Q-105.165 - Signaturen und Zertifikate mit PGP und TLS/SSL

Q-105.165 - Signaturen und Zertifikate mit PGP und TLS/SSL

aus Tobit KB importiert - vom 26.01.2007 - Beitrag bei Tobit

Problem

Wie können Signaturen im David InfoCenter erzeugt werden?

Antwort

Zwei Möglichkeiten bestehen um Signaturen zu erzeugen bzw. zu verwenden:

1. **Clientbasierte Verschlüsselung (PGP)**
   Die Einbindung von Signaturen erfolgt nicht unmittelbar im David InfoCenter, sondern über PGP. Im David InfoCenter können Sie lediglich die Integration der Signatur via Button aktivieren bzw. deaktivieren.

   PGP (Pretty Good Privacy) stellt ein Verfahren zur Nachrichtenverschlüsselung und zur Erstellung so genannter digitaler Unterschriften (Signaturen) dar. Dazu verfügen der Absender und der Empfänger über jeweils zwei Code-Schlüssel. Nach der Installation von PGP auf seiner Workstation kann sich ein Anwender diese Code-Schlüssel erzeugen. Als zusätzliche Sicherheit ist hierbei ebenfalls ein besonderes Passwort zu definieren. Es wird ein geheimer Schlüssel (Private Key) und ein öffentlicher Schlüssel (Public Key) benötigt.

   Der Public Key dient zum Verschlüsseln von Nachrichten, die an Ihre eigene Adresse gesendet werden sollen. Daher ist dieser Schlüssel all denjenigen Personen zur Verfügung zu stellen, die Ihnen PGP-Nachrichten schicken wollen. Im Gegenzug müssen Sie über die Public Keys aller Personen verfügen, denen Sie verschlüsselte Nachrichten senden möchten. Public Keys können z.B. als eMail-Anhang ausgetauscht oder von speziellen Servern aus dem Internetheruntergeladen werden. Diese Schlüssel werden dann auf dem eigenen Computer vomPGP-Programm an einem so genannten Schlüsselbund (Keyring) verwaltet.

   Der Private Key dient zum Entschlüsseln von Nachrichten, die mit Ihrem Public Key verschlüsselt wurden. Geben Sie aus diesem Grund Ihren Private Key niemals heraus und bewahren Sie ihn an einem sicheren Ort auf. Mit Hilfe des Private Keys kann man außerdem eine eMail so kennzeichnen, dass sich mit dem zugehörigen Public Key überprüfen lässt, ob sie wirklich vom angegebenen Absender stammt und ob der Inhalt auf dem Übertragungsweg verändert wurde. Diese Kennzeichnung nennt man digitale Signatur.

   Der Nachrichten Editor des David InfoCenters stellt spezielle Funktionen zur Nutzung von PGP zur Verfügung. Voraussetzung hierfür ist, dass auf der entsprechenden Workstation PGP bereits installiert und korrekt eingerichtet wurde und für den entsprechenden Benutzer am Service Layer das Recht »PGP Verschlüsselung« aktiviert ist (Option »Rechte« bei der Benutzerkonfiguration).Ist dies der Fall, so enthalten die Symbolleisten im Nachrichten Editor des David InfoCenters drei zusätzliche Buttons:

   - **PGP Verschlüsseln**
     Wählen Sie diesen Button, wenn Sie die Nachricht, die aktuell im Nachrichten Editor geöffnet

ist, verschlüsselt versenden möchten. In diesem Fall wird die Verschlüsselung unmittelbar nach Betätigung des »Senden«-Buttons vorgenommen. Sie müssen natürlich über den Public Key des Empfängers verfügen, um eine PGP-Verschlüsselung durchführen zu können. Wird aus der im »An«-Feld eingetragenen Adresse ein Empfänger erkannt, dessen Public Key sich bereits am lokalen Keyring befindet, so wird dieser Schlüssel automatisch zur Verschlüsselung der Nachricht verwendet. Es erfolgt also keine weitere Abfrage. Existiert kein zur eingetragenen Empfängeradresse passender Public Key auf dem lokalen Computer, so öffnet sich direkt nach dem Betätigen des »Senden«-Buttons ein Dialogfenster, in dem alle zur Verfügung stehenden Public Keys zur Auswahlangeboten werden. Selektieren Sie hier den gewünschten Schlüssel und bestätigen Sie die Auswahl mit »OK«.

