22. August 2008 Studie · Privatsphäre & Krypto

Mail Test

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

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

Ein Tool zum Test des Umgangs von E-Mail Clients mit verschiedenen Arten von E-Mails

Standard-Mailclients zeigen oft unterschiedliches Verhalten bei verschlüsselten oder signierten Mails.

Dieses Service erzeugt eine Vielzahl unterschiedlicher Testmails und sendet Sie an einen bestimmten Empfänger. Testen Sie Ihren Mailclient, ob dieser Abweichungen vom Sollverhalten zeigt. Um Missbrauch durch Versendung von Massen-Mails zu verhindern, ist eine Anmeldung erforderlich.

Anfragen bitte an mailtest@a-sit.at.

Links

MailServlet (service nicht mehr verfügbar)

Zweck des Testmailservice

Dieses Service ist in der Lage, eine Vielzahl unterschiedlicher Testmails zu erzeugen. Dabei können verschlüsselte, signierte und klartextliche Mails erzeugt und an einen bestimmten Empfänger gesendet werden. Da nicht zu erwarten ist, dass alle Standard Mailclients auch auf alle mit Hilfe dieses Dienstes erzeugten Mails einwandfrei reagieren, kann dieses Testmailservice dazu verwendet werden, Abweichungen vom Sollverhalten festzustellen. Hierzu besteht einerseits die Möglichkeit frei definierte Mails zu erzeugen und andererseits auf ein Set von vordefinierten Mails zurückzugreifen. Dieses Dokument beschreibt, wie das Set aus vordefinierten Standardmails vom Mailclient mindestens behandelt werden muss. Auf keinen Fall darf auch nur eine dieser Standardmails zu einem Fehler oder gar zum Stillstand des Mailsystems führen.

Die Standardmails werden mit dem Button Send the precompiled set of testmails aktiviert. Um auch verschlüsselte Standardmails erzeugen zu können, muss das Verschlüsselungszertifikat des Empfängers über das Menü geladen werden. Sollte noch kein solches Zertifikat verfügbar sein, so muss erst ein geeignetes Zertifikat anhand der im Dokument “Zertifikatsrequest” beschriebenen Schritte besorgt

werden. (Geeignete Zertifikate sind Zertifikate im *.p7c *.cer oder *.der Format). Geladen werden diese Zertifikate durch die Wahl des entsprechenden Zertifikatfiles und durch Drücken des Buttons “Load Certificate”

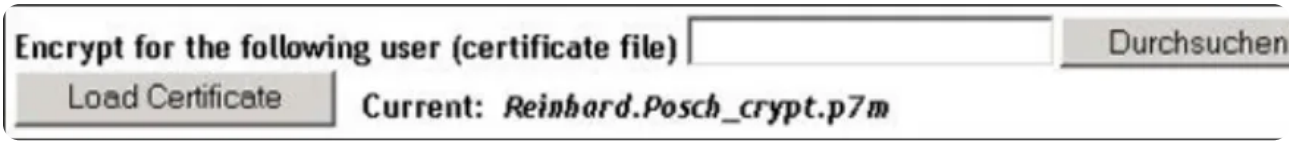
Fingerprint

Um signierte Mails erzeugen zu können, besitzt das Mailtestservice eine Vielzahl

unterschiedlicher Signaturzertifikate, in Abhängigkeit vom verwendeten Signaturalgorithmus (SHA-1/RSA, SHA-1/DSA, SHA-1/ECDSA). Diese Signaturzertifikate werden mit Hilfe der signierten Mails verteilt und können anhand der Fingerprints hinsichtlich Authentizität geprüft werden. Die sha1 Fingerprints der verwendeten Signaturzertifikate können der folgenden Tabelle entnommen und verglichen werden:	**Col2**
Fingerprints	**Fingerprints**
Sig_DSA	B3:07:C1:77:C6:6B:EC:C3:AF:30:85:F5:86:5A:0B:FD:BD:D2:09:9C
Sig_ECDSA-192	6C:9C:6D:66:5D:74:2B:31:F6:E5:7D:5F:05:1C:4A:F6:B4:93:82:67
Sig_ECDSA-256	19:8E:B3:2D:34:AF:E5:B2:44:25:BC:28:B2:B4:21:AA:B2:8A:58:84
Sig_RSA	51:DC:09:9F:F6:9F:84:B0:61:F5:F7:69:E8:6C:F8:4B:7A:EB:96:D6

Explizit/Implizit Signed Mails

Elektronische Signaturen können in unterschiedlichen Formaten erzeugt werden. S/MIME bietet zwei Varianten, bei der die eigentliche Nachricht in der Signatur entweder gekapselt (“implicitsigned”) oder als eigene Einheit im Klartext (“clear-signed” oder “explicit-signed”) übertragen wird. Da die zweite Vorgehensweise den Vorteil bietet, dass auch Mailclients ohne S/MIME-Funktionalität die Nachricht darstellen -aber nicht verifizieren- können, wird sie in der Praxis im Allgemeinen bevorzugt.



