DFN-PKI: „Root im Browser"-Problem gelöst

Gute Nachricht für alle Anwender, die ihre Zertifizierungsstelle (CA) an den DFN-Verein auslagern. Einer der wichtigsten Erweiterungswünsche für die DFN-PKI konnte - kurz vor Redaktionsschluss der DFN-Mitteilungen - erfüllt werden: Die Root (Wurzel) der DFN-PKI wird in die wichtigsten Standardbrowser automatisch verlinkt! Das heißt, dass bei Nutzung von Zertifikaten der DFN-PKI die bisher problematischen Pop-up-Fenster mit Meldungen wie „wollen Sie diesem Zertifikat wirklich vertrauen" nicht mehr erscheinen. Insbesondere bei Webservern hat sich das oft als Problem erwiesen, aber auch bei der Prüfung von E-Mail Signaturen wurde aufgrund der bisher fehlenden Verlinkung „fälschlicherweise" eine ungültige Signatur angezeigt.

Vertrauen durch Verkettung

Anstelle des bisher selbst signierten Wurzelzertifikats wurde ein neues Wurzelzertifikat der DFN-PKI mit einer in Webbrowsern verankerten Zertifizierungsstelle der T-Systems verkettet. Die T-Systems Business Services GmbH kann als Tochterunternehmen der Deutschen Telekom auf die Konzerneinheit T-Systems Enterprise Services GmbH und deren Organisationseinheiten zurückgreifen. Diese betreibt seit August 1994 das hochsichere Trust Center der Deutschen Telekom, das seit 1996 nach ISO 9002 und seit Januar 2001 nach ISO 9001:2000 zertifiziert ist. Außerdem wird mit der T-TeleSec Public Key Service (PKS) eine Plattform zur Ausgabe von bisher mehr als 2 Millionen Zertifikaten und digitalen bzw. elektronischen Signaturen betrieben. Das Trust Center zeichnet sich durch einen sehr hohen Sicherheitsstandard aus, Personal und Arbeitsabläufe werden durch ausgebildete Administratoren überwacht und laufend Qualitätskontrollen unterzogen.

Die hier realisierte Lösung wird von der T-Systems erstmalig in einem Kundenprojekt bereitgestellt. Möglich wurde dies u.a. nur aufgrund der professionellen Betriebsumgebung der DFN-PKI beim DFN-CERT in Hamburg. Dort werden neben der obersten Zertifizierungsstelle, der DFN-PCA, auch alle an den DFN-Verein ausgelagerten Zertifizierungsstellen betrieben. Im Vorfeld der Leistungserbringung wurde die CA-Umgebung des DFN-Vereins hinsichtlich Einhaltung der Policies der Deutsche Telekom Root CA und der erforderlichen Sicherheitsmaßnahmen nach aktuellem Stand der Technik begutachtet und mit positivem Ergebnis bewertet.

Neues Sicherheitsniveau „Global"

Eine Voraussetzung für die Verkettung ist ein regelmäßiges Audit der Betriebsumgebung der DFN-PKI in Hamburg durch die T-Systems. Dadurch soll sichergestellt werden, dass die vereinbarten organisatorischen und betrieblichen Abläufe immer korrekt und damit vertrauensvoll erfolgen. Von der Verkettung können deshalb alle Anwender profitieren, deren Zertifizierungsstelle an den DFN-Verein ausgelagert ist. Zur Umsetzung des Konzeptes wurde neben dem bisherigen Sicherheitsniveau „Classic" ein neues Sicherheitsniveau „Global" – der Name ist hier Programm – eingerichtet.

Mit dem neuen Sicherheitsniveau ist auch eine neue Policy erforderlich. Aber keine Angst: Die neue Global-Policy ist weitgehend identisch mit der bisherigen Classic-Policy, so dass sich für die Anwender keine wesentlichen Neuerungen ergeben. Obwohl inhaltlich nahezu unverändert, hat sich in der Darstellung der Policy jedoch vieles geändert. Mit der neuen Version 2.1 wurden die Policies aller Sicherheitsniveaus in einem Dokument zusammengeführt, wobei die Unterschiede der Sicherheitsniveaus hervorgehoben sind. Die Darstellung erfolgt nun kompakter und übersichtlicher, so dass sich die neue Policy deutlich einfacher liest.

