Merkblatt „Die Bedienstetenchipkarte der RUB“

Sie haben heute eine neue Bedienstetenchipkarte erhalten, die auch die Funktion eines Bedienstetenausweises hat. Diese zeigt Ihr Bild, Ihren Namen und eine eindeutige Nummer. Darüber hinaus enthält sie einen Chip mit einem Prozessor, welcher in der Lage ist, selbständig komplexe Verschlüsselungsverfahren durchzuführen. Mit dem Chip ist es möglich, Ihre Bedienstetenchipkarte für digitale Signaturen, das heißt „elektronische Unterschriften“ zu benutzen.

Öffentlicher Schlüssel, Privater Schlüssel, Zertifikat

Es gibt zwei grundsätzlich verschiedene Verfahren zur Verschlüsselung von Daten: symmetrische und asymmetrische Verfahren. Beim symmetrischen Verfahren exisitert nur ein Schlüssel, mit dem die Daten sowohl verschlüsselt als auch entschlüsselt werden. Beim asymmetrischen Verfahren existieren zwei verschiedene, aber zusammengehörende Schlüssel. Daten, welche mit einem der beiden Schlüssel verschlüsselt wurden, lassen sich nur mit dem anderen Schlüssel wieder entschlüsseln. Daraus resultieren die sogenannten „Public Key“-Verfahren. Einer der beiden Schlüssel bleibt geheim und steht nur dem Besitzer zur Verfügung („privater Schlüssel“), der zweite wird öffentlich gemacht und steht allen Interessierten zur Verfügung („öffentlicher Schlüssel“). Daten, die mit einem öffentlichen Schlüssel verschlüsselt werden, lassen sich nur mit dem zugehörenden privaten Schlüssel des Besitzers wieder entschlüsseln. Daten, die mit einem privaten Schlüssel verschlüsselt werden, sind nur mit dem passenden öffentlichen Schlüssel zu entschlüsseln. So läßt sich sichergestellen, dass die Daten vom Besitzer des privaten Schlüssels stammen und nicht verändert wurden.
Dieser Mechanismus ist die Grundlage der digitalen Signatur. Bei der Erstellung jeder Chipkarte werden diese zwei Schlüssel (privat und öffentlich) von dem auf der Chipkarte vorhandenen Prozessor generiert. Der private Schlüssel kann nicht ausgelesen werden und steht ausschließlich auf der Chipkarte für Ver-/Entschlüsselungen zur Verfügung. Der öffentliche Schlüssel wird in den zentralen, öffentlichen Verzeichnisdienst der RUB transferiert. Dabei muss aber gewährleistet werden, dass der Schlüssel echt ist. Dies erreicht man dadurch, dass der öffentliche Schlüssel von der RUB als Aussteller der Karte mit dem gleichen mathematischen Verfahren signiert wird und damit ein sogenanntes Zertifikat ausgestellt wird. Dieses Zertifikat wird neben dem öffentlichen Schlüssel in der Public Key Infrastructure (PKI) der RUB abgelegt.

Digitale Signatur

Die Verschlüsselung eines kompletten Dokuments mit Hilfe der Chipkarte würde sehr lange dauern. Deshalb wird zur Absicherung von größeren Datenmengen ein anderer Weg gegangen: die digitale Signatur. Hierfür wird zunächst ein Hash-Wert (eine Art Prüfsumme oder Fingerabdruck des Dokuments) ermittelt. Die Besonderheit dieses Hash-Werts liegt darin, dass es nicht möglich ist, zu einem vorgegebenen Hash-Wert ein beliebiges sinnvolles Dokument zu erzeugen. Es ist deshalb praktisch unmöglich, innerhalb eines Dokuments Veränderungen so vorzunehmen, dass sich der Hash-Wert nicht ändert. Deshalb ist ein Dokument durch seinen Hash-Wert zweifelsfrei zu identifizieren.
Dieser Hash-Wert wird nun zusammen mit einigen Rahmendaten (z.B. Datum der Signatur, Name des Signierenden sowie einige technisch notwendige Daten) mit dem privaten Schlüssel der Chipkarte des Benutzers verschlüsselt. Das Ergebnis ist die digitale Signatur.
Will man nun diese digitale Signatur auf ihre Echtheit hin überprüfen, benötigt man zunächst wieder das Dokument. Über dieses Dokument wird wiederum mit dem gleichen Verfahren der Hash-Wert gebildet. Jetzt wird mit dem öffentlichen Schlüssel des Benutzers, der sich in der PKI befindet, die digitale Signatur entschlüsselt. Stimmt das Ergebnis mit dem ermittelten Hash-Wert überein, so ist die digitale Signatur gültig. Unterscheiden sich die Hash-Werte, so ist die digitale Signatur ungültig.

