Die neue RA-Oberfläche in der DFN-PKI

Vieles wird einfacher – Neues wird möglich

Derzeit erledigen Registrierungsstellen (RA) in der DFN-PKI ihre Aufgaben - wie z.B. das Genehmigen von Zertifikatanträgen - über eine Webschnittstelle im Browser. Diese Art der Bearbeitung stößt jedoch an ihre Grenzen, etwa wenn es um die Integration in eine lokale Infrastruktur oder die Speicherung von Zertifikaten auf kryptographischen Geräten geht. Die neue RA-Oberfläche der DFN-PKI bietet als lokale Java-Anwendung nun erweiterte Möglichkeiten wie die Integration lokaler Nutzerverzeichnisse, das Beschreiben von Smartcards oder die Erstellung von Serverzertifikaten ohne OpenSSL. Eingebaute Assistenten helfen dabei, Vorgänge schnell und bequem zu bearbeiten.

Die Webschnittstelle für Registrierungsstellen (RA-Webschnittstelle) in der DFN-PKI hat sich durch ihre einfache Bedienung als schneller Weg zur Genehmigung und Bearbeitung von Zertifikatanträgen etabliert. Wenn jedoch mehrere Anträge gleichzeitig bearbeitet werden sollen oder eine Suche nach Zertifikaten oder Anträgen durchgeführt werden muss, sind bequemere Bedienmöglichkeiten vorstellbar. Und spätestens wenn größere Anforderungen aufkommen, wie z.B. das Einbinden eines lokalen Verzeichnisdienstes mit Nutzerdaten oder das Beschreiben von kryptographischen Geräten (z.B. Smartcards, USB-Krypto-Token), für die auch noch ein lokales Schlüssel-Backup erstellt werden soll, stößt die RA-Webschnittstelle an ihre Grenzen. Außerdem kennen viele RA-Mitarbeiter wahrscheinlich auch die folgende Situation: Ein Serverzertifikat wird gebraucht, und dazu muss nicht nur ein Zertifikatantrag mit OpenSSL erzeugt werden ("Wie waren doch gleich die richtigen Parameter?"), sondern dieser Antrag muss zusätzlich noch über zwei verschiedene Webschnittstellen hochgeladen bzw. genehmigt werden.

Um diesen Anforderungen gerecht zu werden, ist ab sofort eine neue RA-Oberfläche in der DFN-PKI verfügbar. Diese wird als lokale Anwendung ausgeführt und bietet als Alternative zur RA-Webschnittstelle alle dort vorhandenen sowie eine Reihe weiterer Funktionen an. Im Hintergrund kommuniziert die Anwendung verschlüsselt über die SOAP-Schnittstelle der DFN-

PKI, die seit ihrer Einführung im letzten Jahr bereits als stabile Grundlage für andere erfolgreiche Projekte dient [DFN-Mitteilungen Heft 73, "Feuerprobe für DFN-PKI - Die Zertifizierungsstelle der FH Landshut"]. Da die Anwendung in Java geschrieben ist, kann sie auf allen Plattformen, auf denen eine Java-Laufzeitumgebung verfügbar ist, ausgeführt werden und fügt sich dort in das Gesamtbild der lokalen Benutzeroberfläche ein. Durch die Verteilung mittels der Java WebStart Technologie ist keine lokale Installation erforderlich, und es wird stets die neuste Version direkt vom Server der DFN-PCA geladen.

Neues Erscheinungsbild

Die neue RA-Oberfläche wird über ein zweigeteiltes Hauptfenster bedient (Abbildung 1). Auf der linken Seite befindet sich eine Baumansicht mit allen Zertifizierungsstellen (CA), die für die jeweilige RA relevant sind. Hier zeigt sich bereits ein Vorteil dieser Oberfläche: Einrichtungen, die neben Zertifikaten ihrer ausgelagerten Zertifizierungsstelle(n) auch Grid-Zertifikate ausstellen, können in der Baumansicht direkt auf die gewünschte CA umschalten und müssen dafür nicht in eine andere Anwendung wechseln. Für jede CA werden in Unterpunkten genau die Funktionen aufgeführt, die auch in der RA-Webschnittstelle angeboten werden.