Attachment

Das Attachment der Standardmails besteht aus einem *.pdf File (Attachment.pdf), das die Kurzanleitung des Testmail-Services enthält. Nachfolgend werden die einzelnen vordefinierten Mails und die mindestens notwendige Verarbeitung durch den zu testenden Mailclient beschrieben. Die erzeugten Standardmails haben je eine Betreffzeile, die die Mail charakterisiert. **“A mail with a signed attachment - [ASNE] -**

11.09.2001 22:19" Diese Betreffzeile besteht aus einer verbalen Kurzbeschreibung (A mail with a signed attachment), einem Beschreibungskürzel ([ASNE]) und der Absendezeit (z.B. 11.09.2001 22:19). Die Absendezeit dient zur Messung der Reaktionszeit der einkommenden Mails aus dem Internet.

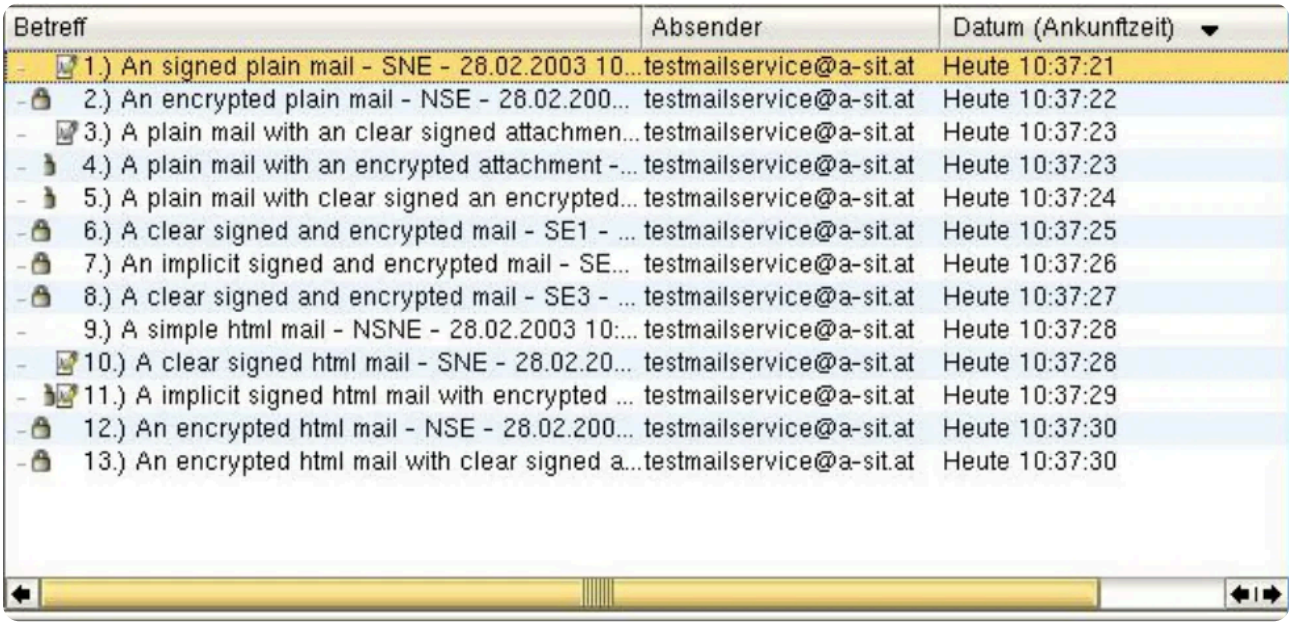
Der Mailinhalt besteht im wesentlichen aus zwei Teilen. Der erste Teil ist eine Beschreibung des Sollverhaltens des zu testenden Mailclients - der zweite Teil eine Auflistung der eingestellten Mailparameter. Mailtext und Mailparameter werden durch eine waagerechte Linie getrennt.

Zweck des Testmailservice

Dieses Service ist in der Lage, eine Vielzahl unterschiedlicher Testmails zu erzeugen. Dabei können verschlüsselte, signierte und klartextliche Nachrichten erzeugt und an einen bestimmten Empfänger gesendet werden.

Die Einstellungen zur Erzeugung signierter und verschlüsselter Testmails werden im Folgenden beschrieben:

