Kurzdokumentation zum Krypto-Modul von KT-Mail

Das Krypto-Modul zu KT-Mail ermöglicht ein automatisches Ver-/Entschlüsseln von E-Mails nach dem Open-PGP-Standard. (Für Detailinformationen zum Open-PGP-Standard und zum organisatorischen Konzept der automatischen Ver-/Entschlüsselung siehe Datei \KTMAIL\KRYPTO\SIGNATUR\INDEX.HTM auf der CD/DVD.)

Nachstehend werden folgende Themen behandelt:

A. Installation des Krypto-Moduls
B. PGP-Schlüsselaustausch mit Korrespondenzpartnern
C. Tägliche Nutzung der Verschlüsselung

A. Installation des Krypto-Moduls

1. KT-Mail installieren, falls noch nicht geschehen.

2. Dateien im KT-Programmverzeichnis ergänzen/aktualisieren:
   (a) Falls der Makro POSTLAUF im KT-Programmverzeichnis älter als Vers. 2.1.4 ist (siehe Notizzeile), diesen Makro durch die Datei KT\POSTLAUF auf der CD/DVD ersetzen. (Dabei die bisherigen Einstellungen in den Zuweisungsbefehlen am Makroanfang in den neuen Makro übernehmen.)
   (b) Die Datei KT\PGPSETUP von der CD/DVD ins KT-Programmverzeichnis auf der Festplatte kopieren.

3. Dateien im KTSERVER-Verzeichnis von KT-Mail ergänzen/aktualisieren:
   (a) Falls die Datei FILETYPE.EXE im KTSERVER-Verzeichnis älter als Vers. 2.0 ist (Aufruf ohne Parameter, dann Strg+C), diese Datei durch die Datei KTSERVER\FILETYPE.EXE auf der CD/DVD ersetzen.
   (b) Falls die Datei MAILIN.EXE im KTSERVER-Verzeichnis älter als Vers. 2.2.4 ist, diese Datei durch die Datei KTSERVER\MAILIN.EXE auf der CD/DVD ersetzen.
   (c) Falls die Datei MAILOUT.EXE im KTSERVER-Verzeichnis älter als Vers. 1.2 ist, diese Datei durch die Datei KTSERVER\MAILOUT.EXE auf der CD/DVD ersetzen.
   (d) Die Dateien KTSERVER\KRYPTO.* von der CD/DVD ins KTSERVER-Verzeichnis auf der Festplatte kopieren.

4. Verzeichnis KTSERVER\PGP installieren:
   (a) Unter dem KTSERVER-Verzeichnis von KT-Mail das Unterverzeichnis PGP anlegen und den Inhalt von KTSERVER\PGP*.* von der CD/DVD dorthin kopieren.
   (b) Falls unter Windows gearbeitet wird und KT-Mail in einem anderen Verzeichnis als C:\KTSERVER installiert ist, die 3 PIF-Dateien P1.PIF, P2.PIF und P3.PIF über den Explorer laden (rechte Maustaste, dann "Eigenschaften") und den hinterlegten Programmpfad entsprechend anpassen.

5. Eigenen PGP-Schlüssel erzeugen und für KT-MAIL/Krypto verankern:
   (a) Im Betriebssystem ins Verzeichnis \KTSERVER\PGP wechseln und Befehl "**pgpk -g**" (g = generate - s. Befehl "pgpk" ohne Zusatz) eingeben, um ein eigenes Schlüsselpaar (privat/öffentlich) zu erzeugen - vgl. Datei SIGNATUR\TUTOR5.HTM, Abschnitt "Schritt 5A: Erstellen eines Postschlüssels". Folgende Schritte sind dabei zu durchlaufen: Schlüsseltyp wählen ("DSS/Diffie-Hellman"), Schlüssellänge wählen (z.B. "3"=2048/1024 Bits), User-ID eingeben (z.B. "Emil Mustermann <emil@mustermann.de>"), Gültigkeit des Schlüssels in Tagen angeben, Paßworttext eingeben (ohne ' ', '=' oder '"'; außerdem Paßworttext unbedingt merken oder im Safe o. ä. hinterlegen!) und abschließend beliebige Tasten für den Zufallsgenerator drücken, sobald Sie dazu aufgefordert werden.
   (b) Den öffentlichen Teil des eigenen Schlüssels über den Befehl "**pgpk -x <eindeutiger Teil der User-ID> -o Exportdateiname**" ("x" = ex-

tract, "o" = outfile) zum Weitergeben in eine ASCII-Datei exportieren (vgl. Datei SIGNATUR\TUTOR5.HTM, Ende des Tutorialschritts 5A).
Bsp.: "pgpk -x emil@mustermann.de -o emuster.asc"

