Rollout von Zertifikaten leichter gemacht

SOAP-Schnittstelle erweitert die Möglichkeiten in der DFN-PKI

Die Beantragung, Genehmigung und Ausstellung von Zertifikaten in der DFN-PKI funktioniert für einzelne Nutzer mit Hilfe eines Webbrowsers einfach und bequem. Doch was ist zu tun, wenn es gilt, mehrere hundert oder gar tausend Anträge für Nutzer- oder Serverzertifikate zu bearbeiten? Wie können Zertifikate der DFN-PKI auf USB-Kryptotoken oder SmartCards gebracht werden, die bereits im Einsatz sind? Für diese Fragen gibt es jetzt eine Antwort: Eine SOAP-Schnittstelle, die eine maschinelle Kommunikation mit den Servern der ausgelagerten Zertifizierungsstellen in der DFN-PKI ermöglicht.

Neue Schnittstelle

Im bisherigen Ablauf einer Zertifizierung in der DFN-PKI stellt der Zertifikatnehmer einen Antrag, der danach durch die Registrierungsstelle genehmigt wird. Beide Vorgänge werden in einem Webbrowser auf einer für Menschen konzipierten Benutzeroberfläche durchgeführt. Jeder Antrag muss einzeln gestellt und von der Registrierungsstelle einzeln digital signiert und genehmigt werden. Eine Möglichkeit, über diese Webschnittstellen auch eine größere Anzahl von Nutzerzertifikaten zu bearbeiten, ist das sogenannte Self-Service Verfahren. Dabei werden policy-konform geprüfte Nutzerdaten von der Registrierungsstelle in einer Datei an die Zertifizierungsstelle übermittelt und der Nutzer kann sich sein Zertifikat über die Webschnittstelle „abholen". Aber auch bei diesem Verfahren ist menschliche Interaktion notwendig.

Die SOAP-Schnittstelle der DFN-PKI ermöglicht jetzt eine Kommunikation nicht mehr nur zwischen Mensch und Maschine, sondern auch zwischen Maschine und Maschine. Die in der Webschnittstelle wählbaren Aktionen wie „Zertifikat beantragen", „Antrag bearbeiten", „Antrag genehmigen" oder „Antragsdatei hochladen" wer-

den in der SOAP-Schnittstelle als ein entfernter Prozeduraufruf durchgeführt. Eine lokal entwickelte Software kann mit Hilfe dieser Prozeduraufrufe alle notwendigen Schritte für eine Zertifizierung durchführen und dabei sowohl die Rolle des Zertifikatnehmers als auch die der Registrierungsstelle einnehmen. Die SOAP-Schnittstelle bietet damit alle Möglichkeiten, die auch in der Webschnittstelle zur Verfügung stehen. Darüber hinaus kann der Zertifizierungsprozess durch den Einsatz lokaler Software individuell an die jeweiligen Anforderungen angepasst werden *(Abbildung 1)*.

Die neuen Möglichkeiten in der DFN-PKI

- Einbindung existierender Prozesse
- Verwendung lokaler Datenquellen
- Automatisierte Ausstellung von sehr vielen Zertifikaten
- Lokale Initialisierung kryptographischer Geräte
- Erzeugung eines lokalen Schlüssel-Backup
- Diverse Abfragen für Statistiken

Abb. 1: Erweiterungen der DFN-PKI

Anwendungen

Durch die Bereitstellung der SOAP-Schnittstelle besteht nun die Möglichkeit, bereits vorhandene lokale Strukturen und Prozesse in die DFN-PKI einzubinden. Die Erzeugung der Schlüssel und der Zertifikatanträge sowie deren Genehmigung können jetzt durch eine selbst entwickelte Software durchgeführt werden. Da diese Software lokal - und nicht auf den vom DFN betriebenen Servern der ausgelagerten Zertifizierungsstelle - läuft, kann auch bei der Beschaffung der Zertifikatdaten (Name, E-Mail Adresse etc.) direkt auf lokale Quellen wie z.B. einen Verzeichnisdienst oder eine Datenbank zugegriffen werden. Entscheidend ist, dass die Eingabe dieser Daten entsprechend der Policy der DFN-PKI vorgenommen wurde, das heißt insbesondere, dass eine persönliche Identifizierung durch Vorlage eines Ausweispapiers durchgeführt wurde. Wenn eine persönliche Identifizierung bereits in den lokalen Prozessen - z.B. Ausweisvorlage bei der Immatrikulation - verankert ist, genügen die Daten den Anforderungen der DFN-PKI Policy. An der Fachhochschule Landshut wurde die Integration der lokalen Infrastruktur in die DFN-PKI bereits erfolgreich durchgeführt. Einen Erfahrungsbericht dazu gibt der Artikel von Herrn Hartmann in diesem Heft.