Sichere Authentifizierung

Zur sicheren Authentifizierung wird der Mechanismus der digitalen Signatur verwendet, das Verfahren nennt sich „Challenge-Response-Verfahren“. Vereinfacht dargestellt läuft es so ab: die Applikation, welche sich von der (angeblichen) Identität eines Benutzers überzeugen möchte, sendet dem Klientenprogramm einen Zufallswert („Challenge“). Der Klient lässt diesen Wert von der Chipkarte verschlüsseln und sendet das Ergebnis zurück („Response“). Die Applikation entschlüsselt diese Antwort mit dem öffentlichen Schlüssel des (angeblichen) Benutzers und prüft, ob der von ihr geschickte Zufallswert herauskommt. Falls ja, wurde der Benutzer eindeutig identifiziert und damit authentifiziert.

Umgang mit der Bedienstetenchipkarte

Ihre Bediensten- Chipkarte ist nicht übertragbar. Zur Benutzung der Karte ist eine fünfstellige PIN erforderlich, die Ihnen bei der Kartenausgabe ausgehändigt wurde. Die Erst-PIN müssen Sie unverzüglich ändern. Weitere Änderungen der PIN sind jederzeit selbstständig möglich. Bei Ausscheiden aus dem Dienst der RUB ist die Karte bei der Ausgabestelle wieder zurückzugeben.
Hinweis: Sollten Daten mit einem öffentlichen Schlüssel verschlüsselt werden, ist das zugehörige Originaldokument gesondert aufzubewahren, da bei Verlust der Bedienstetenchipkarte die Daten nicht wiederhergestellt werden können.

Verlust der Bediensteten-Chipkarte

Einen Verlust der Karte müssen Sie unverzüglich bei der Ausgabestelle melden, damit Missbrauch verhindert werden kann.
Dies ist auch über die Leitwarte der RUB möglich. Die Karte und das darauf befindliche Zertifikat werden gesperrt. Im Regelfall erhalten Sie unverzüglich eine neue Bedienstetenchipkarte.
Wenn vor Ausgabe einer neuen Karte die alte wiedergefunden wird, wird ein neues Zertifikat aufgebracht.

Dienstvereinbarung zur Bediensteten-Chipkarte

Die Dienstvereinbarung zur Bediensteten-Chipkarte finden Sie im Intranet der RUB unter
www.rub.de/Bedienstetenchipkarte
Dort finden Sie auch die Information, wie Sie einsehen können, welche personenbezogenen bzw. –beziehbaren Daten über Sie im Zusammenhang mit der Nutzung der Bedienstetenchipkarte gespeichert sind. Bitte beachten Sie, dass nach Rückgabe Ihrer Bedienstetenchipkarte diese Daten nicht alle sofort gelöscht werden können. Ihre Zertifikatsdaten werden weiterhin vorgehalten, damit es möglich ist, früher von Ihnen ausgestellte digitale Signaturen zu überprüfen. Die Speicherung Ihrer Zertifikatsdaten entspricht der maximalen Gültigkeitsdauer des Zertifikats von 50 Jahren ab Datum der Ausstellung.

Ihre Kontakt-Adresse

Informationen, die für Sie im Zusammenhang mit der Nutzung der Bedienstetenchipkarte wichtig sind, werden Ihnen über Ihre RUB-eMail-Adresse oder, falls Sie es auf Ihrem Antrag entsprechend vermerkt haben, per Post an Ihre Dienstanschrift gesendet.

Ausgabestelle

Dezernat für Personalangelegenheiten, Sachgebiet 3.1, UV 2 / 271,Tel.: 25676

Leitwarte

Tel: 23333