- E-Mail erstellen
- E-Mail signieren
- E-Mail verschlüsseln

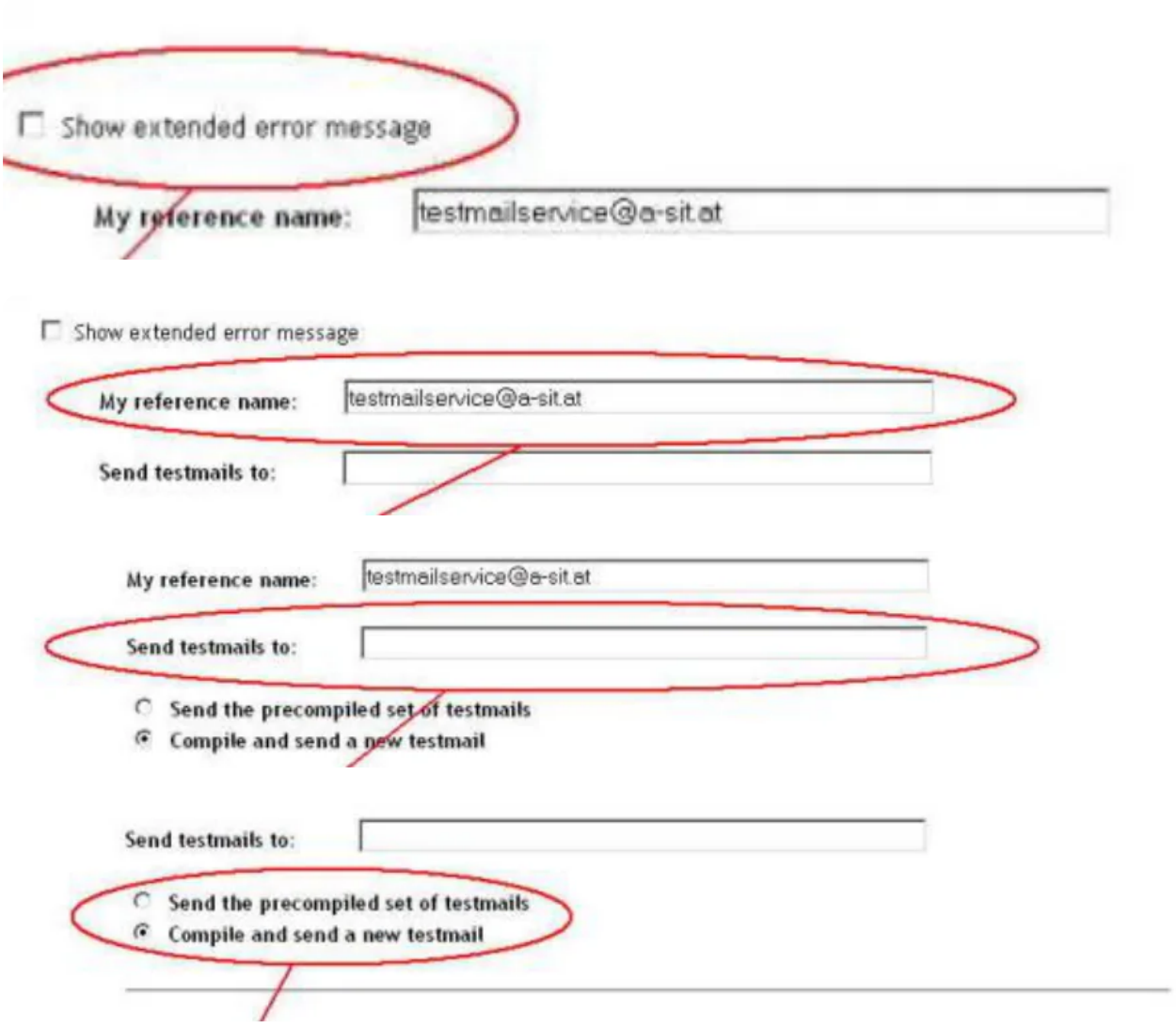


Sollen erweiterten Fehlermeldungen angezeigt werden? Ist diese Option ausgewählt, so werden zusätzlich zur Standardausgabe alle Fehlermeldungen in detaillierter Form ausgegeben.

Wer ist der Absender dieser Mail? Hier wird die Email-Adresse des Absenders eingetragen. **Achtung:** Es sollte der voreingestellte Name nicht verändert werden, damit die vorbereiteten Zertifikate auch zum Absender passen und der zu testende Mailclient keine Fehlermeldungen erzeugt.

Wer ist der Empfänger dieser Email? Hier wird die Email-Adresse des Empfängers eingetragen.

Soll eine einzelne Mail erstellt werden, oder soll eine Serie von vorbereiteten Testmails erzeugt werden?

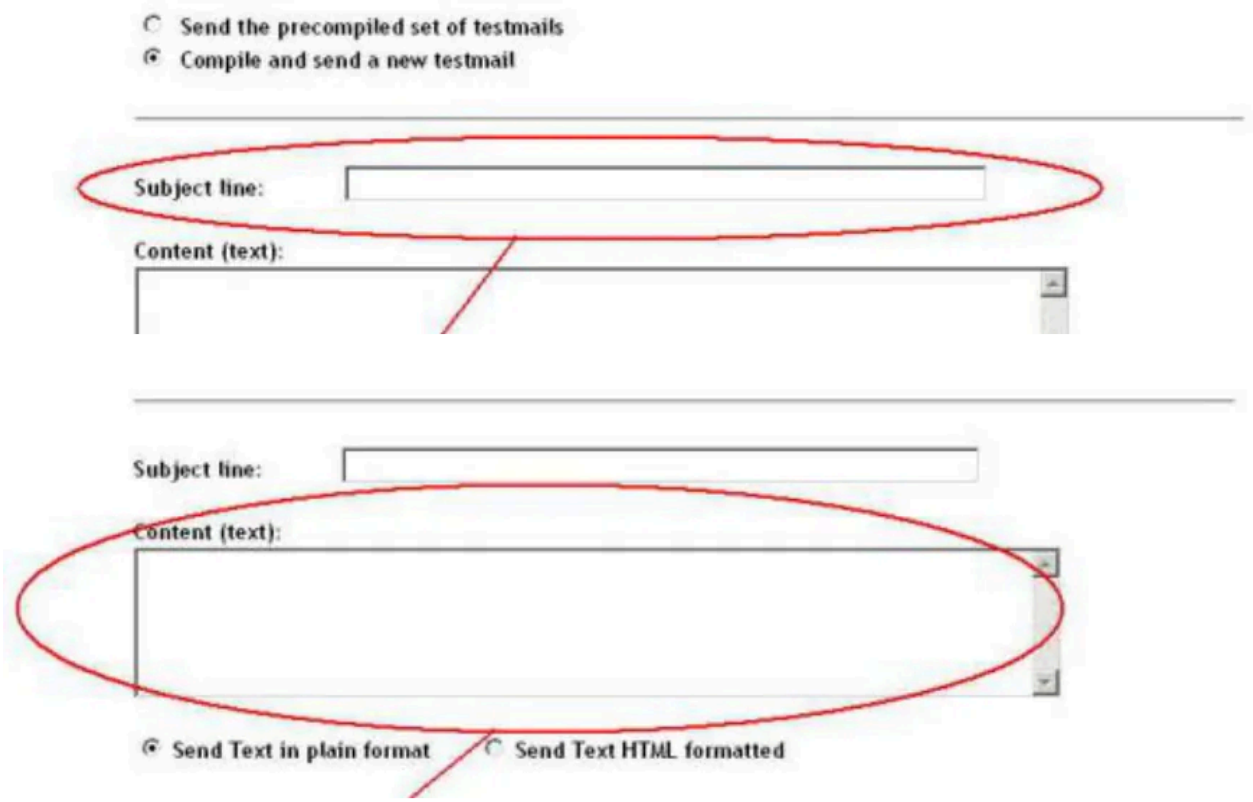


Hier wird eingestellt ob eine einzelne Mail mit den gewählten Einstellungen, oder ob eine Serie von Testmails gesendet werden soll. Diese Serie von Test-Mails setzt sich aus 11 Mails zusammen:

[NSNE] Nicht verschlüsselte und nicht signierte Mail [NSE1-3] Verschlüsselte und nicht signierte Mail [NSAE] Nur Attachment verschlüsselt - Mail nicht signiert [SNE] Nicht verschlüsselte aber signierte Mail [SE1-3]drei verschlüsselte und signierte Mails [SAE] Attachment verschlüsselt - ganze Mail signiert [ASNE] Nicht verschlüsselte Mail - Attachment signiert [ASE] Verschlüsselte Mail - Attachment signiert [ASAE] Nur Attachment verschlüsselt und signiert Alle weiteren Einstellungen werden nun unwirksam. Die Nachricht wird wie das Subject durch einen Standardtext ersetzt. Das Attachment wird durch ein Standard-Attachment (Attachment.pdf) ersetzt.

Eine detaillierte Beschreibung dieser vordefinierten Mails finden Sie unter: *"Testmailservice pre- defined"*
Welches Subject soll die Mail bekommen? Hier wird das Subject der Mail eingetragen.

Welche Nachricht soll verschickt werden?

