

# Mehr Netzsicherheit für Hochschulen

## USB-Sticks als Zugangsschlüssel

**(BS/Heike Lischewski)** An der Fernuniversität Hagen und mehreren anderen Hochschulen in Nordrhein-Westfalen wurde erfolgreich eine Public-Key-Infrastruktur-Lösung erprobt. Um die Flexibilität zu erhöhen, kommt dabei ein so genannter eToken zum Einsatz. Er kann an jeden beliebigen PC über eine USB-Schnittstelle angeschlossen werden und stellt eine sichere Arbeitsumgebung bereit.

Mit Hilfe eines Zertifikats einer vertrauenswürdigen Stelle wird die Zugehörigkeit eines kryptografischen Schlüssels zu bestimmten Personen, Organisationen oder Computern bestätigt. Schlüssel und Zertifikate sind dabei Dateien mit einem bestimmten Inhalt. "Der persönliche Schlüssel befindet sich heute meist auf einer intelligenten Chipkarte, das Zertifikat ist dagegen auf dem Rechner am Arbeitsplatz gespeichert", erläutert der Sicherheitsexperte.

### Zugang von verschiedenen Rechnern aus

Doch Studierende benötigen meist an verschiedenen Computern auf dem Uni-Gelände Zugang zum Hochschulnetz. Außerdem ist die Installation eines Chipkartenlesegeräts an jedem Rechner sehr aufwändig. "Deshalb haben wir nach einem bequemeren Weg gesucht", berichtet Henning Mohren, Projektleiter an der Fernuniversität Hagen.

Die Lösung heißt eToken, stammt von der israelischen Firma Aladdin Knowledge Systems und ist ein USB-Stick in der Größe eines normalen Hausschlüssels.

### Komfortable Lösung als eToken

Der eToken enthält eine integrierte Smartcard, auf der ein privater



Mehr Sicherheit für die Hochschulnetze in NRW durch PKI-Lösungen.

Fotos: BS/NK Networks & Services

Schlüssel und das Zertifikat gespeichert sind. Wird dieser Speicherstick in den USB-Anschluss eines beliebigen Computers im Hochschulnetz gesteckt und das dazugehörige Passwort eingegeben, ist der sichere Zugriff auf Netz, Anwendungen, Websites und E-Mail-System möglich. Ein Knopfdruck auf den eToken generiert ein One-Time-Passwort, das in Verbindung mit einem persönlichen Code nur wenige Sekunden gültig ist und den sicheren Zugriff auf das Hochschulnetz über das In-

ternet auch von externen Rechnern aus gewährleistet.

In Pilotprojekten an mehreren NRW-Hochschulen wurde die Technologie bereits erfolgreich erprobt. So an der Fernuniversität in Hagen. "Bereits seit 1996 testen wir hier PKI-Lösungen im Rahmen von Förderprojekten und setzen sie im Produktionsbetrieb ein", berichtet Mohren. Um die Akzeptanz zu erhöhen, wurden Überlegungen angestellt, die Web-gestützten Zertifizierungsdienste für den Nutzer so einfach wie

möglich zu gestalten. Eine Automatisierung des bis dahin durch Administrationspersonal manuell zu bedienenden Verfahrens lag folglich nahe. Die Fernuni entwickelte hierzu einen "Zertifizierungsautomaten", der Studierenden und Mitarbeitern die benötigten Zertifikate ausstellt. Hierbei wird eine automatische SSL-Zertifizierung eingesetzt, bei der das persönliche Erscheinen in Hagen nicht mehr erforderlich ist – für eine Fernuniversität mit Studierenden aus ganz Deutschland ein wichtiger Aspekt.

Zur sicheren Identifikation und Authentisierung können die beim Immatrikulationsvorgang verifizierten Adressdaten herangezogen werden. Die kryptografischen Anforderungen werden durch die clientseitige Verwendung von modernen Browser-Technologien erfüllt. "Ein derartiges Online-Verfahren zum Beantragen eines Zertifikats ist auch für Studierende, die bis dahin keine Kenntnis auf dem Gebiet der PKI-Nutzung haben, einfach durchführbar", hat Mohren festgestellt.

Grundlage der Identifikation ist die bestehende Benutzerdatenbank an der Hochschule. Die Benutzer werden dabei einfach mittels der vorhandenen Datensätze identifiziert. Um ein Zertifikat zu erhalten, muss der Student an einem von ihm selbst

gewählten, beliebigen internetfähigen Arbeitsplatz die Website der Fernuni in Hagen aufrufen und seine Matrikelnummer angeben. Der Webserver sucht aus der Benutzerdatenbank den entsprechenden Datensatz heraus, generiert ein Passwort und schickt dieses per Post an die gefundene Adresse. In einem zweiten Schritt wird das Passwort dem Adress-Satz hinzugefügt. Hat der Student das Passwort erhalten, kann er über ein weiteres Webformular sein Zertifikat beantragen.

"Durch die Ablösung der bisherigen Softwarezertifikate mit dem eToken erreicht die Fernuniversität in Hagen eine zuverlässige Zweifaktor-Authentisierung", ist sich Mohren sicher. Mit dem Einsatz des USB-Sticks lasse sich die bisherige Arbeitsplatz- und Browser-Bindung aufheben. Auch weitere Nutzungsmöglichkeiten des eToken für eine sichere Authentisierung werden an der Fernuni in Hagen bereits getestet. So ist ein Ziel das Single Sign-on, bei dem sich der Anwender anhand seines eToken und des eToken-Passworts sicher an verschiedenen Applikationen anmelden kann. "Damit braucht man sich nicht mehr verschiedene Passworte zu merken und hat jederzeit eine Garantie für den Schutz seiner persönlichen Daten", betont Robert Dürr.