Auf der rechten Seite des Fensters werden in einer Listenansicht alle Elemente zu dem jeweils ausgewählten Unterpunkt der CA angezeigt. Im oberen Teil des Fensters befindet sich eine Symbolleiste, die rechts ein Eingabefeld zum Filtern der aktuell angezeigten Liste enthält. Die Eingabe eines Suchbegriffs in dieses Feld wirkt sich unmittelbar während der Eingabe auf die angezeigten Elemente in der Liste aus, was eine schnelle Suche ermöglicht. Über die Symbole auf der linken Seite der Symbolleiste können direkt Aktionen mit einem ausgewählten Listenelement durchgeführt werden.

Bestimmte Aktionen, wie z.B. das Genehmigen oder Löschen von Anträgen, können auch auf mehrere in der Liste selektierte Einträge angewendet werden, indem zunächst wie üblich per "Strg-Mausklick" die Listenelemente markiert werden und anschließend das gewünschte Aktionssymbol ausgewählt wird (Abbildung 1).

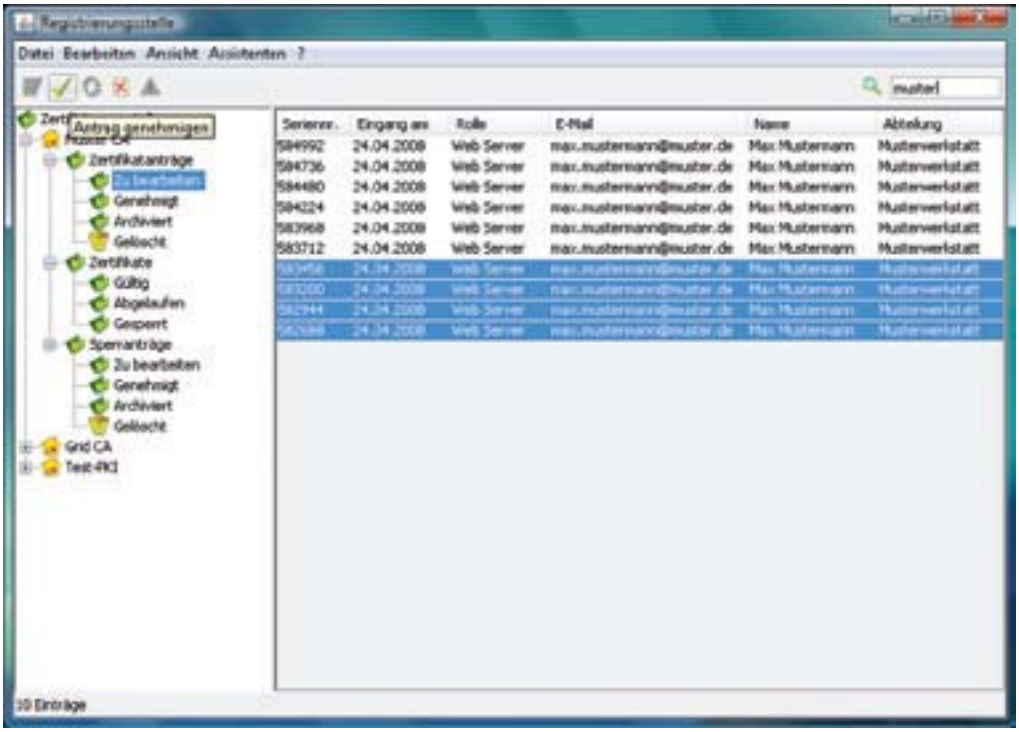
Das Bearbeiten einzelner Anträge erfolgt in einem eigenen Dialogfenster, das sich nach einem Klick auf das ausgewählte Listenelement öffnet (Abbildung 2). Das Dialogfenster ist gegenüber der RA-Webschnittstelle ebenfalls verbessert worden. Alle änderbaren Daten werden getrennt von den nicht änderbaren Informationen unter verschiedenen Karteireitern angezeigt. Für die Eingabe alternativer Namen wird eine Auswahlliste angeboten, die der Nachrichtenempfängerliste in Mozilla Thunderbird ähnelt.

Assistenten

Die größte Neuerung gegenüber der RA-Webschnittstelle sind jedoch die so genannten „Assistenten". Dies sind integrierte Hilfsprogramme, die viele Arbeitsschritte automatisiert erledigen können. Dabei werden nur wenige Eingaben des Nutzers verlangt und alle weiteren Schritte automatisch im Hintergrund erledigt.

