Die Ermittlung und Verwendung des CCK in der MAS

(MultiAnalyzer Software)

Version A1

Index of contents

1 History

Date	Version	Author	Comment
2017-09-11	A1	GH/SZ	• Initiale Version

2 Die TETRA Schlüssel

Es gibt drei wesentliche Schlüssel für das BDBOS Netzwerk:

- Der **DCK** Schlüssel wird zur individuellen Kommunikation vom/zum Endgerät verwendet. Der DCK ist kein fester Schlüssel er wird aus der Authentifizierung generiert. Er ändert sich mit jeder Authentifizierung des Endgerätes (zum Beispiel bei der Registrierung nach dem Einschalten oder Zellwechsel). Um den DCK eines Endgeräts zu ermitteln wird der geheime **K** Schlüssel des Endgerät benutzt.

- Der **CCK** Schlüssel wird zur Gruppen-Kommunikation benutzt. Ist dieser bekannt kann die gesamte Gruppen-Signalisierung ausnahmslos entschlüsselt werden. Der CCK Schlüssel ist für eine Zelle identisch aber von Zelle zu Zelle verschieden. Jeder CCK Schlüssel ist etwa 3 Wochen lang gültig, bevor er manuell (per Script) aktualisiert wird. Der CCK wird verschlüsselt über die Luft übertragen. Um den CCK zu entschlüsseln wird der dazugehörige DCK Schlüssel benutzt. Da der CCK für alle Endgeräte gleich ist, genügt die Kenntnis eines DCK um einmalig den CCK für die gesamte Zelle zu ermitteln.

- Der **SCK** Schlüssel wird für DMO und für eine TMO Zelle im „Fall-Back-Modus“ verwendet. Im Im „Fall-Back-Modus“ hat die Zelle die Verbindung zum Backbone verloren und kann auch nicht mehr auf das Authentication-Center zugreifen, um den K für das jeweilige Endgerät abzufragen. Er ist statisch und wird nicht über die Luft übertragen (Ausnahme: Schlüssel-Update über die Luft). Der SCK wird per Konfiguration in das Endgerät geschrieben.

Ziel des Dokumentes ist den Vorgang zu beschreiben einen CCK Schlüssel zu ermitteln, diesen aus der Aufnahme zu extrahieren und dauerhaft der Entschlüsselung zur Verfügung zu stellen.

2.1 Vom DCK zum CCK

Der **CCK** Schlüssel wird verschlüsselt als **SCCK** (**S**ealed **C**ommon **C**ypher **K**ey) über die Luft in einer individuellen Nachricht (zum Beispiel während der Registrierung des Endgerätes nach dem Einschalten) übertragen. Dieser **SCCK** ist mit dem individuellen Schlüssel **DCK** des Endgerätes verschlüsselt. Um an den CCK zu gelangen muss darum der benutzte DCK ermittelt werden.

Der DCK wird jedes mal während einer **Authentifizierung** generiert. Dazu wird sowohl von der Infrastruktur als auch vom Endgerät der **K** des Endgerätes benutzt, ohne diesen selbst über die Luft zu übertragen. Die Authentifizierung findet bei jedem unverschlüsselten Einbuchen (egal ob Zellwechsel oder initiales Einschalten) statt. Wenn der CCK der Zelle dem Endgerät noch nicht bekannt ist, fordert es ihn an. Bei einem Zellwechsel zurück in eine Zelle, die schon mal besucht wurde, kann der CCK dem Endgerät schon bekannt sein, es fordert ihn darum nicht noch mal an. Beim Einschalten des Endgerätes ist der CCK nicht bekannt und wird darum angefordert. Zudem hat das Endgerät beim Einschalten auch noch keinen DCK generiert. Beide Schlüssel (DCK,CCK) werden also beim **Einschalten**, dem initialen Registrieren, dem Endgerät zugänglich gemacht.

Mit Hilfe des K-Schlüssels des Endgerätes kann die MultiAnalyzer Software das Generieren des DCK nachvollziehen und ebenfalls den verschlüsselten SCCK zu einem CCK entschlüsseln.

