DFN-Test-PKI

Die DFN-PKI zum Ausprobieren

Die Vorbereitungen für den neuen Dienst in der DFN-weiten Public Key Infrastruktur DFN-PKI sind in vollem Gang. Dass der Dienst ab 2006 mit Einführung des X-WiN im DFNInternet-Dienst enthalten ist, macht ihn nun für alle DFN-Anwender besonders attraktiv. Zentrale Komponente des Dienstes ist die Möglichkeit, Zertifizierungsstellen an den DFN-Verein auszulagern. Schon jetzt können Sie sich ein Bild davon machen, wie das in der Praxis funktioniert.

Wie sind die Arbeitsabläufe, wenn die Zertifizierungsstelle an den DFN-Verein ausgelagert wird? Wie sehen die Webschnittstellen aus, die den teilnehmenden Einrichtungen vom DFN-Verein zur Verfügung gestellt werden? Wer kann diese Schnittstellen nutzen? Wie funktioniert das Zustellen der Zertifikate? Welche Voraussetzungen müssen erfüllt sein? Das sind Fragen, die sich wahrscheinlich jede Einrichtung stellt, die den neuen DFN-PKI Dienst nutzen möchte. Die besten Antworten auf solche Fragen lassen sich durch eigene Erfahrung finden. Deshalb haben wir für Sie die DFN-Test-PKI eingerichtet.

Abbildung 1: Startseite für Nutzer und Administratoren

Probieren geht über Studieren

Wenn Sie sich im Rahmen der DFN-PKI für die Auslagerung Ihrer Zertifizierungsstelle an den DFN-Verein entscheiden, werden Ihnen speziell für Ihre Einrichtung vom DFN-Verein zwei Webschnittstellen für

- ***Nutzer und Administratoren*** – z.B. zum Beantragen und Sperren von Zertifikaten
- ***Registrierungsstellen*** – z.B. zum Bearbeiten von Zertifikatanträgen

zur Verfügung gestellt. Damit können alle benötigten Angaben erfasst und an die ausgelagerte Zertifizierungsstelle übermittelt werden. In der DFN-Test-PKI haben Sie die Möglichkeit, die Funktionalität dieser Webschnittstellen zu testen. Sie können alle Arbeitsschritte von der Beantragung eines Zertifikats bis zu dessen Ausstellung durchlaufen und noch weitere Funktionen kennen lernen.

Im Regelbetrieb stehen diese Schnittstellen jeweils den Nutzern und Administratoren bzw. den lokalen Registrierungsstellen zur Verfügung. In der DFN-Test-PKI nehmen sie, je nachdem in welcher Schnittstelle Sie sich befinden, unterschiedliche Rollen wahr:

- Über die Schnittstelle für Nutzer und Administratoren die Rolle eines Nutzers oder Administrators, der für sich bzw. die von ihm betreuten Server Zertifikate beantragen möchte.
- Über die Schnittstelle für Registrierungsstellen die Rolle einer Registrierungsstelle, die die eingegangenen Anträge prüft und an die ausgelagerte Zertifizierungsstelle weiterleitet.

Unentgeltliche Nutzung für DFN-Anwender
Der Dienst DFN-PKI einschließlich der Auslagerung einer Zertifizierungsstelle an den DFN-Verein ist ab Januar 2006 im Dienst DFNInternet enthalten. Für Anwender im DFN fallen damit keine zusätzlichen Entgelte an, wenn dieser Dienst in Anspruch genommen wird.

Beide Webschnittstellen haben grundsätzlich das gleiche Erscheinungsbild, bieten aber unterschiedliche Funktionen. Diese können über „Registerkarten" (Abbildung 1) ausgewählt werden, die wiederum eine Reihe von Unterfunktionen bieten. Über das DFN-Logo gelangen Sie jeweils auf eine Seite mit den DFN-Ansprechpartnern für allgemeine und technische Fragen zur DFN-Test-PKI und zur DFN-PKI.

Ein Beispiel: Ihr Nutzerzertifikat vom Antrag bis zum Einsatz

Im folgenden Beispiel wird gezeigt, wie Sie in der DFN-Test-PKI ein Nutzerzertifikat beantragen, durch die Registrierungsstelle bearbeiten lassen und schließlich in Ihre Anwendung importieren können.

