TECHNISCHE
UNIVERSITÄT
DARMSTADT
Fachbereich Informatik
Theoretische Informatik – Kryptographie und Computeralgebra
Herr Prof. Dr. rer. nat. Johannes Buchmann

Security of Digital Enhanced Cordless Telecommunication (DECT) devices for residential use

Diplomarbeit

Betreuer: Erik Tews
e_tews@cdc.informatik.tu-darmstadt.de

Alexandra Mengele
alexandra-mengele@web.de

Darmstadt, 09.04.2009

Ehrenwörtliche Erklärung

Hiermit versichere ich, dass ich die vorliegende Diplomarbeit ohne Hilfe Dritter und nur mit den angegebenen Quellen und Hilfsmitteln angefertigt habe. Ich habe alle Stellen, die ich aus den Quellen wörtlich oder inhaltlich entnommen habe, als solche kenntlich gemacht. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Darmstadt, am 09. April 2009

Abstract

The Digital Enhanced Cordless Telecommunication (DECT) standard provides voice, data and networking applications; currently there are about 31.5 million DECT devices only in Germany. Attacks and new analysis methods were published on www.dedected.org in 2008. In this thesis DECT devices of different manufacturers were analysed with the help of the named methods; due to that it was firstly possible to deliver insight into the current security status of DECT devices for residential use. The amount of implemented security mechanisms as recommended by the European Telecommunication Standard Institute (ETSI) is revealed through these examinations. Finally this thesis arrives to the conclusion that none of the tested devices provides a global protection of authenticity and privacy.

Zusammenfassung

Der Digital Enhanced Cordless Telecommunication (DECT) Standard ist ein Standard für Schnurlostelefone und kabellose Datenübertragung; allein in Deutschland werden zum jetzigen Zeitpunkt schätzungsweise 31.5 Millionen Geräten betrieben. 2008 wurden neue Angriffsszenarien und Analysemöglichkeiten auf www.dedected.org veröffentlicht. Um erstmals einen Einblick in den aktuellen Sicherheitsstatus der zurzeit auf dem Markt befindlichen Geräte geben zu können, wurden in dieser Arbeit Geräte verschiedener Hersteller mit den genannten Analysemethoden untersucht. Die Untersuchungen legen offen, inwieweit die vom European Telecommunication Standard Institute ETSI empfohlenen Sicherheitsmechanismen implementiert sind. Letztendlich kann als Ergebnis der Arbeit festgehalten werden, dass keines der untersuchten Geräte einen ganzheitlichen Schutz der Sicherheitsziele Authentizität und Privatheit bietet.

Table of Figures

Table Directory

Table of Contents

Table of Abbreviations

A11, A12	Authentication Processes
A21, A22	Authentication Processes
AC	Authentication Code
B1, B2	Authentication Key Stream Processes
CK	Cipher Key
DCK	Derived Cipher Key
DECT	Digital Enhanced Cordless Telecommunication™
DECT card	COM-ON-AIR PCMICA Card type 2 from, DOSCH+AMAND
ETSI	European Telecommunications Standard Institute
FP	Fixed Part
FritzBox	FRITZ!Box Fon WLAN 7270
FT	Fixed Radio Termination
IV	Initialization value obtained from frame counter
K	Authentication Key
KS	Session Authentication
KS’	Reverse Authentication Key
KSG	Key Stream Generator
MC	Multi Carrier
PABX	Private Automatic Branch Exchange
PP	Portable Part
PT	Portable Radio Termination
RAND_F	Value generated and transmitted by the PP
RAND_P	Value generated and transmitted by the FP
RES1	Value computed and transmitted by PP
RES2	Value computed and transmitted by FP
RF	Radio Frequency

RFP	Radio Fixed Part
RFPI	RFP Identity
RS	Value transmitted by FP in authentication protocol
RSSI	Radio Signal Strength Indicator
PRNG	Pseudo Random Number Generator
SCK	Static Cipher Key
TDD	Time Division Duplex
TDMA	Time Division Multiple Access
UAK	User Authentication Key
UPI	User Personal Identity

1 Preliminary note

1.1 Subject of this thesis

Digital Enhanced Cordless Telecommunication (DECT) is a standard for cordless communication. In 1992 it was standardized and is today the de facto standard for cordless telephony. Since 1st January 2009 the use of the predecessor technologies Cordless Telephone 1 (CT1) and CT2 is illegal in Germany [7].

DECT can be used for a wide range of applications and can use various DECT frequency allocations. In more than 100 countries DECT frequencies are available and support voice, data and networking application within a range up to 500 metres [9]. The North American Personal Wireless Telecommunication Standard PWT is based on DECT and provides the same services as DECT [1]. Since 1997 interoperability between devices from different manufacturers has been ensured by the mandatory use of the Generic Access Profile (GAP). Due to the standardisation for interworking mass production of system components is possible, which *"provides significant cost benefits enabling highly attractive price/performance ratios for DECT equipment."* [1]

The DECT security architecture intends to protect the security objectives authenticity and privacy. To achieve this several security services and two proprietary algorithms are used.

This thesis gives an overview of the current security situation of DECT devices for residential use, called in the following consumer devices. On the one hand structural attacks on the actual reverse engineered authentication algorithms as well as the influence of weak Pseudo Random Number Generators (PRNG) are demonstrated. On the other hand a selection of several DECT consumer devices was analyzed to get an idea of the implemented security services.

Finally the lack of security and recommendations to ensure authenticity and privacy are pointed out.

1.2 Proceeding

To point out the relevance of DECT, a brief survey of the DECT standard, its application range and its spreading in Germany is given in section 2.

In section 3 the security architecture and the optional applicable security services are illustrated.

The threats resulting on the one hand from omitting individual security services on the other hand from design flaws are figured out in section 4.

Section 5 describes the proceeding of passive eavesdropping and impersonation of a base station. The existence of the optional security services is analysed for 36 devices to classify them into security levels.

Finally the current lack of security as existent at the tested consumer devices is highlighted in section 6. Furthermore for improvement of DECT security medium-term and long-term suggestions are given.

2 The DECT standard

Digital Enhanced Cordless Telecommunications (DECT) is a standard developed by the European Telecommunications Standard Institute (ETSI) to provide a general radio access technology for wireless telecommunication [1]. In Europe it works in the preferred 1880 to 1900 MHz band. This standard *'can be adapted for many applications and can use various frequency allocations internationally'* [9]. DECT frequencies are available in more than 100 countries and support voice, data and networking applications within a range of up to 500 metres. The ordinary consumer knows the technology mainly from the voice application at the cordless phones at home; but the technology also dominates *'the **P**rivate **A**utomatic **B**ranch e**X**change (PABX) market and is used in the wireless local loop to replace copper in the 'last mile' for user premises.'* [9] Furthermore the standard can be used to provide GSM access, cordless terminal mobility CTM or a local area access supporting voice telephony, fax, modem, E-Mail, Internet and other services.

Since 1992 it is mostly used for voice application, but it can be also used for data and networking applications. The standard and the used security mechanism are open to everyone on www.etsi.org. The developed authentication algorithm and ciphering algorithm are only available under a Non-Disclosure-Agreement to the DECT devices manufacturers.

A DECT system is composed of a Fixed Part (FP), utilising on or more base stations, and one or more Portable Parts (PP). The DECT base standard offers protocols and messages to deal with the air interface between the FP and the PP. Since October 1997 the GAP [5] has been mandatory for voice telephony equipment to ensure interoperability between devices from different manufacturers.

Due to the use of Multi Carrier, Time Division Multiple Access, Time Division Duplex (MC, TDMA, TDD) radio access method and Dynamic Channels

Selection and Allocation DECT can offer excellent quality of service without frequency planning.

Basic DECT frequency allocation uses 10 carrier frequencies (MC) in the 1880 to 1900 MHz range. The time spectrum is subdivided into time-frames, which are repeated every 10 ms. One time-frame is composed of 24 individually accessible timeslots that can be used for transmission or reception (TDMA). The 10 ms time-frames are divided in two halves (TDD). The first 12 timeslots are used for FP transmission (downlink) and the other 12 are used for PP transmission (uplink). Due to the use of TDMA structure DECT offers the possibility of 12 simultaneous basic DECT (full duplex) voice connections per transceiver. In comparison to technologies with only one link per transceiver (e.g. CT2) DECT is the more cost-effective technology.

A DECT base station is constantly transmitting on at least one channel. The unique base station identity, system capabilities, Radio Fixed Part (RFP) status and paging information for incoming call set-up are sent out within these broadcast messages. PPs analyse the broadcast information to learn if they have access rights, determine whether system capabilities match with the services required by them and -if communication is required- whether the RFP has free capacity for a radio link with the PP. DECT devices scan their environment at least every 30 seconds. Thereby they receive and measure the local Radio Frequency RF signal strength on all idle channels; and create a list of free and occupied channels, the so-called Radio Signal Strength Indicator (RSSI) list. Thus the PP or FP is able to pick the best channel for a new communication link. The PP constantly checks the channels with the best RSSI value whether it has access rights for the sending base station. A low RSSI value symbolizes free and non-interfered channels, whereas a high RSSI value symbolizes busy or interfered channels. Dynamic Channel Selection and Allocation guarantees that radio links are always set-up on the least interfered available channel. [1]

A call setup can be PP or FP originated. During a PP originated call setup the PP selects the best available channel for set-up and accesses the FP on this channel. During a FP originated call setup a page message containing the unique portable identity is sent by the FP. When the page message has been received, the PP sets up a radio link on the best available channel. The call initiating party sends a {CC-SETUP} (see appendix section 9) message containing information like the portable identity or the fixed identity to the contrary one [2]. If any of the setup requests cannot be met or the {CC-SETUP} message contains errors or inconsistencies, the contrary party sends a {CC-RELEASE-COM} to reject the call. If the call can be confirmed, a {CC-CONNECT} message is sent to the call initiator.

The significance of the security implementation of DECT can be shown with estimation for the spreading of DECT. The RFP identity (RFPI) of all nearby DECT FPs can be found using a DECT card (Figure 1), a notebook with a Linux installation and the software from www.dedected.org.

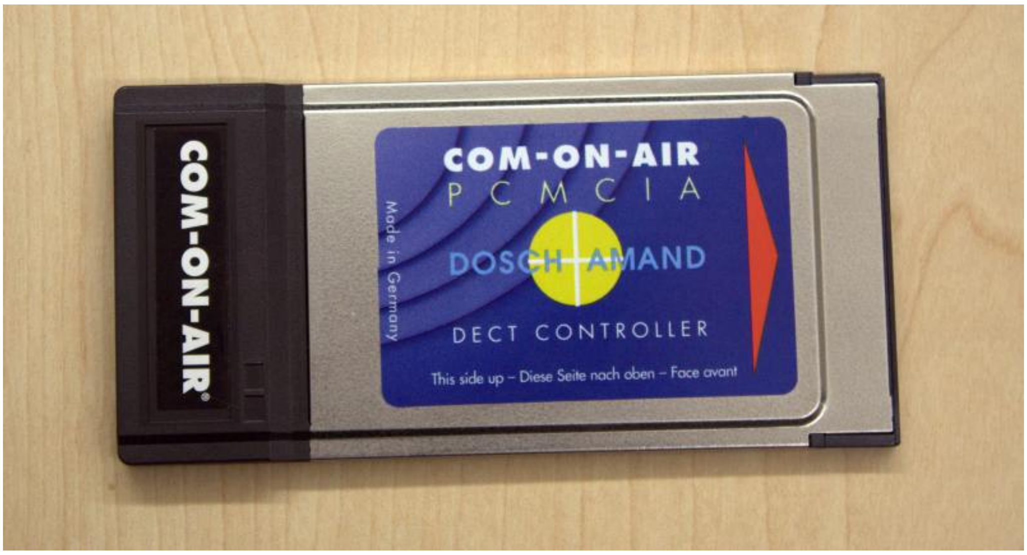


Figure 1: A DECT Card of type 2 from DOSCH+AMAND

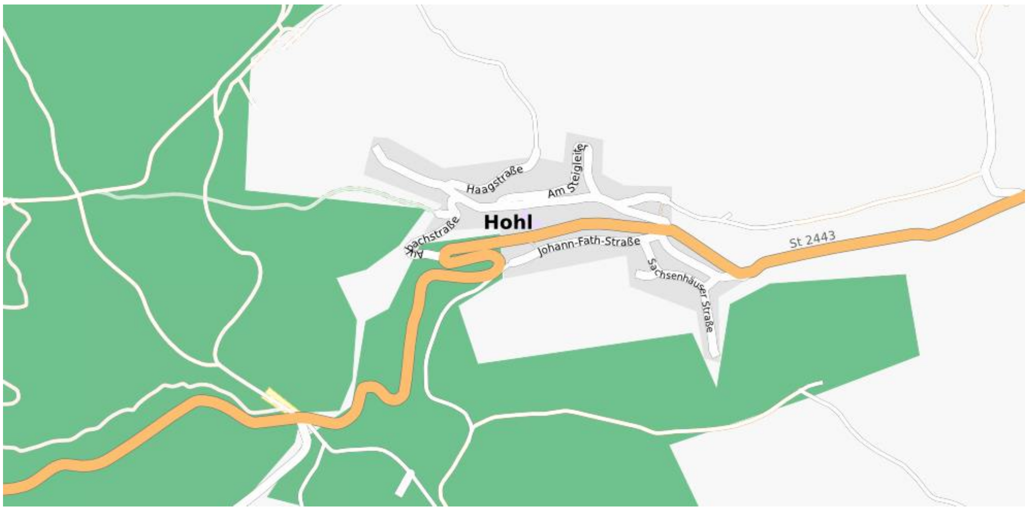


Figure 2: Hohl, 471 residents according to [10]

The data of two closed villages Hohl and Molkenberg that offer no industrial area was analysed (Figure 2). The measurements result in 2.6 residents per FP in Hohl and 2.3 residents per FP in Molkenberg (see appendix: 2. and 3. section, Table 1). In 2007 about 82 million people lived in Germany [8]. Even by appliance of the lower results from Hohl the estimation for Germany is about 31.5 million DECT base stations.

Table 1: Number of inhabitants per base station

Village	Population	Number of base station	Number of inhabitants per base station
Hohl	471	181	2.6
Molkenberg	68	30	2.3

Radio access technology always comes along with serious security risks. The DECT standard provides security services to prevent misuse. Via subscription and authentication procedures unauthorised access can be avoided. Because of the subscription process the network opens its services to a particular PP. The subscription process can be performed either by the manufacturer or by the consumer over the air and assures that the FP and the PP are in possession of the same authentication key. A PP can have multiple subscriptions that are added to a list kept in the portable. The PP will only log onto a FP contained in that list. The subscription procedure executes a mutual authentication. According to the implementation the authentication of a FP or a PP can be executed separately for each call establishment. Furthermore a ciphering concept should avoid eavesdropping. During the authentication procedure a cipher key is calculated at both sides. This key is used to encrypt and decrypt data sent over the air.

A detailed description of the security architecture and its used security services is given in the following section.

3 DECT security architecture

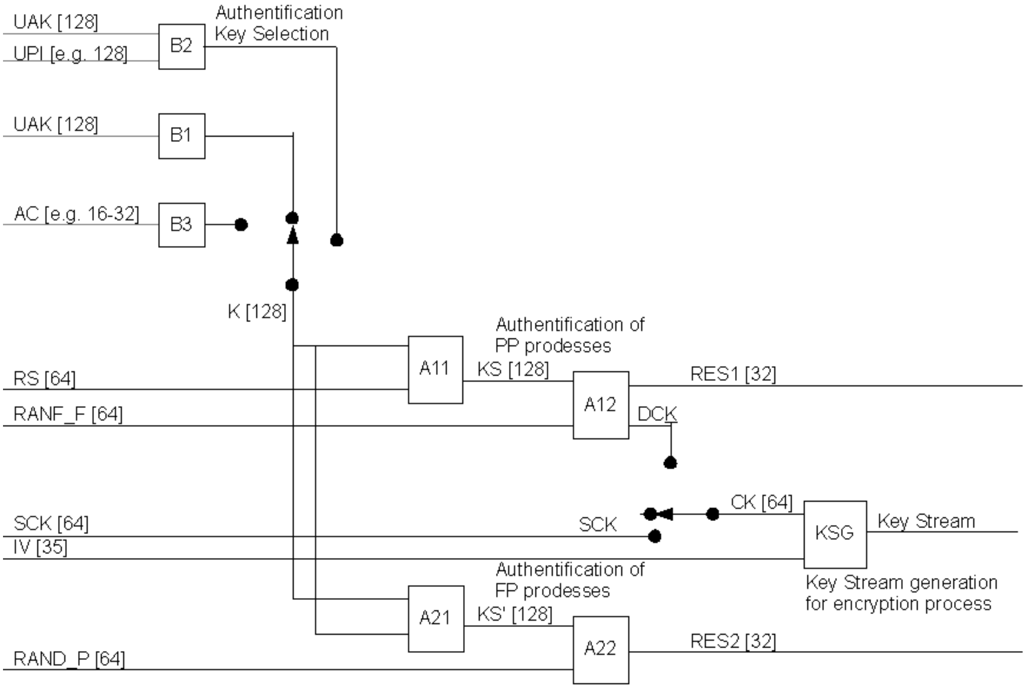


Figure 3: Survey of the DECT security architecture

This clause provides an overview of the disclosed security architecture defined in [4] (Figure 3). The security architecture provides subscription, authentication and ciphering. The key stream is only used for the encryption process, whereas the authentication algorithms can be used to derive authentication session keys and cipher keys. The specification of the authentication algorithms A11, A12, A21, A22 and the key stream generator have not been disclosed by the ETSI and have only been advertised to the manufacturers of DECT hardware. However, the authentication algorithms have been successfully reverse engineered (4.2.1). Table 2 and Table 3 provide an overview of the used cryptographic parameters and keys.

Table 2: Cryptographic parameters

Value	Description
IV	35 bits; It is obtained from frame counter and used to generate the key stream for encryption process in conjunction with CK.
RAND_F	64 bits; FT => PT; It is generated by the FT, local network subscribers' or home network and shall be randomly generated for each instance.
RAND_P	64 bits; PT => FT; It is generated by the PT and shall be randomly generated for each instance.
RES1	32 bits; It is computed by the PT; PT => FT; *RES1 := A12(RAND_F, KS)*
RES2	32 bits; It is computed by the FT; FT => PT; *RES2 := A22(RAND_P, KS')*
RS	64 bits; It is generated by the FT, local network or subscribers' home network and can enable roaming between networks in this way. Different values may be used for the 'authentication of a PT' and the 'authentication of a FT'. However a single value can be used several times.
UAK	128 bits; *UAK := KS'*
XRES1	32 bits; it is generated by the FT, local network or subscribers' home network; *XRES1 := A12(RAND_F, KS)*
XRES2	32 bits; it is generated by the PT; *XRES2 := A22(RAND_P, KS')*

Table 3: Cryptographic keys

Authentication key K: The DECT Standard offers three alternative options to derive the authentication key K whereas the first option is mostly used in the residential environment.
1. The User Authentication Key UAK is secret authentication data contained in the subscribers' (users') registration data. It is stored in a non-volatile memory within the PP or DECT Authentication Module DAM. *B1 : K[i] := UAK[i mod LEN_UAK]; 128 bits* 2. The User Personal Identity UPI is typically a short value with 16-32 bits entered manually by the user in the PT and used in combination with the

UAK to combine user authentication with 'authentication of a PT or a FT'. *B2 : K[i] := (UAK[i mod LEN_UAK] + UPI[i mod LEN_UPI]) mod 2; 128 bits* 3. The Authentication Code AC is stored or manually entered and should be only used for a short term coupling between the FP and the PP. *B1: K[i] := AC[i mod LEN_AC]; 128 bits*

Authentication sessions keys
KS := A11(RS, K); 128 bits;
KS' := A21(RS, K); 128 bits;

Cipher keys DCK := A12(KS, RAND_F); 64 bits SK is shared by the FT and the PT; 64 bits

The structure of the messages used below is illustrated in the appendix in section 9.

Key allocation

Prior to the first use of a PP in conjunction with a FP the key-allocation procedure has to be done. This procedure can be initiated either by the manufacturer or the user before the first use. The same PIN has to be entered in both devices, whereas sometimes the FP is provided with a fixed default PIN that the user has to enter on the PP [6]. A mutual authentication is performed (Figure 4) between the Fix Radio Termination (FT) and the Portable Radio Termination (PT) whereby the PT authenticates itself against the FT and the FT authenticates itself against the PT. In both authentication procedures the same random value RS is used. The AC that is stored in both devices is used as Key K. By sending the {KEY-ALLOCATE} message with the two random values RS and RAND_F to the PT the FT initiates the service. After receiving the {KEY-ALLOCATE} message the PT computes the values KS and RES1 for the 'authentication of a PT' part of this procedure. In addition the PT generates the random value RAND_P and computes the expected result XRES2 for the 'authentication of a FT' part. The values RES1 and RAND_P are sent by the PT to the FT within the {AUTHENTICATION-REQ} message. In a third step the FT compares the received value RES1 with the expected result XRES1. Only if both values are equal, the 'authentication of a PT' part is terminates successfully. Furthermore the FT computes the result RES2 for the 'authentication of a FT' part and sends this value within the {AUTHENTICATION-REP} message to the PT.

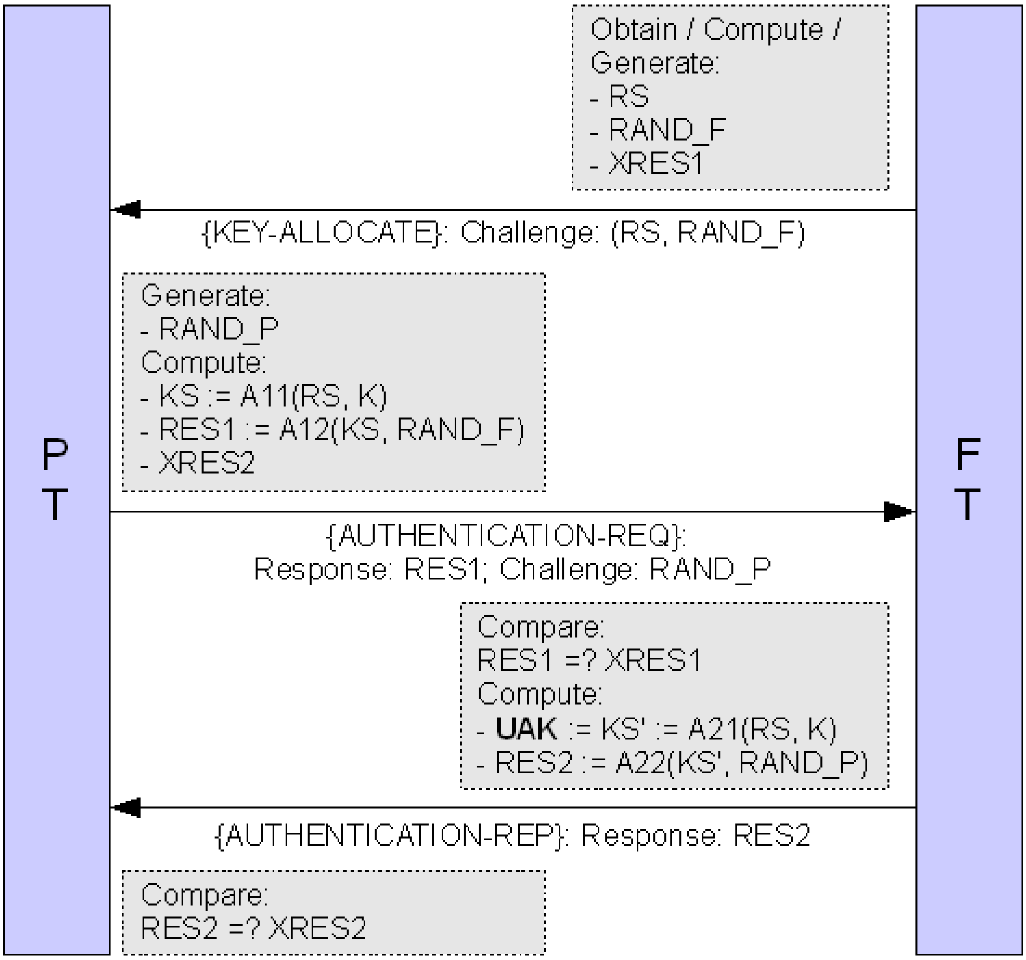

P T
F T
Obtain / Compute / Generate:
- RS
- RAND_F
- XRES1
{KEY-ALLOCATE}: Challenge: (RS, RAND_F)
Generate:
- RAND_P
Compute:
- KS := A11(RS, K)
- RES1 := A12(KS, RAND_F)
- XRES2
{AUTHENTICATION-REQ}:
Response: RES1; Challenge: RAND_P
Compare:
RES1 =? XRES1
Compute:
- UAK := KS' := A21(RS, K)
- RES2 := A22(KS', RAND_P)
{AUTHENTICATION-REP}: Response: RES2
Compare:
RES2 =? XRES2

Figure 4: Key allocation

Finally the PT compares the expected and the received values. If both values are identical, the authenticity of the FT is accepted by the PT and the key allocation procedure is finished successfully. The value KS', which is generated on both sides within the 'authentication of a FT', is stored as UAK after the successful mutual authentication; both devices erase the used AC value. After the key allocation procedure the FT and the PT share a 128 bit secret key, the so-called UAK.

Optional security services

The DECT security architecture is intended to prepare the following five optional security services:

- Authentication of a PT
- Authentication of a FT
- Mutual authentication
- Data confidentiality
- User authentication

Authentication of a PT

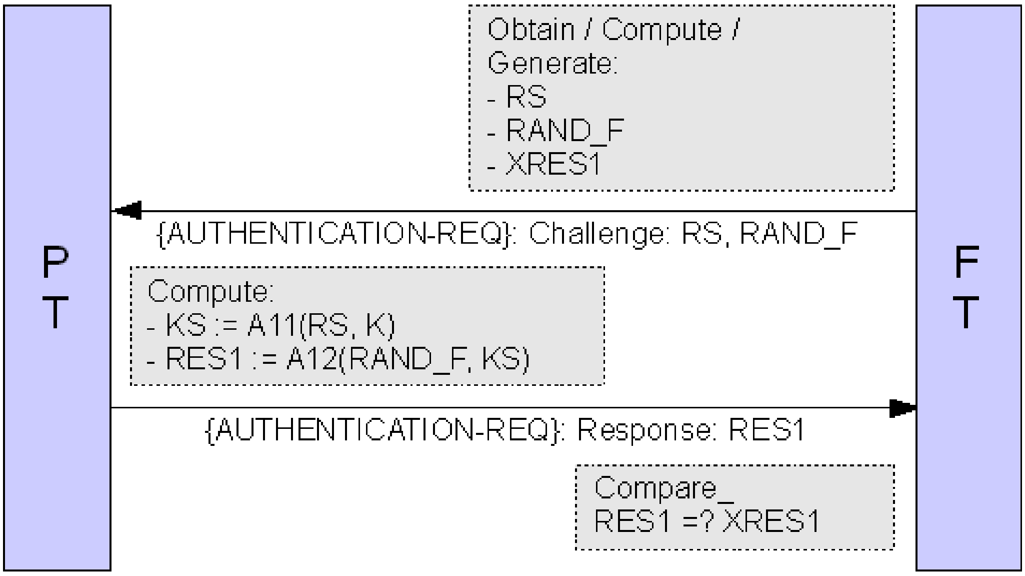

P
T
F
T
Obtain / Compute / Generate:
- RS
- RAND_F
- XRES1
{AUTHENTICATION-REQ}: Challenge: RS, RAND_F
Compute:
- KS := A11(RS, K)
- RES1 := A12(RAND_F, KS)
{AUTHENTICATION-REQ}: Response: RES1
Compare_
RES1 =? XRES1

Figure 5: authentication of a PT

This mechanism uses the secret authentication key K known by the PT and the FT. The FT initiates the service 'authentication of a PT' by sending a {AUTHENTICATION-REQ} message to the PT. The {AUTHENTICATION-REQ} message contains the two random values RS and RAND_F. The service is invoked at the beginning of a call and can be re-invoked anytime during a call.

In Figure 5 the challenge-response mechanism for 'authentication of a PT' is shown. In a first step the FT obtains, generates or computes the three values RS, RAND_F and the expected result XRES1.

The FT sends the {AUTHENTICATION-REQ} message that contains the random values RS and RAND_F to the PT. After reception of the values RS and RAND_F the PT calculates the response RES1 in the exact same manner as the FT calculated the value XRES1 and sends it to the FT within the {AUTHENTICATION-REP}. The PT demonstrates its knowledge of the common authentication key because the computation of the RES1 value is only possible with the 'right' authentication key.

In the last step the FT receives the response RES1 and compares it to the expected XRES1. Only if both values are equal, the FT accepts the authenticity of the PT. If the values are not consistent the call is cleared. This mechanism allows the FT to check if the PT uses the same authentication key without sending this key over the air.

Authentication of a FT

Even this mechanism uses the authentication key that is known to the FT and the PT to ensure the authenticity of the FT. The PT initiates this service by sending a {AUTHENTICATION-REQ} message that contains the random value RAND_P to authenticate a FT making or receiving a call through it. The service is invoked at the beginning of a call and can be re-invoked anytime during a call. The used authentication key and the value RS are not necessarily the same as those used in the 'authentication of a PT'-process.