Weitere Verbesserungen der DFN-PKI

Neben dem neuen Sicherheitsniveau Global gibt es weitere Verbesserungen in der DFN-PKI. So wurden die Webschnittstellen für Nutzer und Registrierungsstellen vollständig überarbeitet. In den neuen Schnittstellen werden keine Frames mehr verwendet, die Menüführung ist übersichtlicher und wurde um einige Punkte erweitert. Handlungsanweisungen zu den Hauptmenüpunkten und bessere Erläuterungen der Eingabefelder erleichtern die Nutzung der Webschnittstellen. Das Formular für den Zertifikatantrag wird in Anlehnung an die im Papierformat vorliegenden Formulare im PDF-Format generiert. Die Suche nach Zertifikaten ist durch die Möglichkeit der Verwendung von Wildcards erleichtert worden und in der Schnittstelle für Registrierungsstellen wird z.B. der Status von Anträgen und Zertifikaten durch Kennbuchstaben angezeigt. Für Anwender, die eine große Anzahl von Nutzerzertifikaten für Mitarbeiter oder Studierende ausstellen wollen, stehen in beiden Webschnittstellen Menüpunkte für die Self-Service Funktionen zur Verfügung. Alle Funktionen der neuen Webschnittstellen können Sie in der aktuellen Version der DFN-Test-PKI ausprobieren, die Sie zusammen mit einer neuen Anleitung unter der bekannten Adresse www.dfn.de/pki/testpki-zugang finden. Wenn Sie bereits Zugangsdaten für die DFN-Test-PKI erhalten haben, können Sie diese auch für die neue Version weiter nutzen.

Durch Einsatz einer Online-CA werden Zertifikate seit Oktober 2006 wesentlich schneller ausgestellt: Maximal 10 Minuten nach Eingang eines genehmigten Zertifikatantrags erhält der Nutzer oder Administrator sein beantragtes Zertifikat. Dafür wurde ein neuer Zertifizierungsrechner mit einem Hardware Security Module (HSM) in Betrieb genommen. Dieses nach FIPS 140-1 Level 3 evaluierte HSM ermöglicht es, den Zertifizierungsrechner dauerhaft an die restliche Infrastruktur angeschlossen zu halten und kontinuierlich Zertifikate auszustellen. Die Qualität der Dienstleistung erhöht sich damit deutlich, da die bisher auftretende Wartezeit von bis zu einem Arbeitstag entfällt.

Was müssen Sie tun?

Das Wichtigste zuerst: Alle ausgestellten Zertifikate gelten unverändert weiter. Wenn Sie mit der bisherigen Situation zufrieden sind, brauchen Sie nichts zu tun. Wenn Sie jedoch Ihre CA an den DFN-Verein ausgelagert haben und die neuen Funktionalitäten nutzen wollen, sind einige Anpassungen erforderlich. Die Kollegen der DFN-PCA werden deshalb mit allen Anwendern in den kommenden Wochen Kontakt aufnehmen und mit Ihnen den Übergang zum Sicherheitsniveau Global sowie die Umstellung Ihrer Webschnittstellen besprechen. Falls ein Umstieg für Sie besonders eilig ist, können Sie sich auch direkt an die PKI-Ansprechpartner wenden. Die Kontaktdaten finden Sie unter www.dfn.de/pki/kontakt.

Noch ein Hinweis für alle Anwender, die ihre Zertifizierungsstelle in Zukunft an den DFN-Verein auslagern: Diese haben die Möglichkeit, sofort im neuen Sicherheitsniveau Global mit den neuen Webschnittstellen zu starten und die Vorteile von Anfang an zu nutzen. Details zu den Neuerungen in der DFN-PKI gibt es auch auf der kommenden DFN-Betriebstagung am 27. Februar 2007 in Berlin. Weitere Informationen zur DFN-PKI finden Sie unter www.dfn.de/pki. Wenn Sie Fragen zur DFN-PKI haben oder Ihre Zertifizierungsstelle an den DFN-Verein auslagern wollen, schicken Sie bitte eine E-Mail an pki@dfn.de.

Dr. Marcus Pattloch