bbw-it wiki

Digitale Signaturen

Im Modul 183 behandelten Sie unter anderem das Prinzip der digitalen Signatur. Dies soll nun praktisch angewendet werden.

Für die Bearbeitung dieses Themas stehen 4 Lektionen zur Verfügung.

Zuvor aber ein paar Kontrollfragen zum Verständnis von digitalen Signaturen. Beantworten Sie die Fragen immer zuerst für sich selbst bevor Sie die Antwort überprüfen.

Kontrollfrage 1

Warum ist es nicht möglich digitale Signaturen mit symmetrischen Verschlüsselungsverfahren zu erstellen?

Bei symmetrischen Verschlüsselungen brauchen beide Kommunikationspartner den gleichen Schlüssel. Es ist also nicht möglich, auf Grund der korrekten Entschlüsselung nachzuweisen, wer die Verschlüsselung vorgenommen hat, was aber der wichtigste Aspekt der digitalen Signatur ist.

.

Kontrollfrage 2

Sie wollen ein mehrere MB grosses Dokument mit einem asymmetrischen Verfahren digital signieren. Welches Objekt wird dazu mit welchem Schlüssel verschlüsselt?

Ein Hash (SHA1 oder ähnlich) wird mit dem privaten Schlüssel des Signierers verschlüsselt und üblicherweise zusammen mit dem eigentlichen Dokument verpackt.

.

Kontrollfrage 3

Welche Schritte unternimmt der Empfänger, um die digitale Signatur zu überprüfen?

Er entschlüsselt den verschlüsselten Hash mit dem öffentlichen Schlüssel des Signierers und vergleicht diesen Hash dann mit dem aus dem dazu gehörenden Dokument erstellten Hash. Wenn diese beiden Hashes übereinstimmen, dann ist nachgewiesen, dass nur der Inhaber des zum öffentlichen Schlüssel gehörenden privaten Schlüssel als Absender in Frage kommt.

.

Kontrollfrage 4

Ist es möglich, digitale Blankounterschriften zu erstellen? Wenn ja, wie? Wenn nein, warum nicht?

Es ist nicht möglich, weil die digitale Signatur zwingend an ein Dokument gebunden ist und dieses nach der Erstellung der Signatur nicht ausgetauscht werden kann, ohne dass dies bemerkt wird.

.

Aufgabe 1

Lesen Sie das Oracle-Tutorial zum Austausch von signierten Dokumenten: https://docs.oracle.com/javase/tutorial/security/toolfilex/index.html [https://docs.oracle.com/javase/tutorial/security/toolfilex/index.html].

Erstellen Sie dann gemäss dieser Anleitung (ohne den optionalen Zusatz, Zertifizierung) ein digital signiertes Dokument. Deponieren Sie dann sowohl Ihr signiertes File als auch Ihren öffentlichen Schlüssel hier im Wiki im entsprechenden Ordner auf Ihrer Klassenseite (im persönlichen, Ihren Namen tragenden Unterordner)

Erstellen Sie auch ein File, welches zwar richtig signiert wurde, an dem aber danach Änderungen erfolgten und kopieren Sie dieses ebenfalls in den gleichen Ordner.

Versuchen Sie dann bei Dokumenten von anderen Klassenmitgliedern die Signaturen der abgelegten Dokumente zu überprüfen.

Aufgabe 2

Lesen Sie das Oracle-Tutorial über das JDK Security API: https://docs.oracle.com/javase/tutorial/security/apisign/index.html [https://docs.oracle.com/javase/tutorial/security/apisign/index.html].

Erstellen Sie dann eine kleine GUI-Applikation, in welcher man ein Datenfile und ein Schlüsselfile auswählen kann. Ausserdem kann die Option “signieren” oder “Signatur überprüfen” gewählt werden. Dann führt die Applikation die gewählte Funktion aus. Das File, welches die Signatur für ein Dokument enthält, soll den gleichen Namen haben wie das Dokument, aber mit der Extension .sig.

Kopieren Sie auch die auf diese Weise erstellten Dokumente und Signaturen ins Wiki und überprüfen Sie die Files von anderen Klassenmitgliedern.