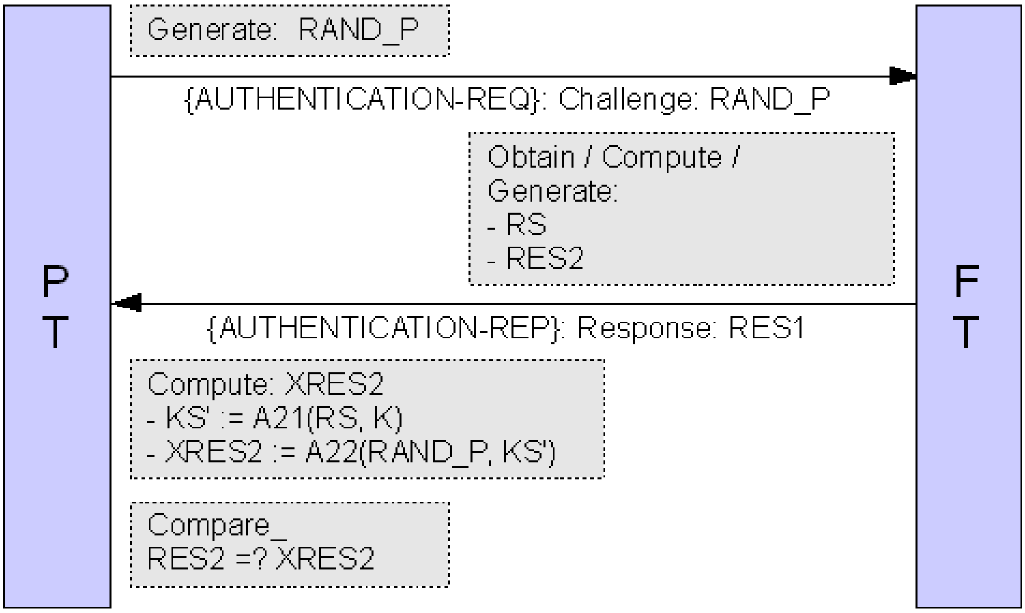

Generate: RAND_P
{AUTHENTICATION-REQ}: Challenge: RAND_P
Obtain / Compute / Generate:
- RS
- RES2
{AUTHENTICATION-REP}: Response: RES1
Compute: XRES2
- KS' := A21(RS, K)
- XRES2 := A22(RAND_P, KS')
Compare_
RES2 =? XRES2
P T
F T

Figure 6: authentication of a FT

In Figure 6 the challenge-response mechanism for 'authentication of a FT' is shown. First of all the PT generates a value RAND_P and sends it to the FT. In the following step the FT obtains, computes or generates the two random values RS and RES2 and sends them to the PT within the {AUTHENTICATION-REP}. Thereby the FT shows its knowledge of the common authentication key because the knowledge of this is needed to compute RES2.

Finally after receiving the values RS and RES2, the PT calculates the expected response XRES2 in the exact same manner as the FT computed the response RES2. If the comparison between the values RES2 and XRES2 is successful, the PT accepts the authenticity of the FT. Thanks to this mechanism the PT is able to make sure that the FT uses the same key without the need of sending this key over the air.

The design is different from the 'authentication of a PT' design. According to [1] this design allows the PT to move in a roaming environment without knowledge of the UAK.

Mutual authentication

Mutual authentication can be achieved by three methods:

- Direct method:

  This method combines the 'authentication of a PT' and the 'authentication of a FT' by back-to-back execution.

- Indirect method 1:

  This method combines 'authentication of a PT' with data confidentiality. The PT authenticates itself against the FT but the FT does not authenticate directly. To do so, the later illustrated mechanism 'data confidentiality' is used. The PT and the FT compute a cipher key from the authentication key within the 'authentication of a PT'. Because the FT is unable to encrypt or decrypt the data sent to or from the PT, if it does not know the authentication key, the FT can prove its authenticity by encrypting all data that is sent to the PT. For this mutual authentication method the PT has to make sure that the data confidentiality mechanism is used and drop any unencrypted call.

- Indirect method 2:

  This mechanism provides the authenticity of PT and FT with the aid of the data confidentiality service in conjunction with the static cipher key. The FT and PT show their authenticity by encrypting all data sent to each other. It is absolutely necessary that the FT and the PT ensure that data confidentiality service is used and drop any unencrypted call.

Data confidentiality

Data confidentiality is reached by encrypting the communication data with a key stream. The key stream is computed with a key stream generator in conjunction with a cipher key CK. The cipher key can be derived (Derived Cipher Key DCK) or static (Static Cipher Key SCK).

The DCK is one output of the authentication algorithm A12, beside the values RES1 and XRES1. Thus the PT computes the DCK as a part of the 'authentication of a PT' procedure and the FT obtains it in the first step the authentication procedure. The DCK can either be used for one call or reused for several calls. Given that the authentication algorithm A12 produces different DCKs for each 'authentication of a PT', one DCK can only be used until the next 'authentication of a PT'. The establishment of a DCK is not possible without 'authentication of PT'. Because the output of the authentication algorithm A12 is needed, it is not possible to establish a DCK through the 'authentication of a FT'.

For applications without an 'authentication of a PT' process the possibility of using the SCK is given. The PT and the FT share a static (fixed) key. However the DECT security standards do not include service for management of static keys.

Ciphering can be initiated either by the PT by sending a {CIPHER-SUGGEST} message to the FT or by the FT via sending a {CIPHER-REQUEST} to the PT.

User authentication

The 'authentication of a user' is achieved by using the 'authentication of the PT' mechanism and therein an authentication key K, which is derived from the User Personal Identity UPI value. The user enters the UPI manually into the PP each time this service is required. It is combined with the secret UAK, to determine the authentication key as shown in Table 3.

Recapitulation

This section provided an overview of the security services recommended by the ETSI. These security services are all optional; the next section presents the security threats resulting from the omitting of security services and weaknesses of the security architecture.

4 Security threats

4.1 Security threat analysis by ETSI

There are different security threats for the DECT system. For this thesis only the threats to consumer devices are considered. In Annex A of [4] an overview of the following five threats is given:

- **Impersonating a subscriber identity:**

  The identity of another DECT subscriber is used to make a call. The reason could be to avoid call charges, achieve anonymity or untraceability. Because a successful attack to avoid call charging will highly discrete the system this threat is a strong one and countermeasures -like 'authentication of a PT'- have to be provided.

- **Illegal use of a handset (PP):**

  PPs, which are not allowed to, may be used in a DECT network, even if the costs are billed correctly. This might be possible by the illicit use of a type approved PP (medium threat) or by use of a non type approved portable phone (strong threat).

  To decrease the threat level for the illicit use of type approved PP the use of PIN on the PP or the use of an electric serial number in conjunction with a black list are suggested. The implementation of a type approval procedure downsizes the threat level of the use of non type approved PP; however the ETSI does not consider this a serious attack.

- **Illegal use of a FP**

  In this case a call is made using a dedicated FP without authorization by the operator of the FP. Such an attack can be used for a Denial-of-Service attack, to avoid call charges or to avoid the costs for an own FP. Because the threat level depends on how DECT is operated, no rating can be given. An automatic protection is provided if countermeasures against the first threat are implemented.

- **Impersonating of a FP**

  By the impersonation of a FP an attacker can attract calls that are meant for another FP. Thus it is possible to eavesdrop on the user data, to handle the calls or change data in the PP (like subscription registration data), if the implementation allows such changes. Furthermore user data can be revealed and calls can be irregularly routed.

  With a special authentication protocol or a mandatory encryption, which cannot be switched off by the FP, the system can be protected against this threat.

- **Illegally obtaining user and user related signalling information**

  The privacy of data sent over the air interface is always threatened. An attacker could be able to obtain the calling number, called number or even other signalling information. In [4] this threat is subdivided into five subcategories:

  - passive eavesdropping
  - active attack by someone having limited knowledge of the system
  - active attack with all knowledge but limited resources
  - active attack with all knowledge and 'unlimited' resources
  - Academic attacks showing theoretical weaknesses, without being able to practically use them, but thereby discreating the system

Although the ETSI mentioned that privacy in residential applications is a desirable marketing option, at the time of this thesis no manufacturer of consumer devices uses this property for marketing purposes (section 5). Furthermore the threat of obtaining signalling information was appreciated as a weak threat that does not need any countermeasures. As shown in section 5 signalling information can often read along, why the threat should be rated as a strong threat that needs countermeasures like encryption. Even the threat of passive eavesdropping on a call is appreciated as a medium threat; whereas the analysis in section 5 illustrates that the threat of passive eavesdropping is a strong threat if no countermeasures are implemented. Via the use of encryption the threat goes down to a weak one.

The standard recommends procedures that enable the FP to authenticate the PP. The opposed authentication is only recommended if the FP can cause information changes in the portable phone. Encryption of the communication data is only a desirable property for the residential use for ETSI purposes; encryption of signalling information is mentioned only as a desirable option for business applications.

This thesis demonstrates the status of current research and shows the effects of absent security mechanisms.

4.2 Security analysis of the authentication algorithm DSAA

4.2.1 Structure DSAA

The DECT authentication services use the algorithms A11, A12, A21 and A22. These algorithms are only available under a nondisclosure agreement. In 2008 researchers disclosed these algorithms and presented attacks on the DSAA algorithm [6].

The four A-algorithms are wrappers around the authentication algorithm DSAA (Figure 8). The algorithm works with two inputs, a 128 bit key and a 64 bit random value, and outputs 128 bit. A11 does not modify the DSAA output. A21 changes every second bit of the DSAA output, starting with the first bit. A22 returns the last four bytes of the DSAA output and A12 returns the middle eight bytes of the DSAA as DCK and the last four bytes of the DSAA as result.

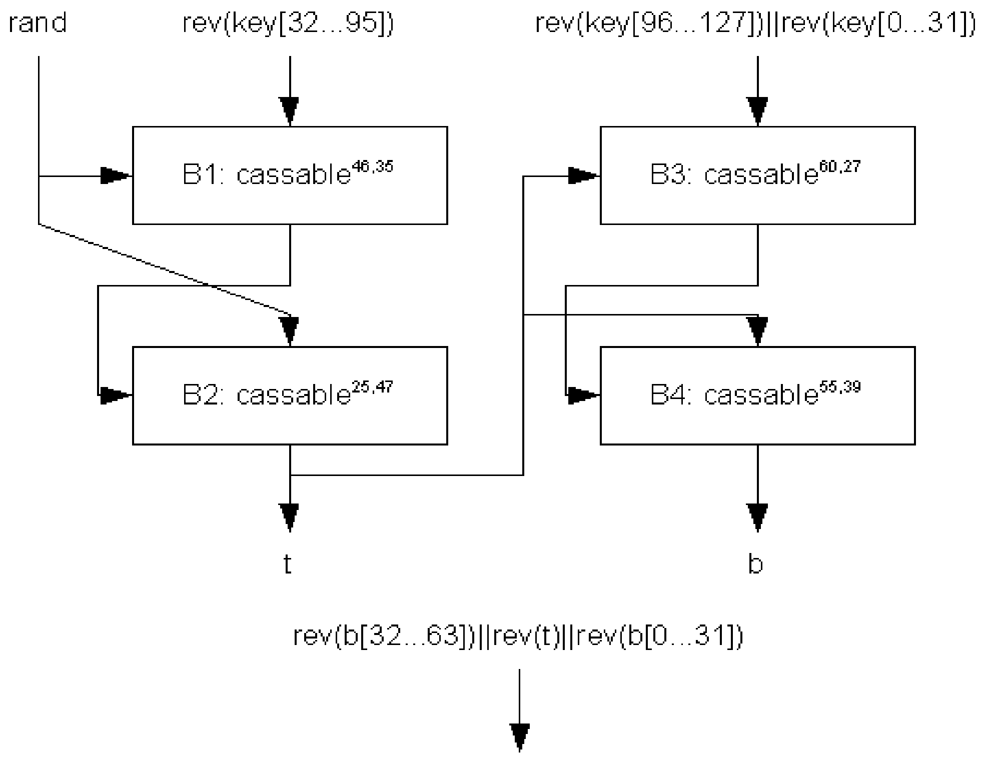


Figure 7: DSAA overview according to [6]

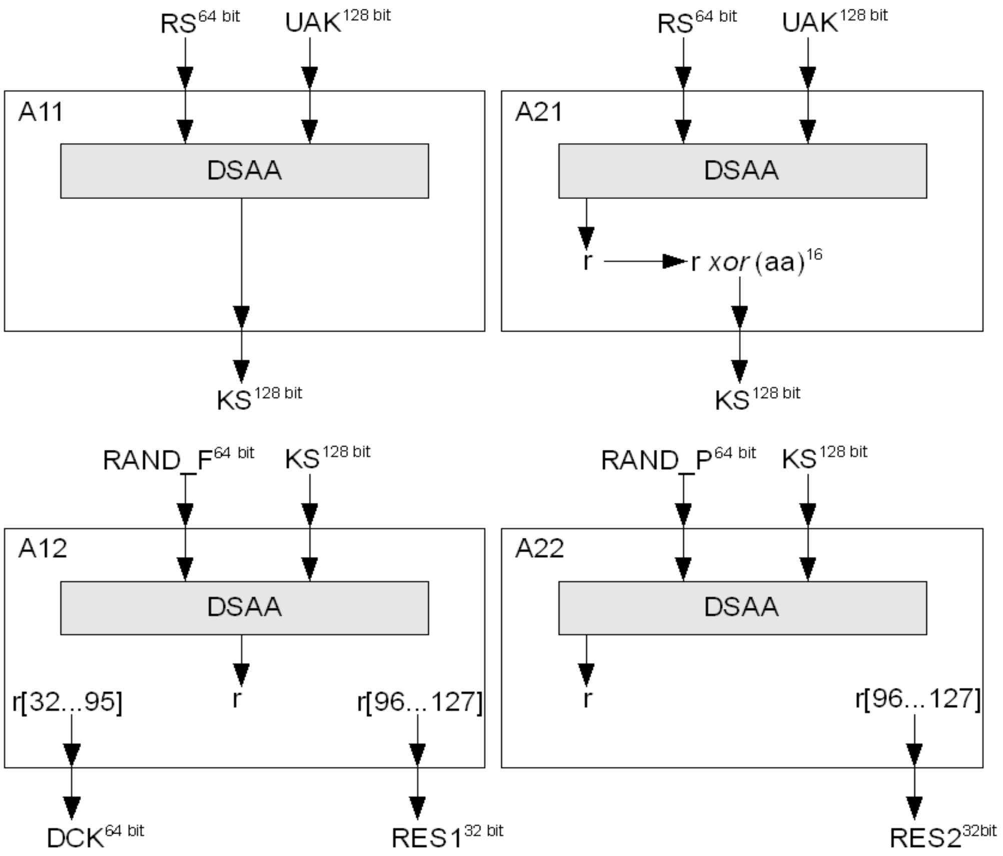


Figure 8: The four DSAA algorithms according to [6]

The DSAA is a cascade of four similar block ciphers. The block cipher does a key addition six times, applying a bricklayer of S-Boxes (see appendix, 1. section), followed by a mixing step. The sixth and last round is not followed by a final key addition. Thus the last round is completely invertible besides the key addition and the effective number of rounds is reduced to five (Figure 9). The following functions are used in the cassable block ciphers:

- $\sigma_i : GF(2)^{64} \rightarrow GF(2)^{64}$ *with* $1 \leq i \leq 4$ denotes bit permutations for deriving the round key from the cipher key.
- $\lambda_i : (Z/256Z)^8 \rightarrow (Z/256Z)^8$ *with* $1 \leq i \leq 3$ denotes the mixing functions used in the block ciphers.
  - $\lambda_1(A, B, \ldots, H) \rightarrow (2A+E, 2B+F, 2C+G, 2D+H, 3E+A, 3F+B, 3G+C, 3H+D)$
  - $\lambda_2(A, B, \ldots, H) \rightarrow (2A+C, 2B+D, 3C+A, 3D+B, 2E+G, 2F+H, 3G+E, 3H+F)$
  - $\lambda_3(A, B, \ldots, H) \rightarrow (2A+B, 3B+A, 2C+D, 3D+C, 2E+F, 3F+E, 2G+H, 3H+G)$
- $\gamma : GF(2)^{64} \rightarrow GF(2)^{64}$ is a bricklayer transform that is defined as:

  $$\gamma(A \| B \| C \| D \| E \| F \| G \| H) = \rho(A) \| \rho(B) \| \rho(C) \| \rho(D) \| \rho(E) \| \rho(F) \| \rho(G) \| \rho(H),$$

  with $A, B, C, D, E, F, G, H \epsilon GF(2)^8$ and $\rho : GF(2)^8 \rightarrow GF(2)^8$ denoting the application of the invertible S-Box.

The round keys $K_i \epsilon GF(2)^{64}$ with $1 \leq i \leq 6$ are computed iteratively from the cipher key $K_0 \epsilon GF(2)^{64}$ by applying i times the parameterized function:

$$\sigma_{(m,\, l)} : (k_0, k_1, \ldots, k_{63}) \rightarrow (k_m, k_{(m+l) \bmod 64}, k_{(m+2l) \bmod 64}, \ldots, k_{(m+3l) \bmod 64})$$

$$K_i = \sigma^i_{(m,\, l)}(K)$$

The different function used in each round can be summed up to one round function:

$$f_r : (X, K) \rightarrow \lambda_{(((r-1) \bmod 3)+1)}\, (X \text{ xor } \sigma^r(K)) \text{ with } 1 \leq r \leq 6$$

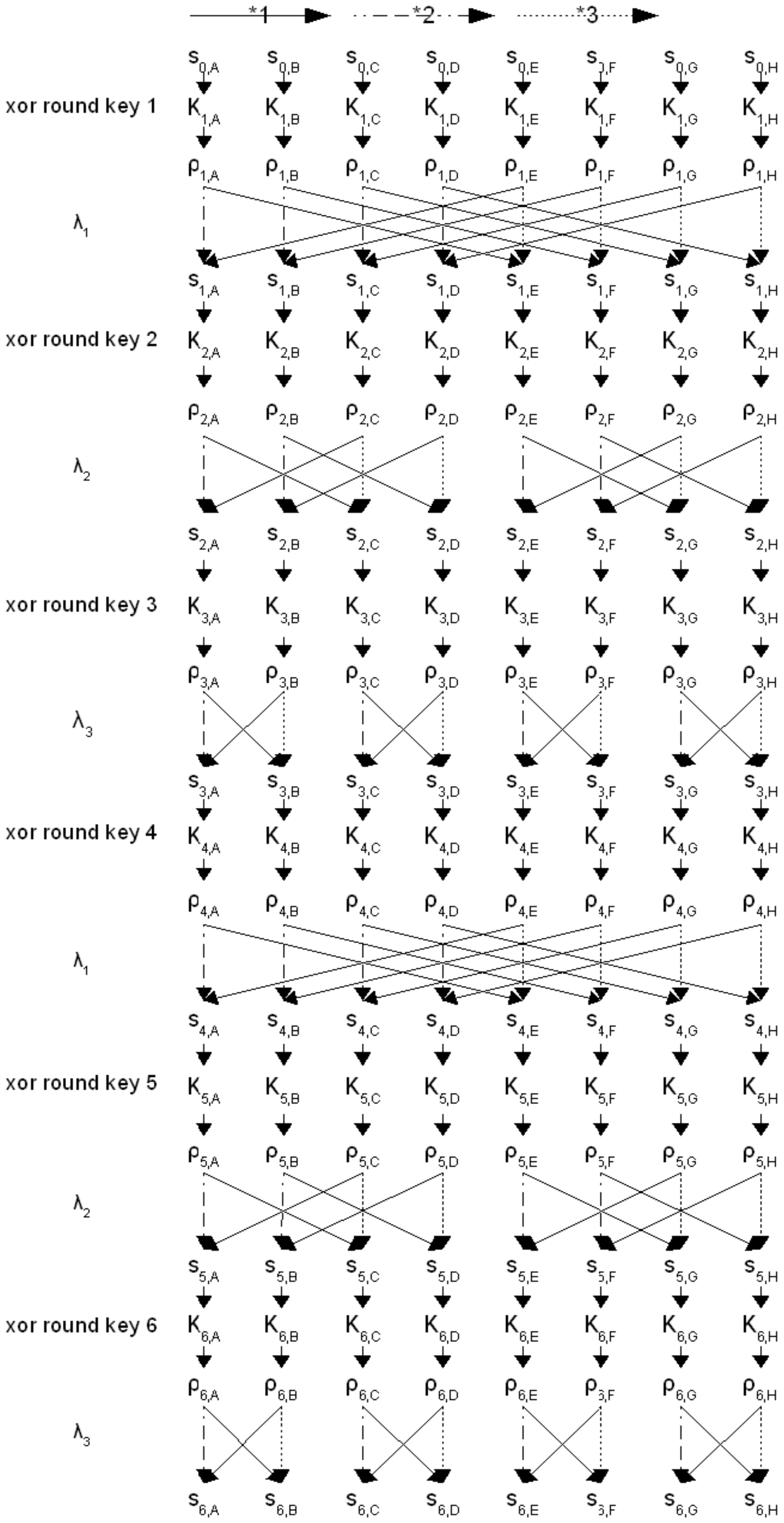

*1
*2
*3
s0,A s0,B s0,C s0,D s0,E s0,F s0,G s0,H
xor round key 1
K1,A K1,B K1,C K1,D K1,E K1,F K1,G K1,H
ρ1,A ρ1,B ρ1,C ρ1,D ρ1,E ρ1,F ρ1,G ρ1,H
λ1
s1,A s1,B s1,C s1,D s1,E s1,F s1,G s1,H
xor round key 2
K2,A K2,B K2,C K2,D K2,E K2,F K2,G K2,H
ρ2,A ρ2,B ρ2,C ρ2,D ρ2,E ρ2,F ρ2,G ρ2,H
λ2
s2,A s2,B s2,C s2,D s2,E s2,F s2,G s2,H
xor round key 3
K3,A K3,B K3,C K3,D K3,E K3,F K3,G K3,H
ρ3,A ρ3,B ρ3,C ρ3,D ρ3,E ρ3,F ρ3,G ρ3,H
λ3
s3,A s3,B s3,C s3,D s3,E s3,F s3,G s3,H
xor round key 4
K4,A K4,B K4,C K4,D K4,E K4,F K4,G K4,H
ρ4,A ρ4,B ρ4,C ρ4,D ρ4,E ρ4,F ρ4,G ρ4,H
λ1
s4,A s4,B s4,C s4,D s4,E s4,F s4,G s4,H
xor round key 5
K5,A K5,B K5,C K5,D K5,E K5,F K5,G K5,H
ρ5,A ρ5,B ρ5,C ρ5,D ρ5,E ρ5,F ρ5,G ρ5,H
λ2
s5,A s5,B s5,C s5,D s5,E s5,F s5,G s5,H
xor round key 6
K6,A K6,B K6,C K6,D K6,E K6,F K6,G K6,H
ρ6,A ρ6,B ρ6,C ρ6,D ρ6,E ρ3,F ρ6,G ρ6,H
λ3
s6,A s6,B s6,C s6,D s6,E s3,F s6,G s6,H

Figure 9: Structure of the cassable block cipher according to [6]

4.2.2 Security analysis of DSAA

DSAA only provides at most 64 bit of symmetric security [6]. The following attacks are attacks on the structure of DSAA and show *"serious design flaws, which might allow attacks with a complexity below 2^{64}. Especially the block cipher used in DSAA seems to be weak and can be completely broken using differential cryptanalysis."* [6] However at that time they do not have an influence on the security of DECT.

1. **A practical attack on cassable**

There is a property of DSAA that enables an attacker to recover the secret key [5]. The functions λ_i are used to diffuse local changes in the states and complete diffusion seems to be achieved after the first three rounds. Although every byte depends on another byte after the third round, the entire diffusion is not achieved. For the components of output vectors that are formed as

$$c = (a * 2 + b) \ mod \ 256$$

the lowest bit of c is equal to the lowest bit of b (see Figure 9).

Assume now there are two inputs m and m' where every second byte is the same such as $m_B = m'_B$, $m_D = m'_D$, $m_F = m'_F$, $m_H = m'_H$:

$$m = m_A \| m_B \| m_C \| m_D \| m_E \| m_F \| m_G \| m_H \ with \ m_i \in \{0, 1\}^8$$

$$m' = m'_A \| m'_B \| m'_C \| m'_D \| m'_E \| m'_F \| m'_G \| m'_H \ with \ m'_i \in \{0, 1\}^8$$

Now these both inputs get encrypted.

Let $s_i = s_{i,A} \| \ldots \| s_{i,H}$ and $s'_i = s'_{i,A} \| \ldots \| s'_{i,H}$ be the states after i rounds of the cassable block cipher (Figure 9). The equalities $s_{1,B} = s'_{1,B}$, $s_{1,D} = s'_{1,D}$, $s_{1,F} = s'_{1,F}$, $s_{1,H} = s'_{1,H}$ hold after the first and the second round and get destroyed after the third round. However after the third round $s_{3,A} \equiv s'_{3,A} \ mod \ 2$, $s_{3,C} \equiv s'_{3,C} \ mod \ 2$, $s_{3,E} \equiv s'_{3,E} \ mod \ 2$, $s_{3,G} \equiv s'_{3,G} \ mod \ 2$ holds and the key addition in round 4 keeps this property. But the appliance of the S-Box $\rho_{4,j}$ destroys this property as well.

If now an attacker is up to encrypt m and m′ with the same secret key and can see the two outputs s_6 and s'_6, he can invert λ_3 and $p_{6,i}$ due to key independency. For the recovery of the values $s_{3,A}$ *xor* $K_{4,A}$ and $s_{3,E}$ *xor* $K_{4,E}$ just the 32 bits $K_{6,A}$, $K_{6,C}$, $K_{6,E}$ and $K_{6,G}$ of the round key 6 and 16 bits $K_{5,A}$ and $K_{5,E}$ of the round key 5 are required. Because of the overlaps in the round key bits these are 38 different bits for *B1*, 36 different bits for *B2*, 42 different bits for *B3* and 40 different bits for *B4 (*Figure 9*)*. The attacker can now recover with a secret key guess the following four values:

- $s_{3,A}$ *xor* $K_{4,A}$
- $s_{3,E}$ *xor* $K_{4,E}$
- $s'_{3,A}$ *xor* $K_{3,A}$
- $s'_{3,E}$ xor $K_{4,E}$

The attacker verifies if following equations hold:

- $s_{3,A}$ *xor* $K_{4,A} \equiv s'_{3,A}$ *xor* $K_{3,A}$ *mod 2*
- $s_{3,E}$ *xor* $K_{4,E} \equiv s'_{3,E}$ *xor* $K_{4,E}$ *mod 2*

The secret key guess can be eliminated if one of these conditions fails. This way about 75 % of the possible key space can be eliminated with computational costs of about 2^k invocations of the cassable block cipher with *k* different key bits for the required round key parts of round keys 5 and 6.

This procedure can be repeated with another pair on the remaining key space. By iterating this procedure with 15 pairs only 2^{34} possible keys are expected to remain. This number of remaining possible keys can be checked by exhaustive search[1]. For *cassable*^{25,47} the total workload amount would be $2^{36.7}$.

[1] The exhaustive search iteratively generates possible solutions, checks if this solution solves the problem and continues until the solution is found.

2. **A known-plaintext attack on three rounds using a single plaintext/ciphertext pair**

For an attack on the first three rounds of the cassable block cipher only one plaintext/ciphertext pair is needed [6].

Assume an attacker has the ciphertext $S_3 = s_{3,A} \| s_{3,B} \| s_{3,C} \| s_{3,D} \| s_{3,E} \| s_{3,F} \| s_{3,G} \| s_{3,H}$ for a plaintext $m = m_A \| m_B \| m_C \| m_D \| m_E \| m_F \| m_G \| m_H$ after three rounds. $Z = (z_0, \ldots, z_7) = S_2 \text{ xor } K_3$ can be obtained by inverting λ_3 and the s-Box layer ρ because of key independency. The diffusion is not complete for Z, for example the following relation holds for z_0:

$$\begin{aligned} z_0 = \; & \rho((2 * \rho(m_0 \text{ xor } K_{1,A}) + \rho(m_4 \text{ xor } K_{1,E})) \text{ xor } K_{2,A}) + \\ & \rho((2 * \rho(m_2 \text{ xor } K_{1,C}) + \rho(m_6 \text{ xor } K_{2,G})) \text{ xor } K_{2,C}) \text{ xor } K_{3,A} \end{aligned}$$

z_0 depends on only 41 key bits because of overlaps in the key bits for B1, for B2 it depends on 36 key bits, for B3 on 44 key bits and for B4 on 46 key bits (Figure 9). The equations for z_i can be used to eliminate 255/256 of the searched key space.

2^{36} invocations of the cassable for B2 and 2^{46} invocations of the cassable for B4 are needed to obtain the dependent key bits. By means of this attack on B2 and B4 a reduced version of DSAA can be attacked. A version that uses 6 rounds of cassable for B1 and B3 and 3 rounds of cassable for B2 and B4 can be attacked with costs of 2^{44} invocations of the reduced DSAA.