(c) Neuen Schlüssel mit Key-ID in der Datei KRYPTO.TAB vermerken. Dazu in Komforttext "Makro pgpsetup"->"Schlüsselliste mit Fingerprints laden" aufrufen und aus der erstellten Liste die Key-ID des neuen Schlüssels notieren ("0x????????" im Block der entsprechenden User-ID). Dann "Makro pgpsetup"->"Datei KRYPTO.TAB laden" aufrufen und dort statt der Mustermann-Zeile die Daten des eigenen Schlüssels (E-Mail-Adresse bzw. Domain als erste Angabe und Key-ID als vierte Angabe) eintragen. (Die 2. und 3. Angabe bleiben unverändert.)

B. PGP-Schlüsselaustausch mit Korrespondenzpartnern

1. Den eigenen öffentlichen Schlüssel (s. Ergebnis des obigen Punkts A.5b) dem Korrespondenzpartner per E-Mail zusenden oder auf die eigene Homepage stellen.

2. Den öffentlichen PGP-Schlüssel des Korrespondenzpartners per E-Mail empfangen oder von seiner Homepage holen.

3. Den öffentlichen PGP-Schlüssel des Korrespondenzpartners in den eigenen Schlüsselbund aufnehmen: "Makro pgpsetup"->"PGP-Schlüsseldatei importieren".

4. Echtheit der Schlüssel sicherstellen (wichtig!):
   (a) "Makro pgpsetup"->"Schlüsselliste mit Fingerprints laden".
   (b) Den Korrespondenzpartner anrufen und am Telefon die Daten der beiden PGP-Schlüssel (Schlüssellänge, Key-ID, Fingerprint und User-ID) verifizieren.
   (c) Sobald Schlüssel überprüft wurde, Schlüsselprüfung mit eigener Signatur "abzeichnen": "Makro pgpsetup"->"PGP-Schlüssel signieren".
   (Hinweis: Details zur Validierung von PGP-Schlüsseln finden Sie in der Datei SIGNATUR\TUTOR5.HTM, Abschnitt "Schritt 5B: Validieren eines PGP-Schlüssels".)

5. Schlüssel des Korrespondenzpartners in Datei KRYPTO.TAB aufnehmen:
   (Hinweis: Dieser Schritt ist nur erforderlich, falls die in der User-ID des PGP-Schlüssels enthaltene E-Mail-Adresse nicht mit der akt. E-Mail-Adresse des Korrespondenzpartners übereinstimmt oder der Schlüssel für einen ganzen Domain gelten soll oder für den Schlüssel eine der speziellen KT-Mail/Krypto-Optionen [Verschlüsselung/Signatur stets erzwingen, PGP-MIME-Erweiterungen verwenden] aktiviert werden soll.)
   (a) "Makro pgpsetup"->"Datei KRYPTO.TAB laden".
   (b) Daten des Korrespondenzpartners und der User-ID seines Schlüssels gemäß den Musterzeilen ("Redtenbacher" oder "LfD-BaWue") eintragen - Details siehe Datei SIGNATUR\DOKU2.HTM, "Die Sicht des Mailserver-Administrators".

C. Tägliche Nutzung der Verschlüsselung mit KT-Mail/Krypto

1. Eingangsmails: Hier ist nichts zu tun - die Entschlüsselung und ggf. Signaturprüfung erfolgt automatisch.

2. Ausgangsmails: Sofern für den angegebenen Empfänger nicht bereits eine Verschlüsselung/Signatur über die Datei KRYPTO.TAB erzwungen wird (s. Punkt B.5 oben bzw. Datei SIGNATUR\DOKU2.HTM), kann vom Absender über die Zusätze "!V!", "!S!" oder "!VS!" am Ende des Betreff-Vermerks der E-Mail eine Verschlüsselung bzw. Signatur explizit ausgelöst werden (vgl. Datei SIGNATUR\DOKU1.HTM, Abschnitt 1, "Die Sicht des Endbenutzers").