Mehr Sicherheit für Anbieter und Verbraucher

Weniger Vertrauen der Verbraucher durch Phishing und Online-Betrug

Unsicherheiten beim Online-Handel führen bei Usern oft zu einem Abbruch der Transaktionen. Und durch Phishing und Online-Betrug verlieren Verbraucher das Vertrauen ins Internet. Um dieses wieder zu gewinnen, benötigen Sie als Website-Betreiber eine einfache und zuverlässige Möglichkeit, die Sicherheit der Übertragung zu demonstrieren und deren Echtheit nachzuweisen. Zwischen Herstellern von Sicherheitslösungen und Internet-Browsern wurde dafür der erweiterte Validierungsstandard für SSL-Zertifikate entwickelt, um korrekte Websites von gefälschten zu unterscheiden.

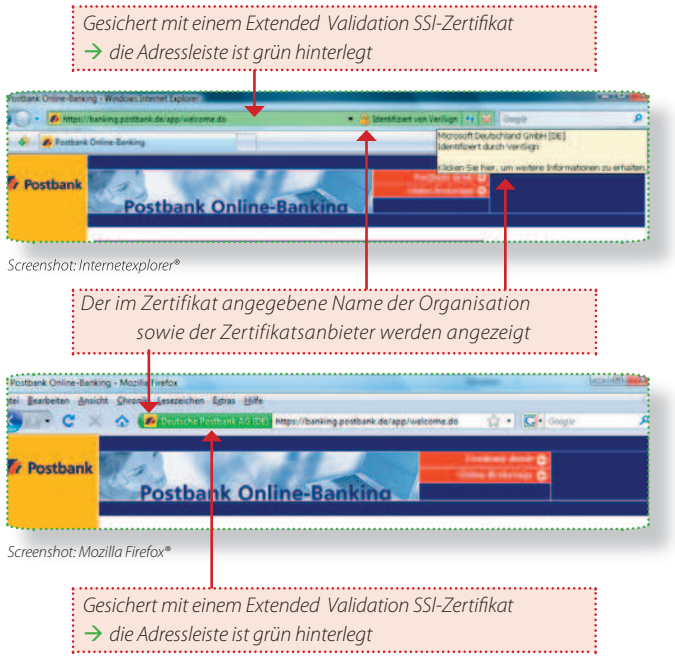
Grünes Licht für sichere Online-Services

Sicherheit ist für Internetnutzer ein zentrales Anliegen. Das Handlungsversprechen **Grünes Licht für sicherere Online-Services** von Deutschland sicher im Netz e.V. (DsiN) unterstützt Sie als Anbieter von Internet-Diensten und -Lösungen, Ihre Verantwortung für die Sicherheit im Netz durch Nutzung neuer Technologien wahrzunehmen. Die Angriffe auf Serverinfrastrukturen sind vielfältig und die entstehenden Schäden beträchtlich.
Eine sichere und wirtschaftliche Nutzung der Technologien setzt detailliertes Wissen über mögliche Risiken sowie innovative Sicherheitslösungen voraus. Die DsiN-Partner eco - Verband der deutschen Internetwirtschaft e.V., Microsoft Deutschland GmbH und TeleTrusT Deutschland e.V. informieren Sie über den Einsatz von Extended Validation Certificates. Durch diese können Sie die Vertrauenswürdigkeit Ihrer Dienste optimieren.

Grünes Licht in der Browserzeile

Extended Validation Certificate

Extended Validation Zertifikate bieten in Webbrowsern Informationen zur eindeutigen Identifizierung Ihres Unternehmens an, welches hinter Ihrer Website steht. Wenn User auf eine Website zugreifen, die mit einem Zertifikat gesichert ist, dass den Extended Validation-Standard erfüllt, wird die URL-Adressleiste grün hinterlegt. Neben der grünen Adressleiste wird in einem Extrafeld der Name der Organisation im Zertifikat und die Zertifizierungsstelle anzeigt.



Die Anzeige wird vom Browser und dem Zertifikatsanbieter gesteuert, weshalb Phishing-Betrüger und Fälscher eine Website nur noch schwer kopieren können, um Kunden zu täuschen. In älteren Browsern werden die Extended Validation Zertifikate mit den Sicherheitssiegeln angezeigt, die bereits auf den bestehenden SSL-Zertifikaten vorhanden sind.