4.3 Pseudo random number generator

There are usually $2^{77.288}$ possible values for the UAK if a 4 digit PIN number is used in the key allocation procedure. Thus an attacker can predict the subset of random numbers that are generated during key allocation and thereby the number of possible values for the UAK decreases. The attacker can now sniff challenge-response pairs ((RAND_F, RS), SRES1) after the key allocation and can use them as 32-bit filters. In practice some weak PRNGs implemented in the firmware of several base stations were found, one weak PRNG provides only 24 bits of entropy for the 64 bit value RS. *"This leads to a very practical and devastating attack against DECT PTs using vulnerable DECT stacks."* [6]

5 Measurements

In this section results of 36 tested consumer devices are illustrated. Mainly the call establishment of an outgoing call was analysed. This by the PP initiated procedure can include the following messages.

- {CC-SETUP} is sent by the PT to initiate a call through the FT. This message includes always the unique identities of the PP and FP and may include also other information.
- {CC-CONNECT} is sent by the FT to the PT to show the acceptance of a call. It can include different information, like the Equipment Manufacturer Code EMC.
- {CIPHER-REQUEST} is sent by the FT to the PT to enable the encryption. It includes e.g. information about the cipher algorithm and the cipher key type.
- {AUTHENTICATION-REQ} is sent by the FT or PT to authenticate the other party. The message includes e.g. the random value and possibly the random value RS.
- {AUTHENTICATION-REP} is sent by the FT or the PT to prove its authenticity. It includes the computed result value.

In Figure 10 a call establishment is shown including security mechanisms.

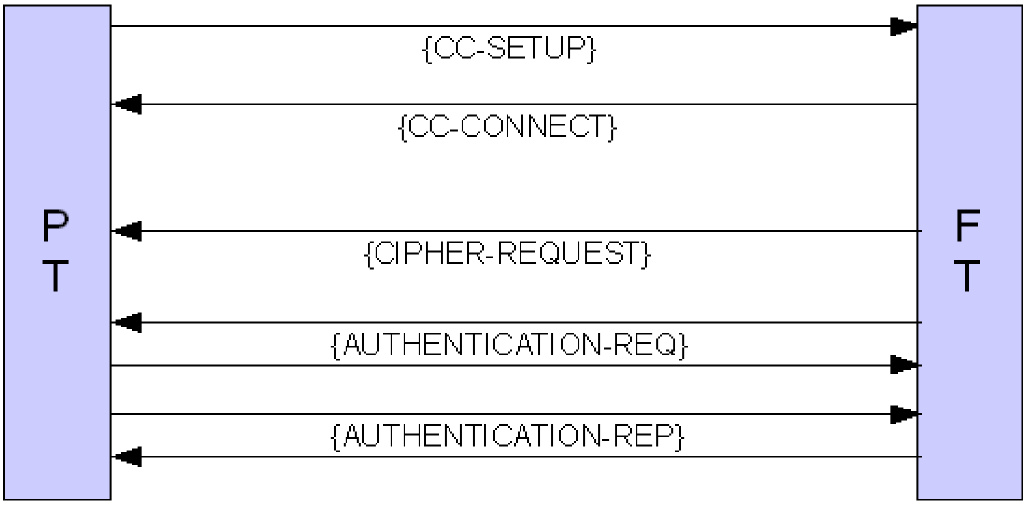


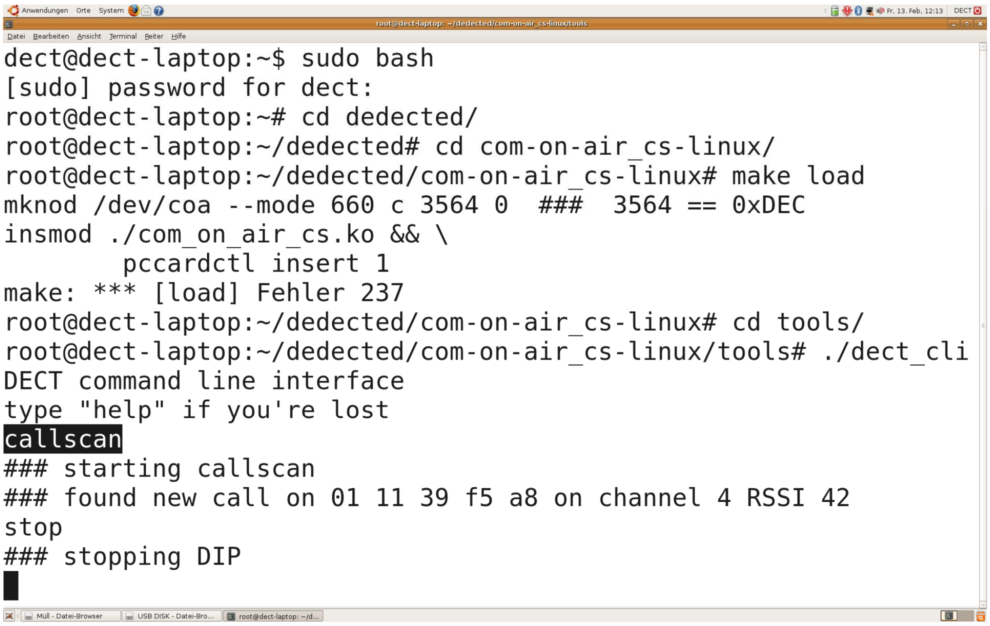
Figure 10: PT initiated outgoing call

5.1 Eavesdropping of active calls

Via tape-recording of call establishments between the FP and the PP it can be testified whether the communication is encrypted, authentication is implemented, signalling data is sent in plain text or if the weak FritzBox PRNG is used.

5.1.1 Procedure

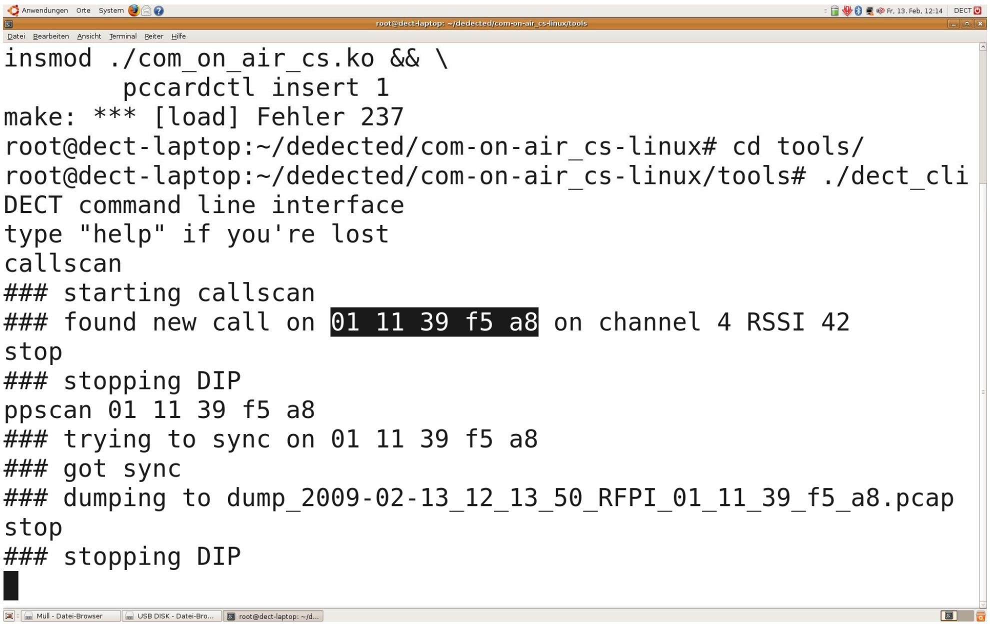
The function *'callscan'* shows the RFPI and the RSSI value for all active calls in the reachable environment. Thus the function is convenient to detect the searched device (Figure 11).



```
dect@dect-laptop:~$ sudo bash
[sudo] password for dect:
root@dect-laptop:~# cd dedected/
root@dect-laptop:~/dedected# cd com-on-air_cs-linux/
root@dect-laptop:~/dedected/com-on-air_cs-linux# make load
mknod /dev/coa --mode 660 c 3564 0  ###  3564 == 0xDEC
insmod ./com_on_air_cs.ko && \
        pccardctl insert 1
make: *** [load] Fehler 237
root@dect-laptop:~/dedected/com-on-air_cs-linux# cd tools/
root@dect-laptop:~/dedected/com-on-air_cs-linux/tools# ./dect_cli
DECT command line interface
type "help" if you're lost
callscan
### starting callscan
### found new call on 01 11 39 f5 a8 on channel 4 RSSI 42
stop
### stopping DIP
```

Figure 11: Scan for active calls in the reachable environment

After obtaining the RFPI a synchronisation of the DECT card and the FP can be established by using the function *'ppsan'* (Figure 12). This function generates a dump file with all data sent between the FP and the PP and saves this data in a .pcap file.


Anwendungen Orte System
root@dect-laptop: ~/dedected/com-on-air_cs-linux/tools
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
Müll - Datei-Browser
USB DISK - Datei-Bro...
root@dect-laptop: ~/d...

```
insmod ./com_on_air_cs.ko && \
        pccardctl insert 1
make: *** [load] Fehler 237
root@dect-laptop:~/dedected/com-on-air_cs-linux# cd tools/
root@dect-laptop:~/dedected/com-on-air_cs-linux/tools# ./dect_cli
DECT command line interface
type "help" if you're lost
callscan
### starting callscan
### found new call on 01 11 39 f5 a8 on channel 4 RSSI 42
stop
### stopping DIP
ppscan 01 11 39 f5 a8
### trying to sync on 01 11 39 f5 a8
### got sync
### dumping to dump_2009-02-13_12_13_50_RFPI_01_11_39_f5_a8.pcap
stop
### stopping DIP
```

Figure 12: Synchronisation with a FP and generation of a dump file

To get all data of a call establishment, the generation of the dump file has to be awaited before starting the phone call. After the phone call *'dect_cli'* has to be closed by typing *'stop'* and *'quit'* into the terminal.

pcap2cchan dumpfilename.pcap enables to see all C-channel information exchanged between the FP and the PP during the record time (Table 4). This data can show if authentication and ciphering are active and if signalling information is sent in plain text.

Table 4: Recorded data

```
phone  : addr:91 ctrl:00 len:01 crc:b7b5
phone  : addr:11 ctrl:02 len:8d crc:1b5d -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 00
c6 66 7d bd 06 07 a0 a5 00 b6 04 30 c0 e0 80 2c 03 8f 01 c0
7b 06 81 00 02 18 01 42
station: addr:11 ctrl:01 len:01 crc:b636
station: addr:13 ctrl:00 len:29 crc:f43c -> 0011 CC
(Call Control) messages :{CC-CONNECT}    83 07 7b 06 81 00 02
01 01 01
phone  : addr:13 ctrl:21 len:01 crc:4e7c
phone  : addr:11 ctrl:20 len:25 crc:15f0 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 05 32 35 37 31
33
station: addr:13 ctrl:02 len:6d crc:dbce -> 0101 MM
(Mobility Management) messages :{AUTHENTICATION-REQUEST}
05 40 0a 03 01 18 18 0c 08 06 77 e2 c7 50 73 be 29 0e 08 38
ce 25 91 cb ba 71 c8
station: addr:11 ctrl:21 len:01 crc:5676
phone  : addr:13 ctrl:01 len:01 crc:ae3c
```

```
station: addr:13 ctrl:20 len:39 crc:ca68 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 0a 81 00 02 32
01 0e 1a 02 09 01
phone  : addr:11 ctrl:02 len:21 crc:a733 -> 0101 MM
(Mobility Management) messages :{AUTHENTICATION-REPLY}    85
41 0d 04 4a 8d 57 08
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:11 ctrl:01 len:01 crc:b636
station: addr:13 ctrl:02 len:19 crc:3e49 -> 0101 MM
(Mobility Management) messages :{CIPHER-REQUEST}    05 4c 19
02 81 98
phone  : addr:11 ctrl:20 len:25 crc:07fe -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 7b 05 81 00 02 30
00
```

5.1.2 Results

With the recorded .pcap files (see appendix section 7) it is possible to check the implementation of following security services:

- Encryption of voice data
- Encryption of signalling information
- Authentication of a PT
- Authentication of FT
- Strength of the PRNG

Encryption of voice data

Encryption of the communication data is announced either by the FT via sending a {CIPHER-REQUEST} message to the PT or by the PT via sending a {CIPHER-SUGGEST} message to the FT. Another way to determine if encryption is enabled is using the function *postprocess.sh.* This function generates a .wav files from the .pcap file. Via playback of the voice data it is possible to hear if the voice data is encrypted (Figure 13). If encryption was active there is only noise to hear.

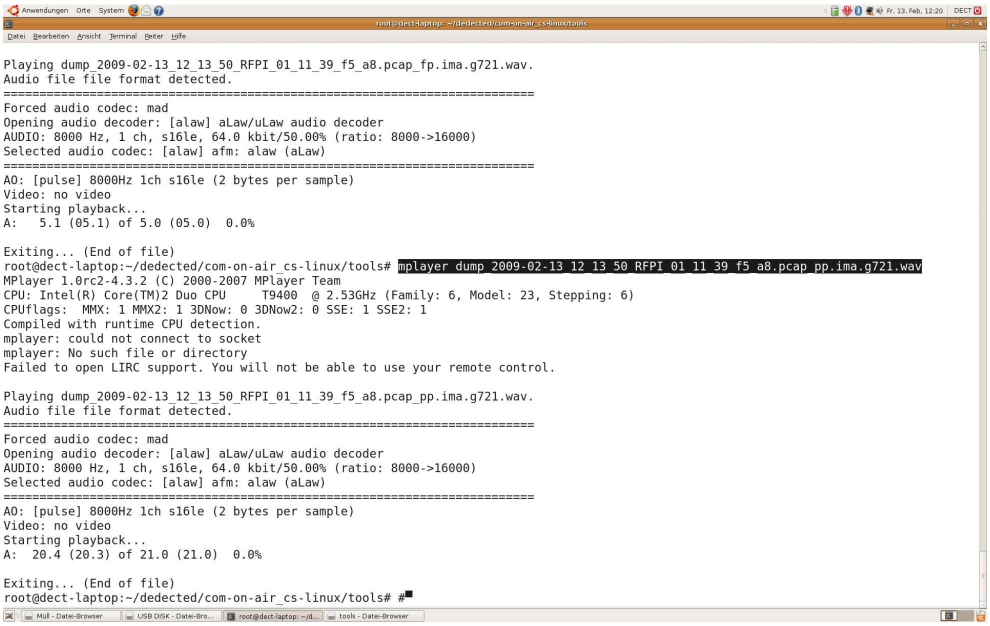
The encryption of the tested devices was always initiated by the FT. The sent {CIPHER-REQUEST} message always appeared in the following form:

05 4c 19 02 81 98

This message determines that encryption is executed with the DECT standard cipher algorithm and the cipher key DCK.

As illustrated in

Table 5 the communication from 14 of the 36 tested devices could be eavesdropped. That means that one third is not protected against the simple attack of passive eavesdropping. An attacker does not need any further knowledge of security or cryptography. He does not need expensive or extraordinary hardware to execute the passive eavesdropping successfully either. With a simple consumer notebook, a cheap DECT card, basic Linux knowledge and publicly available software every person is able to run this attack.



```
Playing dump_2009-02-13_12_13_50_RFPI_01_11_39_f5_a8.pcap_fp.ima.g721.wav.
Audio file file format detected.
==========================================================================
Forced audio codec: mad
Opening audio decoder: [alaw] aLaw/uLaw audio decoder
AUDIO: 8000 Hz, 1 ch, s16le, 64.0 kbit/50.00% (ratio: 8000->16000)
Selected audio codec: [alaw] afm: alaw (aLaw)
==========================================================================
AO: [pulse] 8000Hz 1ch s16le (2 bytes per sample)
Video: no video
Starting playback...
A:   5.1 (05.1) of 5.0 (05.0)  0.0%

Exiting... (End of file)
root@dect-laptop:~/dedected/com-on-air_cs-linux/tools# mplayer dump 2009-02-13 12 13 50 RFPI 01 11 39 f5 a8.pcap pp.ima.g721.wav
MPlayer 1.0rc2-4.3.2 (C) 2000-2007 MPlayer Team
CPU: Intel(R) Core(TM)2 Duo CPU     T9400  @ 2.53GHz (Family: 6, Model: 23, Stepping: 6)
CPUflags:  MMX: 1 MMX2: 1 3DNow: 0 3DNow2: 0 SSE: 1 SSE2: 1
Compiled with runtime CPU detection.
mplayer: could not connect to socket
mplayer: No such file or directory
Failed to open LIRC support. You will not be able to use your remote control.

Playing dump_2009-02-13_12_13_50_RFPI_01_11_39_f5_a8.pcap_pp.ima.g721.wav.
Audio file file format detected.
==========================================================================
Forced audio codec: mad
Opening audio decoder: [alaw] aLaw/uLaw audio decoder
AUDIO: 8000 Hz, 1 ch, s16le, 64.0 kbit/50.00% (ratio: 8000->16000)
Selected audio codec: [alaw] afm: alaw (aLaw)
==========================================================================
AO: [pulse] 8000Hz 1ch s16le (2 bytes per sample)
Video: no video
Starting playback...
A:  20.4 (20.3) of 21.0 (21.0)  0.0%

Exiting... (End of file)
root@dect-laptop:~/dedected/com-on-air_cs-linux/tools# #
```

Figure 13: Playback of the voice communication data recorded via ppscan

Table 5: Overview of ciphering status

DECT device	{CIPHER-SUGGEST}	{CIPHER-REQUEST}	Encryption active?
AEG Colombo Coral	-	-	-
AEG Cromo 3400	-	X	X
AEG Fame 400	-	-	-
Audioline Big Tel 100	-	X	X
Audioline Slim DECT 500	-	X	X
Bang&Olufsen BeoCom 6000	-	X	X

Doro Phone Easy DECT315	-	X	X
Grundig Sinio1	-	-	-
Hagenuk Accento 4000	-	-	-
Hagenuk AIO 600	-	-	-
Hagenuk Stick SR	-	-	-
iDECT x2i	-	X	X
Loewe Alphatel 5000	-	-	-
Motorola D701	-	-	-
Orchid DECT LR 4610	-	X	X
Panasonic KX-TG 8220	-	-	-
Philips CD650	-	X	X
Philips SE250	-	-	-
Philips Zenia Voice	-	-	-
Sagem D23XL	-	X	X
Siemens Gigaset A260	-	X	X
Siemens Gigaset A580	-	X	X
Siemens Gigaset C450 IP	-	X	X
Siemens Gigaset E360	-	X	X
Siemens Gigaset S680	-	X	X
Siemens SL785	-	X	X
T-Home Sinus 45	-	X	X
T-Home Sinus 101	-	X	X
T-Home Sinus 102	-	X	X
T-Home Sinus 212	-	X	X
T-Home Sinus 501	-	X	X
T-Home Sinus 710 Komfort	-	-	-
T-Home Sinus A301	-	X	X
T-Home Sinus C31	-	-	-
Tiptel Dectline	-	-	-
TopCom Butler 800	-	X	X
Sum	**0**	**22**	**22**

Encryption of signalling information

Another weakness of DECT is the possibility of sending unencrypted signalling information in the C channel. Even if encryption is active, the called or calling phone number is sometimes sent in plaintext. That is a not negligible security risk, especially for unlisted numbers.

The called number is sent to the FT as Keypad Information inside an {CC-INFO} message. This information starts always with *'x3 7b 3c'* followed by a byte that determines the length. The called number is displayed as shown in Table 6. The calling number can also read along as shown in Table 7.

Table 6: Called phone number sent in plain text

```
phone  : addr:91 ctrl:00 len:01 crc:b7b5
phone   : addr:11 ctrl:02 len:8d crc:1b5d -> 0011 CC    (Call
Control) messages :{CC-SETUP}     03 05 05 07 80 a8 00 c6 66
7d bd 06 07 a0 a5 00 b6 04 30 c0 e0 80 2c 03 8f 01 c0 7b 06
81 00 02 18 01 42
station: addr:11 ctrl:01 len:01 crc:b636
station: addr:13 ctrl:00 len:29 crc:f43c -> 0011 CC    (Call
Control) messages :{CC-CONNECT}    83 07 7b 06 81 00 02 01 01
01
phone  : addr:13 ctrl:21 len:01 crc:4e7c
phone   : addr:11 ctrl:20 len:25 crc:15f0 -> 0011 CC    (Call
Control)
messages :{CC-INFO}    03 7b 2c 05 32 35 37 31 33
```

Table 7: Calling phone number sent in plain text

```
station: addr:13 ctrl:20 len:79 crc:e954 -> 0011 CC   (Call
Control) messages :{CC-SETUP}    03 05 05 07 80 a8 01 11 31
da 55 06 07 a0 a5 01 11 39 f5 a8 e0 80 e4 4f 77 04 c0 80 fe
db
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:11 ctrl:22 len:09 crc:3859 -> 0011 CC   (Call
Control) messages :{CC-ALERTING}    83 01
.
.
.
station: addr:13 ctrl:00 len:a1 crc:bf4a -> 0111 COMS (Con-
nection Oriented Message Service) messages :NULL    87 7b 77
24 c0 80 01 00 00 11 0b 02 d8 80 c0 01 7x 3x 2x 0x x0 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

As in Table 8 illustrated, more than every second device sends signalling information in plaintext. Even six devices with activated encryption send the called phone number in plaintext. Accordingly an attacker without special security knowledge can read along signalling information and learn sensitive data.

Table 8: Test results: Signalling data sent over the C channel

DECT device	Phone number sent in plaintext?
AEG Colombo Coral	Yes
AEG Cromo 3400	No
AEG Fame 400	Yes
Audioline Big Tel 100	No
Audioline Slim DECT 500	No
Bang&Olufsen BeoCom 6000	Yes
Doro Phone Easy DECT315	No
Grundig Sinio1	Yes
Hagenuk Accento 4000	Yes
Hagenuk AIO 600	Yes
Hagenuk Stick SR	Yes
iDECT x2i	No
Loewe Alphatel 5000	Yes
Motorola D701	Yes
Orchid DECT LR 4610	No
Panasonic KX-TG 8220	Yes
Philips CD650	No
Philips SE250	Yes
Philips Zenia Voice	Yes
Sagem D23XL	No
Siemens Gigaset A260	Yes
Siemens Gigaset A580	Yes
Siemens Gigaset C450 IP	Yes
Siemens Gigaset E360	Yes
Siemens Gigaset S680	No
Siemens SL785	No
T-Home Sinus 45	Yes
T-Home Sinus 101	No
T-Home Sinus 102	No
T-Home Sinus 212	No
T-Home Sinus 501	No

T-Home Sinus 710 Komfort	Yes
T-Home Sinus A301	No
T-Home Sinus C31	Yes
Tiptel Dectline	Yes
TopCom Butler 800	No
Sum	**20**

Authentication of a PT

The implementation of the security service 'authentication of a PT' can also be verified. By not using this mechanism several attacks like using the identity of another PT to avoid call charges, to ensure anonymity or using stolen or non-type approved handsets are possible [4]. By sending the {AUTHENTICATION-REQ} message as shown in Table 4, the FT initiates this service. Because the DCK is needed for successful ciphering this service has to be executed for each device that uses ciphering. Sometimes the {AUTHENTICATION-REQ} message is not displayed in the C channel although ciphering is active. It is imaginable that one DCK is used several times or it is used for a short time and the re-authentication of PT is done in the encrypted part of the call. However the service is nevertheless active.

About 60% execute this service and are thus protected against the illegal use of a handset (Table 9).

Table 9: Test results: Authentication of a PT

DECT device	**Authentication of a PT**	
	Active?	{AUTHENTICATION-REQ} visible?
AEG Colombo Coral	-	-
AEG Cromo 3400	X	-
AEG Fame 400	-	-
Audioline Big Tel 100	X	-
Audioline Slim DECT 500	X	-
Bang&Olufsen BeoCom 6000	X	-

Doro Phone Easy DECT315	X	-
Grundig Sinio1	-	-
Hagenuk Accento 4000	-	-
Hagenuk AIO 600	X	X
Hagenuk Stick SR	-	-
iDECT x2i	X	-
Loewe Alphatel 5000	-	-
Motorola D701	-	-
Orchid DECT LR 4610	X	-
Panasonic KX-TG 8220	-	-
Philips CD650	X	X
Philips SE250	-	-
Philips Zenia Voice	-	-
Sagem D23XL	X	-
Siemens Gigaset A260	X	X
Siemens Gigaset A580	X	X
Siemens Gigaset C450 IP	X	X
Siemens Gigaset E360	X	X
Siemens Gigaset S680	X	X
Siemens SL785	X	X
T-Home Sinus 45	X	X
T-Home Sinus 101	X	-
T-Home Sinus 102	X	-
T-Home Sinus 212	X	-
T-Home Sinus 501	X	X
T-Home Sinus 710 Komfort	-	-
T-Home Sinus A301	X	X
T-Home Sinus C31	-	-
Tiptel Dectline	-	-
TopCom Butler 800	X	-
Sum of X	**23**	**11**

Authentication of FT

This mechanism counteracts the impersonation of a base station. None of the 36 tested devices supports this security mechanism. Consequently each base station can be impersonated.

Pseudo random number generator

As mentioned in section 4.3 a weak random generator can be used to execute serious attacks. The in the FritzBox implemented PRNG is a weak one and produces only 24 bits of entropy for the 64 bits value Rand [6]. To test if the same weak random generator is used generated random values need to be compared with the subset of the 2^{22} values generated by the FritzBox PRNG. In this manner it can be ensured with a high probability if one of the tested devices uses the weak FritzBox PRNG.

On the one hand random values are contained in the {AUTHENTICATION-REQUEST} message (Table 4). In table 9 these random numbers are listed. Only one device is equipped with the weak FritzBox PRNG, but about the PRNG strength of the other devices no conclusion can be done.

Table 10: Test results: PRNG

DECT device	RAND_F	PRNG (FritzBox)
Hagenuk AIO 600	bb 20 ed 0b 78 41 dd 13	Yes
Philips CD650	15 ea a7 d6 f9 ee 05 80	No
Siemens Gigaset A260	05 80 97 d6 f5 74 93 66	No
Siemens Gigaset A580	67 e6 8d 14 2b 42 3f b7	No
Siemens Gigaset C450 IP	c2 87 10 c3 9e a9 e6 a7	No
Siemens Gigaset E360	06 77 e2 c7 50 73 be 29	No
Siemens Gigaset S680	9a 43 90 dd b2 bb d4 21	No
Siemens SL785	2b ba e9 38 67 1a 99 54	No
T-Home Sinus 45	eb a6 07 b4 37 42 9d 36	No
T-Home Sinus 501	8f d7 04 48 51 b5 4e 46	No
T-Home Sinus A301	1d 56 8a 07 bb a8 ec 19	No

On the other hand random values are exchanged during key allocation procedure. Inside the key allocation procedure an 'authentication of a PT' procedure is implemented. To authenticate the FT the PT sends a self generated random value to the FT inside the {KEY-ALLOCATE} message. To authenticate the PT the FT sends a self generated random value to the PT inside the {AUTHENTICATION-REQ} message (Table 11). The recorded key allocations were recorded between different PPs and the FritzBox. Because of that only random value are needed that sent by the PP. None of the tested devices use the same weak PRNG as the FritzBox.

Table 11: Random numbers recorded during the key allocation