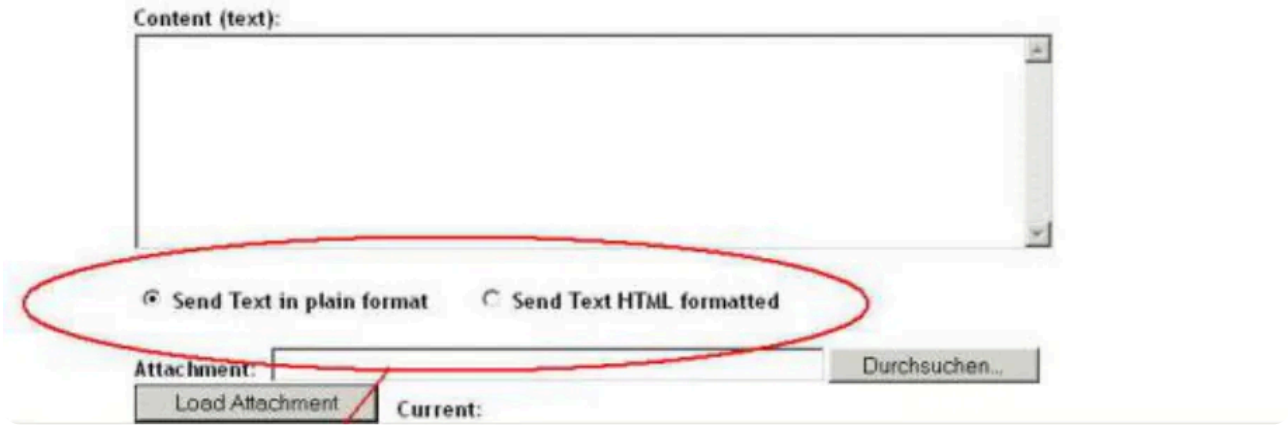


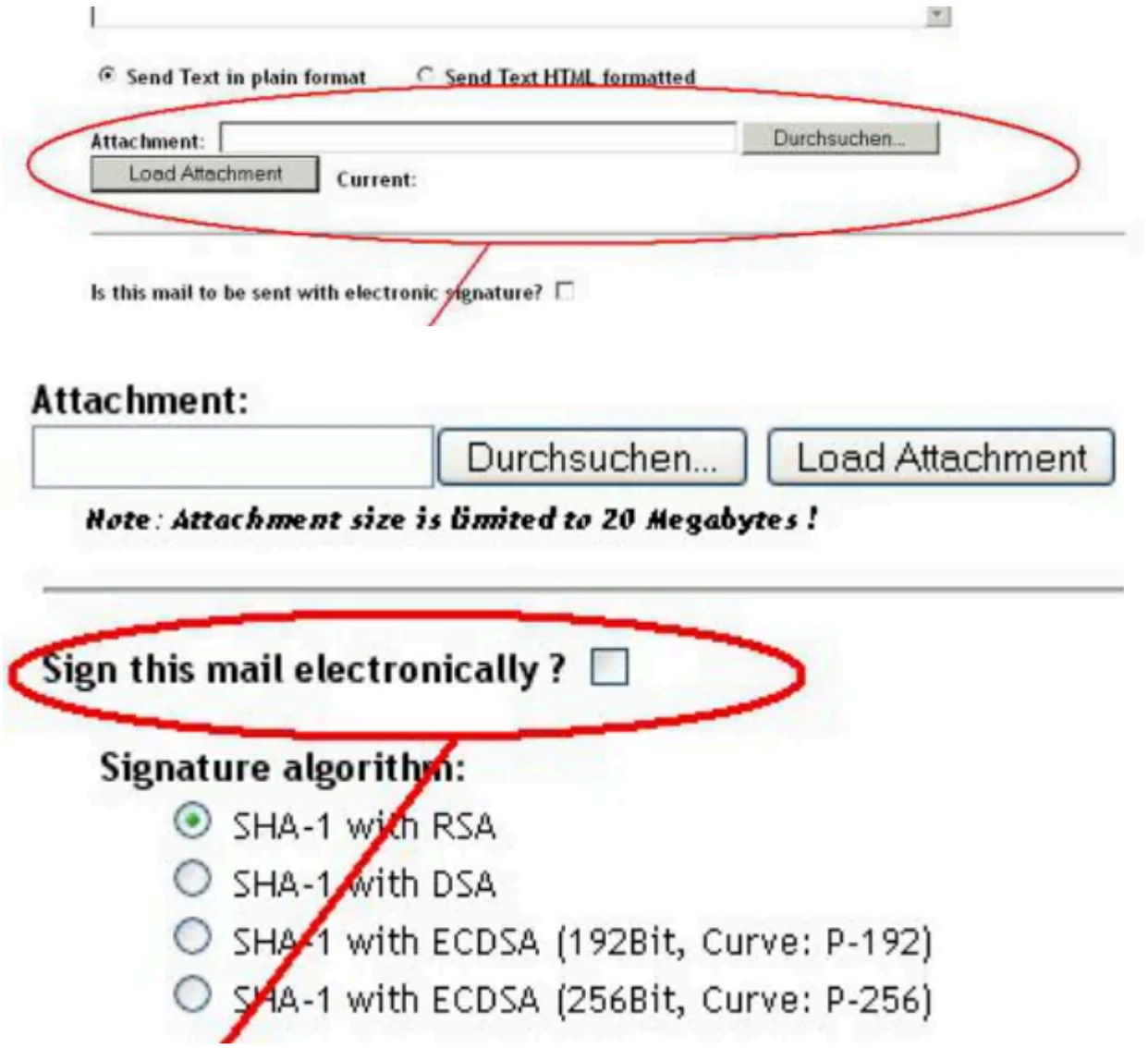
Hier wird der Inhalt der Nachricht eingetragen.

Ist die Nachricht im HTML-Format oder im Text-Format? Hier wird ausgewählt, ob die Nachricht als HTML-Text oder als unformatierter Text bearbeitet werden soll. Wird eine Nachricht als HTML-Nachricht gesendet, so muss der Client diese Darstellung auch unterstützen.

Welche Datei soll der Mail als Attachment beigefügt werden? Hier kann ausgewählt werden, welche Datei an die Mail angehängt werden soll. Hierzu muss erst eine Datei ausgewählt und diese anschließend geladen werden. Danach erscheint der Name der Datei neben dem Button "Load Attachment".