Dafür begeben Sie sich zunächst in die ***Rolle des Nutzers*** und verwenden die Schnittstelle für Nutzer und Administratoren. Unter der Registerkarte *Nutzer* wählen Sie *Beantragen eines Zertifikats*

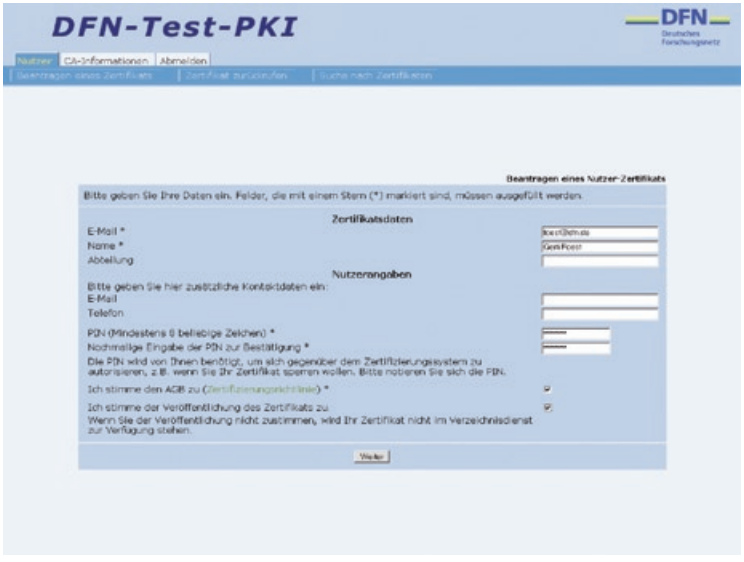

Abbildung 2: Formular zum Beantragen eines Nutzerzertifikats

und dann *Zertifikatantrag für Nutzer*. In dem Formular, das Ihnen darauf hin angezeigt wird, füllen Sie alle mit einem * gekennzeichneten Felder aus und tragen unbedingt Ihre korrekte Mailadresse ein, da diese zur Auslieferung des Zertifikats benötigt wird (Abbildung 2).

Ihre Angaben werden anschließend noch einmal angezeigt und können bei Bedarf geändert werden. Wenn Sie die Angaben bestätigen, wird von der DFN-Test-PKI veranlasst, dass in Ihrem Browser ein Schlüsselpaar generiert wird. Dabei verhalten sich die diversen Browser sehr unterschiedlich und Sie sollten nun jeweils den Aufforderungen Ihres Browsers folgen und der Test-PKI CA vertrauen.

Wenn die Schlüssel erzeugt sind, wird Ihnen Ihr Zertifikatantrag am Bildschirm angezeigt und kurz darauf erscheint automatisch auch das Druckerfenster für den Ausdruck des Zertifikatantrags. In der DFN-Test-PKI ist für Sie lediglich die Seriennummer des Antrags für die nächsten Schritte wichtig. Im Regelbetrieb müssen Sie die Angaben auf dem Ausdruck vervollständigen, unterschreiben und bei Ihrer Registrierungsstelle vorlegen.

Abbildung 3: Liste neuer Zertifikatanträge

Jetzt können Sie sich von dieser Webschnittstelle *Abmelden* und sich in die ***Rolle der Registrierungsstelle*** begeben, um den Antrag weiter zu bearbeiten. Dafür wählen Sie sich in die Webschnittstelle der Registrierungsstelle ein. Unter der Registerkarte *Zertifikatanträge* und dann *Neu* wird Ihnen die Liste aller neuen Zertifikatanträge aus der DFN-Test-PKI angezeigt, die noch nicht bearbeitet und an die Zertifizierungsstelle weitergeleitet wurden (Abbildung 3). Darunter befindet sich auch der von Ihnen in der Rolle des Nutzers gestellte Antrag. Die Auswahl erfolgt durch einen Klick auf die entsprechende Seriennummer.

Nun werden alle Angaben für das von Ihnen beantragte Zertifikat angezeigt und Sie können wählen, wie Sie weiter verfahren wollen. Für unser Beispiel wählen Sie die Operation *Antrag genehmigen ohne ihn digital zu signieren* (diese Operation ist nur in der DFN-Test-PKI möglich). Auf dem Bildschirm erscheint dann die Mitteilung, dass das Zertifikat erstellt und dem Antragsteller per Mail zugesandt wird. In der DFN-Test-PKI erhalten Sie diese Mail an die von Ihnen in der Rolle des Nutzers angegebenen Adresse. Damit ist der Arbeitsablauf abgeschlossen und Sie können sich auch von dieser Schnittstelle *Abmelden*.

Gerti Foest
DFN-Verein
foest@dfn.de

Dr. Marcus Pattloch
DFN-Verein
pattloch@dfn.de

Die Zertifikate der DFN-Test-PKI

Wenige Minuten nach dem Absenden des Zertifikatantrags an die Zertifizierungsstelle erhalten Sie eine E-Mail von der DFN-Test-PKI mit Ihrem Zertifikat und weiteren Hinweisen. Um Ihr eigenes Zertifikat nutzen zu können, müssen Sie zunächst das Wurzel- und CA-Zertifikat der Test-PKI CA und dann das eigene Zertifikat in Ihren Browser importieren. Auch hier verhalten sich die Browser unterschiedlich und Sie müssen wieder den Aufforderungen des jeweiligen Browsers folgen. Wenn Sie alle Zertifikate importiert haben, ist die DFN-Test-PKI mit Ihrem Wurzel- und CA-Zertifikat als vertrauenswürdige Autorität in Ihrem Browser eingetragen und unter den eigenen Zertifikaten finden Sie Ihr Zertifikat der DFN-Test-PKI. Abbildung 4 zeigt, wie diese Einträge bei Mozilla Firefox aussehen.

Alle Zertifikate in der DFN-Test-PKI, einschließlich des Wurzel- und CA-Zertifikats, sind nur für Testzwecke einsetzbar und für die allgemeine Nutzung nicht gültig. Nutzer- und Serverzertifikate laufen nach einer Dauer von 8 Tagen ab. Wir empfehlen, nach Abschluss Ihrer Tests das Wurzel- und CA-Zertifikat der DFN-Test-PKI aus Ihren Anwendungen zu löschen. Sie können diese Zertifikate jederzeit über die Webschnittstellen wieder importieren.

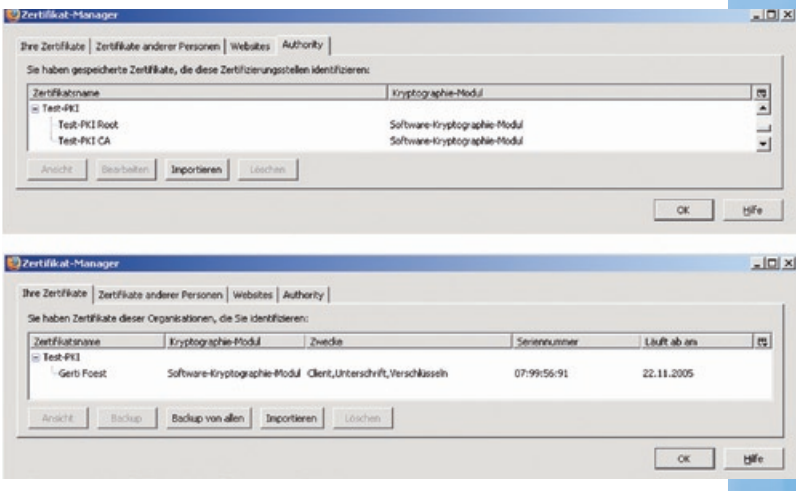

Abbildung 4: Importierte Zertifikate der DFN-Test-PKI

Was ist im Regelbetrieb anders?

Die Webschnittstellen, die jedem Anwender individuell zur Verfügung gestellt werden, können in einigen Punkten den speziellen Anforderungen des Anwenders angepasst werden. So wird z.B. für jeden Anwender der Schriftzug „DFN-Test-PKI" durch das Logo bzw. einen Text des Anwenders ersetzt. Weitere Anpassungen können individuell abgesprochen werden.

Wer in Ihrer Einrichtung die Webschnittstelle für Nutzer und Administratoren nutzen darf, können Sie selbst entscheiden. Die Webschnittstelle für Registrierungsstellen kann nur von den Mitarbeitern Ihrer Registrierungsstelle genutzt werden, die von Ihrer Einrichtung autorisiert wurden und ein entsprechendes Zertifikat der DFN-PKI erhalten haben. Alle über die Schnittstelle für Nutzer und Administratoren erstellten Anträge müssen von den Antragstellern in der Registrierungsstelle vorgelegt werden. Diese prüft die Identität des Antragstellers sowie die vervollständigten Angaben und die Unterschrift auf dem Zertifikatantrag. Dann kann der Antrag von der Registrierungsstelle digital signiert an die Zertifizierungsstelle weitergeleitet werden.