```
[4294945576][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK-
>FP_DLC_LCE_TASK 000 026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 C9 6F
3C 15 01 0B 8E CC 0E 08 DE 78 2B 02 16 1C 99 DB]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08
C9 6F 3C 15 01 0B CC 0E 08 DE 78 2B 02 16 1C 99 DB
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content C9 6F 3C 15
01 0B 8E CC
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content DE 78 2B 02
16 1C 99 DB
[4294945589][DECTSTUB] To IRC case 4 : slot 0x6, from state
0x8
[4294945646][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK-
>FP_MM_TASK 000 023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C
08 35 0E 4F 09 69 42 60 5C 0D 04 B5 50 E3 E0]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00
0C 08 35 0E 4F 09 69 42 60 5C 0D 04 B5 50 E3 E0
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01
48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 35 0E 4F 09
69 42 60 5C
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content B5 50 E3 E0
[4294945647][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK-
>FP_DLC_LCE_TASK 000 008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 94 59 F3 4D]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 94 59
F3 4D
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 94 59 F3 4D
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[0]: 0xC0
```

Table 12: Random numbers generated by portable part

Mobile phone	Random numbers	PRNG (FritzBox)
Binatone Veva 1210	99 af c5 db f1 07 1d 54	No
	b1 ca e3 fc 35 4f 69 83	
	23 27 2b 2f 33 37 3b 60	
	25 39 4d 61 75 89 9d d1	
	e5 fa 0f 45 5b 71 87 9d	
	df e9 f3 fd 07 11 1b 25	
	7f 85 8b 91 97 9d c4 cb	
	17 20 49 53 5d 67 71 7b	
	1f 27 2f 58 61 6a 73 7c	
	f9 18 37 56 75 b5 d5 f5	
Siemens A2	35 0e 4f 09 69 42 60 5c	No
	ad 04 5b b2 ff 6e b7 56	
Siemens Gigaset 4000 Comfort	4b d3 31 e0 d7 2e 9a 14	No
	67 cf 6c fd 91 ee 42 86	
	13 8b 32 2c c7 5a 0d a0	
	9e ae 6d 07 a3 1a 99 78	
	0f 03 38 ec ca a9 43 46	
	7e 05 ec 59 b8 61 d0 57	
	b5 7d da 5e 17 5b 84 3c	
	3d f8 93 10 21 1c d1 aa	
	53 c6 19 5c d7 8a ad 48	
Siemens Gigaset SL56	cb 4e 11 a5 6c 7a 45 38	No
	9b 98 8c 78 11 c1 06 47	
	66 7a 44 47 9d 04 ed 61	
	98 17 39 ed 64 83 b2 d0	
	66 1c 90 89 12 83 95 3d	
	50 fb 82 f7 5a d9 de 33	
	e0 b9 1d 46 de 77 4f 9c	
	ee 35 9c 33 0a b3 f2 2f	
	a8 15 0a af 2c b9 5e 0b	
	51 8a 2f 1a 6b a8 eb f6	

Tabelle 13: Overview about the checked DECT devices

DECT device	Is the same weak PRNG as in the FritzBox implemented?
Binatone Veva 1210	No
Siemens A2	No
Siemens Gigaset 4000 Comfort	No
Siemens Gigaset SL56	No

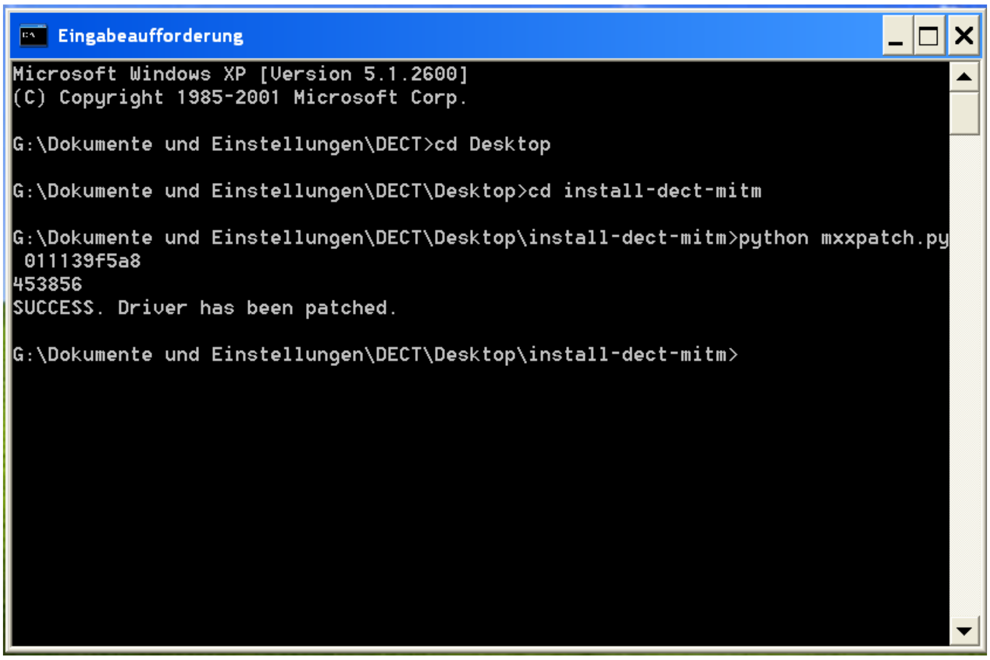
5.2 Impersonation of the base station

Even if the devices work with activated encryption they are not protected against attacks. Impersonation of a FP is an attack using the missing security mechanism 'authentication of a FP'. If this security mechanism is not implemented or inactive an attacker is enabled to make the portable phone believe it is communicating with a specific base station. To do this a simple DECT card is needed. A python script developed by the team members of www.dedected.org allows patching the driver in such a way that the DECT card identifies itself against the portable phone with a defined RFPI and accepts all responses from the portable phone.

With the help of this software it is possible to do the following impersonation attack:

For the attack the RFPI of the FP that is paired with the portable phone and its IPUI are needed. To be more efficient, the first step is to pair the portable phone with the FritzBox. This step enables the attacker to see both the IPUI and the RFPI directly in the DECT-Monitor in a web browser connected to his computer. It is not necessary to search all C channel messages for these two identities.

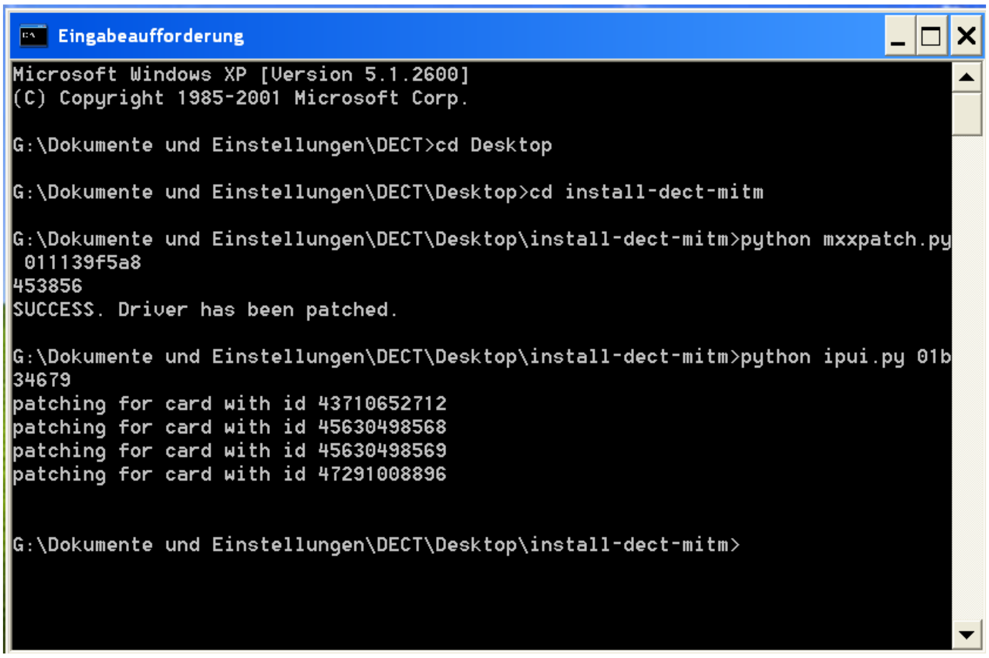
In a first step (as shown in Figure 14) the driver of the DECT card has to be patched with the RFPI of the FritzBox in such a way, that the DECT card identifies itself with the obtained RFPI.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

G:\Dokumente und Einstellungen\DECT>cd Desktop

G:\Dokumente und Einstellungen\DECT\Desktop>cd install-dect-mitm

G:\Dokumente und Einstellungen\DECT\Desktop\install-dect-mitm>python mxxpatch.py
 011139f5a8
453856
SUCCESS. Driver has been patched.

G:\Dokumente und Einstellungen\DECT\Desktop\install-dect-mitm>
```

Figure 14: Patching the driver of the DECT card with a choiced RFPI

The DECT card has to be inserted into the PCMICA slot for a short period of time. Afterwards the patching with the right IPUI can be done as shown in Figure 15.

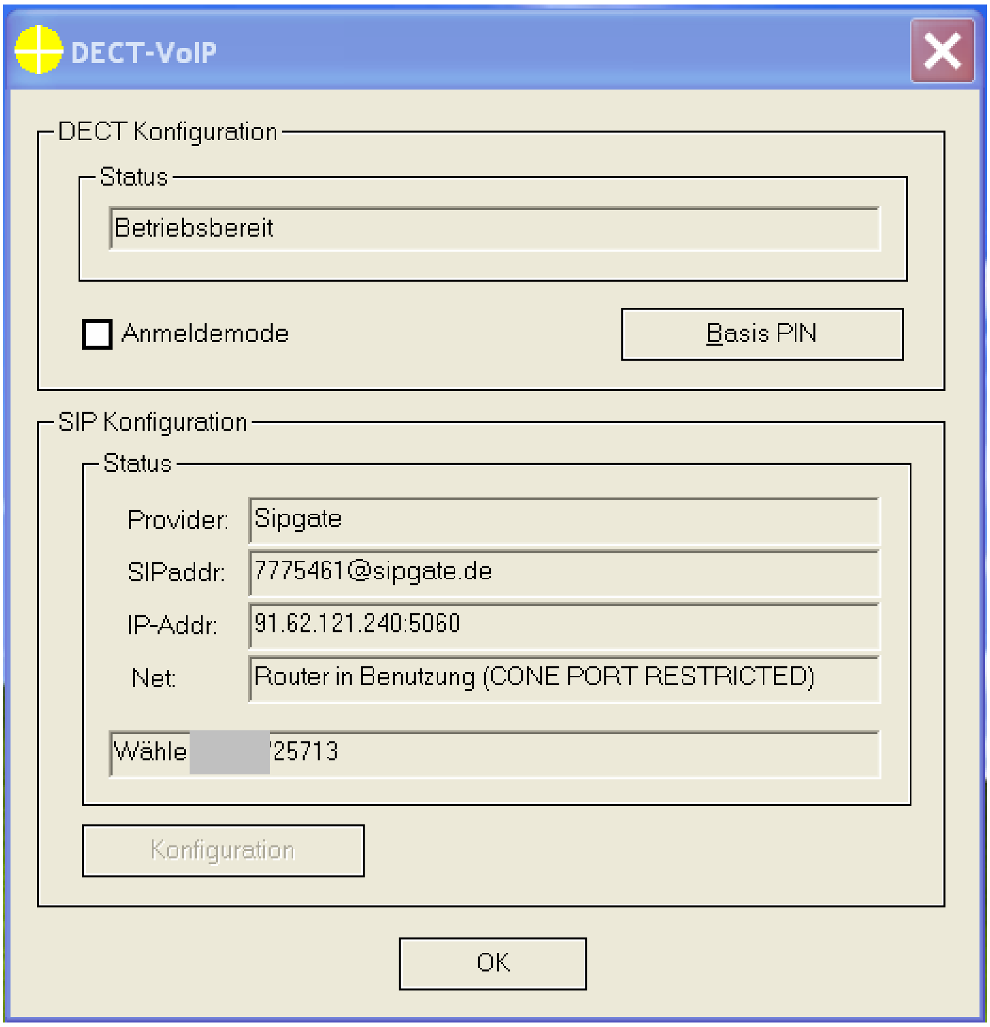


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

G:\Dokumente und Einstellungen\DECT>cd Desktop

G:\Dokumente und Einstellungen\DECT\Desktop>cd install-dect-mitm

G:\Dokumente und Einstellungen\DECT\Desktop\install-dect-mitm>python mxxpatch.py
 011139f5a8
453856
SUCCESS. Driver has been patched.

G:\Dokumente und Einstellungen\DECT\Desktop\install-dect-mitm>python ipui.py 01b
34679
patching for card with id 43710652712
patching for card with id 45630498568
patching for card with id 45630498569
patching for card with id 47291008896


G:\Dokumente und Einstellungen\DECT\Desktop\install-dect-mitm>
```

Figure 15: Patching with a chosen IPUI

For a successful impersonation attack it is necessary to make the 'right' FP inoperable or to achieve a better radio strength. For the tests it was satisfactory to switch the FritzBox off. During a successful attack the portable phone does not recognize the change of the FP and all outgoing calls can be routed. Thus it is possible to see the dialled number in the user interface of the DECT card (Figure 16).

The impersonation attack worked for all 36 tested devices.



DECT-VoIP

DECT Konfiguration

Status: Betriebsbereit

☐ Anmeldemode

SIP Konfiguration

Status

Provider: Sipgate

SIPaddr: 7775461@sipgate.de

IP-Addr: 91.62.121.240:5060

Net: Router in Benutzung (CONE PORT RESTRICTED)

Wähle [redacted]25713

Figure 16: Successful Impersonation attack

Furthermore this attack disables the encryption and the data can be recorded in plaintext. This implies that even a device that normally encrypts its data can fall back to an unencrypted data transmission by the use of the impersonation of a base station. In addition, the common user can not recognize this attack during outgoing calls.

The impersonation of a base station worked for all tested devices. This means that no manufacturer implemented the security mechanism 'authentication of a FT' and even active encryption does not protect against eavesdropping. Although it is a very effective attack, it should be mentioned that making the original base station inoperable is more complex than passive eavesdropping.

5.3 Recapitulation

By executing the test scenarios described above, we get the following results:

Table 14: Level of security

DECT device	Authentication of a		Encryption		Level of security
	PT	FT	Voice data	Signalling data	
AEG Colombo Coral	-	-	-	-	0
AEG Cromo 3400	X	-	X	X	3
AEG Fame 400	-	-	-	-	0
Audioline Big Tel 100	X	-	X	X	3
Audioline Slim DECT 500	X	-	X	X	3
Bang&Olufsen BeoCom 6000	X	-	X	-	2
Doro Phone Easy DECT315	X	-	X	X	3
Grundig Sinio1	-	-	-	-	0
Hagenuk Accento 4000	-	-	-	-	0
Hagenuk AIO 600	X	-	-	-	1
Hagenuk Stick SR	-	-	-	-	0
iDECT x2i	X	-	X	X	3
Loewe Alphatel 5000	-	-	-	-	0
Motorola D701	-	-	-	-	0
Orchid DECT LR 4610	X	-	X	X	3
Panasonic KX-TG 8220	-	-	-	-	0
Philips CD650	X	-	X	X	3
Philips SE250	-	-	-	-	0
Philips Zenia Voice	-	-	-	-	0
Sagem D23XL	X	-	X	X	3
Siemens Gigaset A260	X	-	X	-	2

Siemens Gigaset A580	X	-	X	-	2
Siemens Gigaset C450 IP	X	-	X	-	2
Siemens Gigaset E360	X	-	X	-	2
Siemens Gigaset S680	X	-	X	X	3
Siemens SL785	X	-	X	X	3
T-Home Sinus 45	X	-	X	-	2
T-Home Sinus 101	X	-	X	X	3
T-Home Sinus 102	X	-	X	X	3
T-Home Sinus 212	X	-	X	X	3
T-Home Sinus 501	X	-	X	X	3
T-Home Sinus 710 Komfort	-	-	-	-	0
T-Home Sinus A301	X	-	X	X	3
T-Home Sinus C31	-	-	-	-	0
Tiptel Dectline	-	-	-	-	0
TopCom Butler 800	X	-	X	X	3
Sum	**23**	**0**	**22**	**16**	

The level of security depends on the number of implemented security services. The more security services are active, the higher is the level of security. As final result one can keep in mind that the tested devices support the following security modes:

- 'Identity only' mode: 13 devices
- 'Authentication of PT' mode: 1 device
- 'Authentication of PT in conjunction with active encryption of voice data' mode: 6 devices
- 'Authentication of PT in conjunction with active encryption of voice and signalling data' mode: 16 devices

All these security levels do not provide security against the impersonation of a base station. The only level of security that is recommendable to counter other threats is: Mutual authentication in conjunction with active encryption of voice and signalling data.

"In fact 64 bit of symmetric security might be sufficient to hold off unmotivated attackers, most of the currently deployed DECT systems might be much easier attackable, because encryption and an authentication of the base station are not always required. This allows an attacker spending about 30$ for a DECT card to intercept most DECT phone calls and totally breach the security architecture of DECT."[6]
The results show that currently no satisfying security protection for authenticity and privacy is provided.

6 Conclusion

This thesis gave an overview of the recommended security mechanisms and its appliance in residential devices. Furthermore the resulting threats were demonstrated. Finally it one can keep in mind that none of the tested devices provided all optional security mechanisms (section 3). The direct consequence of which is that none of the tested devices provides holistic protection. Furthermore the structural weakness of the authentication algorithm can lead to future practical attacks on the security of DECT.

To ensure DECT security, finally some recommendations are given. All security mechanisms should be mandatory to avoid a fall back to unencrypted mode like the 'impersonation of a base station' attack has shown. In addition, a strong PRNG shall be implemented. Avoiding further attacks on the encryption algorithm re-keying should be used, which uses a cipher key only a short period of time and renew it periodically. An upgrade of DECT security to public well analyzed methods and algorithms for key exchange, traffic encryption and integrity protection can ensure long term secure authentication and privacy.

LIST OF LITERATURE

[1] DECT Forum: DECT The standard explained, February 1997

[2] European Telecommunication Standard Institute: ETSI EN 300 175-5 V2.2.0: Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 5: Network (NWK) layer, June 2008

[3] European Telecommunication Standard Institute: ETSI EN 300 175-6 V2.2.0: Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 6: Identities and addressing, June 2008

[4] European Telecommunications Standard Institute: ETSI EN 300 175-7 V2.1.1: Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 7: Security Features, August 2007.

[5] European Telecommunication Standard Institute: ETSI EN 300 444 V2.1.0: Digital Enhanced Cordless Telecommunications (DECT); Generic Access Profile (GAP), June 2008

[6] Stefan Lucks, Andreas Schuler, Erik Tews, Ralf-Philipp Weinmann and Matthias Wenzel: Attacks on the DECT authentication mechanisms, 2008

[7] http://www.bundesnetzagentur.de/enid/2/2__8/Betriebsverbot_fuer_Telefone_CTss__und_CT2_4se.html

[8] http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Navigation/Statistiken/Bevoelkerung/Bevoelkerungsstand/__Bevoelkerungsstand.psml

[9] http://etsi.org/WebSite/Technologies/DECT.aspx

[10] http://www.openstreetmap.de/

APPENDIX

1 The DSAA S-Box

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
00	b0	68	6f	f6	7d	e8	16	85	39	7c	7f	de	43	f0	59	a9
10	fb	80	32	ae	5f	25	8c	f5	94	6b	d8	ea	88	98	c2	29
20	cf	3a	50	96	1c	08	95	f4	82	37	0a	56	2c	ff	4f	c4
30	60	a5	83	21	30	f8	f3	28	fa	93	49	34	42	78	bf	fc
40	61	c6	f1	a7	1a	53	03	4d	86	d3	04	87	7e	8f	a0	b7
50	31	b3	e7	0e	2f	cc	69	c3	c0	d9	c8	13	dc	8b	01	52
60	c1	48	ef	af	73	dd	5c	2e	19	91	df	22	d5	3d	0d	a3
70	58	81	3e	fd	62	44	24	2d	b6	8d	5a	05	17	be	27	54
80	5d	9d	d6	ad	6c	ed	64	ce	f2	72	3f	d4	46	a4	10	a2
90	3b	89	97	4c	6e	74	99	e4	e3	bb	ee	70	00	bd	65	20
a0	0f	7a	e9	9e	9b	c7	b5	63	e6	aa	e1	8a	c5	07	06	1e
b0	5e	1d	35	38	77	14	11	e2	b9	84	18	9f	2a	cb	da	f7
c0	a6	b2	66	7b	b1	9c	6d	6a	f9	fe	ca	c9	a8	41	bc	79
d0	db	b8	67	ba	ac	36	ab	92	ab	d7	e5	9a	76	cd	15	1f
e0	4e	4a	57	71	1b	55	09	51	33	0c	b4	8e	2b	e0	d0	5b
f0	47	75	45	40	02	d1	3c	ec	23	eb	0b	d2	a1	90	26	12

2 Measured RFPI in Molkenberg

30 base stations in Molkenberg (68 residents)			
00 D0 5x xx xx	00 76 Dx xx xx	00 D6 Fx xx xx	01 17 3x xx xx
00 D2 3x xx xx	00 F0 4x xx xx	00 62 Ax xx xx	00 65 2x xx xx
00 43 0x xx xx	00 35 Bx xx xx	00 AA 7x xx xx	00 3A 6x xx xx
00 7B 1x xx xx	00 76 Ex xx xx	00 61 Ax xx xx	00 D7 2x xx xx
00 3A 7x xx xx	01 01 Fx xx xx	00 97 Ex xx xx	00 99 Ex xx xx
00 FE 2x xx xx	00 87 8x xx xx	00 97 Ex xx xx	00 20 2x xx xx
00 98 Ax xx xx	00 DA 9x xx xx	00 25 Fx xx xx	
00 B4 1x xx xx	00 D7 2x xx xx	00 4D Fx xx xx	

3 Measured RFPI in Hohl

181 base stations in Hohl (471 residents)			
00 2E 5x xx xx	00 42 8x xx xx	00 7C 2x xx xx	00 BF 3x xx xx
00 05 5x xx xx	00 43 6x xx xx	00 7C 8x xx xx	00 BF 5x xx xx
00 06 Ex xx xx	00 43 Dx xx xx	00 80 2x xx xx	00 BF 8x xx xx
00 08 4x xx xx	00 44 7x xx xx	00 80 2x xx xx	00 C0 Dx xx xx
00 09 5x xx xx	00 45 Fx xx xx	00 80 2x xx xx	00 C0 Dx xx xx

00 0A Ex xx xx	00 46 Bx xx xx	00 82 4x xx xx	00 C3 Dx xx xx
00 0D 3x xx xx	00 47 7x xx xx	00 82 4x xx xx	00 CA 9x xx xx
00 10 1x xx xx	00 48 Fx xx xx	00 82 5x xx xx	00 CE Bx xx xx
00 14 8x xx xx	00 4C Bx xx xx	00 82 5x xx xx	00 CE Dx xx xx
00 19 7x xx xx	00 4D Bx xx xx	00 86 Dx xx xx	00 D1 1x xx xx
00 1B 6x xx xx	00 4E 0x xx xx	00 86 Dx xx xx	00 D2 1x xx xx
00 1B Bx xx xx	00 4F Ex xx xx	00 88 6x xx xx	00 D5 Bx xx xx
00 1C 4x xx xx	00 50 9x xx xx	00 8D 4x xx xx	00 D7 2x xx xx
00 1F 2x xx xx	00 52 2x xx xx	00 8E Bx xx xx	00 D7 Bx xx xx
00 20 0x xx xx	00 54 0x xx xx	00 90 4x xx xx	00 D7 Fx xx xx
00 22 Ex xx xx	00 5A 7x xx xx	00 93 0x xx xx	00 E1 8x xx xx
00 24 7x xx xx	00 5A 8x xx xx	00 97 4x xx xx	00 E1 Bx xx xx
00 24 9x xx xx	00 5A Fx xx xx	00 97 Bx xx xx	00 E2 Ex xx xx
00 24 Cx xx xx	00 5D 2x xx xx	00 98 Cx xx xx	00 E9 6x xx xx
00 26 2x xx xx	00 5D 4x xx xx	00 98 Fx xx xx	00 EE Bx xx xx
00 26 7x xx xx	00 5D 7x xx xx	00 99 3x xx xx	00 EF 4x xx xx
00 29 3x xx xx	00 5F 0x xx xx	00 99 Ex xx xx	00 EF Cx xx xx
00 2C 1x xx xx	00 5F Ex xx xx	00 9D Ex xx xx	00 F4 6x xx xx
00 2C 4x xx xx	00 62 Cx xx xx	00 9E 7x xx xx	00 F4 Cx xx xx
00 2C 4x xx xx	00 62 Cx xx xx	00 9F 7x xx xx	00 F4 Ex xx xx
00 2D Dx xx xx	00 63 Cx xx xx	00 A3 Bx xx xx	00 F7 3x xx xx
00 2E 5x xx xx	00 64 Ax xx xx	00 A6 5x xx xx	00 F7 3x xx xx
00 2F 9x xx xx	00 64 Cx xx xx	00 A6 Fx xx xx	00 F7 5x xx xx
00 30 3x xx xx	00 65 2x xx xx	00 A7 0x xx xx	00 F7 8x xx xx
00 31 3x xx xx	00 65 Dx xx xx	00 AA 7x xx xx	00 F8 5x xx xx
00 31 4x xx xx	00 68 6x xx xx	00 AA Cx xx xx	00 F9 Ex xx xx
00 31 7x xx xx	00 6A 1x xx xx	00 AC 0x xx xx	00 F9 Ex xx xx
00 31 Bx xx xx	00 6B 4x xx xx	00 AE 3x xx xx	00 F9 Ex xx xx
00 32 0x xx xx	00 6D 0x xx xx	00 AE 3x xx xx	00 FF 4x xx xx
00 32 7x xx xx	00 70 6x xx xx	00 AE 4x xx xx	00 FF Ax xx xx
00 32 Cx xx xx	00 72 3x xx xx	00 AE 5x xx xx	01 00 2x xx xx
00 33 Ex xx xx	00 72 7x xx xx	00 B1 4x xx xx	01 01 Bx xx xx
00 33 Fx xx xx	00 74 Ax xx xx	00 B1 8x xx xx	01 18 5x xx xx
00 35 4x xx xx	00 75 9x xx xx	00 B1 8x xx xx	01 1F 4x xx xx
00 38 Fx xx xx	00 77 0x xx xx	00 B2 9x xx xx	01 26 Ex xx xx
00 3B 1x xx xx	00 77 1x xx xx	00 B2 Cx xx xx	10 03 46 0x xx
00 3C Dx xx xx	00 77 3x xx xx	00 B4 5x xx xx	10 03 46 0x xx
00 3D 7x xx xx	00 78 3x xx xx	00 B6 0x xx xx	10 0C 26 Ax xx
00 3E Dx xx xx	00 7A Cx xx xx	00 B9 2x xx xx	
00 3F 2x xx xx	00 7A Dx xx xx	00 BA 9x xx xx	
00 3F 2x xx xx	00 7B 6x xx xx	00 BB Cx xx xx	

4 FP identities [3]

RFPI A				
E	PARI			RPN
Yes / No	A	EMC	FPN	RPN
1 bit	*3 bits*	*16 bits*	*17 bits*	*3 bits*

RFPI B					
E	PARI				RPN
Yes / No	B	EIC	FPN	FPS	RPN
1 bit	*3 bits*	*16 bits*	*8 bits*	*4 bits*	*8 bits*

E	indicates if there are any secondary access rights available
PARI	Primary Access Rights Identity
A	000
B	001
EIC	Equipment Installer Code
EMC	Equipment Manufacturer Code
FPN	Fixed Part Number
FPS	Fixed Part Sub-number
RPN	Radio Fixed Part Number

The measured base stations only are up to the type of RFPI A and RFPI B. Due to anonymity the values FPN‖RPN or rather FPS‖RPN are blackened in section 3.

5 Pseudocode for DSAA

```
Algorithm 1 DSAA (rand $\in \{0, 1\}^{64}$, key $\in \{0, 1\}^{128}$)
    t ← step1(rev(rand), rev(key[32…95]))
    b ← step2(t, rev(key[96…127])||rev(key[0…31]))
    return rev(b[32…63])||rev(t)||rev(b[0…31]))
```

```
Algorithm 2 step1(rand $\in \{0, 1\}^{64}$, key $\in \{0, 1\}^{64}$)
    k = $\text{cassable}^{46,35}_{\text{rand}}$(key)
    return $\text{cassable}^{25,47}_{\text{k}}$(rand)
```

```
Algorithm 3 $\text{cassable}^{\text{start,stop}}_{\text{key}}$(m $\in \{0, 1\}^{64}$)
    t ← key
    s ← m
    for I = 0 to 1 do
        t ← sigma(start, step, t)
        s ← lambda1(gamma(s xor t))
        t ← sigma(start, step, t)
        s ← lambda2(gamma(s xor t))
        t ← sigma(start, step, t)
        s ← lambda3(gamma(s xor t))
        end for
  return s
```

```
Algorithm 4 step2(rand $\in \{0, 1\}^{64}$, key $\in \{0, 1\}^{64}$)
    k = $\text{cassable}^{60,27}_{\text{rand}}$(key)
    return $\text{cassable}^{55,39}_{\text{k}}$(rand)
```

```
Algorithm 5 rev(in $\in \{0, 1\}^{i+8}$)
    Ensure: Byte-reverses the input in
        For j = 0 to i – 1 do
            k ← i - j -1
            out[j * 8…j * 8 + 7] ← in[k *8…k * 8 +7]
        end for
        return out
```

Algorithm 6 lambda1(in ∊ {0, 1}^{64})

```
out[0…7]← in[32…39] + 2 * in[0…7]
out[32…39]← in[0…7] + 3 * in[32…39]
out[8…15] ← in[40…47] + 2 * in[8…15]
out[40…47] ← in[8…15] + 3 * in[40…47]
out[16…23] ← in[48…55] + 2 * in[16…23]
out[48…55] ← in[16…23] + 3 * in[48…55]
out[24…31] ← in[56…63] + 2 * in[24…31]
out[56…63] ← in[24…31] + 3 * in[56…63]
return out
```

Algorithm 7 lambda2(in ∊ {0, 1}^{64})

```
out[0…7] ← in[16…23] + 2 * in[0…7]
out[16…23] ← in[0…7] + 3 * in[16…23]
out[8…15] ← in[24…31] + 2 * in[8…15]
out[24…31] ← in[8…15] + 3 * in[24…31]
out[32…39] ← in[48…55] + 2 * in[32…39]
out[48…55] ← in[32…39] +   3 * in[48…55]
out[40…47] ← in[56…63] +   2 * in[40…47]
out[56…63] ← in[40…47] +   3 * in[56…63]
return out
```

Algorithm 8 lambda3(in ∊ {0, 1}64)

```
out[0…7] ← in[8…15]   + 2 * in[0…7]
out[8…15] ← in[0…7] + 3 * in[8…15]
out[16…23] ← in[24…31] +   2 * in[16…23]
out[24…31] ← in[16…23] +   3 * in[24…31]
out[32…39] ← in[40…47] +   2 * in[32…39]
out[40…47] ← in[32…39] +   3 * in[40…47]
out[48…55] ← in[56…63] +   2 * in[48…55]
out[56…63] ← in[48…55] +   3 * in[56…63]
return out
```

Algorithm 9 sigma(start, step, in $\in \{0, 1\}^{64}$)

```
out ← $(00)^8$
for i = 0 to 63 do
    out[start] ← in[i]
    start ← (start + step) mod 64
end for
return out
```

Algorithm 10 gamma(in $\in \{0, 1\}^{64}$)

```
for i = 0 to 7 do
    out[i*8…i *8+7] ← sbox[in[i*8…i*8 +7]]
end for
return out
```

6 Sniffed messages during the pairing process

- Sent between the FritzBox and the portable part of Siemens A2

```
[4294945576][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK
000 026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 C9 6F 3C 15
01 0B 8E CC 0E 08 DE 78 2B 02 16 1C 99 DB]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 C9 6F 3C
15 01 0B CC 0E 08 DE 78 2B 02 16 1C 99 DB
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content C9 6F 3C 15 01 0B
8E CC
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content DE 78 2B 02 16 1C
99 DB
[4294945589][DECTSTUB] To IRC case 4 : slot 0x6, from state 0x8
[4294945646][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK
000 023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 35
0E 4F 09 69 42 60 5C 0D 04 B5 50 E3 E0]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
35 0E 4F 09 69 42 60 5C 0D 04 B5 50 E3 E0
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 35 0E 4F 09 69 42
60 5C
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content B5 50 E3 E0
[4294945647][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK
000 008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 94 59 F3 4D]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 94 59 F3 4D
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 94 59 F3 4D
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[0]: 0xC0
```

```
[00048393][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 CF 86 A2 30
79 DD 0F 66 0E 08 C0 89 AD 3F 76 D2 00 69]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 CF 86 A2
30 79 DD 0F 66 0E 08 C0 89 AD 3F 76 D2 00 69
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content CF 86 A2 30 79 DD
0F 66
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content C0 89 AD 3F 76 D2
00 69
[00048401][DECTSTUB] To IRC case 4 : slot 0xA, from state 0x8
[00048479][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 AD
04 5B B2 FF 6E B7 56 0D 04 8D 14 0A 83]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
AD 04 5B B2 FF 6E B7 56 0D 04 8D 14 0A 83
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content AD 04 5B B2 FF 6E
B7 56
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 8D 14 0A 83
[00048480][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 A8 68 85 9A]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 A8 68 85 9A
```

```
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content A8 68 85 9A
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[0]: 0xC0
```

- Sent between the FritzBox and the Binatone Veva 1210

```
[4294963435][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK
000 026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 9F C4 E9 FF
74 B1 53 22 0E 08 88 D3 FE E8 63 A6 44 35]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 9F C4 E9
FF 74 B1 53 22 0E 08 88 D3 FE E8 63 A6 44 35
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 9F C4 E9 FF 74 B1
53 22
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content 88 D3 FE E8 63 A6
44 35
[4294963456][DECTSTUB] To IRC case 4 : slot 0x4, from state 0x8
[4294963508][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK
000 023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 99
AF C5 DB F1 07 1D 54 0D 04 06 D6 F2 36]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
99 AF C5 DB F1 07 1D 54 0D 04 06 D6 F2 36
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 99 AF C5 DB F1 07
1D 54
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 06 D6 F2 36
[4294963509][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK
000 008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 5A FF 93 F9]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 5A FF 93 F9
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 5A FF 93 F9
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[4]: 0xC0
```

```
[00005157][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 A1 B1 B9 BD
3F FE 9E AE 0E 08 AE BE B6 B2 30 F1 91 A1]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 A1 B1 B9
BD 3F FE 9E AE 0E 08 AE BE B6 B2 30 F1 91 A1
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content A1 B1 B9 BD 3F FE
9E AE
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content AE BE B6 B2 30 F1
91 A1
[00005169][DECTSTUB] To IRC case 4 : slot 0x0, from state 0x8
[00005233][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 DF
E9 F3 FD 07 11 1B 25 0D 04 70 7B BA AE]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
DF E9 F3 FD 07 11 1B 25 0D 04 70 7B BA AE
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content DF E9 F3 FD 07 11
1B 25
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 70 7B BA AE
```

```
[00005234][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 93 89 A4 F9]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 93 89 A4 F9
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 93 89 A4 F9
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[4]: 0xC0
```

```
[00011002][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 BD 96 83 09
4C 6E FF 37 0E 08 AE 85 90 1A 5F 7D EC 24]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 BD 96 83
09 4C 6E FF 37 0E 08 AE 85 90 1A 5F 7D EC 24
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content BD 96 83 09 4C 6E
FF 37
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content AE 85 90 1A 5F 7D
EC 24
[00011025][DECTSTUB] To IRC case 4 : slot 0x2, from state 0x8
[00011073][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 B1
CA E3 FC 35 4F 69 83 0D 04 11 CC 95 46]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
B1 CA E3 FC 35 4F 69 83 0D 04 11 CC 95 46
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content B1 CA E3 FC 35 4F
69 83
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 11 CC 95 46
[00011074][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 EF 46 F2 B4]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 EF 46 F2 B4
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content EF 46 F2 B4
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[4]: 0xC0
```

```
[00024439][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 C9 57 98 FF
4C 95 79 0F 0E 08 FE 60 AF C8 7B A2 4E 38]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 C9 57 98
FF 4C 95 79 0F 0E 08 FE 60 AF C8 7B A2 4E 38
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content C9 57 98 FF 4C 95
79 0F
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content FE 60 AF C8 7B A2
4E 38
[00024451][DECTSTUB] To IRC case 4 : slot 0x6, from state 0x8
[00024513][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 7F
85 8B 91 97 9D C4 CB 0D 04 0C 81 88 ED]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
7F 85 8B 91 97 9D C4 CB 0D 04 0C 81 88 ED
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 7F 85 8B 91 97 9D
C4 CB
```

```
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 0C 81 88 ED
[00024514][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 8E 6F D5 3C]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 8E 6F D5 3C
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 8E 6F D5 3C
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[4]: 0xC0
```

```
[00033370][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 AD B1 3F F8
1B 6A 52 CE 0E 08 BA A6 28 EF 0C 7D 45 D9]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 AD B1 3F
F8 1B 6A 52 CE 0E 08 BA A6 28 EF 0C 7D 45 D9
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content AD B1 3F F8 1B 6A
52 CE
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content BA A6 28 EF 0C 7D
45 D9
[00033380][DECTSTUB] To IRC case 4 : slot 0xA, from state 0x8
[00033443][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 23
27 2B 2F 33 37 3B 60 0D 04 DA E8 B2 DD]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
23 27 2B 2F 33 37 3B 60 0D 04 DA E8 B2 DD
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 23 27 2B 2F 33 37
3B 60
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content DA E8 B2 DD
[00033444][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 15 28 A1 BA]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 15 28 A1 BA
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 15 28 A1 BA
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[4]: 0xC0
```

```
[00037224][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 07 46 66 F6
BE 9A 08 C1 0E 08 F8 B9 99 09 41 65 F7 3E]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 07 46 66
F6 BE 9A 08 C1 0E 08 F8 B9 99 09 41 65 F7 3E
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 07 46 66 F6 BE 9A
08 C1
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content F8 B9 99 09 41 65
F7 3E
[00037236][DECTSTUB] To IRC case 4 : slot 0x0, from state 0x8
[00037298][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 17
20 49 53 5D 67 71 7B 0D 04 8A B3 DA 5F]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
17 20 49 53 5D 67 71 7B 0D 04 8A B3 DA 5F
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
```

```
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 17 20 49 53 5D 67
71 7B
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 8A B3 DA 5F
[00037299][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 4F 9F E7 3C]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 4F 9F E7 3C
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 4F 9F E7 3C
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[4]: 0xC0
```

```
[00041053][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 AB AE 2C ED
8D 3D 65 49 0E 08 BC B9 3B FA 9A 2A 72 5E]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 AB AE 2C
ED 8D 3D 65 49 0E 08 BC B9 3B FA 9A 2A 72 5E
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content AB AE 2C ED 8D 3D
65 49
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content BC B9 3B FA 9A 2A
72 5E
[00041076][DECTSTUB] To IRC case 4 : slot 0xA, from state 0x8
[00041127][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 25
39 4D 61 75 89 9D D1 0D 04 59 83 2A FC]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
25 39 4D 61 75 89 9D D1 0D 04 59 83 2A FC
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 25 39 4D 61 75 89
9D D1
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 59 83 2A FC
[00041128][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 83 33 4D 53]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 83 33 4D 53
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 83 33 4D 53
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[4]: 0xC0
```

```
[00044793][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 C9 F5 EB 64
A3 C0 F1 E9 0E 08 C6 FA E4 6B AC CF FE E6]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 C9 F5 EB
64 A3 C0 F1 E9 0E 08 C6 FA E4 6B AC CF FE E6
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content C9 F5 EB 64 A3 C0
F1 E9
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content C6 FA E4 6B AC CF
FE E6
[00044804][DECTSTUB] To IRC case 4 : slot 0x0, from state 0x8
[00044883][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 1F
27 2F 58 61 6A 73 7C 0D 04 A3 84 5A 8C]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
1F 27 2F 58 61 6A 73 7C 0D 04 A3 84 5A 8C
```

```
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 1F 27 2F 58 61 6A
73 7C
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content A3 84 5A 8C
[00044884][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 84 4B CD 91]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 84 4B CD 91
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 84 4B CD 91
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[4]: 0xC0
```

```
[00049113][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 FD 61 2F 88
DB 72 A6 4C 0E 08 CA 56 18 BF EC 45 91 7B]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 FD 61 2F
88 DB 72 A6 4C 0E 08 CA 56 18 BF EC 45 91 7B
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content FD 61 2F 88 DB 72
A6 4C
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content CA 56 18 BF EC 45
91 7B
[00049125][DECTSTUB] To IRC case 4 : slot 0x0, from state 0x8
[00049187][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 E5
FA 0F 45 5B 71 87 9D 0D 04 D3 46 3A 0B]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
E5 FA 0F 45 5B 71 87 9D 0D 04 D3 46 3A 0B
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content E5 FA 0F 45 5B 71
87 9D
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content D3 46 3A 0B
[00049188][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 17 88 BD BA]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 17 88 BD BA
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 17 88 BD BA
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[4]: 0xC0
```

```
[00051799][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 9D A3 3C F3
14 E7 1E 62 0E 08 82 BC 23 EC 0B F8 01 7D]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 9D A3 3C
F3 14 E7 1E 62 0E 08 82 BC 23 EC 0B F8 01 7D
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 9D A3 3C F3 14 E7
1E 62
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content 82 BC 23 EC 0B F8
01 7D
[00051813][DECTSTUB] To IRC case 4 : slot 0x2, from state 0x8
[00051869][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 F9
18 37 56 75 B5 D5 F5 0D 04 A5 4B 78 92]
```

```
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
F9 18 37 56 75 B5 D5 F5 0D 04 A5 4B 78 92
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content F9 18 37 56 75 B5
D5 F5
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content A5 4B 78 92
[00051870][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 19 A8 16 44]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 19 A8 16 44
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 19 A8 16 44
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[4]: 0xC0
```

- **Between the FritzBox and Siemens Gigaset 4000 Comfort**

```
[00077190][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 05 4D 69 7B
F2 B6 94 85 0E 08 F2 BA 9E 8C 05 41 63 72]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 05 4D 69
7B F2 B6 94 85 0E 08 F2 BA 9E 8C 05 41 63 72
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 05 4D 69 7B F2 B6
94 85
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content F2 BA 9E 8C 05 41
63 72
[00077201][DECTSTUB] To IRC case 4 : slot 0x8, from state 0x8
[00077269][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 4B
D3 31 E0 D7 2E 9A 14 0D 04 F0 A4 36 E3]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
4B D3 31 E0 D7 2E 9A 14 0D 04 F0 A4 36 E3
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 4B D3 31 E0 D7 2E
9A 14
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content F0 A4 36 E3
[00077270][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 9A 62 27 C0]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 9A 62 27 C0
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 9A 62 27 C0
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[2]: 0xC0
```

```
[00103016][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 ED 0B F8 81
3D E3 0C 7B 0E 08 F2 14 E7 9E 22 FC 13 64]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 ED 0B F8
81 3D E3 0C 7B 0E 08 F2 14 E7 9E 22 FC 13 64
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content ED 0B F8 81 3D E3
0C 7B
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content F2 14 E7 9E 22 FC
13 64
[00103027][DECTSTUB] To IRC case 4 : slot 0x0, from state 0x8
```

```
[00103101][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 7E
05 EC 59 B8 61 D0 57 0D 04 9F E7 D3 23]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
7E 05 EC 59 B8 61 D0 57 0D 04 9F E7 D3 23
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 7E 05 EC 59 B8 61
D0 57
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 9F E7 D3 23
[00103102][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 D5 CD F0 09]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 D5 CD F0 09
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content D5 CD F0 09
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[2]: 0xC0
```

```
[00107720][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 D9 5F 9C FD
CD D5 59 9F 0E 08 EE 68 AB CA FA E2 6E A8]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 D9 5F 9C
FD CD D5 59 9F 0E 08 EE 68 AB CA FA E2 6E A8
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content D9 5F 9C FD CD D5
59 9F
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content EE 68 AB CA FA E2
6E A8
[00107732][DECTSTUB] To IRC case 4 : slot 0x4, from state 0x8
[00107800][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 67
CF 6C FD 91 EE 42 86 0D 04 2A 1A 56 AD]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
67 CF 6C FD 91 EE 42 86 0D 04 2A 1A 56 AD
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 67 CF 6C FD 91 EE
42 86
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 2A 1A 56 AD
[00107801][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 30 F4 65 94]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 30 F4 65 94
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 30 F4 65 94
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[2]: 0xC0
```

```
[00114441][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 9F D6 F2 E0
69 2D 8F 5E 0E 08 90 D9 FD EF 66 22 80 51]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 9F D6 F2
E0 69 2D 8F 5E 0E 08 90 D9 FD EF 66 22 80 51
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 9F D6 F2 E0 69 2D
8F 5E
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content 90 D9 FD EF 66 22
80 51
```

```
[00114453][DECTSTUB] To IRC case 4 : slot 0x2, from state 0x8
[00114521][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 B5
7D DA 5E 17 5B 84 3C 0D 04 A5 19 02 ED]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
B5 7D DA 5E 17 5B 84 3C 0D 04 A5 19 02 ED
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content B5 7D DA 5E 17 5B
84 3C
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content A5 19 02 ED
[00114522][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 49 A6 20 6A]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 49 A6 20 6A
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 49 A6 20 6A
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[2]: 0xC0
```

```
[00127786][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 9D 29 73 5E
48 C3 86 24 0E 08 8A 3E 64 49 5F D4 91 33]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 9D 29 73
5E 48 C3 86 24 0E 08 8A 3E 64 49 5F D4 91 33
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 9D 29 73 5E 48 C3
86 24
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content 8A 3E 64 49 5F D4
91 33
[00127798][DECTSTUB] To IRC case 4 : slot 0x4, from state 0x8
[00127870][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 13
8B 32 2C C7 5A 0D A0 0D 04 99 24 FD 40]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
13 8B 32 2C C7 5A 0D A0 0D 04 99 24 FD 40
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 13 8B 32 2C C7 5A
0D A0
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 99 24 FD 40
[00127871][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 43 70 C0 D8]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 43 70 C0 D8
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 43 70 C0 D8
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[2]: 0xC0
```

```
[00132875][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 DB A8 91 8D
03 C4 A7 96 0E 08 24 57 6E 72 FC 3B 58 69]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 DB A8 91
8D 03 C4 A7 96 0E 08 24 57 6E 72 FC 3B 58 69
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content DB A8 91 8D 03 C4
A7 96
```

```
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content 24 57 6E 72 FC 3B
58 69
[00132886][DECTSTUB] To IRC case 4 : slot 0x0, from state 0x8
[00132954][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 3D
F8 93 10 21 1C D1 AA 0D 04 8C E2 DB 5B]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
3D F8 93 10 21 1C D1 AA 0D 04 8C E2 DB 5B
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 3D F8 93 10 21 1C
D1 AA
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 8C E2 DB 5B
[00132955][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 54 CD A7 2B]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 54 CD A7 2B
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 54 CD A7 2B
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[2]: 0xC0
```

```
[00140556][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 0F 7C 45 D9
97 B0 23 EA 0E 08 18 6B 52 CE 80 A7 34 FD]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 0F 7C 45
D9 97 B0 23 EA 0E 08 18 6B 52 CE 80 A7 34 FD
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 0F 7C 45 D9 97 B0
23 EA
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content 18 6B 52 CE 80 A7
34 FD
[00140567][DECTSTUB] To IRC case 4 : slot 0x2, from state 0x8
[00140636][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 9E
AE 6D 07 A3 1A 99 78 0D 04 52 6E DF 86]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
9E AE 6D 07 A3 1A 99 78 0D 04 52 6E DF 86
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 9E AE 6D 07 A3 1A
99 78
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 52 6E DF 86
[00140637][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 26 6D 4F 61]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 26 6D 4F 61
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 26 6D 4F 61
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[2]: 0xC0
```

```
[00145644][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 8D D7 7A AC
47 B2 48 35 0E 08 82 D8 75 A3 48 BD 47 3A]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 8D D7 7A
AC 47 B2 48 35 0E 08 82 D8 75 A3 48 BD 47 3A
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
```

```
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 8D D7 7A AC 47 B2
48 35
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content 82 D8 75 A3 48 BD
47 3A
[00145656][DECTSTUB] To IRC case 4 : slot 0x8, from state 0x8
[00145730][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 53
C6 19 5C D7 8A AD 48 0D 04 5F 05 23 7F]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
53 C6 19 5C D7 8A AD 48 0D 04 5F 05 23 7F
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 53 C6 19 5C D7 8A
AD 48
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 5F 05 23 7F
[00145731][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 71 59 CD 09]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 71 59 CD 09
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 71 59 CD 09
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[2]: 0xC0
```

```
[00150636][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 79 A3 4E B8
C3 7E A0 4F 0E 08 4E 94 79 8F F4 49 97 78]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 79 A3 4E
B8 C3 7E A0 4F 0E 08 4E 94 79 8F F4 49 97 78
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 79 A3 4E B8 C3 7E
A0 4F
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content 4E 94 79 8F F4 49
97 78
[00150648][DECTSTUB] To IRC case 4 : slot 0x0, from state 0x8
[00150716][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 0F
03 38 EC CA A9 43 46 0D 04 B6 7A 56 06]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
0F 03 38 EC CA A9 43 46 0D 04 B6 7A 56 06
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 0F 03 38 EC CA A9
43 46
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content B6 7A 56 06
[00150717][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 47 E0 D0 86]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 47 E0 D0 86
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 47 E0 D0 86
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[2]: 0xC0
```

- Between FritzBox and Siemens Gigaset SL56

```
[00199790][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 3F F2 14 E7
9E 22 FC 13 0E 08 20 ED 0B F8 81 3D E3 0C]
```

```
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 3F F2 14
E7 9E 22 FC 13 0E 08 20 ED 0B F8 81 3D E3 0C
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 3F F2 14 E7 9E 22
FC 13
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content 20 ED 0B F8 81 3D
E3 0C
[00199804][DECTSTUB] To IRC case 4 : slot 0x0, from state 0x8
[00199852][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 CB
4E 11 A5 6C 7A 45 38 0D 04 43 69 E3 4E]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
CB 4E 11 A5 6C 7A 45 38 0D 04 43 69 E3 4E
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content CB 4E 11 A5 6C 7A
45 38
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 43 69 E3 4E
[00199853][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 9D 5B DE 44]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 9D 5B DE 44
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 9D 5B DE 44
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[3]: 0xC0
```

```
[00218512][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 A9 17 48 67
F0 3B 5E 6C 0E 08 5E E0 BF 90 07 CC A9 9B]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 A9 17 48
67 F0 3B 5E 6C 0E 08 5E E0 BF 90 07 CC A9 9B
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content A9 17 48 67 F0 3B
5E 6C
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content 5E E0 BF 90 07 CC
A9 9B
[00218526][DECTSTUB] To IRC case 4 : slot 0x4, from state 0x8
[00218576][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 50
FB 82 F7 5A D9 DE 33 0D 04 AF 2B BC 57]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
50 FB 82 F7 5A D9 DE 33 0D 04 AF 2B BC 57
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 50 FB 82 F7 5A D9
DE 33
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content AF 2B BC 57
[00218578][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 BA 3B C8 86]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 BA 3B C8 86
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content BA 3B C8 86
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[3]: 0xC0
```

```
[00224467][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 EF 1E E6 9A
A4 3B 74 53 0E 08 E0 11 E9 95 AB 34 7B 5C]
```

```
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 EF 1E E6
9A A4 3B 74 53 0E 08 E0 11 E9 95 AB 34 7B 5C
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content EF 1E E6 9A A4 3B
74 53
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content E0 11 E9 95 AB 34
7B 5C
[00224529][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 9B
98 8C 78 11 C1 06 47 0D 04 6F 04 D8 B2]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
9B 98 8C 78 11 C1 06 47 0D 04 6F 04 D8 B2
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 9B 98 8C 78 11 C1
06 47
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 6F 04 D8 B2
[00224530][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 FB A6 9D 7F]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 FB A6 9D 7F
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content FB A6 9D 7F
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[3]: 0xC0
```

```
[00231665][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 7B AA 42 B6
4C B1 CF F0 0E 08 6C BD 55 A1 5B A6 D8 E7]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 7B AA 42
B6 4C B1 CF F0 0E 08 6C BD 55 A1 5B A6 D8 E7
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 7B AA 42 B6 4C B1
CF F0
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content 6C BD 55 A1 5B A6
D8 E7
[00231680][DECTSTUB] To IRC case 4 : slot 0x8, from state 0x8
[00231730][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 E0
B9 1D 46 DE 77 4F 9C 0D 04 B9 EF A0 3A]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
E0 B9 1D 46 DE 77 4F 9C 0D 04 B9 EF A0 3A
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content E0 B9 1D 46 DE 77
4F 9C
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content B9 EF A0 3A
[00231731][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 F1 D1 F7 56]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 F1 D1 F7 56
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content F1 D1 F7 56
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[3]: 0xC0
```

```
[00244823][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 83 54 3F 8A
D0 7D 2B 00 0E 08 BC 6B 00 B5 EF 42 14 3F]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 83 54 3F
8A D0 7D 2B 00 0E 08 BC 6B 00 B5 EF 42 14 3F
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 83 54 3F 8A D0 7D
2B 00
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content BC 6B 00 B5 EF 42
14 3F
[00244833][DECTSTUB] To IRC case 4 : slot 0x4, from state 0x8
[00244887][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 66
7A 44 47 9D 04 ED 61 0D 04 2B 43 75 2A]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
66 7A 44 47 9D 04 ED 61 0D 04 2B 43 75 2A
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 66 7A 44 47 9D 04
ED 61
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 2B 43 75 2A
[00244888][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 4A 44 9F 9E]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 4A 44 9F 9E
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 4A 44 9F 9E
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[3]: 0xC0
```

```
[00250676][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 71 D3 02 6A
5E C4 89 AF 0E 08 66 C4 15 7D 49 D3 9E B8]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 71 D3 02
6A 5E C4 89 AF 0E 08 66 C4 15 7D 49 D3 9E B8
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 71 D3 02 6A 5E C4
89 AF
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content 66 C4 15 7D 49 D3
9E B8
[00250689][DECTSTUB] To IRC case 4 : slot 0x6, from state 0x8
[00250739][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 EE
35 9C 33 0A B3 F2 2F 0D 04 81 29 17 40]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
EE 35 9C 33 0A B3 F2 2F 0D 04 81 29 17 40
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content EE 35 9C 33 0A B3
F2 2F
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 81 29 17 40
[00250740][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 85 64 C3 AD]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 85 64 C3 AD
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 85 64 C3 AD
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[3]: 0xC0
```

```
[00254707][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 33 D8 2D 57
6A F4 BB 9C 0E 08 3C D7 22 58 65 FB B4 93]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 33 D8 2D
57 6A F4 BB 9C 0E 08 3C D7 22 58 65 FB B4 93
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 33 D8 2D 57 6A F4
BB 9C
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content 3C D7 22 58 65 FB
B4 93
[00254722][DECTSTUB] To IRC case 4 : slot 0x8, from state 0x8
[00254772][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 98
17 39 ED 64 83 B2 D0 0D 04 47 99 78 BE]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
98 17 39 ED 64 83 B2 D0 0D 04 47 99 78 BE
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 98 17 39 ED 64 83
B2 D0
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 47 99 78 BE
[00254773][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 18 F7 B3 E7]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 18 F7 B3 E7
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 18 F7 B3 E7
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[3]: 0xC0
```

```
[00259221][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 B3 36 74 55
45 4D 49 CB 0E 08 C4 41 03 22 32 3A 3E BC]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 B3 36 74
55 45 4D 49 CB 0E 08 C4 41 03 22 32 3A 3E BC
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content B3 36 74 55 45 4D
49 CB
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content C4 41 03 22 32 3A
3E BC
[00259234][DECTSTUB] To IRC case 4 : slot 0x0, from state 0x8
[00259287][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 A8
15 0A AF 2C B9 5E 0B 0D 04 FC 56 7B 94]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
A8 15 0A AF 2C B9 5E 0B 0D 04 FC 56 7B 94
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content A8 15 0A AF 2C B9
5E 0B
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content FC 56 7B 94
[00259288][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 32 41 F3 69]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 32 41 F3 69
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 32 41 F3 69
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[3]: 0xC0
```

```
[00264020][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 95 D7 76 A6
4E 3A 00 1D 0E 08 8A C8 69 B9 51 25 1F 02]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 95 D7 76
A6 4E 3A 00 1D 0E 08 8A C8 69 B9 51 25 1F 02
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 95 D7 76 A6 4E 3A
00 1D
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content 8A C8 69 B9 51 25
1F 02
[00264034][DECTSTUB] To IRC case 4 : slot 0x8, from state 0x8
[00264085][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 66
1C 90 89 12 83 95 3D 0D 04 4C 62 A8 52]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
66 1C 90 89 12 83 95 3D 0D 04 4C 62 A8 52
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 66 1C 90 89 12 83
95 3D
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 4C 62 A8 52
[00264086][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 A6 BC 1A C6]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 A6 BC 1A C6
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content A6 BC 1A C6
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[3]: 0xC0
```

```
[00269782][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
026 0x05
(MM_KEY_ALLOCATE) [04 0E 00 1A 05 42 0B 02 01 88 0C 08 9B DE FC 6D
A5 C1 73 AA 0E 08 AC E9 CB 5A 92 F6 44 9D]
[DECT_INFOELE] MM mmei:0 OUT KEY_ALLOCATE 0B 02 01 88 0C 08 9B DE FC
6D A5 C1 73 AA 0E 08 AC E9 CB 5A 92 F6 44 9D
[DECT_INFOELE]   IE Var 0B Allocate : Len 2 : Content 01 88
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 9B DE FC 6D A5 C1
73 AA
[DECT_INFOELE]   IE Var 0E Data : Len 8 : Content AC E9 CB 5A 92 F6
44 9D
[00269795][DECTSTUB] To IRC case 4 : slot 0x2, from state 0x8
[00269848][DCTDRV] (FP_MM_DATA_IND) FP_DLC_LCE_TASK->FP_MM_TASK 000
023 0x85
(MM_AUTHENTICATION_REQ) [05 0E 00 17 85 40 0A 03 01 48 00 0C 08 51
8A 2F 1A 6B A8 EB F6 0D 04 88 44 74 CD]
[DECT_INFOELE] MM mmei:0 IN AUTHENTICATION_REQ 0A 03 01 48 00 0C 08
51 8A 2F 1A 6B A8 EB F6 0D 04 88 44 74 CD
[DECT_INFOELE]   IE Var 0A Authenticate : Len 3 : Content 01 48 00
[DECT_INFOELE]   IE Var 0C Rand : Len 8 : Content 51 8A 2F 1A 6B A8
EB F6
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 88 44 74 CD
[00269849][DCTDRV] (FP_MM_DATA_REQ) FP_MM_TASK->FP_DLC_LCE_TASK 000
008 0x05
(MM_AUTHENTICATION_REP) [04 0E 00 08 05 41 0D 04 48 F2 26 F3]
[DECT_INFOELE] MM mmei:0 OUT AUTHENTICATION_REP 0D 04 48 F2 26 F3
[DECT_INFOELE]   IE Var 0D Res : Len 4 : Content 48 F2 26 F3
[DECTDRV] [0]FP_LCE_MM_RELEASE_LINK_REQ: 0101 0000
[DECTDRV] codec_list[3]: 0xC0
```

7 Messages sent during call establishment

AEG Colombo Coral