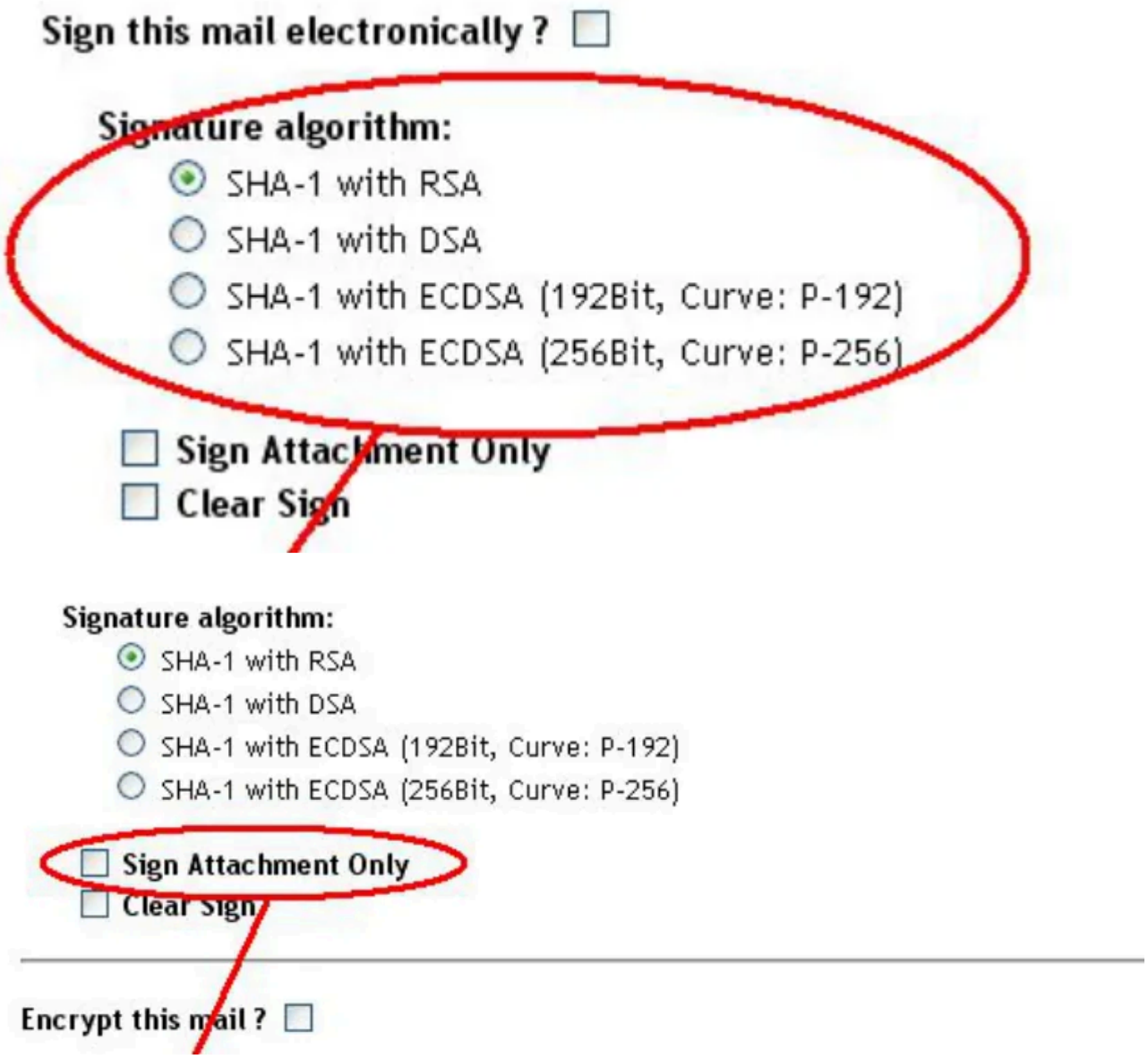
Aktivieren der elektronischen Signatur





Soll die Email signiert werden? Mit dieser Einstellung kann eingestellt werden, ob die Nachricht signiert werden soll. Wird diese Einstellung gewählt, so wird die Mail für ein fix eingestelltes Testzertifikat signiert. Dieses Testzertifikat wird der Nachricht beigelegt.