Generell können alle Assistenten in der neuen RA-Oberfläche auf die individuellen Bedürfnisse jeder Einrichtung angepasst werden, denn die von einem Assistenten durchgeführten Schritte werden jeweils durch einzelne Module realisiert, die in ihrer Reihenfolge und ihren Parametern anpassbar sind. Diese Module gibt es für viele verschiedene Aufgabenbereiche. Für

Abbildung 1: Erscheinungsbild der neuen RA-Oberfläche, Beispiel: Ausgewählte Zertifikatanträge genehmigen



die Ermittlung oder Anpassung von vorhandenen Nutzerdaten, die für die Zertifizierung herangezogen werden sollen, existieren Module zum Lesen und Schreiben in LDAP-Verzeichnisse (auch Microsoft Active Directory oder Novell eDirectory) und SQL-Datenbanken. Weitere Module dienen der Speicherung von Zertifikaten und Schlüsseln auf kryptographischen Geräten oder der Erstellung von Serverzertifikaten. Viele kleinere Hilfsmodule wie z.B. die Generierung von Passwörtern, Schlüsseln und PIN-Briefen runden die Aufzählung ab und und machen die Assistenten zu mächtigen Werkzeugen.

Es gibt bereits fertig integrierte Standardassistenten, von denen jede RA profitieren kann. Zwei Bespiele werden nachfolgend vorgestellt.

Token Assistent

Im PKI-Umfeld wird die Verwendung von kryptographischen Geräten (z.B. Smartcards, USB-Krypto-Token) aufgrund ihrer grundsätzlich höheren Sicherheit und der technischen Entwicklung immer interessanter. Natürlich konnten auch bereits über die RA-Webschnittstelle Zertifikate auf kryptographischen Geräten gespeichert werden, jedoch mussten dabei alle Schritte wie das Initialisieren und Beschreiben des Gerätes sowie die eventuelle Anfertigung einer Sicherheitskopie des Schlüssels manuell durchgeführt werden. Ein Assistent in der neuen RA-Oberfläche hilft hier weiter, indem folgendermaßen vorgegangen wird: Ein Nutzer kommt mit seinem Personalausweis zur RA und möchte ein kryptographisches Gerät verwenden. Der Mitarbeiter der RA startet daraufhin den entsprechenden Assistenten und sucht zunächst die Daten des Nutzers im lokalen Benutzerverzeichnis oder der lokalen Datenbank. Nachdem die selektierten Daten in einem Eingabeformular überprüft wurden, werden auf Klick automatisch ein Schlüsselpaar und ein Zertifikat erstellt und auf ein an den Rechner der RA angeschlossenes kryptographisches Gerät geschrieben. Anschließend wird ein PIN-Brief gedruckt, der dem Nutzer zusammen mit dem Gerät ausgehändigt wird. Die darauf gedruckte PIN wurde während des Zertifizierungsprozesses per Zufall generiert und ermöglicht nur dem Nutzer den Zugang zu den Daten auf dem Gerät.

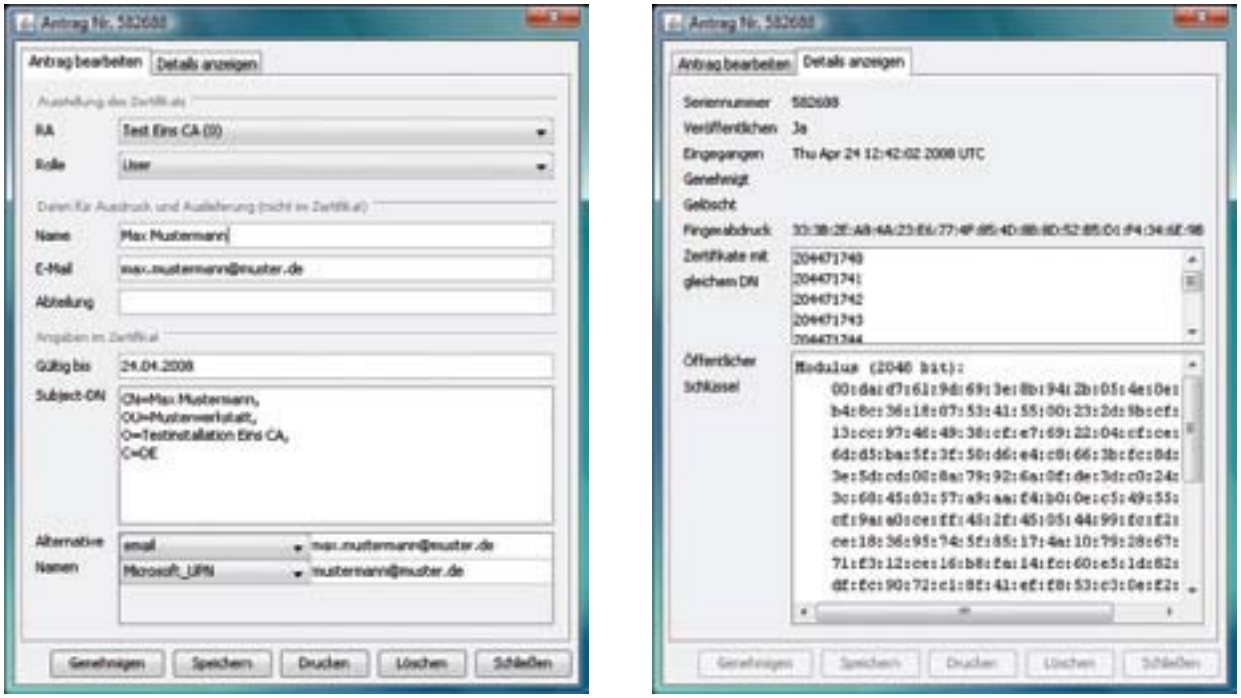
Das Zertifikat ohne den privaten Schlüssel kann zusätzlich von dem Assistenten in ein Verzeichnis geschrieben werden, was z.B. für eine Benutzeranmeldung mit Smartcard erforderlich ist. Optional kann auch eine verschlüsselte Sicherheitskopie des privaten Schlüssels erstellt und in einem Verzeichnis oder einer Datenbank abgelegt werden. Das ist immer dann sehr wichtig, wenn das Zertifikat zur Verschlüsselung von Daten genutzt werden soll, die bei einem Defekt oder bei Verlust des kryptographischen Geräts ansonsten verloren wären.

Für Zertifikate, die nur der Signatur oder Authentifizierung dienen, ist eine Sicherheitskopie nicht relevant, so dass das entsprechende Schlüsselpaar direkt auf dem Gerät generiert werden kann. Dank des Zugriffs auf die kryptographischen Geräte über die standardisierte PKCS#11-Schnittstelle können sämtliche Operationen unabhängig vom Hersteller durchgeführt werden. Der Hersteller muss lediglich eine Implementierung dieses Standards mitliefern, was mittlerweile bei fast jedem Modell auf dem Markt der Fall ist.

Assistent "Serverzertifikat erstellen"

Dieser Assistent bietet Unterstützung bei der Erstellung eines Serverzertifikats. In der zur Zeit vorliegenden Version gilt

Abbildung 2: Dialogfenster "Antrag bearbeiten"



dies zunächst nur für den Fall, dass der RA-Mitarbeiter auch gleichzeitig der Administrator des Servers ist, für den das Zertifikat beantragt wird. In diesem Fall vereinfacht der Assistent den Vorgang der Zertifikaterstellung im Vergleich mit der RA-Webschnittstelle erheblich. In der Webschnittstelle sind dafür mehrere Schritte notwendig: Zunächst müssen ein Schlüsselpaar und ein Zertifikatantrag mit einer externen Software wie z.B. OpenSSL erzeugt werden. Dazu alleine sind schon viele Kommandozeilenparameter notwendig, die nur die wenigsten auswendig kennen. Der erzeugte Antrag muss dann über die öffentliche Webschnittstelle hochgeladen und über die RA-Webschnittstelle digital signiert und genehmigt werden. Das ausgestellte Zertifikat muss anschließend aus der zugesandten E-Mail extrahiert werden, um dann zusammen mit dem Schlüssel und der separat heruntergeladenen CA-Kette in einem Webserver installiert zu werden.