```
phone  : addr:91 ctrl:00 len:01 crc:0c04
phone  : addr:11 ctrl:02 len:59 crc:bdb6 -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 01 1b 56 02
4d 06 07 a0 a5 01 1b 5d 86 00 e0 80
phone  : addr:11 ctrl:00 len:65 crc:8b95 -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 05 05 07
80 a8 01 1b 56 02 4d 06 07 a0 a5 01 1b 5d 86 00 12 03 88 80 c0
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:13 ctrl:01 len:01 crc:158d
phone  : addr:11 ctrl:02 len:39 crc:18d2 -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 7b 77 0a
c0 80 00 4d 28 00 01 00 00 00
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:11 ctrl:20 len:39 crc:b55a -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 7b 77 0a
c0 80 00 4d 17 00 01 00 00 00
phone  : addr:13 ctrl:01 len:01 crc:158d
phone  : addr:11 ctrl:02 len:39 crc:9f43 -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 7b 77 0a
c0 80 00 4d 18 00 01 00 00 00
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:11 ctrl:20 len:09 crc:92fb -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 78
phone  : addr:13 ctrl:01 len:01 crc:158d
phone  : addr:11 ctrl:02 len:15 crc:947b -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 32
station: addr:11 ctrl:01 len:01 crc:0d87
station: addr:13 ctrl:00 len:3d crc:1a09 -> 0011 CC
(Call Control) messages :{IWU-INFO}    83 60 77 0b c0 80 00 00 03 46
64 00 00 00 00
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:11 ctrl:20 len:15 crc:8311 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 35
station: addr:11 ctrl:21 len:01 crc:edc7
station: addr:13 ctrl:22 len:3d crc:804d -> 0011 CC
(Call Control) messages :{IWU-INFO}    83 60 77 0b c0 80 00 00 03 46
64 00 00 00 00
phone  : addr:13 ctrl:01 len:01 crc:158d
phone  : addr:11 ctrl:02 len:15 crc:9e7e -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 37
station: addr:11 ctrl:01 len:01 crc:0d87
station: addr:13 ctrl:00 len:3d crc:1a09 -> 0011 CC
(Call Control) messages :{IWU-INFO}    83 60 77 0b c0 80 00 00 03 46
64 00 00 00 00
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:11 ctrl:20 len:15 crc:fb2d -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 31
station: addr:11 ctrl:21 len:01 crc:edc7
station: addr:13 ctrl:22 len:3d crc:804d -> 0011 CC
(Call Control) messages :{IWU-INFO}    83 60 77 0b c0 80 00 00 03 46
64 00 00 00 00
phone  : addr:13 ctrl:01 len:01 crc:158d
phone  : addr:11 ctrl:02 len:15 crc:967a -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 33
station: addr:11 ctrl:01 len:01 crc:0d87
station: addr:13 ctrl:00 len:3d crc:1a09 -> 0011 CC
```

```
(Call Control) messages :{IWU-INFO}    83 60 77 0b c0 80 00 00 03 46
64 00 00 00 00
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:11 ctrl:20 len:09 crc:ba2c -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 4d
station: addr:13 ctrl:02 len:09 crc:67ec -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    87 4d
phone  : addr:13 ctrl:01 len:01 crc:158d
station: addr:11 ctrl:21 len:01 crc:edc7
phone  : addr:11 ctrl:02 len:09 crc:b107 -> 0011 CC
(Call Control) messages :{CC-RELEASE}    03 4d
station: addr:11 ctrl:01 len:01 crc:0d87
station: addr:13 ctrl:00 len:09 crc:78de -> 0011 CC
(Call Control) messages :{CC-RELEASE-COM}    83 5a
phone  : addr:91 ctrl:00 len:01 crc:0c04
phone  : addr:11 ctrl:02 len:65 crc:4ceb -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 05 05 07
80 a8 01 1b 56 02 4d 06 07 a0 a5 01 1b 5d 86 00 12 03 88 80 c0
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:11 ctrl:20 len:39 crc:3ed2 -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 7b 77 0a
c0 80 00 4d 28 00 01 00 00 00
phone  : addr:13 ctrl:01 len:01 crc:158d
phone  : addr:11 ctrl:02 len:39 crc:28c0 -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 7b 77 0a
c0 80 00 4d 2a 00 01 00 00 00
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:13 ctrl:01 len:01 crc:158d
phone  : addr:11 ctrl:00 len:09 crc:91d8 -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 78
```

AEG Cromo 3400

```
phone  : addr:91 ctrl:00 len:01 crc:b7b4
phone  : addr:11 ctrl:02 len:8d crc:a889 -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 01 15 51 dc
7a 06 07 a0 a5 01 15 57 90 18 e0 80 63 0b 44 00 08 00 1a 01 0c 80 82
01 81
station: addr:11 ctrl:01 len:01 crc:b637
station: addr:13 ctrl:00 len:19 crc:5830 -> 0101 MM
(Mobility Management) messages :{CIPHER-REQUEST}    05 4c 19 02 81
98
station: addr:b7 ctrl:d9 len:52 crc:582f -> reserved     2b 74 7e 73
09 dc d2 f8 c7 13 22 80 31 66 9b 79 00 7d a5 1d
```

AEG Fame 400

```
phone  : addr:11 ctrl:02 len:11 crc:dc7b -> 0011 CC
(Call Control) messages :{CC-RELEASE}    03 4d e2 00
station: addr:11 ctrl:01 len:01 crc:b697
station: addr:13 ctrl:00 len:11 crc:9632 -> 0011 CC
(Call Control) messages :{CC-RELEASE-COM}    83 5a e2 00
phone  : addr:91 ctrl:00 len:51 crc:0c79 -> 0000 LCE
(Link Control Entity) messages :NULL    00 71 05 07 80 a8 00 c5 20
09 75 06 07 a0 a5 00 c5 20 4b a8
phone  : addr:13 ctrl:21 len:01 crc:4edd
phone  : addr:11 ctrl:22 len:85 crc:a77d -> 0101 MM
```

```
(Mobility Management) messages :{LOCATE-REQUEST}    05 54 05 07 80
a8 00 c5 20 09 75 06 07 81 a8 00 c5 20 4b a8 07 01 67 63 03 c2 82 84
78 03 02 84 3b
phone  : addr:13 ctrl:01 len:01 crc:ae9d
phone  : addr:11 ctrl:20 len:15 crc:423a -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 30
station: addr:11 ctrl:21 len:01 crc:56d7
station: addr:13 ctrl:22 len:25 crc:5c6b -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 05 81 02 84 05 01
phone  : addr:13 ctrl:01 len:01 crc:ae9d
phone  : addr:11 ctrl:02 len:11 crc:dc7b -> 0011 CC
(Call Control) messages :{CC-RELEASE}    03 4d e2 00
station: addr:11 ctrl:01 len:01 crc:b697
station: addr:13 ctrl:00 len:11 crc:9632 -> 0011 CC
(Call Control) messages :{CC-RELEASE-COM}    83 5a e2 00
phone  : addr:91 ctrl:00 len:51 crc:0c79 -> 0000 LCE
(Link Control Entity) messages :NULL    00 71 05 07 80 a8 00 c5 20
09 75 06 07 a0 a5 00 c5 20 4b a8
phone  : addr:13 ctrl:21 len:01 crc:4edd
phone  : addr:11 ctrl:22 len:85 crc:a77d -> 0101 MM
(Mobility Management) messages :{LOCATE-REQUEST}    05 54 05 07 80
a8 00 c5 20 09 75 06 07 81 a8 00 c5 20 4b a8 07 01 67 63 03 c2 82 84
78 03 02 84 3b
phone  : addr:13 ctrl:01 len:01 crc:ae9d
phone  : addr:13 ctrl:21 len:01 crc:4edd
phone  : addr:11 ctrl:20 len:09 crc:bc72 -> 0101 MM
(Mobility Management) messages :{TEMPORARY-IDENTITY-ASSIGN-ACK}
05 5d
```

Audioline Big Tel 100

```
phone  : addr:91 ctrl:00 len:01 crc:b7b4
phone  : addr:11 ctrl:02 len:8d crc:8286 -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 01 15 53 aa
56 06 07 a0 a5 01 15 5e 34 e8 e0 80 63 0b 44 00 08 00 1a 01 0c 80 82
01 81
station: addr:11 ctrl:01 len:01 crc:b637
station: addr:13 ctrl:00 len:19 crc:5830 -> 0101 MM
(Mobility Management) messages :{CIPHER-REQUEST}    05 4c 19 02 81
98
phone  : addr:19 ctrl:77 len:33 crc:5101 -> reserved     58 5f fa 07
e9 43 fa a2 5e e0 e7 ff
station: addr:b1 ctrl:85 len:8d crc:10dd -> reserved     2a 94 bf 7e
8e fe c6 82 b6 e5 41 2e db bd 59 d1 c4 a4 5b 78 c9 3b b6 ca d3 9e 77
1f 83 52 37 87 10 1f e3
```

Audioline Slim DECT 500

```
phone  : addr:91 ctrl:00 len:01 crc:b7b4
phone  : addr:11 ctrl:02 len:8d crc:3fcc -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 01 04 62 76
5a 06 07 a0 a5 01 04 6e 6c c0 e0 80 63 0b 44 00 08 00 1a 01 0c 80 a2
01 81
station: addr:11 ctrl:01 len:01 crc:b637
station: addr:13 ctrl:00 len:19 crc:5830 -> 0101 MM
(Mobility Management) messages :{CIPHER-REQUEST}    05 4c 19 02 81
98
```

Bang&Olufsen BeoCom 6000

```
phone  : addr:91 ctrl:00 len:01 crc:a6b1
station: addr:91 ctrl:21 len:01 crc:45f3
phone  : addr:11 ctrl:02 len:59 crc:f1d6 -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 00 1b 31 35
c7 06 07 a0 a5 00 07 e1 c8 20 e0 80
station: addr:11 ctrl:01 len:01 crc:a732
station: addr:13 ctrl:00 len:09 crc:7526 -> 0011 CC
(Call Control) messages :{CC-CONNECT}    83 07
phone  : addr:13 ctrl:21 len:01 crc:5f78
station: addr:13 ctrl:02 len:2d crc:1baa -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 77 07 c0 81 7e 00 42 c0
00
phone  : addr:11 ctrl:20 len:25 crc:e9c7 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 77 05 c0 81 7e 00 40
station: addr:11 ctrl:21 len:01 crc:4772
phone  : addr:13 ctrl:01 len:01 crc:bf38
station: addr:13 ctrl:20 len:19 crc:a7b6 -> 0101 MM
(Mobility Management) messages :{CIPHER-REQUEST}    05 4c 19 02 81
98
phone  : addr:11 ctrl:02 len:25 crc:8d83 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 05 32 35 37 31 33
phone  : addr:13 ctrl:21 len:01 crc:5f78
station: addr:11 ctrl:01 len:01 crc:a732
station: addr:37 ctrl:d6 len:00 crc:fa55
station: addr:69 ctrl:cf len:3c crc:3863 -> reserved     6a 7a 78 8f
1a 3e 63 fa 7c 62 7a 65 f1 1d 94
```

Doro Phone Easy DECT 315

```
station: addr:91 ctrl:21 len:01 crc:54f6
phone  : addr:11 ctrl:02 len:99 crc:445d -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 00 f9 45 c4
8c 06 07 a0 a5 00 ff 37 0a 48 e0 b0 2c 01 ff 63 0b 44 00 08 00 1a 01
0c 80 82 01 81
station: addr:11 ctrl:01 len:01 crc:b637
station: addr:13 ctrl:00 len:19 crc:5830 -> 0101 MM
(Mobility Management) messages :{CIPHER-REQUEST}    05 4c 19 02 81
98
station: addr:6f ctrl:46 len:4d crc:6f87 -> reserved     68 3c 16 74
8d 12 9f 34 a4 5b 89 2d 70 e8 ec 3c b7 99 05
phone  : addr:78 ctrl:2e len:9d crc:b0e4 -> reserved     ca 36 75 0c
2c 55 aa a0 f1 9b 92 8c 06 ed 64 95 4e 38 d2 6f a7 6b 13 99 25 37 9e
61 4c 6d 0b 5c d0 0a 61 12 bc 26 25
station: addr:40 ctrl:e4 len:54 crc:dd3c -> reserved     59 b1 ba 14
3c a6 c9 58 eb 16 f9 fc c1 ce 18 ed 88 09 e4 ba fa
phone  : addr:fa ctrl:8c len:e6 crc:bffd -> 0100 CISS
(Call Independent Supplementary Services) messages :(null)    74 1d
4d af e2 79 e6 65 ba 29 87 3f 0f 94 b4 35 ae e7 7c 91 f7 04 0f d6 49
22 07 c6 9f 36 e9 06 32 29 a7 f9 e0 e5 13 b2 89 f6 b3 8b 7f 59 48 1d
74 84 6f 72 76 6d 0e f2 8b
phone  : addr:ea ctrl:2b len:30 crc:3b07 -> reserved     41 44 71 c6
14 be 30 81 1f 44 36 42
phone  : addr:9e ctrl:99 len:b2 crc:b562 -> reserved     3b 5b 51 95
42 2a 5f d3 4b 09 c7 db 45 ff 30 a8 05 c0 38 ea 52 31 60 b5 e0 88 e9
38 6b 2b 23 20 5b f2 11 ec 51 62 44 29 06 ff e6 80
```

Grundig Sinio 1

```
phone  : addr:91 ctrl:00 len:01 crc:b714
phone  : addr:11 ctrl:02 len:7d crc:b3b4 -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 00 c1 6f 4d
83 06 07 a0 a5 00 a6 30 16 88 e0 80 7b 07 81 03 51 15 00 0c 00
station: addr:11 ctrl:01 len:01 crc:b697
station: addr:13 ctrl:00 len:4d crc:8ad5 -> 0011 CC
(Call Control) messages :{CC-CONNECT}    83 07 7b 0f 81 03 51 0a 00
1a 00 1f 00 29 00 30 00 28 00
phone  : addr:13 ctrl:21 len:01 crc:4edd
station: addr:13 ctrl:02 len:55 crc:26cc -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 11 81 03 51 02 16 0a
00 1a 00 1f 00 29 00 30 00 28 00
phone  : addr:11 ctrl:20 len:25 crc:1551 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 05 32 35 37 31 33
phone  : addr:13 ctrl:01 len:01 crc:ae9d
station: addr:11 ctrl:21 len:01 crc:56d7
phone  : addr:11 ctrl:02 len:15 crc:9339 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 00
station: addr:11 ctrl:01 len:01 crc:b697
station: addr:13 ctrl:00 len:55 crc:a0a6 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 11 81 03 51 05 01 0a
00 1a 00 1f 00 29 00 30 00 28 00
phone  : addr:13 ctrl:21 len:01 crc:4edd
station: addr:13 ctrl:02 len:55 crc:689c -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 11 81 03 51 05 01 0a
00 1a 00 1f 00 29 00 30 00 28 00
phone  : addr:13 ctrl:01 len:01 crc:ae9d
station: addr:13 ctrl:00 len:55 crc:a0a6 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 11 81 03 51 05 01 0a
00 1a 00 1f 00 29 00 30 00 28 00
phone  : addr:13 ctrl:21 len:01 crc:4edd
station: addr:13 ctrl:02 len:55 crc:689c -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 11 81 03 51 05 01 0a
00 1a 00 1f 00 29 00 30 00 28 00
phone  : addr:13 ctrl:01 len:01 crc:ae9d
station: addr:13 ctrl:00 len:55 crc:a0a6 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 11 81 03 51 05 01 0a
00 1a 00 1f 00 29 00 30 00 28 00
phone  : addr:13 ctrl:21 len:01 crc:4edd
```

Hagenuk Accento 4000

```
phone  : addr:91 ctrl:00 len:01 crc:0c04
phone  : addr:11 ctrl:02 len:59 crc:b7d4 -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 01 11 31 da
55 06 07 a0 a5 01 11 39 f5 a8 e0 80
phone  : addr:11 ctrl:00 len:65 crc:8d33 -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 05 05 07
80 a8 01 11 31 da 55 06 07 a0 a5 01 11 39 f5 a8 12 03 88 80 c0
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:13 ctrl:01 len:01 crc:158d
phone  : addr:11 ctrl:02 len:39 crc:30c9 -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 7b 77 0a
c0 80 00 4d 2b 00 01 00 00 00
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:11 ctrl:20 len:15 crc:f92a -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 3x
phone  : addr:11 ctrl:22 len:15 crc:8b1b -> 0011 CC
```

```
(Call Control) messages :{CC-INFO}    03 7b 2c 01 3x
phone  : addr:11 ctrl:20 len:15 crc:8f13 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 3x
phone  : addr:11 ctrl:22 len:15 crc:9f01 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 3x
phone  : addr:11 ctrl:20 len:15 crc:872f -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 3x
phone  : addr:13 ctrl:01 len:01 crc:158d
phone  : addr:11 ctrl:02 len:15 crc:907d -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 3x
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:11 ctrl:20 len:15 crc:852c -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 3x
phone  : addr:13 ctrl:01 len:01 crc:158d
phone  : addr:11 ctrl:02 len:15 crc:907d -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 3x
phone  : addr:11 ctrl:00 len:15 crc:f80b -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 3x
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:13 ctrl:01 len:01 crc:158d
phone  : addr:11 ctrl:02 len:15 crc:8a78 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 3x
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:11 ctrl:20 len:39 crc:b55a -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 7b 77 0a
c0 80 00 4d 17 00 01 00 00 00
phone  : addr:11 ctrl:22 len:15 crc:9d1e -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 3x
phone  : addr:13 ctrl:01 len:01 crc:158d
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:11 ctrl:20 len:09 crc:92fb -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 78
phone  : addr:13 ctrl:01 len:01 crc:158d
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:13 ctrl:01 len:01 crc:158d
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:13 ctrl:01 len:01 crc:158d
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:11 ctrl:22 len:09 crc:146e -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 5a
phone  : addr:11 ctrl:20 len:09 crc:a238 -> 0011 CC
(Call Control) messages :{CC-RELEASE}    03 4d
station: addr:11 ctrl:21 len:01 crc:edc7
station: addr:13 ctrl:22 len:09 crc:09ef -> 0011 CC
(Call Control) messages :{CC-RELEASE-COM}    83 5a
phone  : addr:91 ctrl:00 len:51 crc:12ad -> 0000 LCE
(Link Control Entity) messages :NULL    00 71 05 07 80 a8 01 11 31
da 55 06 07 a0 a5 01 11 39 f5 a8
phone  : addr:11 ctrl:02 len:65 crc:4609 -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 05 05 07
80 a8 01 11 31 da 55 06 07 a0 a5 01 11 39 f5 a8 12 03 88 80 c0
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:11 ctrl:20 len:09 crc:e6b6 -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    87 07
phone  : addr:11 ctrl:22 len:39 crc:fa93 -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    87 7b 77 0a
c0 80 00 4d 2b 00 01 00 00 00
phone  : addr:13 ctrl:01 len:01 crc:158d
phone  : addr:11 ctrl:00 len:09 crc:9c5a -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    87 78
phone  : addr:13 ctrl:21 len:01 crc:f5cd
```

Hagenuk AIO 600

```
phone  : addr:91 ctrl:00 len:01 crc:a6b4
phone  : addr:11 ctrl:02 len:59 crc:fa2b -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 0b e9 00 73
3e 06 07 a0 a5 0b e9 04 98 80 e0 80
station: addr:11 ctrl:01 len:01 crc:a737
station: addr:13 ctrl:00 len:09 crc:7523 -> 0011 CC
(Call Control) messages :{CC-CONNECT}    83 07
phone  : addr:13 ctrl:21 len:01 crc:5f7d
station: addr:13 ctrl:02 len:11 crc:0aab -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b e4 3f
phone  : addr:13 ctrl:01 len:01 crc:bf3d
station: addr:13 ctrl:00 len:6d crc:836c -> 0101 MM
(Mobility Management) messages :{AUTHENTICATION-REQUEST}    05 40 0a
03 01 18 18 0c 08 bb 20 ed 0b 78 41 dd 13 0e 08 a4 3f f2 14 67 5e c2
0c
phone  : addr:13 ctrl:21 len:01 crc:5f7d
phone  : addr:11 ctrl:20 len:21 crc:156f -> 0101 MM
(Mobility Management) messages :{AUTHENTICATION-REPLY}    85 41 0d
04 c0 46 75 05
station: addr:11 ctrl:21 len:01 crc:4777
phone  : addr:11 ctrl:22 len:15 crc:3faa -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 32
station: addr:11 ctrl:01 len:01 crc:a737
phone  : addr:11 ctrl:20 len:15 crc:29a1 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 35
station: addr:11 ctrl:21 len:01 crc:4777
phone  : addr:11 ctrl:22 len:15 crc:35b1 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 37
station: addr:11 ctrl:01 len:01 crc:a737
phone  : addr:11 ctrl:20 len:15 crc:519d -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 31
station: addr:11 ctrl:21 len:01 crc:4777
phone  : addr:11 ctrl:22 len:15 crc:3dad -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 33
station: addr:11 ctrl:01 len:01 crc:a737
station: addr:13 ctrl:02 len:25 crc:548a -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 77 05 c0 81 00 00 46
phone  : addr:13 ctrl:01 len:01 crc:bf3d
phone  : addr:11 ctrl:00 len:11 crc:fdcd -> 0011 CC
(Call Control) messages :{CC-RELEASE}    03 4d e2 00
station: addr:11 ctrl:21 len:01 crc:4777
station: addr:13 ctrl:20 len:11 crc:ea31 -> 0011 CC
(Call Control) messages :{CC-RELEASE-COM}    83 5a e2 dd
phone  : addr:13 ctrl:21 len:01 crc:5f7d
```

Hagenuk Stick SR

```
phone  : addr:91 ctrl:00 len:01 crc:b714
phone  : addr:11 ctrl:02 len:7d crc:07b4 -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 00 fa 65 ee
fa 06 07 a0 a5 00 fa 74 02 68 e0 80 7b 07 81 03 51 15 00 0c 00
station: addr:11 ctrl:01 len:01 crc:b697
station: addr:13 ctrl:00 len:45 crc:991c -> 0011 CC
(Call Control) messages :{CC-CONNECT}    83 07 7b 0d 81 03 51 0a 00
1a 00 1f 00 29 00 28 00
phone  : addr:13 ctrl:21 len:01 crc:4edd
station: addr:13 ctrl:02 len:4d crc:023f -> 0011 CC
```

```
(Call Control) messages :{CC-INFO}    83 7b 7b 0f 81 03 51 02 16 0a
00 1a 00 1f 00 29 00 28 00
```

```
phone  : addr:11 ctrl:20 len:25 crc:1551 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 05 32 35 37 31 33
phone  : addr:13 ctrl:01 len:01 crc:ae9d
station: addr:11 ctrl:21 len:01 crc:56d7
phone  : addr:11 ctrl:02 len:15 crc:9339 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 00
station: addr:11 ctrl:01 len:01 crc:b697
station: addr:13 ctrl:00 len:4d crc:183d -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 0f 81 03 51 05 01 0a
00 1a 00 1f 00 29 00 28 00
phone  : addr:13 ctrl:21 len:01 crc:4edd
station: addr:13 ctrl:02 len:4d crc:e969 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 0f 81 03 51 05 01 0a
00 1a 00 1f 00 29 00 28 00
phone  : addr:13 ctrl:01 len:01 crc:ae9d
station: addr:13 ctrl:00 len:4d crc:183d -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 0f 81 03 51 05 01 0a
00 1a 00 1f 00 29 00 28 00
phone  : addr:13 ctrl:21 len:01 crc:4edd
station: addr:13 ctrl:02 len:4d crc:e969 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 0f 81 03 51 05 01 0a
00 1a 00 1f 00 29 00 28 00
phone  : addr:13 ctrl:01 len:01 crc:ae9d
station: addr:13 ctrl:00 len:4d crc:183d -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 0f 81 03 51 05 01 0a
00 1a 00 1f 00 29 00 28 00
phone  : addr:13 ctrl:21 len:01 crc:4edd
phone  : addr:11 ctrl:20 len:11 crc:eb0c -> 0011 CC
(Call Control) messages :{CC-RELEASE}    03 4d e2 00
station: addr:11 ctrl:21 len:01 crc:56d7
station: addr:13 ctrl:22 len:11 crc:8523 -> 0011 CC
(Call Control) messages :{CC-RELEASE-COM}    83 5a e2 00
phone  : addr:13 ctrl:01 len:01 crc:ae9d
```

iDECT x2i

```
phone  : addr:91 ctrl:00 len:01 crc:b7b4
phone  : addr:11 ctrl:02 len:99 crc:4e47 -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 00 c1 30 c0
f1 06 07 a0 a5 00 b8 9e 76 68 e0 80 7b 0e 81 03 51 15 00 0c 00 14 01
01 06 00 05 6e
phone  : addr:13 ctrl:21 len:01 crc:4e7d
phone  : addr:38 ctrl:d8 len:6e crc:33c2 -> reserved     b1 ea c4 34
16 11 24 e9 8e e1 8e 30 35 08 37 d1 54 de 82 bf 80 fb 88 87 f2 db 5e
phone  : addr:78 ctrl:3d len:dc crc:0014 -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    87 ac f0 c6
39 72 2f c6 dd f7 d6 8c ff ff ff ff ff 91 00 01 b7 b4 11 02 99 03 05
05 07 80 a8 00 c1 30 c0 f1 06 07 a0 a5 00 b8 9e 76 68 e0 80 7b 0e 81
03 51 15 00 0c
phone  : addr:01 ctrl:01 len:06 crc:ea10 -> 0000 LCE
(Link Control Entity) messages :NULL    00
failed : addr:5a ctrl:82 len:31 crc:0ff4 -> reserved     3b c7 a6 d1
f1 5b ec 6b bb 97 29 c4
station: addr:11 ctrl:01 len:01 crc:b637
station: addr:13 ctrl:00 len:19 crc:5830 -> 0101 MM
(Mobility Management) messages :{CIPHER-REQUEST}    05 4c 19 02 81
98
phone  : addr:13 ctrl:21 len:01 crc:4e7d
phone  : addr:da ctrl:83 len:64 crc:5238 -> reserved     de f5 96 fa
30 51 3d 74 c7 ed e2 f2 2b 2e bd 7d ff a1 27 c7 82 68 44 37 5e
phone  : addr:ce ctrl:fd len:66 crc:812c -> reserved     c8 32 1d 39
34 28 76 26 06 6a ba c4 96 24 c4 b3 c9 e8 a9 b4 4a 9e 56 0c da
station: addr:fc ctrl:33 len:a3 crc:923b -> reserved     ff 84 18 cd
a2 53 3d a8 69 62 8b fd e4 35 7b 0d a1 ef 93 d5 48 4f 37 3d 4c b3 ee
1c 83 42 e7 c2 a1 46 36 72 7b 2b cb 09
phone  : addr:fc ctrl:6c len:37 crc:f477 -> 0000 LCE
(Link Control Entity) messages :NULL    20 a7 b9 52 5d 71 23 9e ca
33 c2 9f 76
station: addr:4b ctrl:7a len:0e crc:2207 -> reserved     7c 39 cc
phone  : addr:09 ctrl:1e len:32 crc:6b2c -> 0110 CLMS
(ConnectionLess Message Service) messages :NULL    86 ca 54 54 99 b8
7f 66 68 15 ce e8
station: addr:73 ctrl:50 len:58 crc:5f86 -> reserved     6d 08 6a 8e
b3 50 e5 6f 5f c7 b2 87 f7 51 0c 5a ab db 02 9b ea fc
phone  : addr:8f ctrl:1e len:f4 crc:1d81 -> reserved     51 88 96 dd
5a 78 d1 13 eb a7 ee 45 7c e6 42 ca 11 36 61 88 2e 54 71 39 92 0f c0
aa 59 fe cc d7 62 0f f6 29 4a d8 62 c7 b7 75 2a 53 4a 02 c5 74 e6 66
4c 4d 61 6a 0f 4a d5 27 c1 24 d2
station: addr:0c ctrl:bf len:1e crc:d82f -> reserved     92 16 ea 07
04 2e fb
phone  : addr:1c ctrl:70 len:6b crc:bcba -> reserved     41 4a 50 64
6d 03 c2 ba c6 86 80 41 76 5d 73 38 cb 8f 62 4a 6d 48 59 29 62 ba
phone  : addr:c6 ctrl:c1 len:1f crc:c7e4 -> reserved     3c e7 35 c2
53 92 c4
station: addr:53 ctrl:00 len:4f crc:acdc -> reserved     7c b4 b6 32
8a ce 6f 66 b9 cc d8 ff 7c f4 59 db f3 10 6c
phone  : addr:70 ctrl:5e len:58 crc:01fa -> 0101 MM
(Mobility Management) messages :(null)    f5 cd 11 ca 90 65 01 bd 4b
9a 53 43 55 10 c3 41 91 fb dd 8d 0f b4
station: addr:0f ctrl:ec len:20 crc:036c -> reserved     fb 16 8d 5a
65 cf e0 36
```

Loewe Alphatel 5000

```
phone  : addr:91 ctrl:00 len:01 crc:b714
phone  : addr:11 ctrl:02 len:59 crc:59ff -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 00 1d e0 47
66 06 07 a0 a5 00 1d e2 3b 30 e0 80
station: addr:11 ctrl:01 len:01 crc:b697
station: addr:13 ctrl:00 len:2d crc:e783 -> 0011 CC
(Call Control) messages :{CC-CONNECT}    83 07 7b 07 81 00 50 06 01
07 05
phone  : addr:13 ctrl:21 len:01 crc:4edd
station: addr:13 ctrl:02 len:25 crc:e12a -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 05 81 00 50 02 14
phone  : addr:11 ctrl:20 len:25 crc:1551 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 05 32 35 37 31 33
phone  : addr:13 ctrl:01 len:01 crc:ae9d
station: addr:11 ctrl:21 len:01 crc:56d7
station: addr:13 ctrl:20 len:25 crc:8776 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 05 81 00 50 05 01
phone  : addr:13 ctrl:21 len:01 crc:4edd
station: addr:13 ctrl:22 len:25 crc:6d4e -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 05 81 00 50 05 01
phone  : addr:13 ctrl:01 len:01 crc:ae9d
station: addr:13 ctrl:20 len:25 crc:8776 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 05 81 00 50 05 01
phone  : addr:13 ctrl:21 len:01 crc:4edd
station: addr:13 ctrl:22 len:25 crc:6d4e -> 0011 CC
```

