Q-109.931 - Anforderung digitaler Signaturzertifikate im David Client

Q-109.931 - Anforderung digitaler Signaturzertifikate im David Client

aus Tobit KB importiert - vom 10.12.2009 - Beitrag bei Tobit

Problem

Zur Sicherstellung der Authentizität Ihrer eMails lassen sich in David.fx digitale Signaturen bestellen. Dadurch können Benutzer, für deren eMail-Adressen digitale Signaturen (S/MIME-Zertifikate) vorliegen, eMails digital signieren und optional verschlüsseln. Wie können digitale Signaturen in David.fx angefordert werden und was ist dabei zu beachten?

Antwort

David.fx bietet Ihnen umfangreiche Funktionen für den Einsatz digitaler Signaturen. Dazu wurde das Signaturprodukt »SIGNTRUST CERT« von Signtrust, dem akkreditierten Trustcenter der Deutschen Post, nahtlos integriert. Auf diese Weise haben Sie die Möglichkeit, mit minimalem formalen, zeitlichen und finanziellen Aufwand persönliche S/MIME-Zertifikate der Klasse 2 für David Benutzer anzufordern und in Ihr System einzubinden.

Hinweise:
Zertifikate der Klasse 2 bieten eine hohe Sicherheit und besitzen rechtliche Gültigkeit. Bei Beantragung dieser Zertifikate findet neben der eMail-Überprüfung eine einfache Identitätsfeststellung statt. Im Fall der Signaturzertifikate von David.fx erfolgt diese Identitätsfeststellung per Einschreiben auf dem Postweg.

Die Bereitstellung der S/MIME-Signaturzertifikate ist kostenpflichtig. Die anfallenden Kosten werden über das TSSM (Tobit.Software Site Management) im Tobit.NET abgerechnet.

Voraussetzungen für den Einsatz der Signaturzertifikate

Um den Einsatz und die Anforderungen von Signaturzertifikaten generell zu ermöglichen bzw. zu erlauben, müssen folgende Einstellungen vorgenommen werden:

2. Öffnen Sie auf Ihrem David Server den David.Administrator, markieren Sie im Konfigurationsbaum auf der linken Seite den Punkt »System« mit der rechten Maustaste und wählen Sie aus dem Kontextmenü den Eintrag »Konfigurieren«.
3. Wechseln Sie auf die Registerkarte »Sicherheit« und aktivieren Sie die Option »S/MIME-Signatur global erlauben« sowie optional die Option »S/MIME-Verschlüsselung global erlauben«.

Bestätigen Sie Ihre Änderung durch einen Klick auf »OK«. Wechseln Sie im Konfigurationsbaum in den Bereich »System > Benutzer«. Öffnen Sie die Einstellungen derjenigen Benutzer, die die Option zum Anfordern von Signaturen haben sollen, und wechseln Sie auf die Registerkarte »Rechte«. Aktivieren Sie die Option »S/MIME Signatur nutzen« sowie optional die Option »S/MIME Verschlüsselung nutzen«.

Empfehlung:
Durch Aktivierung der Option »Zertifikate auch beim Remote Access verwenden« stellen Sie sicher, dass die angeforderten S/MIME-Zertifikate ausschließlich zentral auf dem David Server gespeichert werden und dem

David Benutzer somit bei Nutzung des David Client generell, also unabhängig von der Arbeitsstation, bei der er sich gerade befindet, zur Verfügung stehen.

Andernfalls werden die angeforderten Zertifikate nur im Windows Zertifikatsspeicher der lokalen Arbeitsstation gespeichert und sind lediglich an diesem Computer nutzbar.

Bestätigen Sie Ihre Änderung durch einen Klick auf »OK«. Den betreffenden David Benutzern steht nun nach einem Neustart des David Client die Option zur Anforderung digitaler Signaturen zur Verfügung.

Anforderung digitaler Signaturzertifikate im David Client

Gehen Sie folgendermaßen vor, um digitale Signaturen (S/MIME-Zertifikate) direkt im David Client anzufordern:

2. Am unteren Rand des David Client Hauptfensters befindet sich eine Schaltfläche, die den Benutzernamen sowie ein Siegel-Symbol als Aufschrift trägt. Ein Klick mit der linken Maustaste auf diesen Button führt direkt zum Bestellvorgang für David Signaturzertifikate sowie zu deren Verwaltung.

   Daraufhin wird im David Client eine Portalseite angezeigt, in der Sie Informationen zum Einsatz von David Signaturzertifikaten finden. Verfügen Sie bereits über gültige S/MIME-Zertifikate, die korrekt in das System eingebunden sind, werden diese hier aufgeführt.

