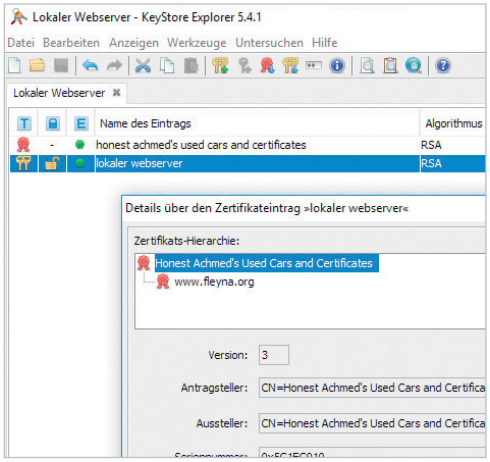
Zertifikate mit dem KeyStore Explorer bearbeiten

Schlüsselfenster



Uwe Schmidt

Kryptografische Schlüssel und Zertifikate kann man auf der Kommandozeile bearbeiten, aber auch deutlich bequemer mit dem KeyStore Explorer, der auf allen relevanten Plattformen verfügbar ist.

Die Verschlüsselung von Verbindungen über das Internet wird mehr und mehr zum Standard. Der Umgang mit den dafür benötigten Zertifikaten gehört zum Alltag. Gut, wenn der Administrator dann die entsprechenden Parameter für die Kommandozeile parat hat. Für alle anderen – oder für die, denen das einfach zu unbequem ist – gibt es den KeyStore Explorer. Als Alternative zu den Java-Tools keytools und jarsigner ermöglicht er den Umgang mit Schlüsseln und Zertifikaten auch ohne die Befehlszeile.

Der KeyStore Explorer öffnet ohne Murren JKS- und PKCS-#12-basierte Keystores und zeigt den Inhalt übersichtlich im Fenster an. Mit einem Doppelklick lassen sich die enthaltenen Schlüssel öffnen. Die Software zeigt alle relevanten Informationen wie den Verschlüsselungsalgorithmus, den Fingerprint in mehreren Hash-Varianten und das Ablaufdatum an. In weiteren Unterfenstern kann der Schlüssel als PEM oder ASN.1 angezeigt und in die Zwischenablage kopiert werden. Ein geladener Schlüsselbund lässt sich in beliebigen Formaten exportieren, ebenso wie einzelne Schlüssel.

Beim Erstellen von Schlüsseln finden RSA, DSA und elliptische Kurven Berücksichtigung. Leider lässt sich beim Generieren des Schlüssels keine zusätzliche Entropie durch Benutzerinteraktion erzeugen. Vor dem Speichern muss man den gültigen Namen eingeben, wobei ein weiteres Fenster das Eingeben der einzelnen Bestandteile des Namens wie OU (Organizational Unit), Ort oder E-Mail-Adresse unterstützt. Auch beim Signaturalgorithmus besteht eine Auswahl, da der KeyStore Explorer neben SHA-1 und SHA-2 auch RIPEMD-160 mit den jeweils üblichen Varianten sowie MD5 und MD2 kennt. Selbstverständlich kann neben der Seriennummer auch die Gültigkeitsdauer des Schlüssels eingestellt werden, die Vorgabe liegt bei einem Jahr.

Danach kann man über das Kontextmenü eine Signaturanfrage für eine CA erstellen. Die entsprechende Antwort steht zum Importieren als Datei oder aus der Zwischenablage zur Verfügung; das für die Zertifikatskette benötigte Root-Zertifikat kann ebenfalls als Datei oder über eine anwendungseigene Zwischenablage aus einem anderen Schlüsselbund kopiert werden. Soll der Schlüssel zum Authentifizieren im Internet dienen, wird er jetzt in den benötigten Formaten exportiert. Die Software fragt bei jeder Speicherung des Schlüsselrings explizit nach einem Kennwort. Wer keines vergeben will, kann die Felder leer lassen.

Beim Erstellen neuer Schlüssel oder beim Signieren eines Certificate Signing Request (CSR) kann der Anwender auch Certificate Extensions zum Schlüssel hinzufügen. Die meisten Erweiterungen nach RFC 5280 sowie die Netscape Certificate Extensions finden Berücksichtigung. Ein einmal erstellter Satz an Erweiterungen lässt sich als Template speichern, routinierte Nutzer werden dies zu schätzen wissen.

Schlüssel können aus der Anwendungsdatei heraus auch zum Signieren von JAR- und MIDlet-Dateien dienen, selbstverständlich akzeptiert der KeyStore Explorer auch die Signatur von CSR-Dateien. Wer den Aufwand nicht scheut, Basiszertifikate in seine Browser zu importieren, kann so zum Beispiel eine firmeninterne CA schaffen, ohne auf weitere Software zurückgreifen zu müssen. Auch zu Analysezwecken ist die Software gut geeignet: So kann man Dateien auf enthaltene Schlüssel oder Keystores untersuchen und deren Typ bestimmen. Diese Funktion ist auch nötig, da der Dateityp beim Importieren von Schlüsseln und Schlüsselpaaren nicht immer automatisch ermittelt wird und somit ein Import mit falschen Parametern fehlschlägt.

Auf Wunsch nimmt der Explorer direkt Kontakt mit einem Webserver auf und zeigt das entsprechende Zertifikat an. Von hier lässt es sich bei Bedarf dem geöffneten Keystore hinzufügen. Außerdem untersucht die Software optional die Zwischenablage des Gastsystems auf Schlüssel oder Zertifikate im PEM-Format (Privacy-enhanced Mail). Enthaltene Schlüssel werden angezeigt, ein direkter Import ist zurzeit jedoch nicht möglich. Unter Windows kann auch der Zertifikatsspeicher des Benutzers ausgelesen, nicht aber beschrieben werden.

Hilfreiches Werkzeug

Der KeyStore Explorer ist ein nützliches Werkzeug für alle, die regelmäßig Zertifikate handhaben müssen. Der Funktionsumfang erfüllt fast alle Wünsche, der gesamte Umgang vom Erstellen des Keystore bis zum Speichern in den gewünschten Anwendungen wird unterstützt. Einzig die Nutzung automatisierter Dienste wie Let's Encrypt fehlt, wobei das wohl bei einem Tool, das in den meisten Fällen nicht auf dem Zielsystem läuft, zu verschmerzen sein dürfte. Da die meisten Administratoren eben nicht täglich an den Zertifikaten schrauben müssen, kommt die Unterstützung sicher vielen gelegen. Der KeyStore Explorer ist Open Source und steht unter der GPL. Unter keystore-explorer.org gibt es fertige Pakete für Windows, Linux und macOS. Die Software benötigt Java ab Version 8, der Quellcode ist auf GitHub zu finden. (un@ix.de)

Uwe Schmidt

lebt und arbeitet in Hannover.