- **PGP Unterschrift**
  Über diesen Button können Sie die aktuelle Nachricht mit Ihrer digitalen Unterschrift versehen. Diese Funktion können Sie entweder in Verbindung mit der PGP-Verschlüsselung oder auch separat verwenden. Wenn Sie z.B. den Inhalt einer Nachricht nicht verschlüsseln, sondern lediglich mit Ihrer Signatur versehen möchten, so aktivieren Sie diesen Button und deaktivierenb Sie den »PGP Verschlüsseln«-Button. Sobald Sie eine zu signierende Nachricht zum Versand freigeben, werden Sie in einem separaten Dialogfenster zur Eingabe Ihres PGP-Passwortes aufgefordert, mit dem Sie sich identifizieren. Ist das angegebene Passwort nicht korrekt, kann keine Signatur stattfinden.
- **PGP Entschlüsseln**
  Dieser Button ermöglicht das Entschlüsseln empfangener PGP-codierter Nachrichten. Bitte beachten Sie, dass Sie ausschließlich Nachrichten entschlüsseln können, die mit Ihrem Public Key verschlüsselt wurden. Klicken Sie auf diesen Button, um die Entschlüsselung der aktuell geöffnetenNachricht zu veranlassen. Daraufhin werden Sie aufgefordert, Ihr PGP-Passwort einzugeben.

  Ein Entschlüsseln der Nachricht findet nur statt, wenn die Angabe dieses Passwortes korrekt ist. Die Entschlüsselung geschieht ausschließlich temporär. Im Tobit Archive System auf dem Server bleibt die entsprechende Datei in codierter Form erhalten. Das bedeutet, dass die Nachricht bei jedem Öffnen erneut entschlüsselt werden muss, also jedes Mal erneut das Passwort eingegebenwerden muss. Wenn Sie wünschen, dass direkt beim Öffnen von PGP-verschlüsselten Nachrichten der Entschlüsselungsdialog erscheint, ohne zuvor den »PGP Entschlüsseln«-Button drücken zu müssen, stellen Sie sicher, dass in der Konfiguration des David InfoCenters unterhalb von »Optionen-> Einstellungen -> Ansicht« die Option »Nachrichten beim Öffnen entschlüsseln«aktiviert ist.

Bei PGP findet die gesamte Ver- und Entschlüsselung auf der Arbeitsstation selbst statt. PGP-verschlüsselte Nachrichten werden generell auch in verschlüsselter Form im Archive-System auf dem Server, z.B. in den Eingangs- und Ausgangs-Archives der Benutzer, abgelegt. Ohne den passenden Private Key ist also keinerlei Zugriff auf die enthaltene Information möglich. Daher können diese Nachrichten auch über nicht gesicherte Leitungen bzw. Verbindungenversendet werden, ohne unbefugten Zugriff auf die Daten befürchten zu müssen.

2. **TLS-Zertifikat-Generator**
   Des Weiteren ist es möglich eine serverbasierte Signatur zu hinterlegen. Dies ist nicht nur für den eMail Transfer geeignet, sondern auch für den MailAccess Server und für die WebBox.

   Das Programm TLSCERT.EXE (Verzeichnis »DAVID\UTIL\WINDOWS\TLSCERT«) dient zur Erstellung von Zertifikat-Requests oder von selbstsignierten Zertifikaten für die Transport-Layer-Security-Dienste (TLS-Dienste) ab David 6.6. TLS kann bei den eMail Diensten, bei den Web Server Diensten und beim Mail Access eingesetzt werden.

   Um eine Übertragung von Nachrichten über eine sichere Verbindung zu gewährleisten, muss sowohl der Absender als auch der Empfänger über ein so genanntes Zertifikat verfügen, das ihn eindeutig

identifiziert.

