DFN-PKI: Mozilla Integration erfolgt!

Das Warten hat ein Ende: Das Wurzelzertifikat der DFN-PKI ist seit August 2009 auch in die Mozilla-Anwendungen integriert.

Text: **Dr. Marcus Pattloch** (DFN-Verein)

Foto: © Enrico Podda, fotolia

Dies betrifft sowohl den Browser Firefox als auch den E–Mail Klienten Thunderbird. Darüber hinaus ist die Integration bereits seit längerem in allen aktuellen Windows Desktop-Systemen sowie Sun Java und Opera erfolgt. Ebenfalls integriert ist das Wurzelzertifikat der DFN-PKI in die Apple Desktop-Systeme (z. B. den Browser Safari) und in mobile Geräte wie iPhone und iPod touch. Eine aktuelle Übersicht finden Sie unter: www.pki.dfn.de/integration.

Die Integration erhöht nicht nur die Sicherheit im Netz, indem z. B. die Signaturen eingehender E-Mails automatisch und weltweit verifiziert werden können, sondern erspart den Nutzern auch Warnmeldungen von Browsern. Und das genau rechtzeitig, da sich vor kurzem die Verhaltensweise der Browser bei einem nicht bekannten Wurzelzertifikat von einer kleinen Warnmeldung zu einer – nun in der DFN-PKI der Vergangenheit angehörenden – umständlichen Fehlermeldung geändert hat.

Alle Softwarehersteller führen in ihren Produkten eine Liste von vertrauenswürdigen Wurzelzertifikaten und verlangen für eine Aufnahme in diese Liste bestimmte Sicherheitsüberprüfungen. Da jeder Hersteller ein eigenes Verfahren für die Aufnahme neuer Wurzelzertifikate hat, erfolgte die Integration in zeitlichen Etappen. Besonders die Aufnahme in die Mozilla-Anwendungen stellte die

Nutzer durch die intensive Diskussion der OpenSource-Community auf eine Geduldsprobe.

Das lange Warten hat sich aber gelohnt, denn nun können die Zertifikate der DFN-PKI in allen wichtigen Anwendungen auf ein bereits vorinstalliertes Wurzelzertifikat zurückgeführt und dadurch verifiziert werden. Für Serverzertifikate ist dabei zu beachten, dass die Zwischenzertifizierungsstellen von einem Server mit ausgeliefert werden müssen, da der Browser nur das Wurzelzertifikat kennt und sonst die Vertrauenskette nicht bis dorthin bilden kann. Dies ist aber mit sehr wenig Aufwand durch den Server-Administrator zu bewerkstelligen und erfordert keine Aktion der Nutzer.

Ein Blick in die Zertifikatverwaltung ab Windows Vista könnte zunächst an dem Erfolg der Integration zweifeln lassen, da das Wurzelzertifikat hier nicht sofort zu sehen ist. Dies liegt an einem neuen Konzept von Microsoft: Zunächst sind nur sehr wenige Wurzelzertifikate vorinstalliert, weitere werden erst bei Bedarf online nachgeladen. Auf einem neu installierten Windows Vista wird das Wurzelzertifikat der DFN-PKI daher erst angezeigt, sobald es benötigt wird, wie z.B. beim Surfen auf https://info.pca.dfn.de. Einmal online nachgeladen, bleibt das Wurzelzertifikat jedoch fest auf dem System installiert.

Die Integration wirkt sich auch auf andere Bereiche positiv aus, wie z.B. auf die Signatur von ausführbaren Programmen, die aus dem Internet heruntergeladen werden. So sorgt die Integration des Wurzelzertifikats in Sun Java dafür, dass digital signierte Anwendungen, wie z.B. die neue RA-Oberfläche der DFN-PKI, seit November 2008 standardmäßig als vertrauenswürdig eingestuft werden. Dem Nutzer wird also auch an dieser Stelle keine Warnung mehr angezeigt.

Mit der Aufnahme des Wurzelzertifikats der DFN-PKI in die am meisten verwendeten Umgebungen wird nun vieles einfacher, gerade auch für Nutzer, die geringe Vorkenntnisse im Umgang mit Verschlüsselung und Signatur haben. Und das Beste daran ist: Die Nutzer müssen nichts tun, sondern profitieren automatisch von der weltweiten Akzeptanz der Zertifikate aus der DFN-PKI. ◆

Überblick der Integration des Wurzelzertifikats der DFN-PKI

✓	Mozilla Firefox	ab Version 3.0.12 bzw. 3.5
✓	Mozilla Thunderbird	ab Version 2.0.0.23
✓	Microsoft Windows	ab Internet Explorer 5
✓	Mac OS X	ab OS X 10.5.4
✓	iPhone und iPod touch	ab iPhone OS 2.x
✓	Sun Java	ab Version 1.6_11 (6u11)
✓	Opera	ab Version 7.5