E-Mail-Sicherheit

- E-Mails werden ohne weitere Maßnahmen im Klartext versendet.
- Der Inhalt kann dann von anderen Personen eingesehen und verändert werden.

E-Mail-Verschlüsselung

- E-Mails mit Inhalten, die nur von berechtigten Personen gelesen werden dürfen, müssen verschlüsselt werden! Diese Verschlüsselung geschieht mit Hilfe von S/MIME.
- Verschlüsselung ist mit allen weit verbreiteten E-Mail-Clients möglich.

Digitale Signatur bei E-Mails

- Mit Hilfe der digitalen Signatur kann eindeutig festgestellt werden, ob ein E-Mail während des Transports verändert wurde. Die Signatur erlaubt eine Identifikation des Absenders/der Absenderin.
- Signaturen können ebenfalls mit Hilfe von S/MIME erstellt werden.
- Digitale Signatur ist mit allen gängigen E-Mail-Clients möglich.

Für weitere Informationen zu signierten E-Mails bieten A-SIT und das Bundeskanzleramt den E-Government Flyer Nr. 204 an:

„Elektronische Signatur und E-MAIL“

Qualifizierte Signatur und E-Mail

- Bei der Signatur von E-Mails wird nur der eigentliche E-Mail-Text gesichert. Kopfzeilen - das beinhaltet auch die Betreff-Zeile oder die Absenderadresse - werden nicht mitsigniert.
- Da also Teile des E-Mails nicht signiert werden, werden auch keine qualifizierten Signaturen im Sinne des Signaturgesetzes als Äquivalen der handschriftlichen Unterschrift angeboten.
- Ebenso bleiben die Kopfzeilen bei verschlüsselten E-Mails unverschlüsselt (z.B. auch die Betreff-Zeile).

Was ist MIME?

- MIME (Multi Purpose Internet Mail Extension) ist ein Standard, nach dem beliebige Daten (Dateien, Bilder, etc.) in das Textformat von E-Mail konvertiert und so per E-Mail übertragen werden können.
- Alle gängigen E-Mail-Clients unterstützen MIME: z.B. Thunderbird, Outlook, Lotus Notes.

Was ist S/MIME?

- Secure/MIME (S/MIME) ist eine Erweiterung von MIME.
- S/MIME ermöglicht es, E-Mails zu verschlüsseln und/oder digital zu signieren.
- Der kryptographische Teil einer S/MIME-Nachricht basiert auf dem Standard PKCS#7. Mit Hilfe dieses Standards werden Container für mit S/MIME verschlüsselte oder signierte Nachrichten erzeugt.

Gängige Containerarten werden in Folge erklärt.

S/MIME Container - Signatur

- **application/pkcs7-mime - signed data**: Die Daten und die Signatur werden in diesem Fall in einem Container kombiniert. Die Nachricht kann nur von S/MIME fähigen E-Mail-Clients gelesen werden.
- **multipart/signed:** Die Nachricht und die dazugehörige Signatur werden getrennt. Dies hat den Vorteil, dass die Nachricht auch von E-Mail-Clients, die S/MIME nicht unterstützen, gelesen werden kann. Die Signatur kann aber von solchen Clients nicht verifiziert werden. Ein Nachteil bei diesem Format ist, dass mögliche Änderungen der E-Mail-Struktur (z.B. durch Mailserver) die Signatur nicht mehr verifizierbar machen.

S/MIME Container - Verschlüsselung

- **application/pkcs7-mime - enveloped data**:
  Die verschlüsselten Daten und die notwendigen symmetrischen Schlüssel werden in diesem Container zusammengefasst.

S/MIME Container - Signatur und Verschlüsselung

- In diesem Fall wird die Nachricht zuerst mit der digitalen Signatur versehen und in ein **application/pkcs7-mime - signed data** Objekt eingebunden.

  Dieser Container wird dann verschlüsselt und in ein **application/pkcs7-mime - enveloped data** Objekt eingebunden.

