TELEKOMMUNIKATION
SICHERHEITSTECHNIK
GEBÄUDEMANAGEMENT
DATENTECHNIK

Alarm-Übertragungsgerät

TAS-LinkII

Handhabung der Schlüssel bei gesicherter IP-Übertragung

Ausgabe 1.3

Inhaltsverzeichnis

Inhaltsverzeichnis (diese Seite)	Seite 2
BSI-Schlüssel	Seite 3
Chiasmus-Schlüssel	Seite 4
AES-Schlüssel	Seite 5
Automatische Schlüsselvergabe	Seite 6

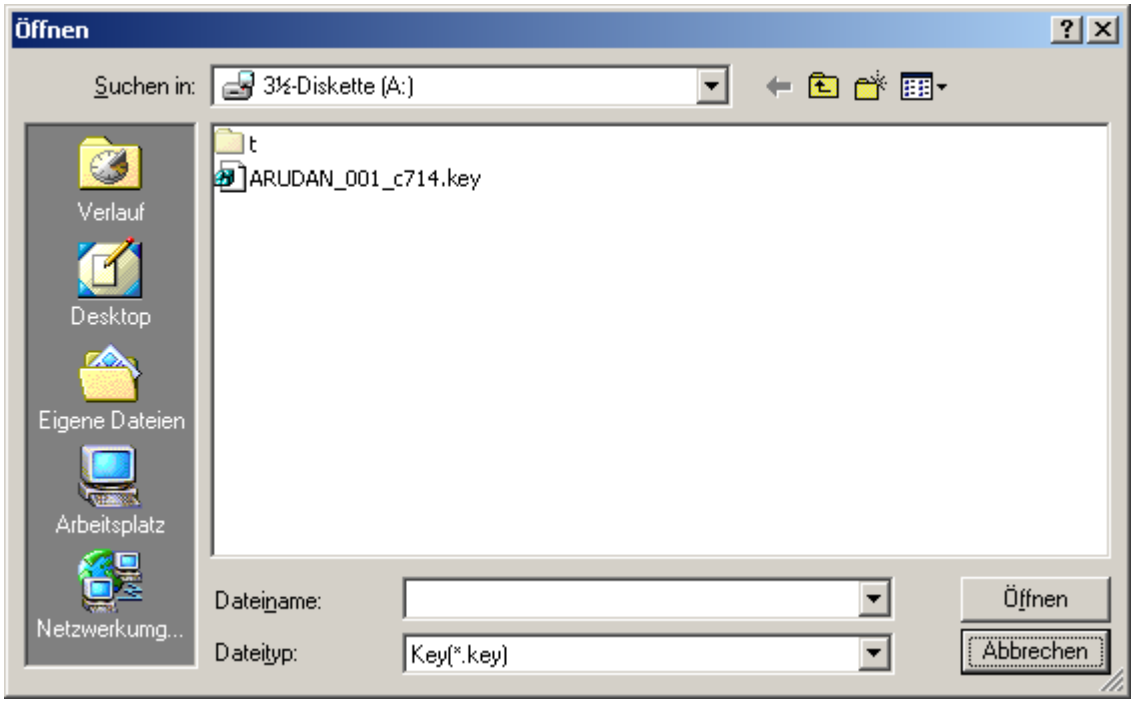
BSI-Schlüssel

Der BSI-Schlüssel ist 160 bit (20 Byte) lang und wird in Form einer Passwort-verschüsselten Datei auf Diskette bereitgestellt. Das Passwort liegt bei der Installation in schriftlicher Form bereit. Beim Einspielen des Schlüssels wird die korrekte Eingabe des Passwortes überprüft. Bei der Eingabe ist unbedingt die Einhaltung der Groß/Klein Schreibweise von Bedeutung. Die Eingabe ist verdeckt d.h. mit symbolischer Darstellung (mit „x“) des eingegebenen Zeichens.

Die Eingabe des Paßwortes bei der BSI-Schlüssel Speicherung

Der Sysconf überprüft die Verknüpfung zwischen dem Paßwort und dem Schlüssel während der Einspielung des Schlüssels.

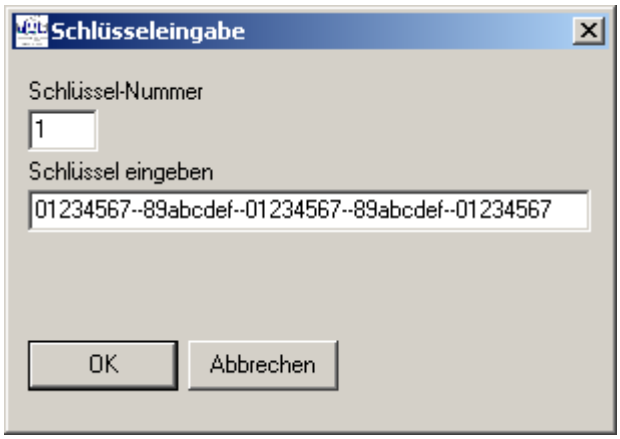
Auf der Diskette wird eine Datei mit Extension *.key gesucht.