Mit dem Zugriff auf lokale Datenquellen, die die notwendigen Zertifikatinformationen enthalten und der Möglichkeit, ohne weitere Interaktionen von Nutzern, Administratoren oder Mitarbeitern der Registrierungsstelle Zertifikatanträge zu stellen bzw. zu genehmigen, ist nun die schnelle Verarbeitung einer großen Anzahl von Zertifikatanträgen ohne weiteres möglich. Die Realisierung an der FH Landshut hat gezeigt, dass über die SOAP-Schnittstelle mehrere hundert Zertifikate innerhalb von wenigen Minuten problemlos ausgestellt und übermittelt werden können.

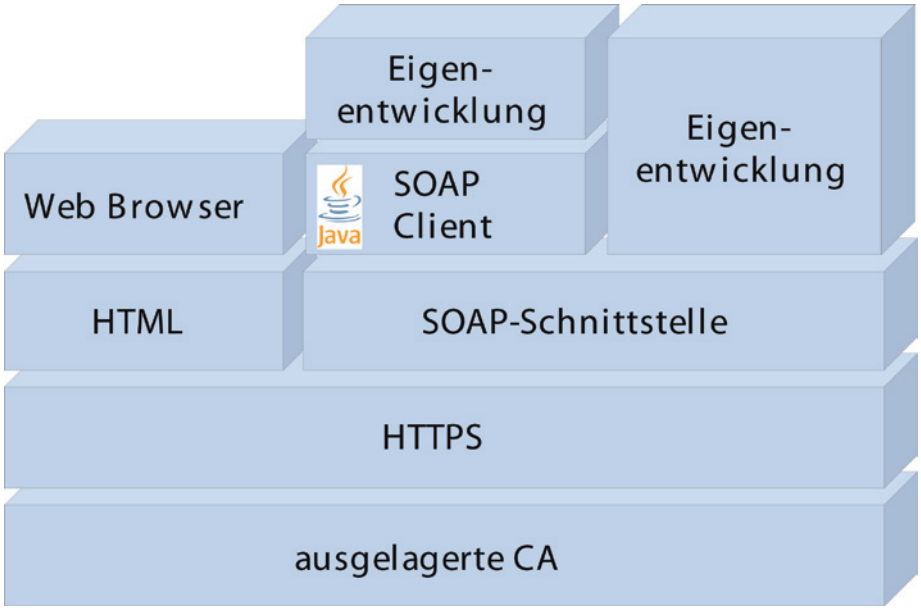
Eine weitere Anwendung der SOAP-Schnittstelle ist die Bestückung von USB-Kryptotoken oder SmartCards mit Zertifikaten der DFN-PKI. Eine lokale Software kann einen Zertifikatantrag erstellen, genehmigen, an die Zertifizierungsstelle übermitteln, das ausgestellte Zertifikat empfangen und auf das kryptographische Gerät schreiben. Interessant ist bei dieser Vorgehensweise die Möglichkeit, zuvor eine lokale Kopie des generierten privaten Schlüssels zu erzeugen und diese in verschlüsselter Form zu speichern. Dies ist unabdingbar, wenn die Zertifikate zur Verschlüsselung eingesetzt werden sollen, da ohne eine Sicherheitskopie des privaten Schlüssels bei einem Defekt oder Verlust des kryptographischen Gerätes die verschlüsselten Daten nicht mehr wiederhergestellt werden können.

Die SOAP-Schnittstelle bietet außerdem die Funktionalität, Listen von Anträgen und Zertifikaten zu erstellen. Durch Auswertung dieser Listen mit einer geeigneten Software können dann für ausgelagerte Zertifizierungsstellen Statistiken in beliebiger Form erstellt werden. Denkbar sind hier einfache Übersichten wie z.B. eine Liste der Gesamtanzahl von Zertifikaten einer Zertifizierungsstelle bis hin zur Anzeige von allen bereits mit einem Zertifikat versehenen Servern der Einrichtung. Eine entsprechende Software könnte die Informationen z.B. auch nutzen, um bald ablaufende Zertifikate zu ermitteln und eine Verlängerung dieser Zertifikate automatisch durchzuführen.

Konzeptionelle Einordnung

Die SOAP-Schnittstelle ist als Ergänzung zu der bestehenden Webschnittstelle zu sehen und kann parallel zu dieser betrieben werden *(Abbildung 2)*. So können Anträge in der Webschnittstelle gestellt und in der SOAP-Schnittstelle genehmigt werden und umgekehrt. Die SOAP-Schnittstelle kann entweder durch eine SOAP-Implementierung für die jeweilige Programmiersprache oder durch einen eigens für die DFN-PKI entwickelten SOAP-Client angesprochen werden. Dieser SOAP-Client wird vom DFN-Verein zur Verfügung gestellt und beinhaltet bereits viele häufig gebrauchte kryptographische Funktionen wie z.B. das digitale Signieren. Damit wird die Kommunikation mit den Servern der ausgelagerten Zertifizierungsstelle deutlich vereinfacht.

