DFN-PKI

Neues Konzept ermöglicht einfachen Einstieg in die Welt der Zertifikate

Der Nutzen von Zertifikaten ist unbestritten, der Weg dorthin war bisher jedoch oft schwierig. Mit dem neuen, erweiterten DFN Zertifizierungsdienst bietet der DFN-Verein seinen Anwendern nun eine Lösung an, um mit wenig Aufwand in die DFN-weite Public Key Infrastruktur (DFN-PKI) einzusteigen. Aber nicht nur für "Neulinge" sondern auch für Anwender, die bereits einen Zertifizierungsdienst in ihrer Einrichtung etabliert haben, ergeben sich mit diesem Konzept wesentliche Vorteile.

Die Sicherheit von Zertifikaten ist grundsätzlich nicht nur höher als die von Passwörtern, auch die Nutzung kann einfach und weitgehend transparent gestaltet werden. An Stelle von vielen Passwörtern – die sich sowieso kein Nutzer merken kann – erhält jede Person nur ein Zertifikat. Wie beim Vorzeigen eines Ausweises kann dem Inhaber beim Einsatz eines Zertifikats Zugang zu lokalen, nationalen und internationalen Diensten und Ressourcen gewährt werden.

Viele Hochschulen und andere wissenschaftliche Einrichtungen wollen Zertifikate einsetzen. Bisher mussten sie dafür einen eigenen Zertifizierungsdienst aufsetzen, mit allen daraus resultierenden technischen und betrieblichen Anforderungen. Selbst für die Ausstellung weniger Zertifikate musste eine Struktur etabliert werden, die den "Spielregeln" (Policies) für einen Zertifizierungsdienst genügt. Das bedeutete einen hohen personellen und technischen Aufwand und damit oft eine große Hürde für den Einstieg.

Mit dem neuen Konzept werden Einstieg und Betrieb wesentlich einfacher, denn die aufwändigen Komponenten können nun an den DFN-Verein "ausgelagert" werden, der sie im Namen der Einrichtung betreibt.

Trennung von Zertifizierung und Registrierung

Die verschiedenen Aufgabenbereiche eines Zertifizierungsdienstes lassen sich klar gegeneinander abgrenzen. Der im Kasten auf der rechten Seite skizzierte Vergleich mit den Meldestellen (Registrierungsstellen) und der Bundesdruckerei (Zertifizierungsstellen) zeigt das deutlich.

An praktisch jeder Einrichtung ist eine Instanz vorhanden, die die Aufgaben einer Registrierungsstelle grundsätzlich wahrnehmen kann, z.B. ein Immatrikulationsbüro oder eine Personalstelle. Durch geeignete Werkzeuge wird erreicht, dass der Aufwand hierfür nicht zu groß wird. Die Realisierung der Aufgaben einer Zertifizierungsstelle erfordert allerdings außer Mitarbeitern mit speziellem technischen Know-How auch besondere Hardwarekomponenten wie einen gesicherten Raum, einen Safe, ein Bankschließfach und speziell gesicherte Rechner ohne Netzzugang.

Gerti Foest
DFN-Verein
foest@dfn.de

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

In Analogie zu den Meldestellen, die nicht gleichzeitig auch eine eigene Bundesdruckerei betreiben, stellt sich die Frage, ob jede Einrichtung neben einer Registrierungsstelle auch eine eigene Zertifizierungsstelle betreiben muss. Das neue Konzept des DFN-Zertifizierungsdienstes gibt darauf eine eindeutige Antwort: Nein!

Auslagerung aufwändiger Komponenten – Was bedeutet das für Sie?

Nach den Regeln (Policies) des neuen DFN-Zertifizierungsdienstes können die Aufgaben von Registrierungs- und Zertifizierungsstellen getrennt voneinander wahrgenommen werden. Damit wird die Auslagerung des technisch aufwändigen Betriebs einer Zertifizierungsstelle ermöglicht. Die Anwender können somit den Betrieb ihrer Zertifizierungsstelle an den DFN-Verein auslagern, der in ihrem Namen Zertifikate für die Nutzer und Ressourcen der Einrichtungen ausstellt.

Wenn Sie für Nutzer und Server in Ihrer Einrichtung Zertifikate benötigen, müssen Sie in Zukunft also keine aufwändige technische Infrastruktur für eine Zertifizierungsstelle aufbauen bzw. betreiben. Lediglich die Registrierungsstelle bleibt in Ihrer Einrichtung.