Was müssen Sie tun?

Um Ihre Zertifizierungsstelle auszulagern, müssen Sie in Ihrer Einrichtung eine oder mehrere Registrierungsstellen organisatorisch etablieren. Möglicherweise können Sie diese bei bereits vorhandenen Organisationseinheiten, wie z.B. dem Immatrikulationsbüro, ansiedeln. An technischen Voraussetzungen benötigen Sie für die Registrierungsstellen nur einen abschließbaren Raum und einem PC mit Internetanschluss, spezielle Serverinstallationen sind auf Anwenderseite nicht notwendig. Die Kommunikation zwischen den Registrierungsstellen und der ausgelagerten Zertifizierungsstelle mit den dahinter liegendenden Prozessen basiert auf der OpenCA Software. Diese Software wurde an die Erfordernisse und Workflows der DFN-PKI angepasst. Alle technisch aufwändigen Komponenten, wie spezielle Server für die verschiedenen Aufgaben im Rahmen dieser Arbeitsprozesse, werden von den Experten der DFN-PCA im Auftrag des DFN-Vereins betrieben.

Auslagerung einer Zertifizierungsstelle - es kann losgehen!

Die DFN-Test-PKI soll Ihnen ein Gefühl für die Arbeitsabläufe vermitteln, die sich ergeben, wenn Sie Ihre Zertifizierungsstelle an den DFN-Verein auslagern. So können sich auch die Personen in Ihrer Einrichtung einen Einblick verschaffen, die z.B. in die Entscheidungsprozesse eingebunden sind oder die später die Aufgaben der Registrierungsstelle übernehmen sollen. Wenn Sie nun „auf den Geschmack gekommen" sind, nehmen Sie mit uns Kontakt auf. Wir beraten Sie gerne in allen Fragen zur Auslagerung Ihrer Zertifizierungsstelle.

Zugang zur DFN-Test-PKI und Kontakt für Fragen
Sie erreichen die Webschnittstellen der DFN-Test-PKI über www.dfn.de/pki/testpki-zugang und finden dort auch eine ausführliche Anleitung zur Nutzung.
Für den Zugang zur DFN-Test-PKI benötigen Sie einen Benutzernamen und ein Passwort. Um diese Zugangsdaten und Antworten auf Ihre Fragen zu erhalten, schicken Sie bitte eine Mail an pki@dfn.de.

Alle Infos zur DFN-PKI unter: www.dfn.de/pki

Startschuss für EU-Domain am 7. Dezember – auch Hochschulen können Top-Level-Domains reservieren

In der ersten Phase der Surise Period können ab dem 7. Dezember 2005 offiziell Internetadressen mit der Länderkennung „.eu" angemeldet werden. Antragsberechtigt sind neben den Inhabern nationaler Marken und Gemeinschaftsmarken auch Hochschulen. Ab dem 7. Februar 2006 folgt dann die zweite Phase der Surise Period, in der unter anderem Geschäftsbezeichnungen, Unternehmenszeichen, Familiennamen sowie Titel von literarischen und künstlerischen Werken als Domain angemeldet werden können. Ab dem 7. April 2006 tritt dann die allgemeine Registrierungsphase in Kraft (auch „Land Rush Periode" genannt), wonach jeder Bürger zur Anmeldung einer EU-Domain berechtigt ist.

Ebenso wie für „.de-Adressen" gilt dabei das Prinzip „Wer zuerst kommt, mahlt zuerst", das im europäischen Juristendeutsch auch als „Windhundprinzip" bezeichnet wird. Hintergrund des dreigliedrigen Vergabeverfahrens sind unter anderem die negativen Erfahrungen mit Domain-Grabbing zu Lasten insbesondere von Markeninhabern.

Wichtig für Hochschulen ist Art. 10 Absatz 3 der „.eu-Festlegungs-Verordnung", der auch eine Anmeldung gebräuchlicher Abkürzungen wie beispielsweise www.uni-stadt.eu erlaubt.

Oberste Registerstelle der EU-Domains ist das Unternehmen „EURid", das jedoch selbst keine Anmeldungen annimmt. Diese sind vielmehr ausschließlich möglich bei einer national zugelassenen Registerstelle. Eine Übersicht, auch deutscher Registerstellen, findet sich unter http://list.eurid.eu/registrars/SearchAlphabetical.htm?lang=de.

Noogie C. Kaufmann