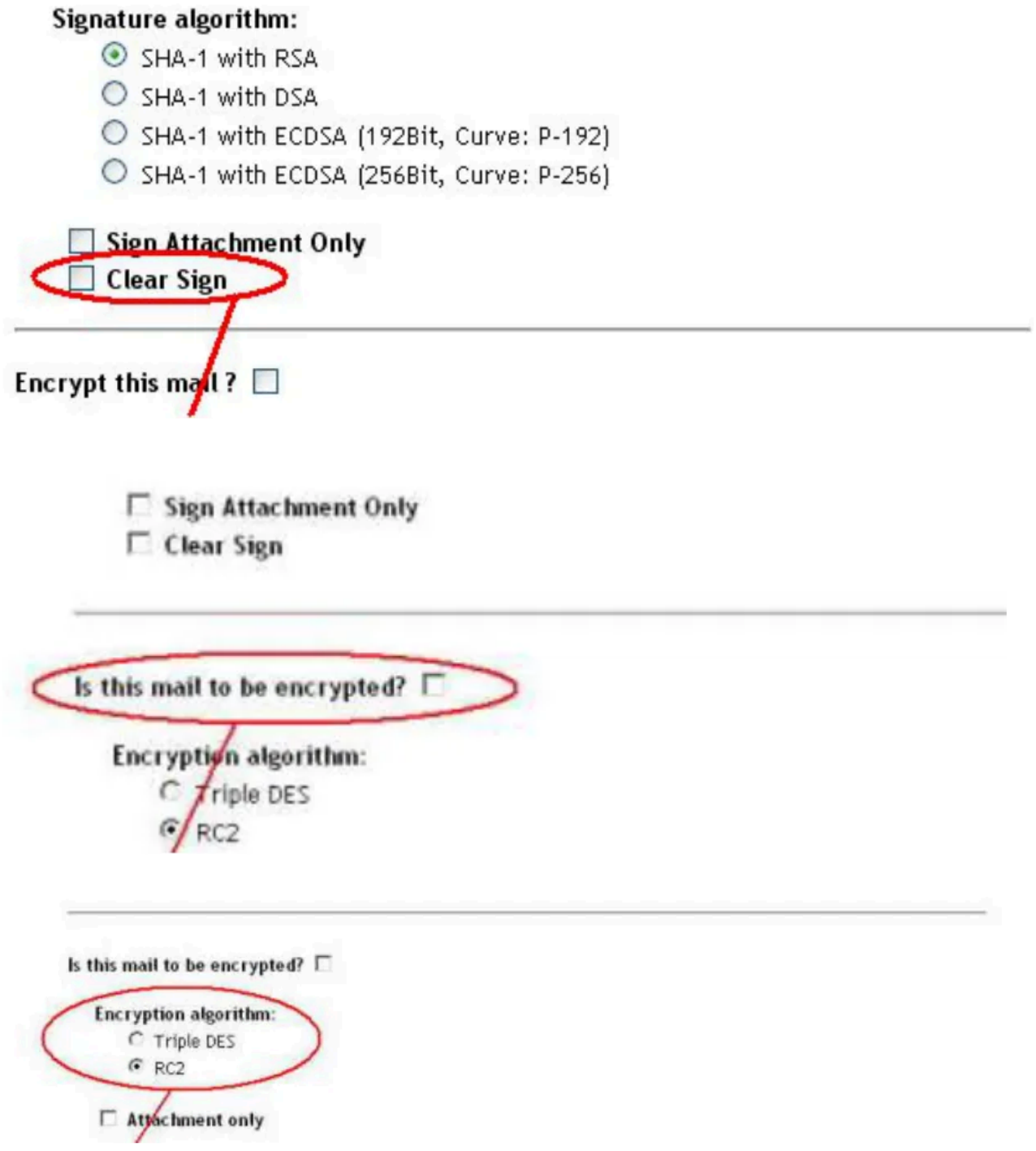
Welcher Algorithmus soll zum Signieren verwendet werden? Hier kann der Algorithmus ausgewählt werden, der zur Erzeugung der Signatur verwendet werden soll. **Achtung:** Nicht alle Mailclients unterstützen auch alle angebotenen Algorithmen!



Soll nur das Attachment signiert werden? Mit dieser Option kann entschieden werden, ob nur das Attachment signiert werden soll. Ist diese Option nicht ausgewählt, so wird die ganze Mail signiert.

Soll die Mail implizit oder explizit signiert werden? Wird diese Option aktiviert, so wird die Signatur als gesonderter Teil der Mail übertragen.

Soll die Mail verschlüsselt werden? Mit dieser Option kann die Verschlüsselung einer Mail aktiviert werden. **Hinweis:** Um eine Mail zu verschlüsseln, wird ein Zertifikat benötigt, das erst geladen werden muss! Siehe **"Welches Zertifikat soll zum Verschlüsseln verwendet werden"** .