Abb. 2: Schnittstellen in der DFN-PKI



Gerti Foest

DFN-Verein
foest@dfn.de

Jan Mönnich

DFN-PCA
moennich@dfn-cert.de

Technik

Mit der SOAP-Schnittstelle wurde ein Webservice implementiert, der auf dem SOAP-Protokoll basiert. Dabei handelt es sich um ein Protokoll, mit dem auf Basis von XML Nachrichten ausgetauscht werden können. Bei diesen Nachrichten kann es sich entweder um generelle Dokumente oder, wie in diesem Fall, um entfernte Prozeduraufrufe (Kommunikationsstil rpc/encoded) handeln. Die Übertragung des Protokolls ist nicht festgelegt, erfolgt jedoch in den meisten Fällen über HTTP(S) und TCP, was auch auf die SOAP-Schnittstelle der DFN-PKI zutrifft.

Die SOAP-Schnittstelle ist analog zu der Webschnittstelle aufgebaut: Die Beantragung von Zertifikaten kann ohne eine Authentifizierung mit entsprechenden SOAP-Aufrufen über eine URL erfolgen. Der Zugang zu einer weiteren URL, über die SOAP-Aufrufe zur Bearbeitung und Genehmigung von Zertifikatanträgen abgesetzt werden können, ist nur mit einer SSL-Client-Authentifizierung mit einem Zertifikat der Registrierungsstelle möglich.

Die Aufrufe in der SOAP-Schnittstelle sind den Aktionen in den bestehenden Webschnittstellen nachempfunden. Einige Beispiele für den Zusammenhang zwischen einer Aktion in einer der Webschnittstellen und dem entsprechenden SOAP-Aufruf sind in *Abbildung 3* dargestellt.

Die SOAP-Schnittstelle ist durch WSDL (Web Service Description Language) für Maschinen beschrieben. Viele SOAP-Implementierungen können auf Basis dieser standardisierten Beschreibung Quellcode für die jeweilige Programmiersprache erzeugen, so dass die Prozeduren direkt als Befehle ausgeführt werden können.

Fazit

Die SOAP-Schnittstelle der DFN-PKI ermöglicht eine maschinelle Kommunikation mit den Servern der ausgelagerten Zertifizierungsstellen in der DFN-PKI und damit die Einbindung eigener Programmentwicklungen in den Zertifizierungsprozess. So kann eine Anpassung des Zertifizierungsvorgangs an verschiedenste lokale Anforderungen erreicht werden. Insbesondere können bereits vorhandene Prozesse jetzt in die DFN-PKI integriert werden. Die Kompatibilität zwischen der gewohnten Webschnittstelle und der neuen SOAP-Schnittstelle ist gegeben, so dass diese miteinander kombiniert werden können. Die Programmierung einer eigenen Anwendung ist aufgrund der Dokumentation der Schnittstelle in WSDL und des sofort verwendbaren SOAP-Clients einfach und schnell umzusetzen.

Bei Interesse an den neuen Möglichkeiten wenden Sie sich bitte an pki@dfn.de, eine ausführliche Dokumentation der Schnittstelle inklusive Beispiel-Quelltexten für mehrere Programmiersprachen senden wir Ihnen dann gerne zu.

Abbildung 3: Zusammenhang Aktion Webschnittstelle / SOAP-Aufruf

Webschnittstelle	SOAP-Aufruf
Nutzer stellt Antrag	**newRequest**
Nutzer druckt Antrag aus	**getRequestPrintout**
RA ruft Antrag auf	**getRawRequest**
RA genehmigt Antrag	**approveRequest**
Nutzer erhält Zertifikat	**getCertificateByRequestSerial**

Umzug des DFN-CERT

Anfang Dezember 2007 ist das DFN-CERT in Hamburg umgezogen. Die neue Adresse lautet:

DFN-CERT Services GmbH
Sachsenstraße 5
20097 Hamburg

Alle bekannten E-Mail-Adressen und Telefonnummern bleiben unverändert.

15. DFN-Workshop „Sicherheit in vernetzten Systemen“

Am 13. und 14. Februar 2008 findet im CCH Hamburg bereits zum fünfzehnten Mal der DFN-Workshop „Sicherheit in vernetzten Systemen“ statt. Der Kanadier Dick Hardt von Sxip Identity wird die Veranstaltung mit einem sehr speziellen Vortrag zum Thema „Identity Management“ eröffnen. Natürlich erwartet die Teilnehmer außerdem eine Reihe vielfältiger interessanter Beiträge: Die aktuell heiß diskutierten Themenbereiche „Online-Durchsuchungen“ und „Botnetze“ bilden zwei Schwerpunkte des Programms.

Im Anschluss an den Workshop findet ein Tutorium zum Thema „Praktische Rechtsfragen“ statt.

Das komplette Programm sowie Informationen zur Anmeldung finden Sie auf den Seiten des DFN-CERT unter https://www.dfn-cert.de/events/ws/2008/