S/MIME und Mozilla Thunderbird bzw. Microsoft Outlook

- Symbole im E-Mail Client zeigen an, ob ein empfangenes E-Mail digital signiert und/oder verschlüsselt wurde. Anhand der Symbole ist auch die Gültigkeit der digitalen Signatur erkennbar.
- **Microsoft Outlook**:  Das linke Symbol zeigt, dass die Nachricht verschlüsselt ist. Das rechte Symbol zeigt dass die Nachricht über eine gültige Signatur verfügt.
- **Mozilla Thunderbird**:  Das untere Symbol zeigt, dass die empfangene Nachricht verschlüsselt ist. Eine gültige Signatur wird durch das obere Symbol angezeigt.
- Signierte Mails, die über eine ungültige Signatur verfügen, werden über die folgenden Symbole angezeigt: Bei Outlook:  und bei Thunderbird: 
- Durch Doppelklicken der Symbole werden weitere Details zur Signatur/Verschlüsselung angezeigt.
- Ein Fehlen des Verschlüsselungssymbols bedeutet, dass die Nachricht nicht verschlüsselt wurde. Ein Fehlen des Signatursymbols bedeutet, dass die Nachricht nicht digital signiert wurde. Die Symbole für fehlerhafte Signaturen treten dann auf, wenn die Nachricht signiert wurde, die Signatur aber ungültig ist.
- Details zum verwendeten Container können im E-Mail-Header abgerufen werden. Bei Thunderbird geschieht das über das Menü Anzeige/ Kopfzeile/Alles und bei Outlook über Ansicht/ Optionen/Internetkopfzeilen.

Achten Sie auf den Signatur- bzw. Verschlüsselungsstatus des E-Mails! Eine Nachricht mit fehlerhafter oder fehlender Signatur könnte manipuliert, ein unverschlüsseltes E-Mail gelesen worden sein.

Wichtige Hinweise

- Verschlüsselte S/MIME-Nachrichten werden vom E-Mail-Client typisch auch verschlüsselt gespeichert. **Wenn der zur Entschlüsselung notwendige Schlüssel verloren geht, kann die Nachricht nicht mehr gelesen werden!**
- Verschlüsselte Nachrichten können von Mailservern nicht auf Viren überprüft werden, da die Server nicht in der Lage sind die Nachrichten zu entschlüsseln. Dateien von verschlüsselten Nachrichten sollten vom lokalen Virenscanner Ihres PCs/Laptops überprüft werden, bevor sie geöffnet werden.

Tools zu S/MIME Containern

A-SIT bietet ein Tool an, mit dem Sie **S/MIME-Container erstellen** können:
http://demo.a-sit.at/it_sicherheit/smime_mailcontainer

- Dieses Tool erlaubt es, Inhalte in Form von signierten oder verschlüsselten S/MIME-Containern abzulegen.
- Die angelegten Container können von jedem S/MIME fähigen E-Mail-Client geöffnet werden.

Zum **Testen der Kompatibilität** Ihres E-Mail-Clients mit typischen S/MIME-Containern bietet A-SIT ein weiteres Tool an:
http://demo.a-sit.at/it_sicherheit/mail_check

- Dieses Tool versendet E-Mails in verschiedenen S/MIME-Formaten an eine angegebene E-Mail-Adresse. Anhand des Verhaltens des E-Mail-Clients kann bestimmt werden, welche S/MIME Formate vom Client unterstützt werden und ob sie vom Client korrekt behandelt werden.

Fragen

Senden Sie ein E-Mail an: technology@a-sit.at

Zentrum für sichere Informationstechnologie - Austria
A-SIT
Secure Information Technology Center - Austria

E-Mail-Sicherheit und S/MIME

E-Government Flyer Nr.205

DIGITALES ÖSTERREICH

Verschlüsselung und elektronische Signatur bei E-Mails mit S/MIME

- Sicherheit von E-Mails
- Verschlüsselung von E-Mails
- Digitale Signatur bei E-Mails
- Qualifizierte Signatur und E-Mail
- MIME und S/MIME
- Testen Sie die Kompatibilität