- **Certificate Type**
  Geben Sie an, ob Sie ein selbstsigniertes Zertifikat oder ein Zertifikat-Request erzeugen wollen. Ein selbstsigniertes Zertifikat wird vollständig selbst erzeugt und bietet keine zusätzliche Kontrollmöglichkeit. Bei einem Zertifikat-Request werden Dateien erzeugt, mit denen bei einer so genannten Certification Authority (wie z.B. VeriSign oder Thawte) ein Zertifikat beantragtwerden kann. Bei Zweifeln an einem Zertifikat kann in diesem Falle die Echtheit durch eine Nachfrage an die Certification Authority überprüft werden.
- **Key Length**Bestimmen Sie den Grad der Verschlüsselung in Bits. Sinnvoll sind Werte zwischen 512 und 4096. Werte kleiner als 512 gelten als unsicher. Am häufigsten verwendet wird der Wert 1024.
  Generell gilt: Je größer die Key Length ist, desto größer ist die Sicherheit.
- **Distinguished Name**
  Tragen Sie hier alle für das Zertifikat erforderlichen Daten ein.
- **Country Name**
  Schreiben Sie in dieses Feld den zweistelligen Ländercode Ihres Landes (z.B. DE für Deutschland, US für USA etc.).
- **State or Province Name**
  Tragen Sie hier den Namen Ihres Landes bzw. Bundesstaates ein.
- **Locality Name**
  In dieses Feld ist der Name Ihrer Stadt einzutragen.
- **Organization Name**
  Fügen Sie in dieses Feld den Namen Ihrer Firma ein.
- **Organizational Unit Name**
  Hier wird der Name Ihrer Abteilung innerhalb Ihrer Firma erwartet.
- **Common Name**
  Tragen Sie hier den Host Namen des Servers ein, für den das Zertifikat verwendet werden soll. Dieser Name kann auch Wildcards wie z.B. *.example.com enthalten, was allerdings mit erhöhten Kosten verbunden ist, falls ein gesichertes Zertifikat bei einer Certification Authority beantragt wird.
- **eMail Address**
  Geben Sie hier eine eMail-Adresse an, an die bei Zweifeln an der Echtheit des Zertifikats Rückfragen gerichtet werden können.
- **Optional Extra Attributes**
  Abhängig von der Art des zu erzeugenden Zertifikats sind hier zusätzliche Angaben zu treffen.
- **Valid Days**
  Dient zur Festlegung der Gültigkeitsdauer bei selbstsignierten Zertifikaten.
- **Common Name**
  In den meisten Fällen ist derselbe Wert anzugeben, der auch als Common Name unterhalb von Distinguished Name eingetragen wurde.
- **Challenge Password**
  Dient zur zusätzlichen Sicherheit und wird bei Zertifikat-Requests an die Certification Authority übertragen. Bevor diese ein Zertifikat erteilt, muss dieses Passwort dann nochmals bestätigt werden.

Nachdem Sie alle erforderlichen Daten angegeben haben, klicken Sie auf den Generate-Button, um den Zertifikat-Request bzw. das selbstsignierte Zertifikat erzeugen zu lassen. Bei einem selbstsignierten Zertifikat wird eine Datei erzeugt, die unter dem Namen RXCERT.PEM (für den Empfang) und/oder unterdem Namen TXCERT.PEM (für den Versand von Nachrichten über eine gesicherte Verbindung) in das Verzeichnis »DAVID\APPS\POSTMAN\CODE« des DavidServers kopiert werden muss.

Bei einem Zertifikat-Request werden zwei Dateien erzeugt, wobei die eine den Schlüssel und die andere den Zertifikat-Request enthält. Der Zertifikat-Requestist an eine Zertifizierungsstelle (wie z.B. VeriSign oder Thawte) zu übertragen. Das geschieht üblicherweise über das WWW oder per eMail.

Sie erhalten daraufhin ein entsprechendes Zertifikat, dessen Inhalt Sie in die erste vom TLS-Zertifikat-Generator erzeugte Datei unterhalb des Schlüssels kopieren. Speichern Sie anschließend diese Datei unter dem Namen RXCERT.PEM (für den Empfang) und/oder unter dem Namen TXCERT.PEM (für den Versand von Nachrichten über eine gesicherte Verbindung) in dem Verzeichnis »DAVID\APPS\POSTMAN\CODE« auf dem David Server ab.

Für den gesicherten Zugriff zwischen der WebBox und einem Browser speichern Sie diese Datei unter dem Namen WBCERT.PEM im Verzeichnis »DAVID\APPS\WEBBOX\CODE«.

Um TLS Verbindungen auch beim Mail Access über den Mail Access Server nutzen zu können, speichern Sie die Datei unter dem Namen MACERT.PEM im Verzeichnis »DAVID\APPS\MASERVER\CODE« ab.

Hinweis
Beim Einsatz unter Linux dürfen zur Benennung der Zertifikat-Dateien ausschließlich Kleinbuchstaben verwendet werden. Hier müssen die Dateinamen also folgendermaßen aussehen:

- rxcert.pem
- txcert.pem
- wbcert.pem
- macert.pem