3. Klicken Sie auf die Schaltfläche »Signatur anfordern«, um ein neues S/MIME-Zertifikat für eine eMail-Adresse zu bestellen, und folgen Sie den Anweisungen des Bestellassistenten:

   Hinweis:
   Für jede eMail-Adresse kann nur ein S/MIME-Signaturzertifikat angefordert werden.

4. Nach Abschluss des Bestellvorgangs wird auf dem David Server im Verzeichnis »\DAVID\CODE\CERT\REQUESTS\« eine »REQ«-Datei erzeugt. Deren Dateiname besteht aus der eMail-Adresse, für die Sie das Zertifikat angefordert haben, und der Dateiendung ».REQ«, z.B. » LEO.BENZ@EXAMPLE.NET.REQ«. Diese Datei ist der private Schlüssel bzw. »private key« des angeforderten S/MIME-Zertifikats.
5. Außerdem erhält der betreffende David Benutzer per Post ein Einschreiben mit seinem persönlichen Authentisierungscode. Erst nach Eintreffen dieses Einschreibens kann das Signaturzertifikat aktiviert und anschließend auch genutzt werden.

Aktivierung von Signaturzertifikaten

Nach Erhalt des persönlichen Einschreibens können Sie das Zertifikat durch Eintragen des zugehörigen Authentisierungscodes aktivieren. Gehen Sie dazu folgendermaßen vor:

2. Stellen Sie sicher, dass Sie als der Benutzer angemeldet sind, für den das Zertifikat bestellt wurde.
3. Öffnen Sie den David Client und klicken Sie auf die Schaltfläche, über die Sie die Signatur angefordert haben (Button mit Benutzername und Siegel-Symbol am unteren Rand des David Client).
4. Tragen Sie in das zugehörige Eingabefeld den Authentisierungscode ein und klicken Sie auf »Übernehmen«.

In der Regel erhält der David Benutzer nun innerhalb von 24 Stunden eine eMail mit dem Betreff »Ihre digitale Signatur«. Klicken Sie in dieser eMail auf den Link mit dem Titel »Signaturzertifikat einbinden«.

Es öffnet sich ein Dialogfenster, das eine Zusammenfassung aller Informationen zum Zertifikat zeigt. Zusätzlich ermöglicht die Option »Ausgehende Nachrichten digital signieren« zu entscheiden, ob die digitale Signatur zukünftig generell aktiviert sein soll, oder nicht. Wenn Sie diese Funktion deaktivieren, müssen Sie die Signatur, falls gewünscht, beim Nachrichtenversand manuell aktivieren.

Klicken Sie auf »Ja«, um das Zertifikat zu installieren. Dadurch wird aus dem öffentlichen Schlüssel (»public key«) im Anhang der eMail (»P7B«-Datei, z.B. »LEO.BENZ@EXAMPLE.NET.P7B«) und dem privaten Schlüssel (»private key«, siehe oben) das S/MIME-Zertifikat des David Benutzers generiert und abhängig von der Einstellung »Zertifikate auch beim Remote Access verwenden« (siehe oben unter »Voraussetzungen für den Einsatz der Signaturzertifikate«) entweder im Windows Zertifikatsspeicher der lokalen Arbeitsstation oder zentral auf dem David Server gespeichert. Der David Benutzer kann fortan das angeforderte S/MIME Zertifikat zum Signieren und Verschlüsseln von eMails verwenden. Je nach Wahl der Einstellung »Ausgehende Nachrichten digital signieren« bei der Installation des Zertifikats (s.o.) ist nun die Nachrichtenoption »Nachricht mit S/MIME digital signieren« beim Verfassen von eMails generell aktiv oder inaktiv.

Sie haben aber dennoch die Möglichkeit, für jeden Sendeauftrag individuell zu entscheiden, ob dieser signiert werden soll, indem Sie die Funktion »Digital signieren« in der Symbolleiste des Nachrichten-Editors manuell aktivieren bzw. deaktivieren.

Falls gewünscht, können Sie auch die bei der Installation des Zertifikats gewählte generelle Voreinstellung nachträglich ändern. Rufen Sie dazu im David Client den Hauptmenüpunkt »Optionen > Einstellungen > Sicherheit« auf und aktivieren bzw. deaktivieren Sie die Option »Nachrichten digitale Signatur hinzufügen«. Bestätigen Sie anschließend Ihre Einstellung durch einen Klick auf »OK«.

Hinweis:
Das Zertifikat gilt ausschließlich für die Absender-eMail-Adresse, die im Bestellassistenten angegeben wurde.

Weiterführende Informationen:

- Sichern und Wiederherstellen von S/MIME-Zertifikaten