Bei der Authentifizierung werden über die Luftschnittstelle zwei Zufallszahlen im Downlink und Eine im Uplink übertragen. Diese drei Zufallszahlen werden von MultiAnalyzer Software benötigt, um die DCK Generierung nachzuvollziehen. Aus diesem Grund muss der Einschaltvorgang mit Registrierung und Authentifizierung **im Downlink wie im Uplink** aufgenommen werden. Dabei muss der **K-Schlüssel** (von der BSI-Karte) des Endgerätes bekannt sein, dessen Einschaltvorgang aufgezeichnet wurde.

Mit Hilfe des bekannten DCKs kann die MultiAnalyzer Software den SCCK entschlüsseln und den entschlüsselten CCK zur Verfügung stellen. Der CCK gilt Zell-weit für alle Endgeräte und muss darum nur einmal ermittelt werden. Der CCK ist im BDBOS-Netz etwa 3 Wochen lang gültig. Erst nach einem Wechsel muss die neue Version erneut ermittelt werden. Ein Wechsel des CCK wird durch eine Änderung der CCK-ID, enthalten im Broadcast der Infrastruktur, angezeigt.

Sobald der CCK einmal ermittelt wurde und dann permanent in die AIE-Konfiguration eingetragen wurde, ist ein erneutes ermitteln über die Luftschnittstelle nicht mehr notwendig. Weitere Aufnahmen der Zelle können nun auch ohne Uplink stattfinden, da der CCK in diesem Fall aus der Konfigurations-Datei geladen wird.

3 Ermittlung des CCK Schlüssel

3.1 Vorbereitung

Zum Ermitteln des CCK werden folgende Dinge gebraucht:

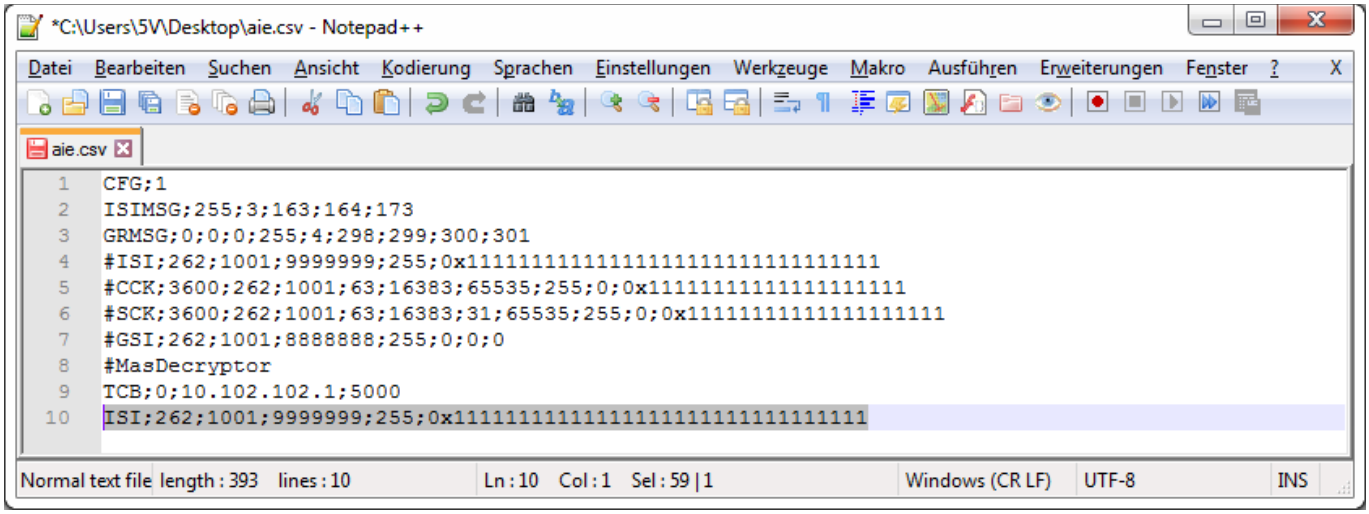
- Ein **Endgerät**.
- Der **K-Schlüssel** von der BSI-Karte des Endgerätes.
- Zwei Aufnahme-Geräte (für **Downlink** und **Uplink**) für den MultiAnalyzer.
- Ein **MASDecryptor** mit freigeschalteten **TAA1** Algorithmen.
- Die richtigen **Empfangsbedingungen** damit sich das Endgerät direkt nach dem Einschalten in die gewünschte Zelle einbucht.