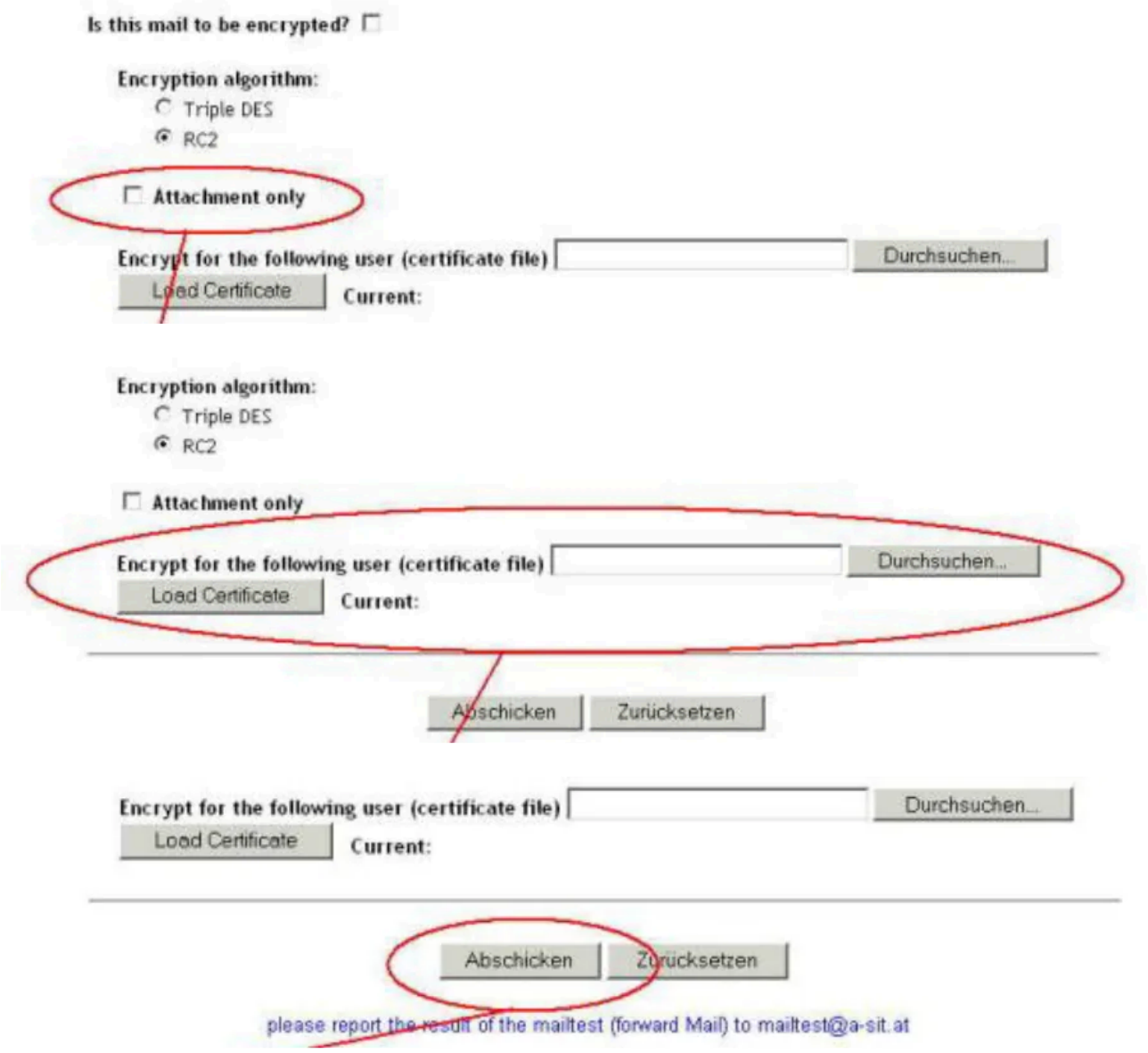


Welcher Algorithmus soll zum Verschlüsseln der Nachricht verwendet werden? Hier kann der Verschlüsselungs-Algorithmus ausgewählt werden. **Achtung:** Auch hier gilt: Nicht alle Mail Clients unterstützen alle Algorithmen.

Soll nur das Attachment verschlüsselt werden? Mit dieser Option kann eingestellt werden, ob nur das Attachment verschlüsselt werden soll. Ist diese Option ausgeschaltet, so wird die ganze Mail verschlüsselt.

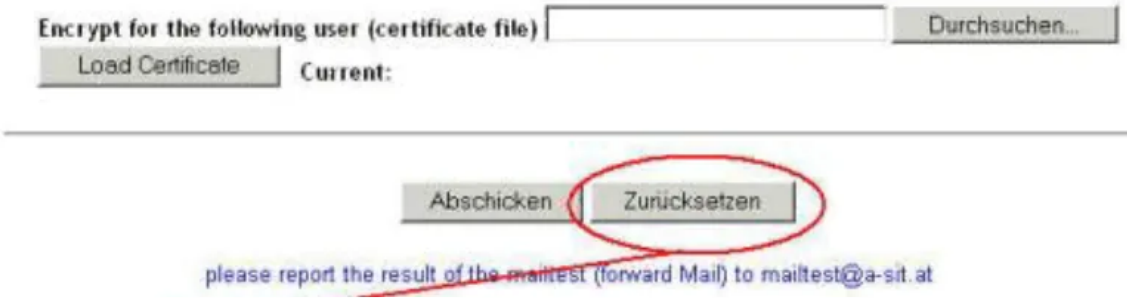
Welches Zertifikat soll zum Verschlüsseln der Nachricht verwendet werden? Hier kann ausgewählt werde, welches Zertifikat zum Verschlüsseln der Mail verwendet werden soll. Um ein Zertifikat verwenden zu können muss es erst ausgewählt und geladen werden. Die Auswahl beginnt mit **"Durchsuche"** (**Achtung:** Nur .der, .cer und .p7c Dateien können geladen werden). Um das ausgewählte Zertifikat zu laden, muss

anschließend **“Load Certificate”** gedrückt werden. Erst danach erscheint der Name der Zertifikatsdatei. **Achtung:** Die Gültigkeit eines Zertifikates wird erst beim Senden der Mail überprüft. Ein möglicherweise defektes oder ungültiges Zertifikat kann erst zu diesem Zeitpunkt erkannt werden. ***Senden der Mail***



Senden der Mail. Die Testmail wird den Einstellungen gemäß zusammengestellt und gesendet, bzw. eine Serie von vorgefertigten Testmails werden gesendet.

Zurücksetzen aller Einstellungen. Setzt alle Einstellungen auf die Anfangswerte zurück. Die geladenen Dateien sind damit nicht mehr gültig. Zur erneuten Verwendung müssen sie nochmals geladen werden.


Encrypt for the following user (certificate file)
Durchsuchen...
Load Certificate
Current:
Abschicken
Zurücksetzen
please report the result of the mailtest (forward Mail) to mailtest@a-sit.at