27. Jänner 2003 Artikel · Digitale Identität · Privatsphäre & Krypto

SMIME Mail Container

Archiviert. Dieser Inhalt wird nicht mehr aktualisiert. Er bleibt zur Information verfügbar.

Quelle https://technology2.a-sit.at/veroeffentlichungen/smime-mail-container/

Mit Hilfe dieses einfachen Java Tools können beliebige Inhalte signiert und/oder verschlüsselt in einen S/MIME Container verpackt und als *.EML File abgelegt werden. *.EML Files lassen sich direkt mit Netscape oder Outlook Express öffnen und Signatur und/oder Verschlüsselungszertifikate können überprüft werden.

Nähere Informationen

Bevor signierte und/oder verschlüsselte S/MIME Container erzeugt werden können, müssen erst Signatur- und Verschlüsselungs-Zertifikate geladen werden. Gültige Signatur-Zertifikate sind PKCS#12 Zertifikate mit den File-Extensions *.PFX oder *.P12

Gültige Verschlüsselungszertifikate sind PKCS#7 Zertifikate mit den File-Extensions *.P7C *.P7B oder DER-codierte Zertifikate mit den Erweiterungen *.DER oder *.CER

Wichtig!

Es findet keine Überprüfung der Zertifikate auf Gültigkeit/Widerruf oder Verwendungszweck statt; d.h. es kann jedes Zertifikat verwendet werden, dessen Schlüssel einem geeigneten Signatur/Verschlüsselungsalgorithmus genügt.

Ist die Option „Detached Signature“ ausgewählt und soll die Nachricht signiert werden („Sign Mail“ ausgewählt), so wird eine S/MIME-Nachricht vom Typ „multipart/signed“ erzeugt, die sich aus zwei Teilen zusammensetzt: der erste Teil liefert den eigentlichen Inhalt und der zweite Teil enthält die Signatur. Ist jedoch die Option „Detached Signatur“ nicht ausgewählt, so wird der Dateninhalt gleich in die Signatur miteingepackt. In diesem Fall besteht die S/MIME-Nachricht (Typ „application/pkcs7-mime) nur aus einem Teil. Der Vorteil der ersten Methode liegt darin, dass der Inhalt der Nachricht auch von einem Mail-Programm gelesen werden kann, das über keine S/MIME-Funktionalität verfügt. Aus diesem Grund ist der Typ „multipart/signed“ auch die bevorzugte Wahl für das Signieren einer Nachricht („Detached Signature“ ist per default ausgewählt). Wird die Nachricht jedoch zusätzlich noch verschlüsselt (Option „Encrypt Mail“ ausgewählt), so ist es nicht von Belang, welcher Typ zum Signieren der Nachricht verwendet wird, da der

gesamte Signatur-Teil in diesem Fall noch in ein „Verschlüsselungspaket“ eingepackt wird, das vom Empfänger zunächst geöffnet weden muss — das heisst, der E-Mail Client des Empfängers muss ohnehin S/MIME unterstützen.

Die Felder „Subject“, „Content“ können nun manuell befüllt werden — oder man verwendet den „Automatic Fill“ Button, um sie automatisch mit Informationen zu belegen, die entsprechend den ausgewählten Signier/Verschlüsselungs-Optionen Auskunft über die kryptographischen Beschaffenheit der zu erzeugenden S/MIME Nachricht geben (siehe Abbildung). Über das Feld „Attachment“ kann eine Datei geladen werden, die der Nachricht als Attachment hinzugefügt werden soll.

Mit „Create/Store“ kann nun der Inhalt der eben zusammengestellten Mail als *.EML File abgelegt werden. Dieser *.EML File lässt sich mit den meisten gängigen Mail Clients öffnen und die Zertifikate können geprüft werden (hier am Beispiel von „Outlook Express“):

Dieses Tool steht nicht mehr zum Download bereit.