3.2 Eintragen des K-Schlüssels in die AIE Konfiguration

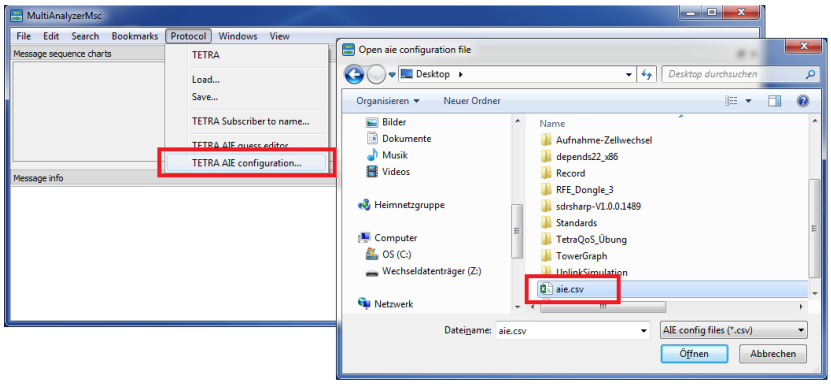
Damit die MultiAnalyzer Software den DCK ermitteln kann, muss der **K-Schlüssel** des Endgerätes bekannt gemacht werden. Dieses geschieht in der Verschlüsselungs-Konfigurations-Datei.

Der K-Schlüssel wird mittels der Zeile „**ISI**“ in der Datei abgelegt. (Ein vorangestelltes „**#**“ Zeichen markiert jeweils eine auskommentierte Zeile.)

- Das Netz „**262**“ (MCC) und „**1001**“ (MNC) identifizieren das Netzwerk. Gegenfalls kann bei einer Testzelle auch auch die MNC „**1002**“ vorkommen. Dieser ist dann einzutragen.
- Die „**9999999**“ ist mit der **ISSI** (Teilnehmer-Nummer, nicht OPTA) des Endgerätes zu ersetzen.
- Die „**0x11111111111111111111111111111111**“ ist mit dem **K-Schlüssel** des Endgerätes zu ersetzen. Dabei ist zu beachten das dem K-Schlüssel ein „**0x**“ vorangestellt wird.