Auswahl der Key-Datei aus der Diskette.

Chiasmus-Schlüssel

Chiasmus wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als Verfahren zu Daten-Verschlüsselung propagiert. BSI stellt ein Windows Tool zu Verschlüsselung der Daten und Erzeugung des Schlüssels unter Windows bereit. Der Schlüssel muß nicht zwingend vom Programm generiert werden. Wichtig ist nur, daß das Übertragungsgerät und die Empfangseinrichtung der Leitstelle den gleichen Schlüssel nutzen. Der Chiasmus-Schlüssel ist **160 Bit** lang. Beim TAS-LinkII wird dieser Schlüssel als einer der nutzbaren Schlüssel in der VPN geschützten IP Übertragung akzeptiert. Die dabei verwendete Eingabemaske öffnet ein Feld mit **40 Positionen** für hexadezimale Zahlen die in 5 von minus Zeichen getrennte Felder unterteilt ist.
(siehe Menü: „Extras“ „Chiasmus-Schlüssel übertragen“)



Eingabe des Chiasmus-Schlüssels

Falls der Schlüssel in Form einer Datei bereitgestellt wird, kann die Datei mit einem Editor geöffnet werden und der Inhalt, nach der Markierung mit <STRG> und <C>, im Clipboard Buffer des PC temporär zwischen gelagert werden. So kann die Eingabe mit <STRG> und <V> sehr erleichtert werden. Hinter jeder Position die hexadezimal eingegeben wird, verbergen sich 4 Bit des Schlüssels. Hier die Erklärung in Form einer Tabelle:

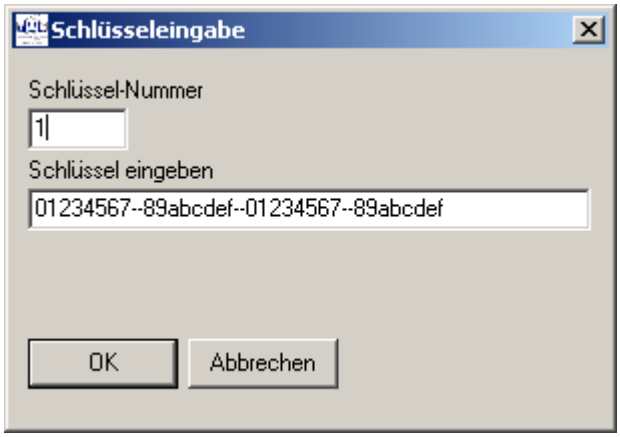
Hexadezimal	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
Binär	0000	1000	0100	1100	0010	1010	0110	1110	0001	1001	0101	1101	0011	1011	0111	1111

Konvertierung der hexadezimalen in binäre Zahlen.

AES-Schlüssel

AES-Schlüssel

Der Advanced Encryption Standard (AES) ist ein Kryptosystem, das im Oktober 2000 vom National Institute of Standards and Technology (NIST) als Standard bekannt wurde. Der AES-Algorithmus bietet ein sehr hohes Maß an Sicherheit. In der IP-VPN Geräte Software angewandten Implementierung, besitzt der AES-Schlüssel eine Blockgröße von **128 Bit**. Die dabei verwendete Eingabemaske öffnet ein Feld mit **32 Positionen** für hexadezimale Zahlen die in 4 von minus Zeichen getrennte Felder unterteilt ist.
(siehe Menü: „Extras“ „AES-Schlüssel übertragen“)



Eingabefenster für den AES-Schlüssel

Erlaubt ist, wie bei den Chiasmus-Schlüssel schon bekannt, die hexadezimale Eingabe, d.h. die einzelnen Positionen können Zahlen von 0 bis 9 sein, sowie die Buchstaben "a,b,c,d,e,f" für dezimal 10 bis 15. Der Eintrag des Schlüssels kann auch wie beim Chiasmus-Schlüssel, aus dem Clipboard Buffer geschehen.

Automatische Schlüsselvergabe

Die automatische Schlüsselvergabe

Wenn die IP-Leitstelle über einen alternativen Zugang verfügt, kann auf die manuelle Speicherung der Schlüssel gänzlich verzichtet werden.
Dann stehen dem Übertragungsgerät:
- die ISDN Schnittstelle,
- die analoge Schnittstelle (PSTN) oder
- der GSM-Anschluss

als Schlüsselgeber zu Verfügung.
Die manuell eingespielten Schlüssel werden von der Anwendung ignoriert, sobald unter „Ziele“ – „NSL“ – „IP-Weg“ – „Weitere Ziel Parameter“ bei „Autom. Schl-Verw. Ruf-Nr“ eine eingetragene Rufnummer steht. Nach dem Start der Anwendung wird die Wahl zu der in Konfiguration hinterlegten Rufnummer gestartet und in einer aktiven Verbindung der Schlüssel von der Leitstelle angefordert. Bei Geräten mit einer GPRS Anwendung wird bei Bedarf die GPRS-Verbindung zuerst unterbunden damit per GSM der Schlüssel abgeholt werden kann.

Beispiel einer Konfiguration mit automatischer Schlüsselvergabe: