Q-107.824 - Datensicherheit (z.B. S/MIME) beim Versand und Empfang von Nachrichten

Inhaltsverzeichnis

- 1 Problem
- 2 Antwort

1 Problem

Bei der eMail-Kommunikation bekommt das Thema Datensicherheit immer mehr Bedeutung. Besonders der Nachrichtenversand mit falschem Absender ist eine der Ursachen für die schnelle und globale Ausbreitung von Viren und Spam. So wird nach Lösungen gesucht, eindeutig festzustellen, ob eine eMail tatsächlich vom angegebenen Absender stammt. Hier ist das digitale Signieren von Nachrichten eine Möglichkeit.

Um eine Nachricht digital zu signieren bzw. zu verschlüsseln unterstützt das David InfoCenter die zwei verbreitetsten Verfahren: PGP und S/MIME.

2 Antwort

Das David InfoCenter unterstützt sowohl das Signieren als auch das Ver- und Entschlüsseln von Nachrichten. Das Ver- und Entschlüsseln mit PGP wird auch mit älteren David Versionen unterstützt. Die digitale Signatur (S/MIME) im David InfoCenter steht Ihnen aber erst ab David V8+ zur Verfügung.

Digital signieren und verschlüsseln

Um eine Nachricht digital zu signieren bzw. zu verschlüsseln, wird in den meisten Fällen eine so genannte asymmetrische Kodierung verwendet. Nach dem Erstellen eines Kodierschlüsselpaars - bestehend aus einem privaten und einem öffentlichen Schlüssel - wird die Nachricht mit dem einen Schlüssel kodiert und vom Empfänger mit dem anderen Schlüssel wieder dekodiert. Die beiden Schlüssel gehören zwar zusammen, können jedoch nicht voneinander abgeleitet werden. Der private Schlüssel wird vor allem zur Dekodierung und Signierung, der öffentliche Schlüssel zur Kodierung und Verifizierung einer Signatur verwendet. Deshalb ist der private Schlüssel allein in der Hand des Besitzers, der öffentliche Schlüssel kann frei verfügbar gemacht werden (z.B. auf der Website oder auf Schlüsselservern).

PGP

- PGP steht für Pretty Good Privacy und bezeichnet eine Methode zur Verschlüsselung und Signatur von eMail-Nachrichten. Dazu können Sie das Programm PGP von Network Associates Inc. oder das frei verfügbare GnuPG verwenden. In den aktuellen Versionen sind die Programme kompatibel zueinander, d.h., mit PGP verschlüsselte Daten können mit GnuPG entschlüsselt werden und umgekehrt.

Zur Signatur bzw. Verschlüsselung von Nachrichten und Texten wird ein Schlüsselpaar verwendet, das aus einem privaten und einem öffentlichen Schlüssel besteht. Mit dem öffentlichen Schlüssel des Empfängers kodieren Sie die an ihn adressierten eMails. Der Empfänger wiederum verwendet seinen privaten Schlüssel, um die Nachricht wieder zu decodieren. Deshalb ist es entscheidend, seinen privaten Schlüssel für niemanden zugänglich aufzubewahren. Das Schlüsselpaar wird mithilfe der eingesetzten Software (z.B. GnuPG) erstellt.

Öffentlichen PGP-Schlüssel versenden

Wie kommt man nun in den Besitz des öffentlichen Empfängerschlüssels? Am besten lassen Sie ihn sich vom Besitzer selbst zusenden. Dazu muss er ihn aus seiner PGP-Software exportieren und per eMail-Anhang an Sie versenden. Sie wiederum importieren diesen eMail-Anhang innerhalb Ihrer PGP-Software, worauf er Ihnen im David InfoCenter zur Verfügung steht. So können Sie sicher sein, dass es sich um einen Originalschlüssel handelt. Alternativ werden öffentliche Schlüssel auf so genannten Schlüsselservern bereitgestellt (z.B. hkp://sks.keyserver.penguin.de).

Sie selber sollten also jedem, mit dem Sie verschlüsselte oder signierte Nachrichten austauschen möchten, Ihren öffentlichen Schlüssel zur Verfügung stellen.**S/MIME**

- Die zweite vom David InfoCenter unterstützte Verschlüsselungsmethode ist S/MIME. Diese Abkürzung steht für Secure/Multipurpose Internet Mail Extension und basiert auf der RSA Public-Key Encryption Technologie.

S/MIME basiert auf einem zertifizierten Schlüsselpaar, das zunächst bei einer Zertifizierungsstelle beantragt werden muss. Man unterscheidet je nach Authentifizierungsaufwand verschiedene Zertifikatsklassen, wobei eine Class-1-Zertifizierung lediglich das Vorhandensein einer funktionierenden eMail-Adresse bestätigt, wohingegen z.B. die Class-3-Zertifizierung auf einer persönlichen Identitätsprüfung anhand von Personaldokumenten basiert.

Öffentlichen S/MIME-Schlüssel versenden und importieren

Um jemandem seinen öffentlichen S/MIME-Schlüssel zukommen zu lassen, schicken Sie ihm einfach eine digital signierte eMail. Dadurch wird gleichzeitig Ihr öffentlicher Schlüssel mitversendet.

Wenn Sie einen empfangenen öffentlichen Schlüssel in Ihr System integrieren möchten, verfahren Sie wie folgt:

1. Öffnen Sie mit einem Doppelklick die signierte eMail im Viewer.
2. Klicken Sie auf das Symbol »Zertifikat anzeigen/installieren«. Es öffnet sich das Dialogfenster »Zertifikat«.
3. Klicken Sie die Schaltfläche »Zertifikat installieren...« an und folgen Sie den Anweisungen des Zertifikatsimport-Assistenten.
4. Zum Abschluss erscheint die Meldung »Der Import war erfolgreich«. Sie können das Zertifikat nun verwenden, um verschlüsselte Nachrichten an den Zertifikatsbesitzer zu senden. Sie finden das gerade importierte Zertifikat unter Start -> Einstellungen -> Systemsteuerung -> Internetoptionen -> Registerkarte »Inhalt« -> Schaltfläche »Zertifikate...« -> Registerkarte »Andere Personen«.

Weitere Informationen zu dem Thema »PGP« erhalten Sie im **KnowledgeBase Artikel 103.167**.

Weitere Informationen zu dem Thema »Einstellungen zur Nutzung der Digitalen Signatur im David InfoCenter« erhalten Sie im **KnowledgeBase Artikel 107.680**.

Quelle: Tobit · 8.06.2006