AIE encryption settings

(How to)

Version 2019.12.0

Index of contents

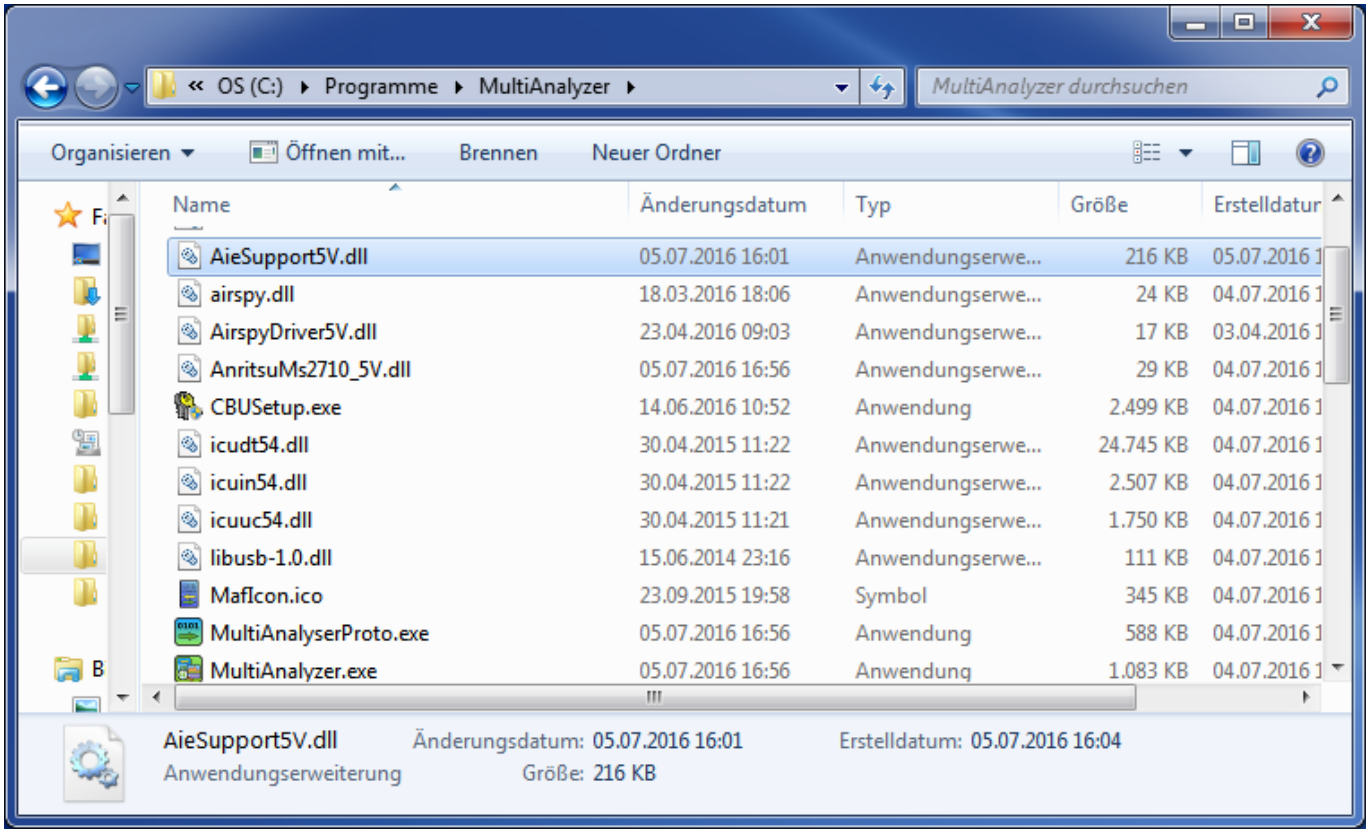
1 History

Date	Version	Author	Comment
2016-07-05	A1	GH	• Initial release
2016-07-16	A2	GH	• ISI added MCC, MNC arguments • GSI can now added • ISIMSG added
2016-09-26	A3	GH	• ESIDB added. • Chapter 4 added.
2016-11-11	A4	GH	• ESIDB chapter reworked.
2016-12-01	A5	GH	• ESIDB chapter removed, not needed anymore
2017-06-24	A6	GH	• TCB keyword added.
2017-09-18	A7	GH	• DSCK keyword added.
2018-04-16	A21	GH	• Change document version scheme to software version. • CCKB keyword added. • Support for common network CCK and SCK. • Add example chapter
2019-01-30	2018.12	GH	• Version update
2020-04-17	2019.12	GH	• Update of encrypted configuration files, chapter 4.

2 Basis

Die MultiAnalyzer Software bietet selber kein Entschlüsselungsverfahren. Sie hat jedoch eine Schnittstelle, die diese bereitstellen kann.

Diese Schnittstelle wird aktiviert, wenn die „AieSupport5V.dll“ geladen werden kann. Dazu muss diese im Installations-Verzeichnis liegen. Sie ist kein Bestandteil der normalen Installation und muss manuell hinzugefügt werden:



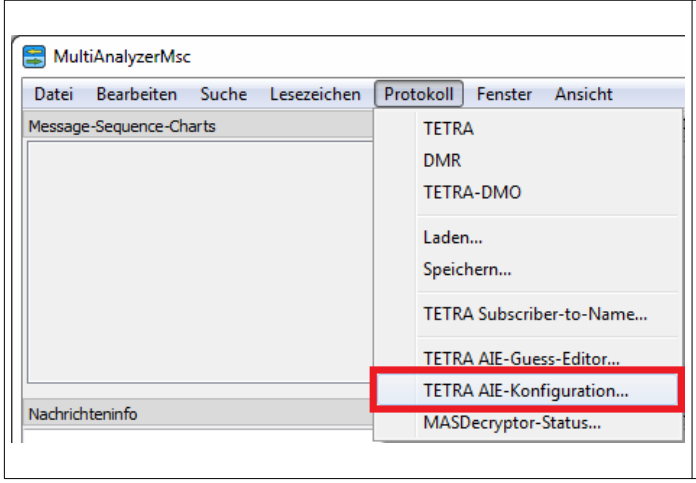
2.1 Schlüssel

Neben dem Entschlüsselungsverfahren aus der DLL müssen noch die Schlüssel bekannt sein. Diese Schlüssel werden in einer Textdatei im CSV Format abgelegt.

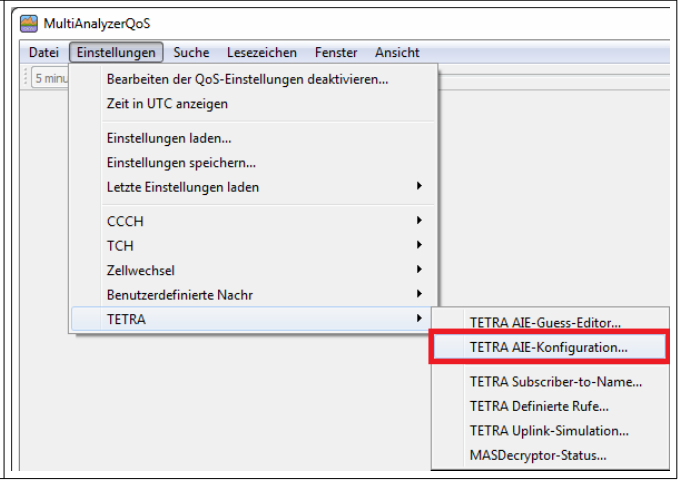
Beim Starten der Analyse wird der Pfad und Dateiname der „AieSupport5V.dll“ übergeben. Diese lädt die Daten daraus und verwaltet fortan die Schlüssel.

Die Schlüssel Datei kann folgendermaßen gesetzt werden:

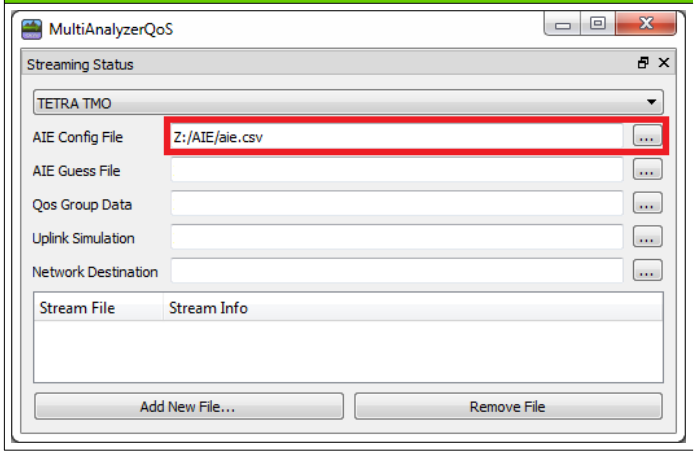
MSC



QoS



QoS-Server



3 Format der Schlüssel-Datei

Pro Zeile wird je ein Datensatz gespeichert. Jeder Datensatz fängt mit einem Schlüsselwort an, das Schlüsselwort wird zwingend groß geschrieben. Dieses definiert die nachfolgenden Parameter der Zeile. Jeder Parameter ist durch ein Semikolon (;) getrennt.

3.1 Schlüsselwörter Beschreibung

Schlüsselwort	Bedeutung		
CFG	Allgemeine Konfigurations-Parameter. Hat einen Parameter:		
	KSGN	Ist der Standard KSGN. Wenn kein spezieller Gruppen oder Einzel-Teilnehmer zugewiesen wurde.	
CCK	Enthält die CCK Informationen (Common Cypher Key). Hat neun Parameter:		
	Kanal	Die Haupt Kanal-Nummer der Zelle	(MAC-SYSINFO: Main carrier)
	MCC	Die Landes-Nummer	(MLE-SYNC: MCC)
	MNC	Die Netz-Nummer	(MLE-SYNC: MNC)
	Color Code	Der Scramble-Kode	(MAC-SYNC: Colour code)
	LA	Zell-Nummer	(MLE-SYSINFO: Location Area)
	CCKid	Die CCK Schlüssel-Nummer	(MAC-SYSINFO: CCK identifier)
	KSGN	Die Verschlüsselung-Methode	(255=Für „CFG“ Wert)
	ECK-Flag	ECK-Schlüssel [CK → TB5 → ECK]	(Benutzer)
	Key	Der Schlüssel (80 Bit)	(Benutzer)
DCK	Enthält die DCK Informationen (Derived Cipher Key). Hat zwölf Parameter:		
	Kanal	Die Haupt Kanal-Nummer der Zelle	(MAC-SYSINFO: Main carrier)
	MCC	Die Landes-Nummer	(MLE-SYNC: MCC)
	MNC	Die Netz-Nummer	(MLE-SYNC: MNC)
	Color Code	Der Scramble-Kode	(MAC-SYNC: Colour code)
	LA	Zell-Nummer	(MLE-SYSINFO: Location Area)
	CCKid	Die CCK Schlüssel-Nummer	(MAC-SYSINFO: CCK identifier)
	ESI	Verschlüsselte SSI	(Ändert sich abhängig von CCKid)
	SSI	Unverschlüsselte SSI	(Benutzer)
	Frame	Aktivierungs-Frame für den DCK.	(Authentifizierung abgeschlossen)
	KSGN	Die Verschlüsselung-Methode	(255=Für „CFG“ Wert)
	ECK-Flag	ECK-Schlüssel [CK → TB5 → ECK]	(Benutzer)
	Key	Der Schlüssel (80 Bit)	(Benutzer)

Schlüsselwort	Bedeutung		
SCK	Enthält die SCK Informationen (Static Cipher Key). Hat zehn Parameter:		
	Kanal	Die Haupt Kanal-Nummer der Zelle	(MAC-SYSINFO: Main carrier)
	MCC	Die Landes-Nummer	(MLE-SYNC: MCC)
	MNC	Die Netz-Nummer	(MLE-SYNC: MNC)
	Color Code	Der Scramble-Kode	(MAC-SYNC: Colour code)
	LA	Zell-Nummer	(MLE-SYSINFO: Location Area)
	SCK-N	Die SCK Schlüssel-Nummer	(MAC-SYSINFO: SCKN)
	SCK-VN	Die SCK Schlüssel-Version	(MAC-SYSINFO: CCK identifier)
	KSGN	Die Verschlüsselung-Methode	(255=Für „CFG“ Wert)
	ECK-Flag	ECK-Schlüssel [CK → TB5 → ECK]	(Benutzer)
	Key	Der Schlüssel (80 Bit)	(Benutzer)
DSCK	Kanal	Die Kanal-Nummer: 0...3999	(Spezifischer Kanal)
		Die Kanal-Nummer: -1	(Gültig für alle Kanäle)
	SCK-N	Die SCK Schlüssel-Nummer	(SYNC-PDU)
	KSGN	Die Verschlüsselung-Methode	(Für DPres-Sync URT)
	Key	Der Schlüssel (80 Bit)	(Benutzer)

Schlüsselwort	Bedeutung			
GRMSG	Identifiziert Gruppen anhand geratener Nachrichten-Typen. Diese Gruppen werden automatisch in die Benutzer-Verwaltung aufgenommen und mit dem definierten Schlüssel entschlüsselt. Hat sechs oder mehr Parameter:			
	Key-Type	Der verwendete Schlüssel-Type:		
		0	CCK: „Key-Arg 1“ = 0	„Key-Arg 2“ = 0
		1	SCK: „Key-Arg 1“ = SCK-N	„Key-Arg 2“ = SCK-VN
		2	GCK: „Key-Arg 1“ = GCK-N	„Key-Arg 2“ = GCK-VN
	Key-Arg 1	Je nach Key-Type.		
	Key-Arg 2	Je nach Key-Type.		
	KSGN	Die Verschlüsselung-Methode.	(255=Für „CFG“ Wert)	
	Anzahl	Anzahl der folgenden Nachrichten.	(1 bis 32)	
	Nachricht 1	Nummer 1 (1...65335)		
	...			
	Nachricht N	NummerN (1...65335)		
ISIMSG	Identifiziert individuelle Teilnehmer anhand geratener Nachrichten-Typen. Diese Teilnehmer werden automatisch in die Benutzer-Verwaltung aufgenommen. Sofern der Teilnehmer-Key bekannt ist (DCK vom Keyserver) wird entschlüsselt.			
	KSGN	Die Verschlüsselung-Methode.	(255=Für „CFG“ Wert)	
	Anzahl	Anzahl der folgenden Nachrichten.	(1 bis 32)	
	Nachricht 1	Nummer 1 (1...65335)		
	...			
	Nachricht N	NummerN (1...65335)		

Schlüsselwort	Bedeutung			
ISI	Definiert einen individuellen Teilnehmer.			
	MCC	Die Landes-Nummer		(MLE-SYNC: MCC)
	MNC	Die Netz-Nummer		(MLE-SYNC: MNC)
	SSI	Unverschlüsselte SSI		(Benutzer)
	KSGN	Die Verschlüsselung-Methode.		(255=Für „CFG“ Wert)
	Key	Der Schlüssel K (128 Bit)		(Benutzer)
GSI	Definiert eine Gruppe.			
	MCC	Die Landes-Nummer		(MLE-SYNC: MCC)
	MNC	Die Netz-Nummer		(MLE-SYNC: MNC)
	SSI	Unverschlüsselte SSI		(Benutzer)
	KSGN	Die Verschlüsselung-Methode.		(255=Für „CFG“ Wert)
	Key-Type	Der verwendete Schlüssel-Type:		
		0	CCK: „Key-Arg 1“ = 0	„Key-Arg 2“ = 0
		1	SCK: „Key-Arg 1“ = SCK-N	„Key-Arg 2“ = SCK-VN
		2	GCK: „Key-Arg 1“ = GCK-N	„Key-Arg 2“ = GCK-VN
	Key-Arg 1	Je nach Key-Type.		
	Key-Arg 2	Je nach Key-Type.		
ESIDB	Verlinkt auf eine Datenbank (Datei) mit Übersetzungen von der verschlüsselten ESI zur unverschlüsselten ISI.			
	Kanal	Die Haupt Kanal-Nummer der Zelle (MAC-SYSINFO: Main carrier)		
	MCC	Die Landes-Nummer		(MLE-SYNC: MCC)
	MNC	Die Netz-Nummer		(MLE-SYNC: MNC)
	Color Code	Der Scramble-Kode		(MAC-SYNC: Colour code)
	LA	Zell-Nummer		(MLE-SYSINFO: Location Area)
	AIE class	Klasse der Verschlüsselung:		
		2	Statische Verschlüsselung	(*Felder SCK-N und SCK-VN folgen*)
		3	Dynamische Verschlüsselung	(*Felder Reserverd und CCKid folgen*)
	SCK-N	Die SCK Schlüssel-Nummer		(MAC-SYSINFO: SCKN)
	SCK-VN	Die SCK Schlüssel-Version		(MAC-SYSINFO: SCK identifier)
	Reserverd	Wird nicht benutzt ist „0“.		
	CCKid	Die CCK Schlüssel-Nummer		(MAC-SYSINFO: CCK identifier)
	File	Datenbank Datei mit den Übersetzungen.		

Schlüsselwort	Bedeutung		
TCB	Gibt die IP-Adresse zur Entschlüsselungs-Hardware an.		
	IP-Type	0	Die IP-Adresse ist vom Type IPv4
	IP-Address	Die IP-Adresse	
	PORT	Der Port	
CCKDB	File	Die Datei für die CCK(s). Die Datei wird automatisch nachgeladen. Sobald ein neuer CCK bekannt wird, wird dieser in die Datei eingefügt.	

3.2 Beschreibung der Parameter

Parameter	Bedeutung
Schlüsselwort	Definiert den Datensatz der Zeile, Werte: „CFG, CCK, DCK, GRMSG, ISI“, ...
Kanal	MCCH Kanal-Nummer der Zelle. Der Wert kann aus dem MAC-SYSINFO „Main carrier“ ausgelesen werden. Werte sind „0….3999“. Der Wert 65535 steht für nicht benötigt. Die Schlüsselwörter CCK und SCK unterstützen diesen Wert wenn kein ECK angeben ist.
MCC	Landes-Nummer. Der Wert kann aus dem MLE-SYNC „MCC“ ausgelesen werden. Die Werte sind „1...1023“. Deutschland ist 262.
MNC	Die Netzwerk-Nummer. Der Wert kann aus dem MLE-SYNC „MNC“ ausgelesen werden. Die Werte sind „1...16383“. BDBOS ist 1001.
Color Code	Der Scrambling-Kode. Der Wert kann aus dem MAC-SYNC „Colour code“. Die Werte sind „0...63“. Je Zelle variieren die Werte. Der Wert 255 steht für nicht benötigt. Die Schlüsselwörter CCK und SCK unterstützen diesen Wert wenn kein ECK angeben ist.
LA	Die Zell-Nummer innerhalb eines Netzwerkes. Der Wert kann aus dem MLE-SYSINFO „Location Area“ ausgelesen werden. Die Werte sind „1...16382“. Der Wert 65535 steht für nicht benötigt. Das Schlüsselwort SCK unterstützt diesen Wert wenn kein ECK angeben ist.
CCKid	Die CCK Schlüssel-Nummer Der Wert kann aus dem MAC-SYSINFO „CCK identifier“ ausgelesen werden. Der Wert steht nicht in jedem MAC-SYSINFO. Er ist nur vorhanden wenn das vorherige Element „Hyperframe/cipher key flag“ eins ist (=Common cipher key identifier). Die Werte sind „1...65335“.
ECK-Flag	Handelt es sich um ein Verschlüsselten Schlüssel (Wert ist 1), sprich der Schlüssel wurde mit TB5 Algorithmus verschlüsselt. Oder handelt es sich um einen klaren Schlüssel (Wert ist 0). Aus einem klaren Schlüssel wandelt die „AieSupport5V.dll“ den Schlüssel automatisch in ein ECK um (sofern dieses unterstützt wird).
Key	Der Schlüssel selber (ECK oder CK). Je nach Type ist der Schlüssel 80 oder 128 Bit lang. Der Schlüssel wird in hexadezimale Schreibweise angeben. Es darf optional ein „0x“ vorangestellt werden. Beispiel 80Bit: „0x11111111111111111111“
ESI	Verschlüsselte SSI. Der Wert ändert sich je neuem CCK (sprich andere CCKid). Der Wert wird in hexadezimale Schreibweise angeben. Es darf optional ein „0x“ vorangestellt werden. Beispiel: „0x3CA016“
SSI	Klare Teilnehmer-Nummer. Der Wert wird in dezimal angeben. Beispiel: „5230025“.
Frame	Der Frame (Zeitpunkt) an dem ein Schlüssel aktiviert wird. Vor diesem Zeitpunkt wird der Schlüssel nicht benutzt. Das Format ist: Hyper-Frame(0...65535)**:**Mult-Frame(1...60)**:**Frame(1...18)**:**Slot(1...4).
KSGN	Nummer des Entschlüsselungsverfahren. Es wird von 0 an gezählt. Also TEA1 = 0, TEA2=1, TEA3=2, TEA4=3.
SCK-N	Die Nummer des statischen Schlüssel. Die Werte sind „0...31“.

Parameter	Bedeutung
SCK-VN	Die Version des statischen Schlüssel. Die Werte sind „0...65535“.
GCK-N	Die Nummer des Gruppen Schlüssel. Die Werte sind „0...31“.
GCK-VN	Die Version des Gruppen Schlüssel. Die Werte sind „0...65535“.
AIE class	Benutzte Verschlüsselung: „2“=Statisch; „3“=Dynamisch.
File	Pfad zu einer Datei. Der Pfad darf relativ sein. Es wird dann vom Pfad von der Konfigurations-Datei ausgegangen. Also ein Name ohne weiteren Pfad bedeutet das die Datei sich im gleichen Verzeichnis befindet.

3.3 Beispiel

Die Datei “*AIE.cfg*”:

```
CFG;1
ISIMSG;255;3;163;164;173
GRMSG;0;0;0;255;4;298;299;300;301
# Example for key data:
ISI;262;1234;2000;255;0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
DCK;3691;262;1234;4;5555;66;0x0ABC;2000;50000:01:01:1;255;0;0xFFFFFFFFFFFFFFFFFFFF
SCK;65535;262;1234;255;65535;1;0;255;0;0xFFFFFFFFFFFFFFFFFFFF
DSCK;-1;0;255;0xFFFFFFFFFFFFFFFFFFFF
# User defined group address:
GSI;262;1234;90900;255;0;0;0
# Activate CCK auto storage:
CCKDB;cckdb.csv
# MasDecryptor connection data:
TCB;0;10.102.102.1;5000
```

Die Datei “*cckdb.csv*”, es werden nur CCK Daten gespeichert. Manuell eingefügte Kommentare gehen beim automatischen Speichern verloren:

```
CFG;1
CCK;65535;262;1234;255;5555;100;255;0;0xFFFFFFFFFFFFFFFFFFFF
CCK;65535;262;1234;255;5555;101;255;0;0xFFFFFFFFFFFFFFFFFFFF
```

4 Verschlüsselung der Schlüssel-Datei

Die Schlüssel-Datei enthält sicherheitskritische Informationen. Insbesondere der **SCK**, **GCK** und **K** Schlüssel müssen besonders geschützt werden. Um diese sicherheitskritischen Informationen zu schützen, gibt es die Möglichkeit diese Textdatei im CSV Format zu speichern und dabei zu verschlüsseln. Für die Verschlüsselung der Textdatei wird die Hardware-Verschlüsselung des am PC angeschlossenen USB-Dongle benutzt. Dabei wird die unverschlüsselte Textdatei in eine Verschlüsselte umgewandelt. Anschließend ist die Rückumwandlung der verschlüsselten Datei in eine unverschlüsselte Schlüssel-Datei **nicht** mehr möglich. Nach dem Laden der verschlüsselten Schlüssel-Datei entschlüsselt die MultiAnalyzer Software die Datei intern mit Hilfe des angeschlossenen Dongles und hält die Daten für die Dauer der Protokoll-Analyse intern im Speicher. Anschließend werden die Daten wieder aus dem Speicher gelöscht.

Des weiteren wird eine unveränderliche Liste in der verschlüsselten Datei abgelegt. Bei der Liste handelt es sich um eine Positivliste mit USB-Dongle Hardware Nummern oder Bereichen, denen es erlaubt ist, die Daten der Schlüssel-Datei zu benutzen. Das bedeutet, stimmt die Dongle Hardware Nummer nicht mit einem Eintrag in der Liste überein, wird die Benutzung die Schlüssel-Datei von der MultiAnalyzer Software abgelehnt. Die Schlüssel-Datei ist damit an ein oder mehrere Dongle gebunden.

Die Entschlüsselung der Schlüssel-Datei wird transparent durchgeführt. Das bedeutet, ist ein positiv gelistetes Dongle mit dem Analyse-Rechner verbunden, ist keine weitere Aktion notwendig.

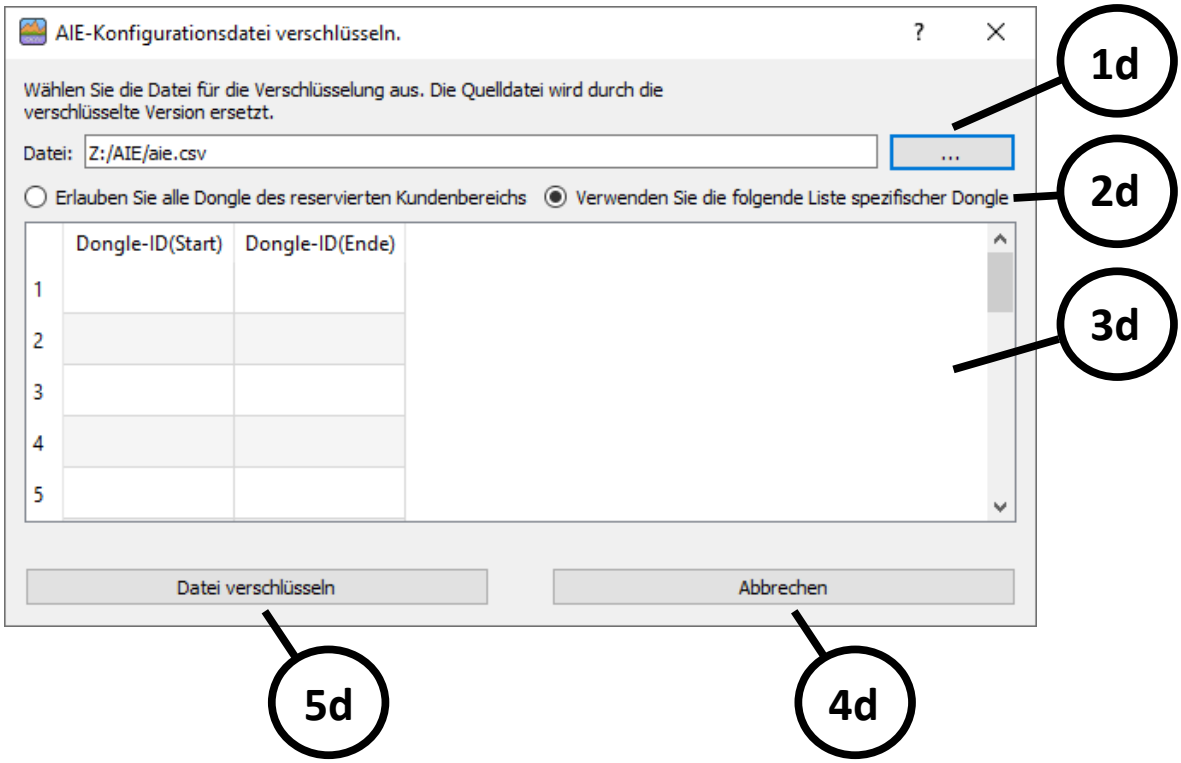
Mit dem Eintrag „`CCKDB;cckdb.csv`“ werden die CCK automatisch in einer weiteren Datei gespeichert. Auch diese CCK-Datenbank kann verschlüsselt werden. Dabei werden die Einstellungen der Schlüssel-Datei entsprechend der folgenden Tabelle mit vererbt.

original Schlüssel-Datei	**original** CCK-Datenbank	**Erklärung**	**neue** CCK-Datenbank
klar	-	Wenn keine cckdb.csv Datei existiert und die Schlüssel-Datei unverschlüsselt ist, dann wird eine neue cckdb.csv Datei **unverschlüsselt** erstellt.	klar
klar	klar	Wenn ein cckdb.csv Datei im Klartext existiert und die Schlüssel-Datei unverschlüsselt, ist dann wird eine geänderte cckdb.csv Datei **unverschlüsselt** abgelegt.	klar
verschlüsselt	-	Wenn keine cckdb.csv Datei existiert und die Schlüssel-Datei verschlüsselt ist, dann wird eine neue cckdb.csv Datei **verschlüsselt** erstellt.	verschlüsselt
klar	verschlüsselt	Wenn ein cckdb.csv Datei verschlüsselt existiert und die Schlüssel-Datei unverschlüsselt ist, dann wird eine geänderte cckdb.csv Datei weiterhin **verschlüsselt** abgelegt.	verschlüsselt
verschlüsselt	klar	Wenn ein cckdb.csv Datei im Klartext existiert und die Schlüssel-Datei verschlüsselt ist, dann wird eine geänderte cckdb.csv Datei **neu verschlüsselt** abgelegt.	***verschlüsselt*** (geändert!)
verschlüsselt	verschlüsselt	Wenn ein cckdb.csv Datei verschlüsselt existiert und die Schlüssel-Datei verschlüsselt ist, dann wird eine geänderte cckdb.csv Datei weiterhin **verschlüsselt** abgelegt.	verschlüsselt

4.1 Eine Datei verschlüsseln

Um eine Schlüssel-Datei oder eine CCK-Datenbank-Datei zu verschlüsseln, muss die Ausgangsdatei unverschlüsselt vorliegen. Das Umschlüsseln von Dateien ist nicht möglich.

Im Programm MultiAnalyzerMsc und MultiAnalyzerQoS befinden sich im Menü jeweils der Punkt „AIE-Konfigurationsdatei verschlüsseln...“. Dieser Punkt ist in der MSC unter „Menü/Protokoll/“ und in der QoS unter „Menü/Einstellungen/TETRA/“ zu finden. Beim Anwählen des Punktes erscheint der Dialog mit den Einstellungen:



Nr	Beschreibung	
1d	Anzeige und Auswahl der Datei die verschlüsselt werden soll.	
2d	Welche Dongle sind für den Datei-Zugriff freigegeben.	
	Erlauben Sie alle Dongle des reservierten Kundenbereichs	Für jeden Kunden ist ein Bereich von 1000 Dongle reserviert. Der komplette Bereich des aktuell angeschlossenen Dongle wird automatisch in die Positivliste eingetragen.
	Verwenden Sie die folgende Liste spezifischer Dongle	Es können bis zu 20 individuelle Dongle und/oder Bereiche in der Liste unter Punkt **3d** eingetragen werden.
3d	Dies ist die Positivliste der zugriffsberechtigten Dongle auf die verschlüsselten Dateien. Es wird jeweils die Dongle-Nummer eingetragen. Für Dongle-Nummer-Bereiche werden die Start-Nummer und die End-Nummer eingetragen. Es können bis zu 20 Einträge vorgenommen werden. Es muss aber mindestens ein Eintrag vorhanden sein.	
4d	Die Verschlüsselung abbrechen. Es werden keine Veränderungen durchgeführt.	
5d	Die Datei wird mit den getroffenen Einstellungen verschlüsselt. **Dabei wird die unverschlüsselte Originalversion der Datei ersetzt!**	