Der Assistent erledigt viele dieser Aufgaben automatisch. Der RA-Mitarbeiter startet den Vorgang über die Auswahlliste

Gerti Foest

DFN-Verein
foest@dfn.de

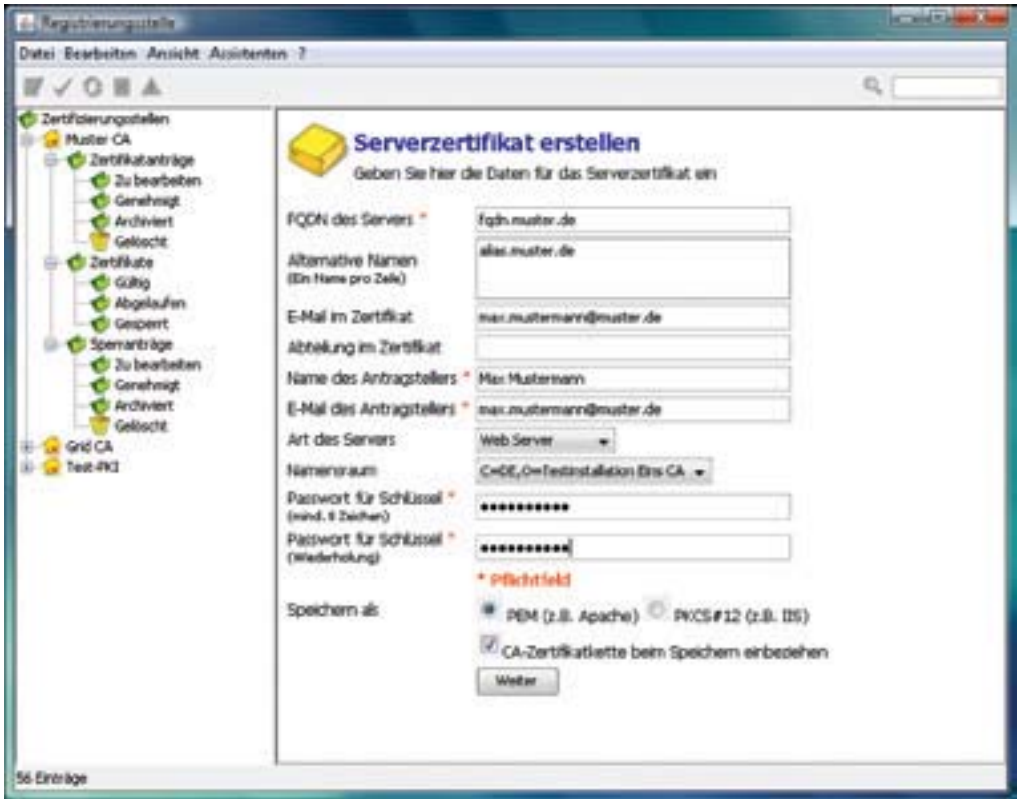
Jan Mönnich

DFN-PCA
moennich@dfn-cert.de

„Assistenten" und erhält im rechten Teil des Fensters ein Eingabeformular (Abbildung 3). Hier werden alle für das Serverzertifikat relevanten Daten eingetragen, wobei auch alternative Namen für Webserver mit mehreren virtuellen Hosts berücksichtigt werden können. Nachdem die Daten eingetragen wurden, übernimmt der Assistent automatisch alle weiteren Schritte wie Hochladen, Genehmigen, Abholen und Speichern des Zertifikats inklusive der CA-Kette in verschiedenen Formaten für unterschiedliche Anwendungen. Das Ausstellen eines Serverzertifikats wird dadurch zu einer Sache von wenigen Minuten.

Es ist geplant, dass die RA die Erstellung von Serverzertifikaten auch für andere Administratoren einer Einrichtung mit Hilfe des Assistenten durchführen kann. Dies setzt allerdings genaue Regelungen für den Umgang mit dem bei der RA erzeugten Schlüssel und ggf. eine Erweiterung der Policy (CPS) einer Einrichtung voraus.

Abbildung 3: Assistent "Serverzertifikat erstellen"



Kurzmeldungen

Fazit

Die neue RA-Oberfläche bietet dank der schnelleren Suchfunktion und der Möglichkeit zur Bearbeitung mehrerer Objekte gegenüber der RA-Webschnittstelle mehr Komfort, was sich besonders bei vielen Zertifikaten bemerkbar macht. Sehr praktisch ist auch die Verwaltung mehrerer CAs unter einer Oberfläche. Insbesondere Einrichtungen, die auch eine Grid-RA betreiben, werden dies zu schätzen wissen.

Das Konzept der „Assistenten" bringt durch die Automatisierung vieler Arbeitsschritte eine deutliche Zeitersparnis beim Arbeiten. Der Assistent für kryptographische Geräte ist für alle Einrichtungen interessant, die diese Geräte einsetzen wollen. Aufgrund der Herstellerunabhängigkeit und den Möglichkeiten zur Anpassung an die eigene Umgebung ist dieser Assistent in vielen Szenarien einsetzbar. Der Assistent zum „Erstellen eines Serverzertifikats" ist für jede RA interessant, die auch mit der Administration von Servern betraut ist. Hier können viel Zeit und Nerven gespart werden, weil der Einsatz externer Software entfällt und nicht zwischen mehreren Webschnittstellen gewechselt werden muss.

Und ein Reinschnuppern lohnt sich allemal, denn die neue RA-Oberfläche ist voll kompatibel zu der bewährten RA-Webschnittstelle, so dass kein Zwang zu einem kompletten Umstieg besteht. Wenn Sie also den neuen Komfort und die neuen Möglichkeiten für Ihre ausgelagerte CA nutzen möchten, senden Sie einfach eine E-Mail an pki@dfn.de. Das DFN-PKI Team stellt Ihnen dann die Software umgehend zur Verfügung.

DFN-PKI: Zeitstempeldienst im Pilotbetrieb

Im Rahmen des Dienstes DFN-PKI steht seit Februar 2008 ein DFN-Zeitstempeldienst zur Verfügung. Damit können z.B. termingebundene Dokumente, Prüfungsanmeldungen, Zertifikatsperrlisten oder Programmcodes mit einem vertrauenswürdigen Zeitstempel versehen werden. Die aktuelle Zeit wird dabei über eine Funkuhr (EMC Professional Net / DCF77) ermittelt und mit einem Zertifikat der DFN-PKI „beglaubigt".

Der Dienst kann von Anwendungen genutzt werden, die in der Lage sind, Anfragen an einen Zeitstempelserver zu stellen und dessen Antwort entgegen zu nehmen, dazu gehören z. B. Adobe Acrobat, OpenTSA, signtool und jarsign. Der Dienst kann nicht direkt aus einem Webbrowser durch Anklicken einer URL genutzt werden.

Zur Zeit läuft der Dienst im Pilotbetrieb und kann in dieser Betriebsphase ohne Anmeldung und Ausfüllen von Formularen genutzt werden. Die weitaus häufigsten Anfragen an den Zeitstempeldienst seit Beginn der Pilotphase im Februar kommen aus Adobe Acrobat Anwendungen, bei denen PDF-Dokumente mit einem Zertifikat der DFN-PKI signiert und zusätzlich mit einem vertrauenswürdigen DFN-Zeitstempel versehen werden.

Informationen und Antworten auf Fragen zum Zeitstempeldienst finden Sie unter

www.pki.dfn.de/zeitstempel.

Für weitere Fragen schicken Sie bitte eine E-Mail an pki@dfn.de

Informationen zu „Automatischen Warnmeldungen" weiter ausgebaut

Über den Dienst „Automatische Warnmeldungen" können DFN-Anwender per E-Mail automatisch generierte Warnmeldungen erhalten, wenn beim DFN-CERT Auffälligkeiten im Zusammenhang mit IP-Adressen Ihrer Einrichtung bekannt geworden sind. So verbessern Sie nicht nur die Sicherheit Ihrer Einrichtung, sondern tragen auch insgesamt zu einem verbesserten Sicherheitsniveau im Deutschen Forschungsnetz bei. Das Informationsangebot rund um den Dienst wurde erheblich ausgebaut. Auf der Webseite http://www.cert.dfn.de/autowarn finden Sie nun eine Reihe von Beispielen sowie einen FAQ, in dem die am häufigsten gestellten Fragen aufgegriffen werden. Die Nutzung des Dienstes ist für DFN-Anwender unentgeltlich und kann durch eine formlose Mail an cert@dfn.de beauftragt werden.