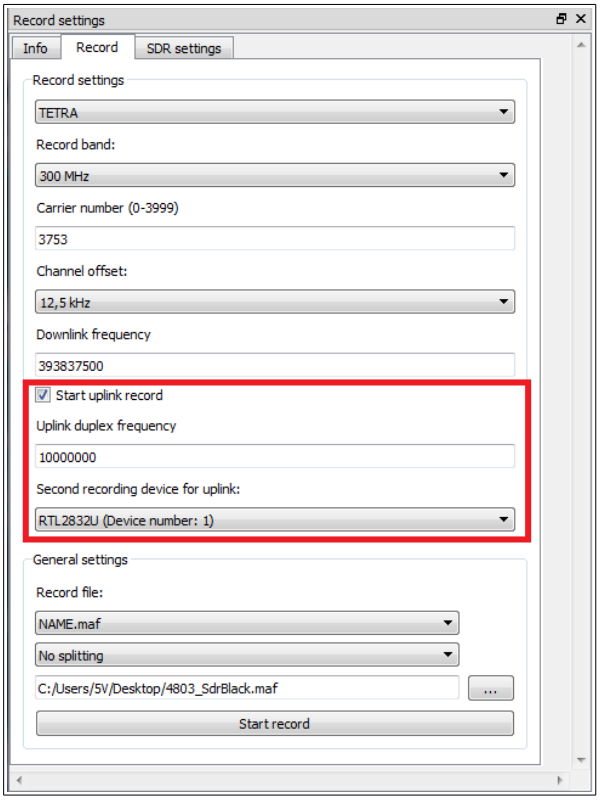


Hinweis: *Die MultiAnalyzerMsc und die MultiAnalyzerQoS müssen die Konfigurations-Datei laden damit die Konfiguration benutzt wird. Dieses passiert über den Menü-Punkt „TETRA AIE configuration...“ im Menü „Protocol“. Dabei wird der Ort der Datei (nicht der Inhalt) gespeichert. Bei jedem Neustart oder erneuten Analyse wird der Inhalt dieser Datei automatisch neu geladen. Sofern der Ort der Datei nicht geändert wird, muss diese Datei also nur einmal den beiden Programmen angeben werden. Ein geänderte Inhalt wird automatisch bei der erneuten Analyse übernommen:*

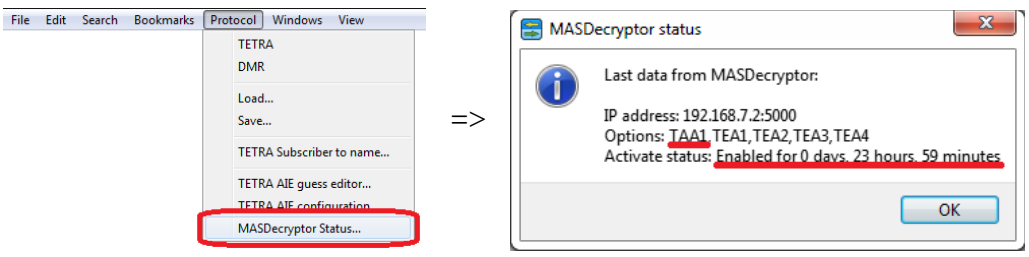


3.3 Die Aufnahme starten

Zum Ermitteln des CCK werden Uplink wie Downlink benötigt:



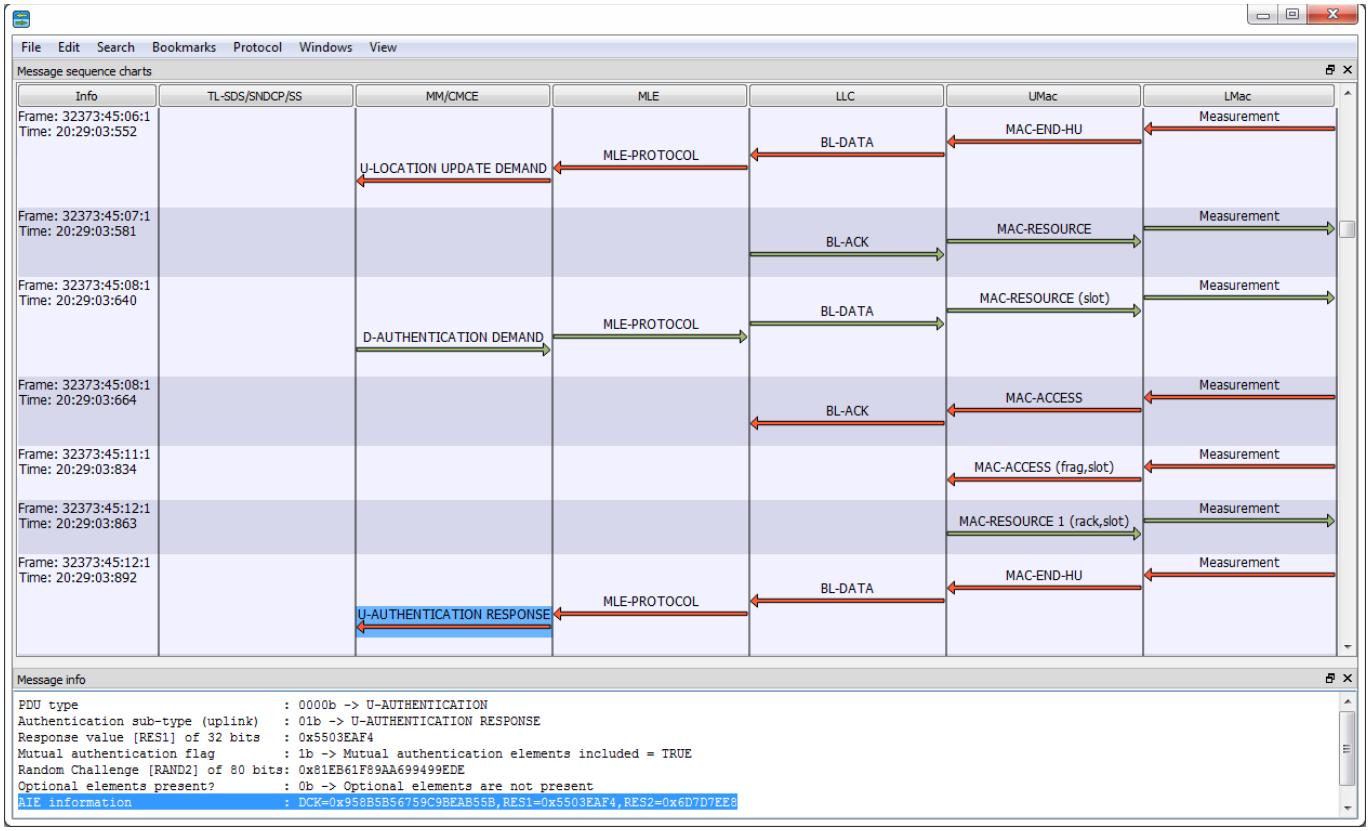
- Die Zelle wird im Downlink ausgewählt (Hier zum Beispiel der Kanal 3753).
- Die Uplink Aufnahme mit dem Hacken „**Start uplink record**“ aktiviert.
- Der Duplex-Abstand ist im BDBOS-Netzwerk **10MHz** (der Wert wird in Hz angeben.)
- In der Drop-Down-Box „**Second recording device for uplink**“ wird nun die Aufnahme-Hardware ausgewählt.
- Mit dem Knopf „**Start Record**“ wird die Aufnahme gestartet.
- Der CCK wird in der MultiAnalyzerMSC ausgeben. Darum wird diese mit dem Knopf „**Message charts**“ gestartet.
- Optional kann überprüft werden, ob die MultiAnalyzerMSC eine Verbindung zum MASDecryptor hat und ob die TAA1 Algorithmen freigeschaltet sind. Dazu wird in der MSC im Menü „Protocol“ der Punkt „MASDecryptor Status...“ verwendet:



3.4 Die Aufnahme und der CCK

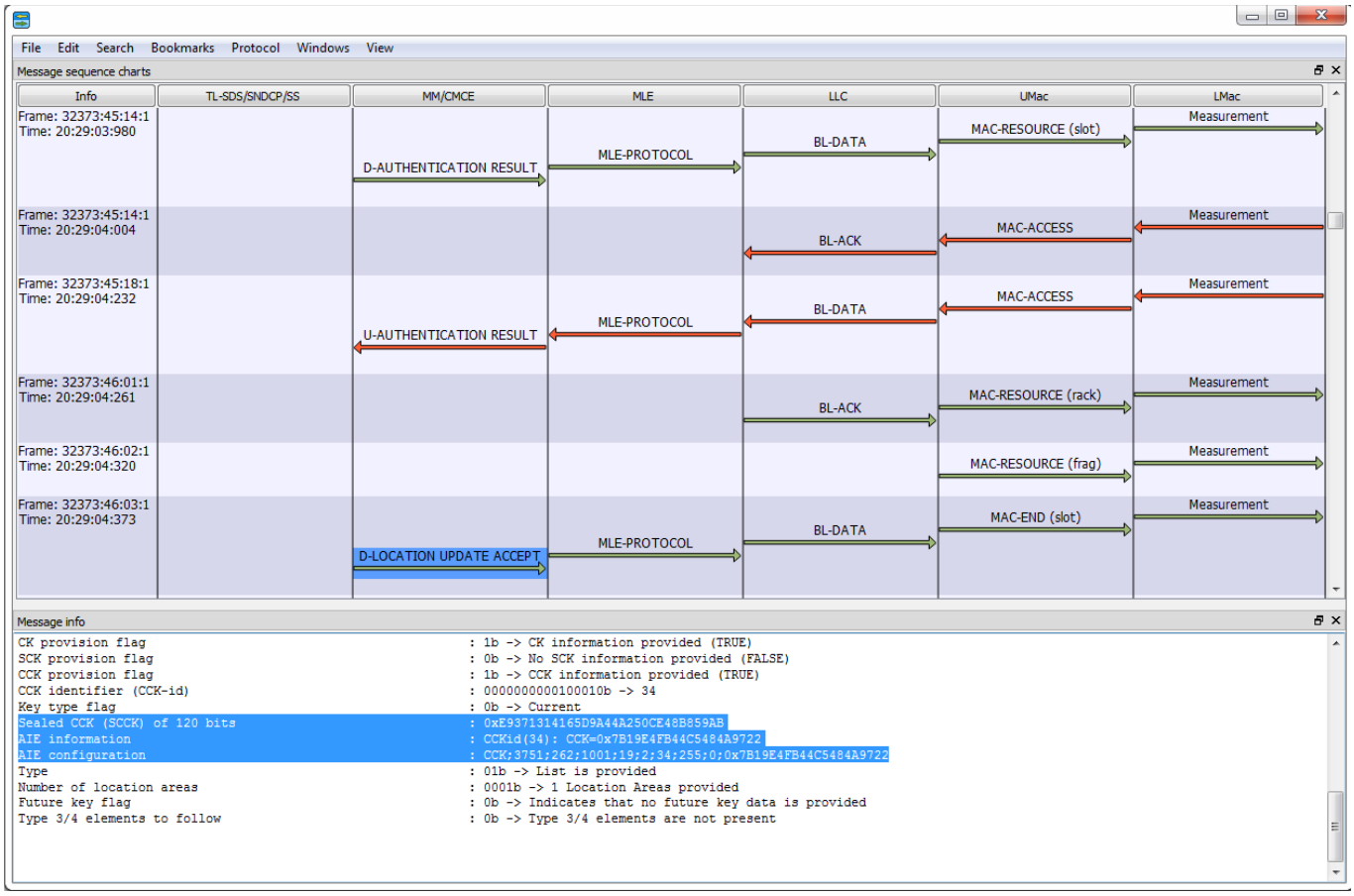
Nach dem die Aufnahme gestartet wurde, kann das Endgerät eingeschaltet werden. Das Endgerät registriert sich nun. Die Registrierung erfolgt unverschlüsselt. Das bedeutet das die ISSI des Endgerätes und diese Daten der Nachrichten in der MSC unverschlüsselt dargestellt werden.

Die benötigten Zufallszahlen werden in den Nachrichten: „**D-AUTHENTICATION DEMAND**“ (downlink) und „**U-AUTHENTICATION RESPONSE**“ (uplink) übertragen. Sofern diese beiden Nachrichten empfangen wurden und der K-Schlüssel für die betreffende SSI eingetragen wurde wird der DCK ermittelt. Der DCK wird unverzüglich in der Nachricht „U-AUTHENTICATION RESPONSE“ ausgeben:



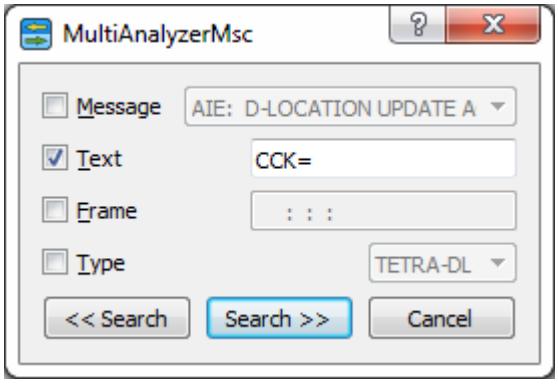
Sofern kein DCK ausgeben wird, steht in der Zeile „**AIE information:**“ der Grund dafür. Siehe dazu mehr in 3.4.1 Fehlermeldungen in der Zeile „AIE information“.

Der verschlüsselte SCCK wird in der Nachricht „**D-LOCATION UPDATE ACCEPT**“ gesendet. Diese Nachricht schließt den erfolgreichen Registrierung-Vorgang ab:



Da der DCK ermittelt wurde, kann nun auch der Zellweite gültige CCK entschlüsselt werden. Wenn kein DCK ermittelt wurde dann fehlen die Zeilen „**AIE information**“. Sollte ein Fehler beim CCK entschlüsseln aufgetreten seinm dann wird der Grund ausgeben, siehe dazu mehr in 3.4.1 Fehlermeldungen in der Zeile „AIE information“.

Hinweis: Der entschlüsselte CCK kann sehr schnell mittels der Suchfunktion aufgefunden werden. Dazu wird der Suchdialog aufgerufen und nach dem Text „**CCK=**“ (in Großschreibung) gesucht:



Sofern ein entschlüsselter CCK vorhanden ist, wird die MSC zur betreffenden „**D-LOCATION UPDATE ACCEPT**“ Nachricht springen. Im Text zur Nachricht stehen dann die CCK Daten.

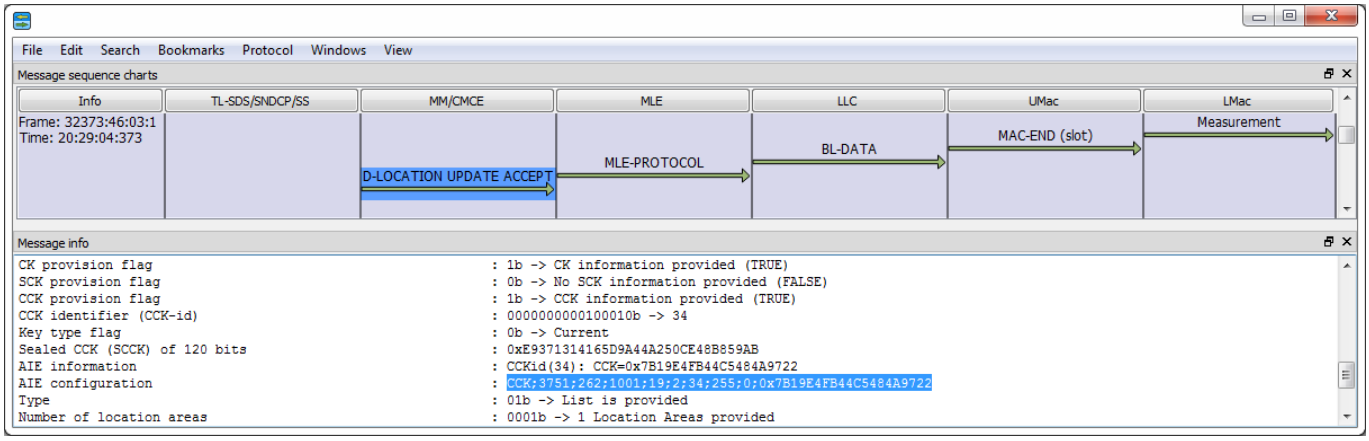
3.4.1 Fehlermeldungen in der Zeile „AIE information“

Mögliche Fehlermeldungen werden im Nachrichtentext „**AIE information:**“ ausgegeben:

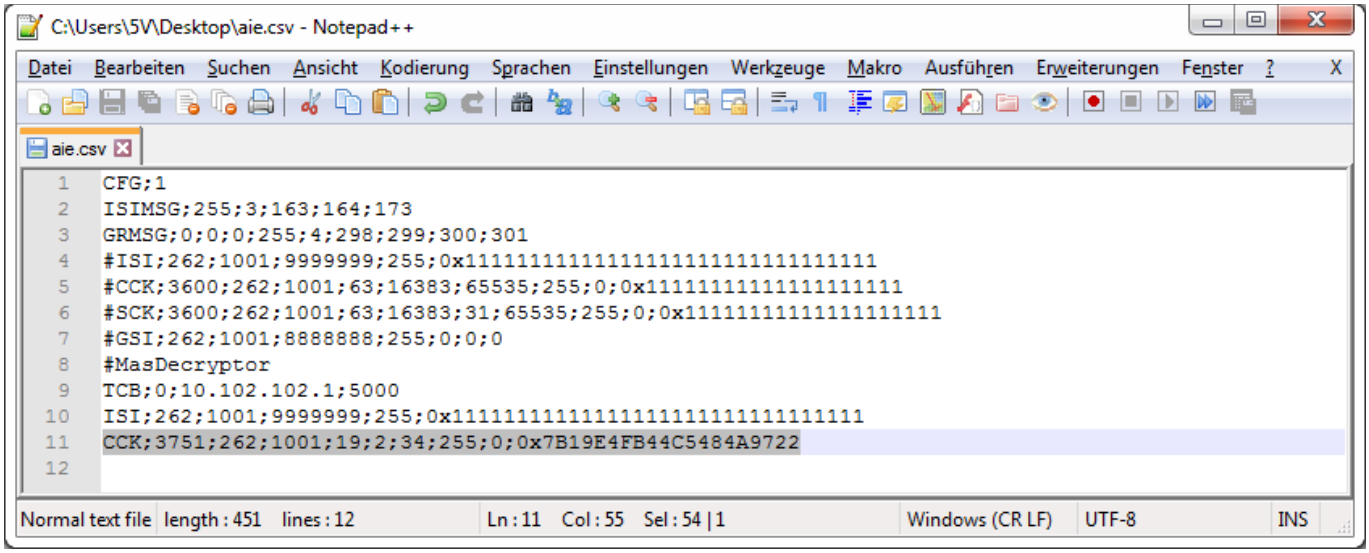
Meldung	Bedeutung
Not connected	Der MASDecryptor ist nicht angeschlossen oder die IP-Adresse ist in der Konfigurations-Datei falsch gesetzt.
Can not generate DCK: No K for subscriber!	Der K-Schlüssel ist nicht in der Konfiguration eingeben. Gegenbefalls die ISSI, MCC und MNC überprüfen.
Can not unseal CCK: Manipulation flag is TRUE!	Der CCK konnte nicht richtig entschlüsselt werden. Dieses kann vorkommen wenn der DCK nicht richtig ermittelt wurde. Ursächlich dafür kann ein falscher K-Schlüssel sein.
MasDecrytor: HW result: -11 oder MasDecrytor: Unsupported or expired algorithm.	Die AIE Algorithmen sind nicht im MASDecryptor vorhanden oder die aktivierte Laufzeit ist abgelaufen.
MasDecrytor: Expired algorithm	Die aktivierte Laufzeit ist abgelaufen.

3.5 Eintragen des CCK in der AIE Konfigurations-Datei

Nachdem der CCK ermittelt wurde und in der Nachricht „**D-LOCATION UPDATE ACCEPT**“ ausgeben wurde, kann dieser permanent in die Konfigurations-Datei eingetragen werden. Es werden nach der Zeile „**Sealed CCK (SCCK) of 120 bits**“ zwei Zeilen „**AIE information:**“ mit den CCK Daten ausgeben. In der oberen Zeile wird der CCK direkt ausgeben, die Untere ist eine Zusammenstellung für die Konfigurations-Datei:



Das bedeutet, dass der Inhalt der untere Zeile markiert, kopiert und in die Konfigurations-Datei eingefügt werden kann:



Damit ist der CCK dauerhaft der MultiAnalyzer Software bekannt gemacht worden. Eine erneute Ermittlung ist für diese Version (CCKid) nicht mehr nötig. Erst bei einem CCK-Wechsel muss die neue Version erneut ermittelt werden.