FAQ: Keyfileaufbau und Konvertierung für Anfänger

Aufbau der Keyfiles.

Dokumentation by mincat

Diese Doku ist nicht komplett und geht nicht bis ins letzte Detail sonderen soll Anfängern einen Einblick in Keyfiles und deren Aufbau geben.

1.) Allgemeines:

Key ist nicht gleich Key. Je nach Verschlüsselungssystem gibt es erhebliche Unterschiede in der Art und Weise wie die Keys funktionieren.
Wir müssen zunächst einmal unterschieden, was für ein Key vor uns liegt. Generell gibt es z.B. den RSA (Masterkey) und den IDEA (Key), es gibt Autoupdate-Key's usw.
Mit AU (A uto U pdate) kann ein Key automatisch erkannt und benutzt werden. Keybundeles die rotieren (Autoroll) werden auch oft AU genannt.
Was sich ändert ist in der Regel nur der normale Key. Und nur dieser muß meist ausgewechselt oder zugefügt werden.

2.) Der Standard-Key:

Ein Standard-Key setzt sich aus einer Reihe von Informationen zusammen:
Cryptsystem
Provider-ID
Keyposition

Key (8 oder 16 Hexzahlen)

Beispiel (Softcam):
N 4E01 00 xxxxxxxxxxxxxxxx ; Dream TV

N = Nagra
4E01 = DreamTV (Diese Kennung ist fest, für jeden Provider!)
00 = Key Nummer 0
xxxxx = Key
Der Kommentar dahinter wird durch ein ; gekennzeichnet!

Statt N sind auch möglich I (Irdeto), V (Viacess), W (Cryptoworks), S (Seca), C (Conax), D (Direct Control Word), B (BetaCrypt), F (Biss) usw.

Bei einigen Cryptsystemen (z.B, Nagra2) kommen noch Zusatzkey's ins Spiel. Der Masterkey ist länger und hat die Keynummer(n) M1, M2 und den Zusatz X1,
dann gibt es noch Ex und Nx-Key's als Erweiterungen.
Was jeder Key in der Emu im Detail macht ließe sich nur mit einer Aufschlüsselung der jeweiligen Cryptalgorythmen erklären.
Die Direct Control Word's lassen wir mal weg, die gehen wieder anders.

3.) Konvertierung
Alle Key's in allen Keyfiles bauen immer auf diesen Daten von SoftCam.key auf. Nur ihre Darstellung variiert von File zu File.
Beim Humax z.B. ist alles in einem Bin-File das mit einem Editor bearbeitet wird, wo unter der Providerkennung der Key eingetragen wird.
Kennt man den Aufbau eines Files, kann man das nächste verstehen und die Daten konvertieren. Z.B.:
camd3.key:
1800:002D01:0000000000:00:xxxxxxxxxxxxxxxx SABC

1800 = Nagra
002D01 = SABC (Diese Kennung ist fest, für jeden Provider!)
0000000000 = Keytyp, in der Regel 0 sonst dem letzten Eintrag im Keyfile entnehmen
00 = Key Nummer 0
xxxxxx = Key
Der Kommentar dahinter wird durch eine leere Stelle gekennzeichnet!

Der Trick ist, N in 1800 (Nagra) bzw. 1801 (Nagra2) zu wandeln bzw. umgekehrt und die Providerkennung auf 4 bzw. 6 Stellen zu bringen (links mit Nullen)
Der Key kann einfach übernommen werden! Diese Kennungen sind

bekannt und nichts geheimnissvolles, in den bestehenden Keyfiles sind alle großen Provider und Cryptsysteme drin.

Bei langen Keys (16 Hexzahlen bzw. 32 Stellen) wird der Key bei manchen Keyfiles in der Mitte mit : oder leerzeichen gesplittet. Das ist aber leicht zu sehen.
Einfach die vorhandenen Key's ansehen.

Komplizierter ist es, wenn Masterkey's (RSA) oder AU-Key's etc. gewechselt werden müssen. Aber auch diese sind im Keyteil immer gleich.

Für einige CI-Module ist der Key nicht in HEX zondern dezimal dargestellt. Dann muß gerechnet werden. Statt 0F ist dann 016 die korrekte Darstellung.
In Window's kann man z.B. Hex nach Dezimal umwandeln um umgekehrt. Immer drei Decimal-Ziffern werden zu zei Hex bzw. umgekehrt.
Hex = 00 bis FF
Dec = 000 bis 255

Sagen wir, wir erhalten einen neuen D+ Key, der da lautet 0123456789ABCDEF0123456789ABCDEF und in der Beschreibung Steht folgendes:
D+ Key 1 = 0123456789ABCDEF
So, wie jetzt ins Keyfile? Da fehlt doch die Hälfte... nein, wir haben alles,was wir brauchen! Denn wir wissen den Rest bereits!
D+ ist Providerid 4101 und Sendet in Nagra2 (1801) und dazur ergibt sich:
Softcam.key:
N 4101 01 0123456789ABCDEF0123456789ABCDEF ; D+
camd3.key:
1801:004101:0000000000:01:0123456789ABCDEF0123456789ABCDEF D+

So, kleine Übung
TV Cabo Key 0 = AA BB CC DD EE FF 00 11 22 33 44 55 66 77 88 99
Softcam.key:
N 4901 00 AABBCCDDEEFF00112233445566778899 ; TV Cabo
camd3.key:
1801:004901:0000000000:00:AABBCCDDEEFF001122334455 66778899 TV Cabo

Aber was, wenn der key so aus sieht:
TV Cabo
00: AA BB CC DD EE FF 00 11
01: 22 33 44 55 66 77 88 99

Macht nichts! Das ist typisch für die Darstellung beim Humax! Einfach beide Teile zusammen fügen. Bei dieer Darstellung wäre der nächste keyblock 02 + 03 was bei Softcam.key und camd3.key dann Key 01 ist usw.!

Wenn man sich mit diesem Basiswissen bewaffnet ein wenig mit den Files beshäftigt, sich diese mal genauer ansieht und auch ruhig mal einige vergleicht dann wird man schnell dahinter kommen, wie welche Files im Detail aufgebaut ist.

Um es mal auszuprobieren, ob es mit dem Verständnis geklappt hat:

Macht eine Kopie vom camd3.key's auf der Box und löscht ALLE Key's raus.

Jetzt versucht mal den Key vom ORF aus der Softcam.key in die leere camd3.key ainzubauen. Wird es damit hell, war alles richtig. Aber vorsicht!
Beim ORF sind derzeit zwei Key's bekannt! Nämlich der für CryptoWorks und der für BetaCrypt.
Wenn es nicht klappt, infach mal den selbst gebauten Key mit dem echten aus der camd3.key vergleichen und nachsehen, wo der Fehler ist. Mit ein wenig Übruung ist das kein großes Problem!

Ich hoffe, das hilft ein wenig weiter!
minicat's sig:Grettings

Minicat

http://www.satnet.ch/softcam/Softcam.key

http://www.satnet.ch/

THX to Minicat
Keymaker