```
(Call Control) messages :{CC-INFO}    83 7b 7b 05 81 00 50 05 01
phone  : addr:13 ctrl:01 len:01 crc:ae9d
station: addr:13 ctrl:20 len:25 crc:8776 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 05 81 00 50 05 01
phone  : addr:13 ctrl:21 len:01 crc:4edd
phone  : addr:11 ctrl:22 len:11 crc:db1a -> 0011 CC
(Call Control) messages :{CC-RELEASE}    03 4d e2 00
station: addr:11 ctrl:01 len:01 crc:b697
station: addr:13 ctrl:02 len:11 crc:8600 -> 0011 CC
(Call Control) messages :{CC-RELEASE-COM}    83 5a e2 00
```

Motorola D701

```
phone  : addr:91 ctrl:00 len:01 crc:0c04
phone  : addr:11 ctrl:02 len:59 crc:404f -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 00 f3 02 13
70 06 07 a0 a5 00 f3 04 d9 88 e0 80
phone  : addr:11 ctrl:00 len:65 crc:9dad -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 05 05 07
80 a8 00 f3 02 13 70 06 07 a0 a5 00 f3 04 d9 88 12 03 88 80 c0
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:13 ctrl:01 len:01 crc:158d
phone  : addr:11 ctrl:02 len:39 crc:18d2 -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 7b 77 0a
c0 80 00 4d 28 00 01 00 00 00
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:11 ctrl:20 len:39 crc:b55a -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 7b 77 0a
c0 80 00 4d 17 00 01 00 00 00
phone  : addr:13 ctrl:01 len:01 crc:158d
phone  : addr:11 ctrl:02 len:39 crc:9f43 -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 7b 77 0a
c0 80 00 4d 18 00 01 00 00 00
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:11 ctrl:20 len:09 crc:92fb -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 78
phone  : addr:13 ctrl:01 len:01 crc:158d
phone  : addr:11 ctrl:02 len:15 crc:947b -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 32
phone  : addr:11 ctrl:00 len:15 crc:820e -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 35
phone  : addr:11 ctrl:02 len:15 crc:9e7e -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 37
phone  : addr:11 ctrl:00 len:15 crc:fa0a -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 31
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:11 ctrl:22 len:15 crc:971d -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 33
phone  : addr:13 ctrl:01 len:01 crc:158d
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:13 ctrl:01 len:01 crc:158d
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:11 ctrl:20 len:09 crc:ba2c -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 4d
phone  : addr:13 ctrl:01 len:01 crc:158d
```

Orchid DECT LR 4610

```
phone  : addr:91 ctrl:00 len:01 crc:b7b4
phone  : addr:11 ctrl:02 len:8d crc:b0a7 -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 00 d1 a1 2b
82 06 07 a0 a5 00 d1 a5 4d a8 e0 80 63 0b 44 00 08 00 1a 01 0c 80 a2
01 81
station: addr:11 ctrl:01 len:01 crc:b637
station: addr:13 ctrl:00 len:19 crc:5830 -> 0101 MM
(Mobility Management) messages :{CIPHER-REQUEST}    05 4c 19 02 81
98
station: addr:68 ctrl:72 len:20 crc:67a1 -> reserved     5f 62 aa 09
ef 4c 0c e6
```

Panasonic KX TG 8220

```
phone  : addr:91 ctrl:00 len:01 crc:ceb4
phone  : addr:11 ctrl:02 len:79 crc:7dd5 -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 00 7c 78 42
f5 06 07 a0 a5 00 d6 71 cb c8 e0 80 77 06 c0 81 05 12 c7 00
phone  : addr:13 ctrl:21 len:01 crc:377d
phone  : addr:11 ctrl:20 len:25 crc:6cf1 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 05 32 35 37 31 33
phone  : addr:11 ctrl:22 len:15 crc:1f8e -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 16
```

Philips CD650

```
phone  : addr:13 ctrl:21 len:01 crc:4e7c
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:00 len:09 crc:6422 -> 0011 CC
(Call Control) messages :{CC-CONNECT}    83 07
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:02 len:6d crc:fb85 -> 0101 MM
(Mobility Management) messages :{AUTHENTICATION-REQUEST}    05 40 0a
03 01 18 18 0c 08 15 ea a7 d6 f9 ee 05 80 0e 08 64 4d be 88 d8 61 9f
bb
phone  : addr:13 ctrl:01 len:01 crc:ae3c
phone  : addr:11 ctrl:00 len:21 crc:1adc -> 0101 MM
(Mobility Management) messages :{AUTHENTICATION-REPLY}    85 41 0d
04 92 9e 6c 7f
station: addr:13 ctrl:00 len:b1 crc:8176 -> 0011 CC
(Call Control) messages :(null)    63 62 7b 28 81 00 02 58 20 03 1e
0c 91 02 02 11 1b 2d 41 4c 65 69 74 75 6e 67 20 62 65 6c 65 67 74 0a
91 02 02 03 1b 2d 41 5b 01 96
station: addr:11 ctrl:21 len:01 crc:5676
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:22 len:19 crc:9cca -> 0101 MM
(Mobility Management) messages :{CIPHER-REQUEST}    05 4c 19 02 81
98
phone  : addr:11 ctrl:22 len:4d crc:5707 -> 0100 CISS
(Call Independent Supplementary Services) messages :{FACILITY}    64
62 05 07 90 a8 00 b6 4b c2 18 7b 31 ef 87 17 42 cc ed
station: addr:9a ctrl:dd len:4b crc:bce7 -> reserved     58 6f e3 a3
8a f2 33 a4 4c 78 c3 23 c5 73 c8 9d 85 46
station: addr:84 ctrl:09 len:97 crc:e083 -> reserved     7e 82 ee 25
11 fb bb b3 10 d4 1a 70 a4 3a d8 15 ab 6c ee 94 05 6f 3d ac 2e 8f 6c
00 2c 40 6c b2 5f 4c 88 63 43
```

```
station: addr:42 ctrl:08 len:e4 crc:7d3d -> reserved     0c e5 8b 1e
1b 95 55 c6 c6 31 d4 90 ea 3e d2 16 64 fc 03 90 42 b1 89 a4 41 10 54
83 7a 9f da 6b 82 c7 cb f2 cb 1f a7 04 15 cf 62 e5 8f f6 e5 22 2d e4
af bf 0d e7 33 cf fc
station: addr:50 ctrl:fd len:e7 crc:d536 -> 0110 CLMS
(ConnectionLess Message Service) messages :NULL    e6 eb 1c 72 44 4e
00 f3 a2 be 52 82 54 3b a8 3c 6d f7 f9 cd ba b5 45 af e5 d0 f5 54 b9
0d 7f ba 0f e7 d4 3a 47 77 d7 6d 33 1d 5b 21 e2 47 8e d8 ca 53 dc f9
c5 bd 70 5c 63
phone  : addr:1c ctrl:91 len:6d crc:4816 -> 0101 MM
(Mobility Management) messages :(null)    b5 36 9c 05 c5 f2 72 23 52
14 d7 71 01 1d 43 09 29 ea 58 32 fa 8a da 5f 56 c6 f6
station: addr:c6 ctrl:18 len:a2 crc:1a2c -> 0100 CISS
(Call Independent Supplementary Services) messages :(null)    04 a0
33 3a b5 b7 ac 5e f6 f9 ce 92 c5 8d e5 b2 36 c6 5b 15 ed d2 d9 17 00
dd b9 ad b9 0b ab 2f 7f 98 2a bb 80 db 03 24
station: addr:38 ctrl:81 len:0e crc:26d7 -> 0110 CLMS
(ConnectionLess Message Service) messages :NULL    f6 20 be
station: addr:c0 ctrl:52 len:e2 crc:92c3 -> reserved     88 35 9c 2a
61 40 97 77 1e 98 1e f5 70 fb 79 c4 c9 08 40 76 86 b2 fc 41 22 41 5c
fd ab ff cb a1 0f 04 1e a5 f1 cc fc a4 da 48 e2 7d 1c 76 b7 91 55 99
5c 0b c6 43 d5 da
station: addr:97 ctrl:ee len:08 crc:ec5a -> reserved     41 67
station: addr:bb ctrl:c5 len:57 crc:99f8 -> reserved     2e fd b9 77
07 95 1e fa 83 5f 69 5b fb d5 be 71 74 52 7e e3 15
phone  : addr:dc ctrl:4d len:55 crc:b598 -> reserved     df dc dc 6b
2f 26 a8 bb 10 0c 35 06 98 7d 3e 9f 6b 60 a5 93 12
phone  : addr:0c ctrl:b4 len:2a crc:f0ab -> 0100 CISS
(Call Independent Supplementary Services) messages :(null)    f4 0e
d4 a1 a8 b8 d2 7d b4 3e
```

Philips SE250

```
phone  : addr:11 ctrl:02 len:59 crc:0c13 -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 00 96 bc 03
cc 06 07 a0 a5 01 01 83 4b 80 e0 80
station: addr:11 ctrl:01 len:01 crc:0d87
station: addr:13 ctrl:00 len:09 crc:df93 -> 0011 CC
(Call Control) messages :{CC-CONNECT}    83 07
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:11 ctrl:20 len:65 crc:e592 -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 05 05 07
80 a8 00 96 bc 03 cc 06 07 a0 a5 01 01 83 4b 80 12 03 88 80 c0
station: addr:11 ctrl:21 len:01 crc:edc7
station: addr:13 ctrl:22 len:09 crc:8094 -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    87 07
phone  : addr:13 ctrl:01 len:01 crc:158d
phone  : addr:11 ctrl:02 len:39 crc:975a -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 7b 77 0a
c0 80 00 4d 17 00 01 00 00 00
station: addr:11 ctrl:01 len:01 crc:0d87
station: addr:13 ctrl:00 len:09 crc:ae4a -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    87 78
phone  : addr:13 ctrl:21 len:01 crc:f5cd
station: addr:13 ctrl:02 len:39 crc:2da3 -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    87 7b 77 0a
c0 80 00 4d 04 00 01 00 00 00
phone  : addr:11 ctrl:20 len:39 crc:bd43 -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 7b 77 0a
c0 80 00 4d 18 00 01 00 00 00
station: addr:11 ctrl:21 len:01 crc:edc7
```

```
phone  : addr:13 ctrl:01 len:01 crc:158d
station: addr:13 ctrl:20 len:09 crc:af6d -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    87 78
phone  : addr:11 ctrl:02 len:09 crc:a1c6 -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 78
station: addr:11 ctrl:01 len:01 crc:0d87
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:11 ctrl:20 len:15 crc:852c -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 32
station: addr:11 ctrl:21 len:01 crc:edc7
phone  : addr:11 ctrl:22 len:15 crc:931f -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 35
station: addr:11 ctrl:01 len:01 crc:0d87
phone  : addr:11 ctrl:20 len:15 crc:8f13 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 37
station: addr:11 ctrl:21 len:01 crc:edc7
phone  : addr:11 ctrl:22 len:15 crc:8b1b -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 31
station: addr:11 ctrl:01 len:01 crc:0d87
phone  : addr:11 ctrl:20 len:15 crc:872f -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 33
station: addr:11 ctrl:21 len:01 crc:edc7
station: addr:13 ctrl:22 len:3d crc:804d -> 0011 CC
(Call Control) messages :{IWU-INFO}    83 60 77 0b c0 80 00 00 03 46
64 00 00 00 00
phone  : addr:13 ctrl:01 len:01 crc:158d
station: addr:13 ctrl:20 len:3d crc:e46b -> 0011 CC
(Call Control) messages :{IWU-INFO}    83 60 77 0b c0 80 00 00 03 46
64 00 00 00 00
phone  : addr:13 ctrl:21 len:01 crc:f5cd
station: addr:13 ctrl:22 len:3d crc:804d -> 0011 CC
(Call Control) messages :{IWU-INFO}    83 60 77 0b c0 80 00 00 03 46
64 00 00 00 00
phone  : addr:13 ctrl:01 len:01 crc:158d
station: addr:13 ctrl:20 len:3d crc:e46b -> 0011 CC
(Call Control) messages :{IWU-INFO}    83 60 77 0b c0 80 00 00 03 46
64 00 00 00 00
phone  : addr:13 ctrl:21 len:01 crc:f5cd
station: addr:13 ctrl:22 len:3d crc:804d -> 0011 CC
(Call Control) messages :{IWU-INFO}    83 60 77 0b c0 80 00 00 03 46
64 00 00 00 00
phone  : addr:13 ctrl:01 len:01 crc:158d
phone  : addr:11 ctrl:02 len:09 crc:4a7b -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    07 4d
station: addr:11 ctrl:01 len:01 crc:0d87
station: addr:13 ctrl:00 len:09 crc:57fe -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    87 4d
phone  : addr:13 ctrl:21 len:01 crc:f5cd
phone  : addr:11 ctrl:20 len:09 crc:a238 -> 0011 CC
(Call Control) messages :{CC-RELEASE}    03 4d
station: addr:11 ctrl:21 len:01 crc:edc7
station: addr:13 ctrl:22 len:09 crc:09ef -> 0011 CC
(Call Control) messages :{CC-RELEASE-COM}    83 5a
```

Philips Zenia Voice

```
phone  : addr:91 ctrl:00 len:01 crc:b7b4
phone  : addr:11 ctrl:02 len:59 crc:fa14 -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 00 1e d0 0f
81 06 07 a0 a5 00 1e d0 08 48 e0 80
phone  : addr:13 ctrl:21 len:01 crc:4e7d
phone  : addr:11 ctrl:20 len:25 crc:15f1 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 05 32 35 37 31 33
phone  : addr:11 ctrl:22 len:39 crc:5703 -> 0011 CC
(Call Control) messages :{IWU-INFO}    03 60 77 0a c0 81 00 ac 81 01
f0 02 00 00
phone  : addr:13 ctrl:01 len:01 crc:ae3d
phone  : addr:11 ctrl:00 len:39 crc:c30e -> 0011 CC
(Call Control) messages :{IWU-INFO}    03 60 77 0a c0 81 00 ac 81 01
f0 02 00 a8
phone  : addr:13 ctrl:21 len:01 crc:4e7d
phone  : addr:11 ctrl:22 len:39 crc:b76d -> 0011 CC
(Call Control) messages :{IWU-INFO}    03 60 77 0a c0 81 00 ac 81 01
f0 02 00 35
phone  : addr:13 ctrl:01 len:01 crc:ae3d
phone  : addr:11 ctrl:00 len:39 crc:babe -> 0011 CC
(Call Control) messages :{IWU-INFO}    03 60 77 0a c0 81 00 ac 81 01
f0 02 00 01
phone  : addr:13 ctrl:21 len:01 crc:4e7d
phone  : addr:11 ctrl:22 len:39 crc:5703 -> 0011 CC
(Call Control) messages :{IWU-INFO}    03 60 77 0a c0 81 00 ac 81 01
f0 02 00 00
phone  : addr:13 ctrl:01 len:01 crc:ae3d
phone  : addr:11 ctrl:00 len:39 crc:c30e -> 0011 CC
(Call Control) messages :{IWU-INFO}    03 60 77 0a c0 81 00 ac 81 01
f0 02 00 a8
phone  : addr:13 ctrl:21 len:01 crc:4e7d
phone  : addr:11 ctrl:22 len:39 crc:b76d -> 0011 CC
(Call Control) messages :{IWU-INFO}    03 60 77 0a c0 81 00 ac 81 01
f0 02 00 35
phone  : addr:13 ctrl:01 len:01 crc:ae3d
phone  : addr:11 ctrl:00 len:39 crc:babe -> 0011 CC
(Call Control) messages :{IWU-INFO}    03 60 77 0a c0 81 00 ac 81 01
f0 02 00 01
phone  : addr:13 ctrl:21 len:01 crc:4e7d
phone  : addr:11 ctrl:22 len:39 crc:5703 -> 0011 CC
(Call Control) messages :{IWU-INFO}    03 60 77 0a c0 81 00 ac 81 01
f0 02 00 00
phone  : addr:13 ctrl:01 len:01 crc:ae3d
phone  : addr:11 ctrl:00 len:39 crc:c30e -> 0011 CC
(Call Control) messages :{IWU-INFO}    03 60 77 0a c0 81 00 ac 81 01
f0 02 00 a8
phone  : addr:13 ctrl:21 len:01 crc:4e7d
phone  : addr:11 ctrl:22 len:39 crc:b76d -> 0011 CC
(Call Control) messages :{IWU-INFO}    03 60 77 0a c0 81 00 ac 81 01
f0 02 00 35
phone  : addr:13 ctrl:01 len:01 crc:ae3d
phone  : addr:11 ctrl:00 len:39 crc:babe -> 0011 CC
(Call Control) messages :{IWU-INFO}    03 60 77 0a c0 81 00 ac 81 01
f0 02 00 01
phone  : addr:13 ctrl:21 len:01 crc:4e7d
phone  : addr:11 ctrl:22 len:39 crc:5703 -> 0011 CC
(Call Control) messages :{IWU-INFO}    03 60 77 0a c0 81 00 ac 81 01
f0 02 00 00
phone  : addr:13 ctrl:01 len:01 crc:ae3d
phone  : addr:11 ctrl:00 len:39 crc:c30e -> 0011 CC
```

```
(Call Control) messages :{IWU-INFO}    03 60 77 0a c0 81 00 ac 81 01
f0 02 00 a8
phone  : addr:13 ctrl:21 len:01 crc:4e7d
phone  : addr:11 ctrl:22 len:39 crc:b76d -> 0011 CC
(Call Control) messages :{IWU-INFO}    03 60 77 0a c0 81 00 ac 81 01
f0 02 00 35
phone  : addr:13 ctrl:01 len:01 crc:ae3d
phone  : addr:11 ctrl:00 len:39 crc:babe -> 0011 CC
(Call Control) messages :{IWU-INFO}    03 60 77 0a c0 81 00 ac 81 01
f0 02 00 01
```

Sagem D23XL

```
phone  : addr:91 ctrl:00 len:01 crc:b7b4
phone  : addr:11 ctrl:02 len:8d crc:221a -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 00 91 a3 b2
24 06 07 a0 a5 00 ba 00 02 00 e0 80 63 0b 44 00 08 00 1a 01 0c 80 82
01 81
station: addr:11 ctrl:01 len:01 crc:b637
station: addr:13 ctrl:00 len:19 crc:5830 -> 0101 MM
(Mobility Management) messages :{CIPHER-REQUEST}    05 4c 19 02 81
98
```

Siemens Gigaset A260

```
phone  : addr:91 ctrl:00 len:01 crc:b7b5
phone  : addr:11 ctrl:02 len:8d crc:ef0a -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 00 bb 0c c3
5d 06 07 a0 a5 00 ba d5 50 c8 e0 80 2c 03 8f 01 c0 7b 06 81 00 02 18
01 42
station: addr:13 ctrl:00 len:25 crc:50f6 -> 0011 CC
(Call Control) messages :{CC-CONNECT}    83 07 7b 05 81 00 02 01 00
phone  : addr:13 ctrl:21 len:01 crc:4e7c
phone  : addr:11 ctrl:20 len:25 crc:15f0 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 05 32 35 37 31 33
station: addr:13 ctrl:02 len:6d crc:b009 -> 0101 MM
(Mobility Management) messages :{AUTHENTICATION-REQUEST}    05 40 0a
03 01 18 18 0c 08 05 80 97 d6 f5 74 93 66 0e 08 9f bb 6e e9 c4 7f 5a
98
station: addr:11 ctrl:21 len:01 crc:5676
phone  : addr:13 ctrl:01 len:01 crc:ae3c
station: addr:13 ctrl:20 len:3d crc:ade7 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 28 03 1b 2d 41 7b 06 81
00 02 32 01 0e
phone  : addr:13 ctrl:21 len:01 crc:4e7c
phone  : addr:11 ctrl:22 len:21 crc:6fc3 -> 0101 MM
(Mobility Management) messages :{AUTHENTICATION-REPLY}    85 41 0d
04 59 60 fc 08
station: addr:13 ctrl:22 len:2d crc:0ba3 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 07 81 00 02 1a 02 09
01
station: addr:11 ctrl:01 len:01 crc:b636
phone  : addr:13 ctrl:01 len:01 crc:ae3c
station: addr:13 ctrl:00 len:19 crc:5831 -> 0101 MM
(Mobility Management) messages :{CIPHER-REQUEST}    05 4c 19 02 81
98
phone  : addr:11 ctrl:00 len:25 crc:a87d -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 7b 05 81 00 02 30 00
station: addr:6f ctrl:4c len:13 crc:63f1 -> 0011 CC
```

```
(Call Control) messages :(null)    a3 83 d9 eb
phone  : addr:1f ctrl:9c len:0a crc:4021 -> reserved     ff 4b
station: addr:a2 ctrl:48 len:b4 crc:2528 -> 0000 LCE
(Link Control Entity) messages :NULL    90 d4 d1 0b 24 46 28 a7 72
4b c9 d3 a4 f8 25 3d 9d 48 6c a8 8a 4d ce e1 80 2a bc 8b 02 35 8e e8
c9 a2 75 d2 17 f9 24 a4 8c 46 64 a5 9e
station: addr:26 ctrl:70 len:82 crc:6af3 -> reserved     e9 96 f7 d4
4b 03 99 21 b1 68 c0 2b bd 28 e0 02 cf 1d 01 94 cf 3f 34 d8 07 a5 55
23 7f 44 2b 02
station: addr:40 ctrl:b2 len:65 crc:516b -> reserved     01 0f 51 61
bb 7f 62 16 4f 4d d8 0e 3d 2a 75 4f 0b 67 2f b2 4e ca 53 c6 25
station: addr:d6 ctrl:e8 len:f7 crc:337b -> reserved     11 45 c8 03
15 c0 8d ce df c5 e3 16 97 12 43 54 7b 61 e7 a4 1d 90 ea 26 1f 88 d0
92 7a b5 38 37 eb 05 40 24 86 55 c6 76 53 4d 67 0d c0 41 c2 a2 6b b3
d1 2c 8f aa d0 53 10 51 3f ac 4b
station: addr:dd ctrl:4d len:1a crc:f050 -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    67 b3 2a b0
76 29
phone  : addr:45 ctrl:ff len:fb crc:4d01 -> reserved     cc 75 96 4a
76 75 0f 5c e2 9f b6 20 11 cf d9 5c 64 92 97 7a 2a 6b a9 03 58 e9 8b
21 f0 18 df 65 b6 3b 85 7b 40 b7 72 dd 59 3b 9f af d2 42 12 9b 23 ea
34 c0 01 82 6e a0 43 2a c3 b2 9e 18
station: addr:92 ctrl:cb len:eb crc:8f2b -> reserved     cb f3 64 23
db 2f b4 cf 5c 8a cb e0 12 eb 1d 5d 94 a4 41 29 47 f1 28 14 97 3a a3
36 95 92 e0 03 a8 7f 83 bd af cc 38 18 0f 2e 61 c7 ec e8 7c 00 0f 12
53 2f 22 d6 65 97 92 fa
station: addr:e4 ctrl:d4 len:16 crc:ade4 -> 0110 CLMS
(ConnectionLess Message Service) messages :NULL    46 52 92 8f 73
station: addr:ac ctrl:80 len:02 crc:f2eb
station: addr:62 ctrl:a6 len:cc crc:015c -> 0000 LCE
(Link Control Entity) messages :NULL    40 b5 8c 28 39 c0 bc ae eb
cb 0c 36 bb d0 58 7b 43 04 df 11 cb 6b 5a 93 e2 e1 a1 4d f0 f6 5f 33
cf fc ee bb c8 99 06 ad cd 9c 34 d5 9d 11 1f dc ed 71 75
station: addr:d5 ctrl:3f len:d3 crc:eb9a -> 0110 CLMS
(ConnectionLess Message Service) messages :NULL    f6 70 af 38 88 20
1e 4a 56 d4 5f 00 65 0e 6a 48 45 d1 f7 6d 49 31 7d 04 23 c4 af 5a ac
43 9f a5 d0 18 5e f1 86 bc 7b bc dc 8a 20 f2 f1 c9 b0 73 3d ec af c8
phone  : addr:1b ctrl:ea len:93 crc:b6bf -> 0100 CISS
(Call Independent Supplementary Services) messages :(null)    c4 54
b2 f4 4d eb fd 6d af 47 78 ed 37 ab be b7 44 ab be 52 32 41 79 75 63
f2 4f 0f ab 24 c4 a4 05 79 db 70
phone  : addr:fa ctrl:1d len:07 crc:d27b -> reserved     2f
station: addr:1a ctrl:df len:ad crc:acb3 -> 0000 LCE
(Link Control Entity) messages :NULL    30 d6 a2 ef f2 33 54 1e 82
77 91 b3 48 0e a6 d2 48 7c 5e df 38 94 3a e6 c0 2a 87 11 0d bc 00 be
81 fd b4 92 0e 80 3e 7f 36 b5 62
phone  : addr:76 ctrl:9b len:e5 crc:0259 -> reserved     d2 55 3a 8d
c7 a4 36 47 9d 6e b5 9c 91 00 51 00 71 05 07 80 a8 00 bb 0c c3 5d 06
07 a0 a5 00 ba d5 50 c8 f6 99 13 21 01 4e 7c 11 22 4d 64 64 05 07 90
a8 00 bb 0c c3 5d 7b
```

Siemens Gigaset A580

```
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:00 len:29 crc:f43c -> 0011 CC
(Call Control) messages :{CC-CONNECT}    83 07 7b 06 81 00 02 01 01
01
phone  : addr:11 ctrl:20 len:25 crc:15f0 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 05 32 35 37 31 33
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:02 len:6d crc:40b2 -> 0101 MM
```

```
(Mobility Management) messages :{AUTHENTICATION-REQUEST}    05 40 0a
03 01 18 18 0c 08 67 e6 8d 14 2b 42 3f b7 0e 08 01 bc 05 7e 9f 49 39
52
phone  : addr:13 ctrl:01 len:01 crc:ae3c
station: addr:11 ctrl:21 len:01 crc:5676
phone  : addr:11 ctrl:02 len:21 crc:3540 -> 0101 MM
(Mobility Management) messages :{AUTHENTICATION-REPLY}    85 41 0d
04 85 a8 4c 22
station: addr:13 ctrl:20 len:3d crc:ade7 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 28 03 1b 2d 41 7b 06 81
00 02 32 01 0e
station: addr:11 ctrl:01 len:01 crc:b636
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:02 len:19 crc:3e49 -> 0101 MM
(Mobility Management) messages :{CIPHER-REQUEST}    05 4c 19 02 81
98
phone  : addr:11 ctrl:20 len:25 crc:07fe -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 7b 05 81 00 02 30 00
station: addr:d3 ctrl:73 len:e3 crc:32da -> reserved     fa cd 02 87
04 c2 0b f4 38 63 d7 c1 33 4a 10 40 de 78 ed 2d 5b 98 43 88 5f 2c f1
87 d7 2c 6b fa bf 1a 98 50 dd c7 cb ff f0 07 b0 31 c3 b4 01 87 77 6c
6c 12 18 14 9f 16
station: addr:57 ctrl:2d len:61 crc:1e1d -> reserved     09 08 5c 97
f5 49 7e a2 fc 1f f5 15 6f 4d 3b 8a e5 c7 b4 8e 04 8b f7 ad
phone  : addr:e3 ctrl:b9 len:af crc:bc56 -> reserved     29 17 38 a8
9d e8 28 17 85 8f a9 95 dc c7 a9 87 58 e5 e2 f8 6e 47 99 b9 89 68 80
b0 05 e3 ff b2 85 54 40 11 d1 5a 5a 38 da 1a 13
station: addr:2e ctrl:a7 len:d4 crc:5a22 -> reserved     9e b1 5c fb
d4 80 a4 b5 37 06 e8 a1 fc fa e6 ca c5 2c 58 f0 4f eb e1 2d 8e 42 13
cd ec 36 f0 c7 f4 50 7f 7c f7 ef 5f 68 92 13 c2 da 89 96 06 26 29 df
16 17 9e
phone  : addr:df ctrl:1e len:10 crc:cf9b -> reserved     ea 3e 16 4f
station: addr:29 ctrl:14 len:29 crc:d877 -> reserved     4d 3b 09 da
eb 95 62 0b 2b 2a
station: addr:cc ctrl:6d len:97 crc:d564 -> 0101 MM
(Mobility Management) messages :(null)    c5 8d 07 0c df b3 eb b7 f3
50 f0 4e 51 6a 38 63 1f ab b2 d8 b1 d1 7c 79 5d 6e d0 ae 72 ad 18 d9
03 7e f4 ca 51
station: addr:f0 ctrl:25 len:25 crc:bfe0 -> 0100 CISS
(Call Independent Supplementary Services) messages :(null)    94 4b
70 d5 d4 fe 1d 91 94
station: addr:4d ctrl:a9 len:34 crc:60ae -> reserved     a2 05 f0 99
63 99 4f 42 32 db af c8 33
station: addr:e2 ctrl:84 len:ce crc:51b3 -> 0100 CISS
(Call Independent Supplementary Services) messages :(null)    74 9b
16 9b 00 14 f5 d0 be f7 91 e9 b4 5c 4a 5d a7 ea 14 85 6a 0e de e4 9f
6e 5f 66 f3 f8 db e9 72 31 e3 48 4e d6 a9 a3 5f 52 8d ee 50 39 b8 c1
0d 6a ed
station: addr:04 ctrl:41 len:65 crc:0969 -> reserved     3f c1 86 6f
f4 f2 58 6a 03 a6 d7 94 59 73 72 42 22 ff ff ff ff ff 76 3a 49
phone  : addr:de ctrl:d8 len:c6 crc:1c73 -> reserved     01 eb c7 98
2c bf 57 fe 0d e7 d2 4f 50 60 26 95 95 8b 84 d3 8f 2e 95 68 f1 b4 ac
14 c6 4f 20 96 0c b6 33 a2 ca 32 aa d9 ed 44 44 77 76 8e 14 78 b0
station: addr:5d ctrl:82 len:da crc:6713 -> reserved     09 59 e9 c3
c1 10 3e 34 82 3e 24 cb ea 6a fb 6a 85 32 8b d1 b2 0f b1 ef 51 18 be
36 8c 59 c0 a1 c2 0d 7a af 09 3a 5d 70 7c 0c be cf 58 bd a0 7b 96 f1
83 03 ab a5
station: addr:11 ctrl:24 len:fe crc:aff5 -> reserved     de bf be 0c
0a f1 85 9e 8c 60 b1 c9 a7 87 a2 1b 8b 8d 8c 16 14 97 76 5b 0e eb ff
48 0a 6c 3e 12 89 db 07 09 2f f2 11 bb 91 a0 5f fb 8b 47 30 82 9b 11
67 c8 1d ea 71 83 cf 9d 3b a1 00 4d c5
```