Ihr Weg zum Extended Validation Certificate

Kann ich ein EV-Zertifikat beantragen?

Die EV-Zertifikate werden von Zertifizierungsstellen angeboten, die den Extended Validation-Standard übernommen haben und regelmäßige Audits durch einen WebTrust-Auditor erfolgreich bestehen.

Folgende Organisationsformen können durch Nachweis entsprechender Urkunden, Handelsregisterauszüge etc. EV-Zertifikate erhalten:

- Behörden
- Kapitalgesellschaften
- Personengesellschaften
- Eingetragene Vereine
- Einzelunternehmen

Wie erhalte ich ein EV-Zertifikat?

Beim Validierungsprozess muss die Zertifizierungsstelle sicherstellen, dass Sie als Antragsteller der Domänenbesitzer sind. Im Anschluss wird die Identität Ihres Unternehmens festgestellt und die Autorisierung überprüft. Für Ihr Unternehmen muss eine Hauptkontaktperson ernannt werden, welche den Vertrag für die Zertifikatserstellung bestätigt. EV-Zertifikate sind bei zugelassenen Zertifizierungsstellen ab ca. 1.000 Euro erhältlich.

Die Prüfung Ihres Antrages umfasst:

- Offizielle Registrierung des Unternehmens und der Website
- Zertifikatsverwendungszweck
- Inhaberschaft der Domain
- Organisationsname

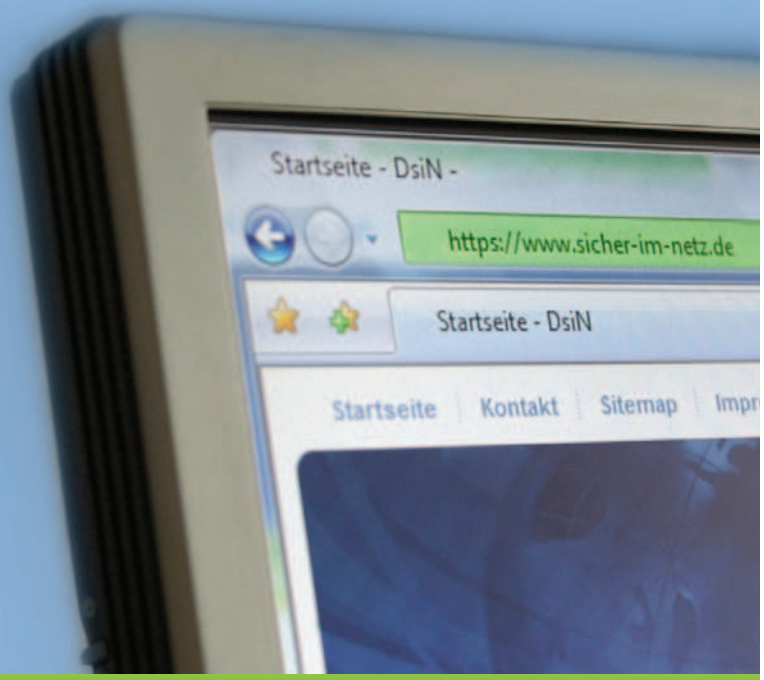
Warum ein Extended Validation Certificate?

Ihre Vorteile auf einen Blick

- Gesteigertes Vertrauen in Ihre Webseite
- Effektiver Schutz gegen Phishing-Betrug
- Förderung des Onlinehandels
- Wettbewerbsvorteile
- Verbesserte optische Kennzeichnung
  - Grüne Adressleiste mit Anzeige der Organisation und der Zertifizierungsstelle
- Zeigt dem Nutzer an, mit wem er kommuniziert
- Verbesserte Prüfung der Zertifikatsinhaber
  - Einsatz bewährter Technologie:
  - Nutzt SSL-Technologie
  - Abwärtskompatibel
  - Ältere Browser zeigen Zertifikate mit Sicherheitssiegel an
- SSL-Zertifikate verfügbar mit 1 oder 2 Jahren Laufzeit

Impressum

Deutschland sicher im Netz e.V.
Albrechtstraße 10 a
10117 Berlin
Tel. +49 (0) 30 27576-310
Fax +49 (0) 30 27576-51310
info@sicher-im-netz.de
www.sicher-im-netz.de



Grünes Licht für sichere Online-Services

Informationen für Anbieter

Deutschland sicher im Netz e. V.

Ein gemeinsames Handlungsversprechen von: