft eines Website-Besuchers hat, Transaktionen vorzunehmen. So hat beispielsweise der europäische Reiseanbieter Opodo identische Online-Bestell-Websites mit und ohne VeriSign Secured Seal™ getestet. Dabei erzielten die Websites mit dem Siegel um 10 % höhere Verkaufszahlen als jene ohne das Siegel. Warren Jonas, der Leiter für Service Management von Opodo meinte dazu: „Wir haben sofort verstanden, welche Auswirkung der Faktor Vertrauen auf die Abbruchraten in der Einkaufskorbphase haben kann, und seither haben wir das VeriSign Seal in alle Zahlungsseiten unseres Netzwerks europäischer Websites eingebunden.“

Im Sommer 2006 untersuchte das bekannte Marktforschungsinstitut TNS die Reaktionen von Online-Einkäufern auf eine Vielzahl an Online-Sicherheitssiegeln und fand dabei heraus, dass das VeriSign Secured Seal weltweit bei weitem das bekannteste Zeichen für Sicherheit im Internet ist. Die Studie zeigte, dass 56 Prozent der Online-Einkäufer auf der ganzen Welt das VeriSign Secured Seal erkennen: acht Mal mehr als die auf Rang zwei folgende Marke.

Diese Ergebnisse unterstreichen nochmals, wie wichtig es ist, sich als Online-Händler für die richtige Marke von SSL-Zertifikaten zu entscheiden. Durch die Anzeige der bekanntesten Sicherheitsmarke im Internet kann die Anzahl an Transaktionen gesteigert und die Gesamteffektivität einer Website als Online-Unternehmen um 10 Prozent und mehr verbessert werden.

Einige Einstellungen im IE7 können die Anzeige dieser Oberflächenkonventionen beeinflussen. Genauer gesagt muss im Browser das „Online Certificate Status Protocol“ (OCSP) aktiviert sein, damit die Oberfläche die genannten Merkmale aufweist. Über OCSP kann der Browser SSL-Zertifikate in Echtzeit überprüfen und sicherstellen, dass sie nicht widerrufen wurden. Ein Großteil der neueren Browserversionen unterstützt OCSP, enthält aber ein Steuerelement auf der Benutzeroberfläche, über das das Protokoll deaktiviert werden kann. Aufgrund der hohen Vertrauenswürdigkeit von EV-Zertifikaten muss im IE7 OCSP aktiviert werden, um die grüne Adressleiste und andere EV-Oberflächenkonventionen für EV-Zertifikate anzeigen zu können. So erkennt der Benutzer nicht nur, dass diese Website einem strengen Authentifizierungsverfahren unterzogen wurde, sondern auch, dass anschließend keine Vorfälle aufgetreten sind, die einen Widerruf des Zertifikats erforderlich gemacht hätten.



*Durch Aktivierung des Phishingfilters (wird bei der Installation empfohlen) wird EV-SSL ebenfalls automatisch aktiviert.*

Neben der direkten Aktivierung von OCSP kann IE7 diese Funktion auch automatisch aktivieren, wenn der Benutzer eine andere Funktion im Produkt aktiviert, die OCSP erfordert. Der so genannte Phishingfilter ergänzt die EV-Funktionspalette durch die Anzeige rot und gelb hinterlegter Adresszeilen für Websites, die bestimmte Trigger-Bedingungen erfüllen, die sie als verdächtige Website einstufen. Es wird empfohlen, diese Funktion gleichzeitig mit der IE7 zu installieren. Durch Aktivierung des Phishingfilters wird auch die EV-Oberfläche aktiviert.

Das Betriebssystem Windows Vista™ geht noch einen Schritt weiter. Im IE7 für Windows Vista werden die OCSP-Funktion und der Phishingfilter standardmäßig aktiviert. Der Browserbenutzer muss die Funktionen bewusst deaktivieren, um sie außer Kraft zu setzen.

Es kann nicht überprüft werden, in wie viel Prozent der Client-Systeme mit IE7 OCSP aktiviert ist. Aufgrund der erheblichen Vorteile der grünen EV-Adressleiste und des Phishingfilters für Endverbraucher, der Auffälligkeit dieser Funktionen auf der Benutzeroberfläche und der Einstufung des Phishingfilters als „Empfohlen“ geht VeriSign davon aus, dass dieser Prozentsatz relativ hoch ist. Website-Administratoren, die EV-SSL-Zertifikate bewerten, sollten sicherstellen, dass diese Funktionen in ihren eigenen Systemen aktiviert sind. Es werden niemals grüne Adressleisten angezeigt, wenn diese Funktionen deaktiviert sind.

## Funktionsweise von Extended Validation

Die EV-Architektur wurde darauf ausgelegt, verlässliche Informationen über die Identität einer Website an den Endverbraucher weiterzugeben, um ihm zu ermöglichen, die richtigen Entscheidungen über die Vertrauenswürdigkeit von Websites zu treffen. Um diese Mission zu erfüllen, mussten an allen Komponenten der Sicherheitsarchitektur des Internets Änderungen vorgenommen werden. EV-Zertifikate verdanken ihre Zuverlässigkeit neben den neuen, einfach verständlichen Oberflächenkonventionen erstens den Änderungen in den Authentifizierungsverfahren und zweitens der Zertifikatsüberprüfung in Echtzeit.

- 1) Der erste Schritt besteht in der Authentifizierung. Das CA/Browser Forum hat die EV-Authentifizierungsrichtlinien über mehr als ein Jahr hinweg sorgfältig zusammengestellt, um sicherzustellen, dass das Authentifizierungsverfahren verlässliche Ergebnisse produziert. Diese Richtlinien schreiben vor, dass qualifizierte CAs Informationen aus erster Hand oder authentifizierte Informationen und keine eigenen Angaben der Antragsteller für Zertifikate verwenden. Sie müssen die bewährten Techniken einsetzen, mit denen seit einem Jahrzehnt bereits Millionen von Zertifikaten erfolgreich authentifiziert wurden. Diese Vorgehensweise gewährleistet, dass alle Informationen des Zertifikats der Wahrheit entsprechen und der Antragsteller dazu berechtigt ist, dieses Zertifikat für diese Organisation zu erwerben. Die Authentifizierungsverfahren sind unter [www.cabforum.org](http://www.cabforum.org) verfügbar. Jede CA muss sich jährlich einer Prüfung durch einen registrierten WebTrust-Prüfer unterziehen, um sicherzustellen, dass die EV-Richtlinien ordnungsgemäß eingehalten werden.
- 2) Nach der Ausstellung eines Zertifikats muss sichergestellt werden, dass das Zertifikat, das dem Kunden angezeigt wird, wahrheitsgemäß die Informationen wiedergibt, die die CA ermittelt hat. Zudem muss überprüft werden, ob Zertifikate, die vorgeben, den EV-Authentifizierungsstandard zu erfüllen, diesen Anspruch auch tatsächlich erfüllen. Die Integrität der Zertifikate kann gewährleistet werden, da in jedes SSL-Zertifikat sichere Hash-Funktionen integriert sind. Sie funktionieren nicht ordnungsgemäß, wenn Manipulationen vorgenommen werden. Die EV-Infrastruktur stellt anschließend durch eine Überprüfung des Zertifikats in Echtzeit sicher, ob das Zertifikat noch gültig ist. Diese Überprüfung beruht auf zwei parallelen Infrastrukturen. Bei der ersten Infrastruktur handelt es sich um das oben erwähnte OCSP. OCSP prüft bei jedem Zertifikat in Echtzeit, ob ein Widerruf vorhanden ist. Wenn ein EV-Zertifikat also beeinträchtigt ist oder aus einem anderen Grund ein Widerruf erforderlich ist, wird das Zertifikat in EV-kompatiblen Browsern als ungültig angezeigt.

Beim zweiten Echtzeitdienst handelt es sich um den Microsoft® Root Store. Eine einfache Metadatenmarkierung gibt den Status jedes EV-Zertifikats an. Um die Möglichkeit auszuschließen, dass eine unzuverlässige oder inkompetente CA fälschlicherweise Zertifikate ausstellt, die als EV-Zertifikate gekennzeichnet sind, obwohl das Unternehmen nicht dem vorgeschriebenen EV-Authentifizierungsverfahren unterzogen wurde, führt IE7 eine Überprüfung in Echtzeit im Microsoft Root Store durch und stellt sicher, dass diese SSL-Root für EV-Zertifikate auch wirklich zugelassen ist. Dadurch wird gewährleistet, dass die grüne Adressleiste sowie die anderen EV-Elemente der Benutzeroberfläche nicht angezeigt werden, wenn eine CA Zertifikate mit EV-Kennzeichnung ausstellt,

obwohl die CA nicht dazu berechtigt ist. Genauso hat Microsoft die Möglichkeit, die Root aus der Liste der anerkannten EV-Roots im Microsoft Root Store zu streichen, wenn eine bestehende CA die jährliche Prüfung nicht besteht oder wiederholt inkorrekte Zertifikate mit EV-Kennzeichnung ausstellt. Dadurch werden die grüne Adressleiste und weitere EV-Elemente der Benutzeroberfläche für alle Zertifikate, die unter der verdächtigen Root ausgestellt wurden, entfernt.

## EV Upgrader erweitert den Schutz für Windows XP Clients

Die EV-Elemente werden in Windows Vista Clients automatisch angezeigt. Bevor IE7 jedoch die EV-Zertifikate als solches in Windows XP anzeigen kann, muss zunächst ein SSL-Root-Update durchgeführt werden. VeriSign hat mit VeriSign® EV Upgrader™ die erste Lösung entwickelt, die es allen IE7-Benutzern ermöglicht, EV-SSL-Zertifikate zu erkennen und anzuzeigen. EV Upgrader nutzt die Update-Funktionen der bestehenden Root in Windows-Betriebssystemen, um die neue EV-Root automatisch und unsichtbar auf dem Client-System zu installieren. Um EV Upgrader für Website-Administratoren möglichst einfach zu gestalten, hat VeriSign ihn in das VeriSign Secured Seal integriert. Auch das VeriSign Secured Seal, das derzeit auf Ihrer Website installiert ist, kann Upgrader bereits enthalten.

Eine detaillierte Beschreibung zu EV Upgrader und seiner Funktionsweise als Bestandteil des VeriSign Secured Seal erhalten Sie im Strategiepapier von VeriSign *EV Upgrader: So machen Sie Windows XP Clients fit für Extended Validation*. Weitere Informationen zu den EV-Zertifikaten von VeriSign oder zum Erwerb der Zertifikate für Ihre Website erhalten Sie unter <http://www.verisign.de/ssl/index.html>.