Um die Aufgaben der Registrierungsstelle einfach und effizient durchführen zu können, stellt Ihnen der DFN-Verein eine angepasste Webschnittstelle zur Verfügung über die alle benötigten Angaben

Ab sofort auch Grid-Zertifikate im DFN

Im Mai 2005 wurde der Aufnahme des DFN-Vereins in die EUGridPMA zugestimmt. Über den DFN Zertifizierungsdienst werden deshalb ab sofort zusätzlich zu allen bisherigen Zertifikaten auch EUGridPMA-konforme Zertifikate ausgegeben, z.B. für die Teilnehmer des DEISA Projekts. Alle Informationen zu Grid-Zertifikaten im DFN finden Sie unter www.dfn.de/pki/grid.

Im Rahmen von Grid-Projekten spielen Zertifikate eine wichtige Rolle, z.B. beim Zugriff auf Supercomputer oder Datenbestände. In der Vergangenheit hat sich eine eigene, weltweite Struktur gebildet, die ihre Rolle in der Koordination der Versorgung von Grids mit Zertifikaten sieht. Der europäische Teil dieser Struktur trägt den Namen EUGridPMA (European Grid Policy Management Authority – www.eugridpma.org). Durch diese abgestimmte Struktur können Grid-Projekte weltweit authentisch und somit sicher zusammenarbeiten.

erfasst werden können und die eine perfekte Schnittstelle zur ausgelagerten Zertifizierungsstelle beinhaltet. Auf diese Weise wird für Sie die Einstiegshürde zum Aufbau eines eigenen Zertifizierungsdienstes deutlich herabgesetzt. Wenn Sie bereits einen eigenen Zertifizierungsdienst betreiben, wird Ihnen nun die Möglichkeit geboten, diesen Betrieb noch wirtschaftlicher zu gestalten.

Das neue Konzept funktioniert

Seit Anfang des Jahres läuft die Pilotphase des neuen DFN Zertifizierungsdienstes. Erste Zwischenergebnisse zeigen, dass die Idee genau richtig ist und das Konzept der Trennung von Registrierung und Zertifizierung funktioniert. Bis zum Ende der Pilotphase wird die Umsetzung weiter ausgearbeitet und verbessert, das heißt insbesondere: Einfache Schnittstellen und Optimierung des Workflows zwischen Registrierungs- und Zertifizierungsstelle.

Der Regeldienst wird Anfang 2006 mit Übergang auf das X-WiN in Betrieb gehen. Anwendern, die sofort einsteigen wollen, steht der Pilotbetrieb offen.

Kontakt für Fragen zum Pilotbetrieb und zum Zertifizierungsdienst im DFN: pki@dfn.de.
Weitere Infos unter: www.dfn.de/pki

Erstellung von Zertifikaten – so funktioniert es!

Das Verfahren für die Ausstellung eines Zertifikats lässt sich gut mit dem Vorgang der Ausstellung eines Personalausweises vergleichen.

Personalausweis		Zertifikat
Ich beantrage einen Ausweis		Ich beantrage ein Zertifikat
Meldestelle		Registrierungsstelle (RA)
Bundesdruckerei		Zertifizierungsstelle (CA)
Meldestelle		Registrierungsstelle (RA)
Ich habe einen Ausweis		Ich habe ein Zertifikat

Benötige ich einen Ausweis, gehe ich zu meiner nächstgelegenen Meldestelle, fülle einen Antrag aus, identifiziere mich mit meinem vorhandenen Ausweis (oder einem anderen anerkannten Dokument) und gebe mein Lichtbild ab.

Die Meldestelle prüft meine Angaben und sendet alle notwendigen Unterlagen an die Bundesdruckerei, die die technischen Systeme betreibt, für mich einen Ausweis herstellt und ihn an die Meldestelle zurücksendet, bei der ich ihn nach angemessener Zeit abholen kann.

Benötige ich ein Zertifikat, wende ich mich mit einem Antrag an eine Registrierungsstelle (RA), die meine Identität überprüft.

Die notwendigen Daten werden an eine Zertifizierungsstelle (CA) übermittelt, die die technischen Systeme betreibt, das Zertifikat erzeugt und es mir entweder direkt oder über die Registrierungsstelle zukommen lässt.