```
phone  : addr:ca ctrl:84 len:54 crc:7a94 -> reserved     39 df 70 1f
95 15 29 c1 a4 a2 d3 59 9d fc 25 ec 89 1b 36 2e e4
station: addr:f4 ctrl:68 len:cb crc:5110 -> 0100 CISS
(Call Independent Supplementary Services) messages :(null)    84 b3
e5 29 d5 d4 e6 ca 02 3e 15 27 b4 e8 ca 85 94 8d 70 3e b7 97 1a b1 e8
a6 c9 28 1e 90 19 a9 a5 8b e2 93 ec 8b 3e 0a ac 3a 16 4a 0e 78 24 aa
30 03
```

Siemens Gigaset C450 IP

```
phone  : addr:13 ctrl:21 len:01 crc:4e7c
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:00 len:09 crc:6422 -> 0011 CC
(Call Control) messages :{CC-CONNECT}    83 07
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:02 len:6d crc:91d8 -> 0101 MM
(Mobility Management) messages :{AUTHENTICATION-REQUEST}    05 40 0a
03 01 18 18 0c 08 c2 87 10 c3 9e a9 e6 a7 0e 08 85 51 8b 4a d1 48 18
be
phone  : addr:13 ctrl:01 len:01 crc:ae3c
station: addr:13 ctrl:00 len:39 crc:4b3c -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 0a 81 00 02 2b 05 32
35 37 31 33
phone  : addr:13 ctrl:21 len:01 crc:4e7c
phone  : addr:11 ctrl:20 len:21 crc:ddb7 -> 0101 MM
(Mobility Management) messages :{AUTHENTICATION-REPLY}    85 41 0d
04 7d 96 51 f8
station: addr:13 ctrl:02 len:7d crc:336e -> 0011 CC
(Call Control) messages :(null)    63 62 7b 1b 81 00 02 58 13 03 11
0c 91 02 02 0c 1b 2d 41 46 65 73 74 6e 65 74 7a 2d 5b 01 91
station: addr:11 ctrl:21 len:01 crc:5676
phone  : addr:13 ctrl:01 len:01 crc:ae3c
station: addr:13 ctrl:20 len:19 crc:b6b2 -> 0101 MM
(Mobility Management) messages :{CIPHER-REQUEST}    05 4c 19 02 81
98
phone  : addr:11 ctrl:02 len:4d crc:9b19 -> 0100 CISS
(Call Independent Supplementary Services) messages :{CISS-REGISTER}
64 64 05 07 90 a8 00 c2 9c 58 9a 7b 06 81 00 02 59 b0 1a
station: addr:19 ctrl:14 len:75 crc:86a5 -> reserved     08 f3 22 66
93 13 7c 9a 96 b9 bf fb ba a9 a4 62 c9 77 db 75 a5 cf 4d 3c f7 35 b2
32 57
station: addr:fb ctrl:fc len:42 crc:7af9 -> 0100 CISS
(Call Independent Supplementary Services) messages :(null)    74 d0
b6 1a 9f 55 7b b2 38 55 8e d4 2f 0c 02 b8
station: addr:76 ctrl:1f len:b8 crc:eac1 -> 0100 CISS
(Call Independent Supplementary Services) messages :(null)    34 f5
88 7f 6a 25 87 1e 11 51 b0 fd 1f c8 b1 23 76 ec 6b f5 b7 fa 2b 80 91
3c b3 c7 74 97 b4 83 3f 1d cf 1e c1 d0 08 52 78 85 49 4b b4 77
station: addr:29 ctrl:35 len:06 crc:bec2 -> 0011 CC
(Call Control) messages :(null)    03
station: addr:f6 ctrl:2a len:6f crc:1c4d -> reserved     81 a3 2e fb
22 b3 35 77 6a 09 b1 cf 30 ac de 9b b4 58 d6 5d 93 c5 53 e6 62 aa 4a
station: addr:4e ctrl:f9 len:90 crc:a8af -> reserved     4b 47 a1 5a
43 77 b0 5b ee 87 dc 05 60 39 26 f8 aa 4f 80 81 df 6c 3c 81 a2 7d 95
ad 42 ce de b3 22 ba f7 5c
station: addr:a1 ctrl:40 len:23 crc:f86e -> reserved     81 1d aa 32
c8 b3 11 1e
phone  : addr:d2 ctrl:b2 len:fe crc:966d -> reserved     ef 1e 21 f0
5a 9f 89 97 ae b5 36 27 7e 56 27 65 68 08 bb 1a 9d a8 78 31 ae 57 e1
6c 5b bc bd 59 95 8b 96 a8 90 30 56 58 11 03 43 9b 2f 1c 59 a8 ef 7b
f4 5b e4 81 2d e1 a3 97 ed 18 7b 33 0c
```

```
station: addr:f3 ctrl:63 len:74 crc:589c -> reserved     a1 d8 fe 0b
12 d1 60 6b b9 b3 58 d8 85 d6 52 05 61 68 90 5c c8 79 bf 7f 65 f0 d3
0b 63
station: addr:22 ctrl:15 len:e5 crc:4c76 -> 0100 CISS
(Call Independent Supplementary Services) messages :(null)    74 b4
d0 ef 09 7f c2 db 63 9a 13 10 f2 8a 76 c2 1d 24 87 4e 81 e0 7e 4f b0
75 21 7b d6 5a 79 01 8a 9c 30 41 2c e7 e4 6f 0f d3 cf e6 2b 6b 1a bb
d7 1b 1b 1b a5 e6 ae 06 3f
station: addr:d2 ctrl:c0 len:18 crc:b882 -> reserved     6a d9 97 63
79 4a
station: addr:78 ctrl:f8 len:b8 crc:9d5c -> 0110 CLMS
(ConnectionLess Message Service) messages :NULL    06 73 59 13 a0 06
92 e8 f5 ef fb 0a 7d 5e 1f 1b 46 c2 66 c9 b7 20 0c c9 56 31 68 59 cd
12 c5 4b ee 2f 0e 9e e8 a2 12 15 2e e4 6f d2 b6 5d
phone  : addr:71 ctrl:f7 len:f3 crc:055c -> 0110 CLMS
(ConnectionLess Message Service) messages :NULL    76 eb e0 54 86 41
90 07 27 2e 16 95 07 9a 72 eb ed 25 8f f1 17 94 63 d2 74 2e 32 1b 23
11 3e 40 8a 5d e9 09 3d 63 01 3b 74 fe 39 73 45 cf f1 61 72 7e 04 83
b8 be 26 d6 b2 d4 2b d6
station: addr:f6 ctrl:99 len:78 crc:757f -> reserved     3e 0b ca 06
00 3a 72 56 3f da f5 a1 b9 ef 6b 69 5e ce d2 3c e9 fd 8e bd 02 a4 ef
fa cb a4
station: addr:ce ctrl:64 len:5c crc:5210 -> 0101 MM
(Mobility Management) messages :(null)    35 71 91 5b 8d 84 90 b3 fb
15 b9 07 d1 e2 eb 75 21 1d 9b c9 f8 3b e6
station: addr:20 ctrl:92 len:7e crc:6353 -> 0110 CLMS
(ConnectionLess Message Service) messages :NULL    b6 8f fb 33 92 9e
0c 7b ed 3d f9 7d b5 6f af b0 52 a7 bd c9 6b a2 51 df 92 83 39 1e 20
39 31
phone  : addr:68 ctrl:ab len:5b crc:34fa -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    37 2b b9 32
17 5c 05 fe 62 e1 80 0d 3b 90 21 31 05 33 eb 1e 0f 7e
station: addr:36 ctrl:ba len:d8 crc:5587 -> reserved     92 38 ef e5
4e 45 1f 42 6e 52 60 bf ae 7a e1 86 84 31 c4 03 1f df 80 38 f8 17 45
ee a1 13 cb 0e 0b f4 e5 b8 7e 3d 14 83 11 1b 9a ac db 2e 21 92 5c 58
cf ec 3b 51
```

Siemens Gigaset E360

```
phone  : addr:91 ctrl:00 len:01 crc:b7b5
phone  : addr:11 ctrl:02 len:8d crc:1b5d -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 00 c6 66 7d
bd 06 07 a0 a5 00 b6 04 30 c0 e0 80 2c 03 8f 01 c0 7b 06 81 00 02 18
01 42
station: addr:11 ctrl:01 len:01 crc:b636
station: addr:13 ctrl:00 len:29 crc:f43c -> 0011 CC
(Call Control) messages :{CC-CONNECT}    83 07 7b 06 81 00 02 01 01
01
phone  : addr:13 ctrl:21 len:01 crc:4e7c
phone  : addr:11 ctrl:20 len:25 crc:15f0 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 05 32 35 37 31 33
station: addr:13 ctrl:02 len:6d crc:dbce -> 0101 MM
(Mobility Management) messages :{AUTHENTICATION-REQUEST}    05 40 0a
03 01 18 18 0c 08 06 77 e2 c7 50 73 be 29 0e 08 38 ce 25 91 cb ba 71
c8
station: addr:11 ctrl:21 len:01 crc:5676
phone  : addr:13 ctrl:01 len:01 crc:ae3c
station: addr:13 ctrl:20 len:39 crc:ca68 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 0a 81 00 02 32 01 0e
1a 02 09 01
phone  : addr:11 ctrl:02 len:21 crc:a733 -> 0101 MM
```

```
(Mobility Management) messages :{AUTHENTICATION-REPLY}    85 41 0d
04 4a 8d 57 08
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:11 ctrl:01 len:01 crc:b636
station: addr:13 ctrl:02 len:19 crc:3e49 -> 0101 MM
(Mobility Management) messages :{CIPHER-REQUEST}    05 4c 19 02 81
98
phone  : addr:11 ctrl:20 len:25 crc:07fe -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 7b 05 81 00 02 30 00
station: addr:b4 ctrl:02 len:bf crc:1ecb -> 0110 CLMS
(ConnectionLess Message Service) messages :NULL    36 1a 12 90 1a 93
1b 39 da 47 a6 23 c1 44 a7 bb e8 78 08 c7 52 4d fc 08 82 22 eb 0b ee
99 26 01 f8 0f c0 3f 14 33 f1 b0 5f d5 1a 21 d8 38 dd
phone  : addr:d3 ctrl:2d len:97 crc:9cc0 -> 0100 CISS
(Call Independent Supplementary Services) messages :(null)    24 f3
b9 ef 4d c9 9d 2a 26 38 c7 2a 75 13 27 20 61 f6 a3 b2 6b 6d a9 97 85
23 a4 27 c1 22 07 3d bd 08 50 5d f2
station: addr:cb ctrl:a6 len:f6 crc:49e4 -> reserved     c9 6a f9 d0
ed d3 ff 99 e8 2a 7b c5 af b2 55 2a f8 9b 37 ad 77 cb 6f 60 9a a7 83
7a 99 b2 29 b8 92 1d 75 91 30 33 af 8c 01 ea 0c 67 d9 bb 9f 43 82 3f
c4 1f f6 4b e7 2d 90 cf 6a 84 39
station: addr:fd ctrl:94 len:05 crc:572e -> 0110 CLMS
(ConnectionLess Message Service) messages :NULL    a6
station: addr:da ctrl:5e len:ef crc:6857 -> 0101 MM
(Mobility Management) messages :(null)    b5 11 87 50 59 f9 df 08 f6
09 5d 3a 47 27 bf 8b 66 76 ee fa 6c 3a b9 9e b5 f8 7e c0 4e 83 5d 0d
c9 08 11 85 e6 5b 14 a9 98 bc 18 6d 29 8f e6 6e 2b d6 6c 95 c6 a5 a0
86 bd 46 9a
station: addr:c6 ctrl:3d len:0f crc:ab66 -> 0000 LCE
(Link Control Entity) messages :NULL    80 25 ad
station: addr:15 ctrl:6b len:9c crc:0a7c -> reserved     dd 21 24 1c
f6 08 b8 8f 01 cf ac 93 4e 21 a1 82 ad d5 2f e4 29 10 b0 c5 4d 26 5b
a8 26 57 41 57 ae fe 20 65 d0 dd e8
phone  : addr:23 ctrl:f9 len:68 crc:992b -> reserved     7f 7c d2 22
94 fb 3a cb 27 a9 b8 91 d9 df 8a bd d0 87 61 7a b5 52 76 1b 8f 47
```

Siemens Gigaset S680

```
phone  : addr:13 ctrl:21 len:01 crc:4e7c
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:00 len:09 crc:6422 -> 0011 CC
(Call Control) messages :{CC-CONNECT}    83 07
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:02 len:2d crc:4d81 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 07 81 00 02 1a 02 09
01
phone  : addr:13 ctrl:01 len:01 crc:ae3c
station: addr:13 ctrl:00 len:b1 crc:936a -> 0011 CC
(Call Control) messages :(null)    63 62 7b 28 81 00 02 58 20 03 1e
0c 91 02 02 11 1b 2d 41 4c 65 69 74 75 6e 67 20 62 65 6c 65 67 74 0a
91 02 02 03 1b 2d 41 5b 01 90
phone  : addr:13 ctrl:21 len:01 crc:4e7c
phone  : addr:11 ctrl:20 len:4d crc:f8ea -> 0100 CISS
(Call Independent Supplementary Services) messages :{CISS-REGISTER}
64 64 05 07 90 a8 00 ba 7d ab ca 7b 06 81 00 02 59 01 90
station: addr:13 ctrl:02 len:b9 crc:f101 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 28 2a 0c 9c 0e 00 02 01
00 02 00 03 00 04 00 05 00 06 00 0d 1a 91 02 02 06 57 e4 68 6c 65 6e
0a 0a 0d 1a 0a 0d 1a 0a 0d 1a 02 0a 0a
station: addr:11 ctrl:21 len:01 crc:5676
phone  : addr:13 ctrl:01 len:01 crc:ae3c
phone  : addr:11 ctrl:02 len:09 crc:80d1 -> 0100 CISS
(Call Independent Supplementary Services) messages :{CISS-RELEASE-
COM}    64 5a
station: addr:13 ctrl:20 len:91 crc:4c4b -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 20 81 00 02 03 04 20
22 43 02 26 08 b0 b0 00 8f 03 a9 b9 c9 26 0b b1 b1 00 4f 70 74 69 6f
6e 65 6e
station: addr:11 ctrl:01 len:01 crc:b636
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:02 len:a1 crc:ef86 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 24 81 00 02 26 08 b0
b0 00 8f 03 a9 b9 c9 26 0b b1 b1 00 4f 70 74 69 6f 6e 65 6e 03 08 20
22 43 02 15 25 71 3f
phone  : addr:13 ctrl:01 len:01 crc:ae3c
station: addr:13 ctrl:00 len:6d crc:6b79 -> 0101 MM
(Mobility Management) messages :{AUTHENTICATION-REQUEST}    05 40 0a
03 01 18 18 0c 08 9a 43 90 dd b2 bb d4 21 0e 08 ac 4c 5f ca 35 a0 0b
65
phone  : addr:13 ctrl:21 len:01 crc:4e7c
phone  : addr:11 ctrl:20 len:21 crc:e8c2 -> 0101 MM
(Mobility Management) messages :{AUTHENTICATION-REPLY}    85 41 0d
04 7b dc 18 d7
station: addr:11 ctrl:21 len:01 crc:5676
station: addr:13 ctrl:22 len:19 crc:9cca -> 0101 MM
(Mobility Management) messages :{CIPHER-REQUEST}    05 4c 19 02 81
98
phone  : addr:13 ctrl:01 len:01 crc:ae3c
station: addr:63 ctrl:64 len:d1 crc:adf2 -> reserved     9c 9d 8b eb
45 a4 83 73 a9 29 77 df 70 4b 3b 78 68 2e 61 aa 1a 1a 8a 23 25 dd ae
86 65 e7 3a 96 b9 78 df af 1d aa 02 25 a3 b7 9a 5d 28 72 31 b6 3a 51
4e b8
station: addr:94 ctrl:fc len:af crc:a0c6 -> reserved     cb 33 6d 4a
d9 a4 7f 61 e8 ad 86 67 f9 f1 e5 f1 cd 4f de b4 74 89 cd 11 46 1e ff
69 25 7b 90 10 ef 63 93 fe 20 f5 d5 0b ee f6 ab
phone  : addr:b2 ctrl:a3 len:34 crc:d870 -> reserved     1f 61 2f 65
fa d3 6f 98 d0 b7 f6 30 1f
station: addr:bf ctrl:4b len:2a crc:65c0 -> reserved     f9 d9 80 75
6a 65 34 e1 a8 9f
phone  : addr:97 ctrl:1a len:1e crc:74cc -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    17 4e 1e ec
cb ab d6
station: addr:4a ctrl:37 len:fd crc:674c -> reserved     c9 6a a5 e9
7b 58 93 7a ab a9 48 cf a0 0a 30 0a b6 37 c5 1a 49 82 b3 05 37 ea f9
58 4a f8 ab d0 04 01 24 e7 21 12 69 ce a4 2a 57 7f d4 a9 e4 2c 35 ca
1a df c7 98 ce eb 86 d3 80 97 b4 57 e5
station: addr:1e ctrl:d8 len:2c crc:e039 -> reserved     7a ca a9 be
07 25 c7 c6 9f e2 e7
station: addr:97 ctrl:ac len:05 crc:ef27 -> 0011 CC
(Call Control) messages :(null)    a3
```

Siemens Gigaset SL785

```
phone  : addr:13 ctrl:21 len:01 crc:4e7c
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:00 len:09 crc:6422 -> 0011 CC
(Call Control) messages :{CC-CONNECT}    83 07
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:02 len:6d crc:1547 -> 0101 MM
(Mobility Management) messages :{AUTHENTICATION-REQUEST}    05 40 0a
03 01 18 18 0c 08 2b ba e9 38 67 1a 99 54 0e 08 13 53 52 2c 88 df 7e
5d
```

```
phone  : addr:13 ctrl:01 len:01 crc:ae3c
phone  : addr:11 ctrl:00 len:21 crc:1e95 -> 0101 MM
(Mobility Management) messages :{AUTHENTICATION-REPLY}    85 41 0d
04 c3 5c 4c f3
station: addr:13 ctrl:00 len:b1 crc:6c84 -> 0011 CC
(Call Control) messages :(null)    63 62 7b 28 81 00 02 58 20 03 1e
0c 91 02 02 11 1b 2d 41 4c 65 69 74 75 6e 67 20 62 65 6c 65 67 74 0a
91 02 02 03 1b 2d 41 5b 01 9d
station: addr:11 ctrl:21 len:01 crc:5676
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:22 len:19 crc:9cca -> 0101 MM
(Mobility Management) messages :{CIPHER-REQUEST}    05 4c 19 02 81
98
phone  : addr:11 ctrl:22 len:4d crc:4ca8 -> 0100 CISS
(Call Independent Supplementary Services) messages :{FACILITY}    64
62 05 07 90 a8 00 b6 4b c2 18 7b d7 d0 8f 15 5d e6 23
station: addr:f5 ctrl:2d len:58 crc:2329 -> 0101 MM
(Mobility Management) messages :(null)    35 29 b8 d4 a0 14 fb c5 5f
8e 69 16 44 a2 2f f5 6b 7f 38 8c 0d 7b
station: addr:bb ctrl:6b len:f7 crc:9029 -> 0110 CLMS
(ConnectionLess Message Service) messages :NULL    96 ab c5 e0 91 9d
26 cf 33 d0 91 9a 8e 41 e5 67 8d b6 e5 7b 1f 6a 61 11 8b 44 51 5f a2
0a 57 d0 4b 9f 26 d9 1f 72 fa 51 58 06 cc de 19 35 e3 b1 94 1b cf e7
dd 63 b8 bf a7 fe ff 7e 41
station: addr:82 ctrl:91 len:29 crc:3fd8 -> 0110 CLMS
(ConnectionLess Message Service) messages :NULL    46 fd e0 41 6f 42
9c e2 3d 10
station: addr:48 ctrl:8c len:c7 crc:47e9 -> reserved     19 d7 86 18
9b d8 b7 f6 5f b1 1c 0f 2c 22 28 1b ae b6 81 dc 66 f3 6f 3e 0c 62 0c
ad b0 5d d7 cd 59 9b e0 78 a5 2e b4 cf 3c 1f f3 00 28 a8 de 7e ec
station: addr:76 ctrl:34 len:80 crc:a40b -> reserved     89 e5 41 7a
a2 47 8e 33 6a 68 a8 cc 4c a5 a1 1f 65 35 40 f0 c4 16 0a c6 b5 27 45
e6 2b 87 8b 75
station: addr:e2 ctrl:aa len:ae crc:531a -> reserved     6a 1e b7 23
c3 6a 62 5f 1a cf d7 3c cd db 34 5b c3 4c aa 8e 34 49 64 14 ca e3 5e
98 2e 79 f0 95 04 55 dc 95 e8 eb 00 0d 76 2d e3
station: addr:ec ctrl:79 len:b5 crc:8c23 -> reserved     79 43 84 57
68 17 da 65 d3 d4 fb b6 ff 5c c4 76 5f 20 4f 25 0c 67 8e 37 2f 68 49
3b 43 3f 41 e4 16 1c 3a cf cd f4 b2 45 64 54 6a 13 25
station: addr:1d ctrl:ac len:3e crc:d03b -> reserved     68 51 6f fd
54 a1 81 9a 1c 81 a4 a8 4c a2 c6
phone  : addr:80 ctrl:4f len:e9 crc:64ab -> reserved     fe ba 02 ee
ab 36 82 fa 58 4f f9 4e 5c 9f 7c c6 fe 0b d2 aa 23 36 8a be ff 4a ce
01 59 e7 39 b9 d4 b9 1a 57 ef 70 1f 01 34 58 a1 79 52 b5 cc f8 fc 6c
bb d9 fa 8e 44 d6 55 76
station: addr:4a ctrl:88 len:52 crc:6cdc -> reserved     62 3d 6a a5
28 a9 5e ab 19 ca 13 71 63 90 b3 35 57 85 3e a4
station: addr:ae ctrl:10 len:ef crc:b1f2 -> reserved     3f 1a 57 ca
3a ab 54 20 e3 9f 65 26 d1 28 8e de 5d cd 58 c3 2d 4d 0f 7b b3 61 4f
f2 97 66 2f b3 8f 73 18 61 fd b7 e6 75 35 19 26 ed b1 0b 94 67 b9 22
51 78 c5 21 94 3e a9 2b 66
station: addr:c3 ctrl:94 len:e8 crc:ae27 -> reserved     2c 42 70 c6
cd 1d 22 7b 75 01 f1 c9 35 f5 5e fd ea 67 53 a3 40 d4 f4 8d 2b df 8c
1b 4f 0a 2c 5f d5 90 47 5a 09 86 9b 5d 26 35 39 4b 94 ed bc 45 68 ec
52 23 eb 56 8d cf 8d cc
station: addr:36 ctrl:5e len:2a crc:41d3 -> reserved     22 36 36 3b
ee 51 f4 99 ef d3
phone  : addr:51 ctrl:f8 len:ea crc:305f -> reserved     cc 21 ec 1c
02 3a 43 9a 9b d5 61 dd 3b 53 46 d3 bb fa c7 6b 9c d0 c7 95 38 8f 29
20 76 24 6d 2a 40 77 48 f9 f2 f7 5d 4e a3 c5 0b b7 6a 26 45 6f 2a d9
ae 0e 3b 2b 7a 86 2b 84
```

```
phone  : addr:bd ctrl:e8 len:1e crc:6e32 -> reserved     0d b3 3b 2b
39 1d 21
station: addr:be ctrl:9f len:fb crc:5b2e -> reserved     38 57 37 92
9e f2 f0 23 a4 a3 e1 e3 46 93 0a 70 9e 49 a2 52 c0 c7 db 11 00 ee 02
28 dd 4f 91 7a 71 82 a1 21 b4 d3 b5 40 50 25 7d 11 ad 13 a4 ff ff ff
ff ff 18 56 53 a4 bf 59 6e 14 f5 f7
station: addr:73 ctrl:e7 len:48 crc:7d72 -> 0011 CC
(Call Control) messages :(null)    f3 c3 5e f9 74 d4 9e fe 32 6a 2e
e4 c0 71 d7 f7 33 d6
phone  : addr:28 ctrl:ea len:49 crc:8bfc -> 0100 CISS
(Call Independent Supplementary Services) messages :(null)    74 a0
cb cf ae 8a 62 e0 ab 08 56 11 cd 12 e6 72 2e af
phone  : addr:e0 ctrl:cd len:2a crc:254b -> 0100 CISS
(Call Independent Supplementary Services) messages :(null)    f4 02
c2 09 f0 5c 16 b0 0b 55
```

T-Home Sinus 45

```
phone  : addr:91 ctrl:00 len:01 crc:b7b5
station: addr:91 ctrl:21 len:01 crc:54f7
phone  : addr:11 ctrl:02 len:79 crc:b994 -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 00 18 24 42
9e 06 07 a0 a5 00 24 c3 ec e0 e0 80 7b 06 81 00 02 18 01 42
station: addr:11 ctrl:01 len:01 crc:b636
station: addr:13 ctrl:00 len:25 crc:50f6 -> 0011 CC
(Call Control) messages :{CC-CONNECT}    83 07 7b 05 81 00 02 01 00
phone  : addr:13 ctrl:21 len:01 crc:4e7c
phone  : addr:11 ctrl:20 len:25 crc:15f0 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 05 32 35 37 31 33
station: addr:13 ctrl:02 len:41 crc:ea59 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 28 0c 9c 09 04 00 02 08
02 10 02 18 82 0c
station: addr:11 ctrl:21 len:01 crc:5676
phone  : addr:13 ctrl:01 len:01 crc:ae3c
phone  : addr:11 ctrl:02 len:25 crc:8e95 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 7b 05 81 00 02 30 00
station: addr:13 ctrl:20 len:6d crc:79a3 -> 0101 MM
(Mobility Management) messages :{AUTHENTICATION-REQUEST}    05 40 0a
03 01 18 18 0c 08 eb a6 07 b4 37 42 9d 36 0e 08 12 f9 d1 bf 8e 05 0c
e8
station: addr:11 ctrl:01 len:01 crc:b636
phone  : addr:13 ctrl:21 len:01 crc:4e7c
phone  : addr:11 ctrl:20 len:21 crc:019d -> 0101 MM
(Mobility Management) messages :{AUTHENTICATION-REPLY}    85 41 0d
04 e1 aa fc cb
station: addr:13 ctrl:02 len:c9 crc:4786 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 28 15 9c 09 04 00 02 08
02 10 02 18 82 0c 9c 07 03 00 02 09 04 18 82 7b 17 81 00 02 26 03 b0
b0 00 26 03 b5 b5 00 26 03 b6 b6 00 26 03 b1 b1 00
station: addr:11 ctrl:21 len:01 crc:5676
phone  : addr:13 ctrl:01 len:01 crc:ae3c
station: addr:13 ctrl:20 len:19 crc:b6b2 -> 0101 MM
(Mobility Management) messages :{CIPHER-REQUEST}    05 4c 19 02 81
98
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:8d ctrl:49 len:6f crc:df55 -> reserved     32 ed a6 74
76 ea 92 3f 81 36 54 c2 85 1e 4e d6 a6 d3 f4 2b 62 4a e1 83 d1 0d c0
station: addr:0c ctrl:49 len:8f crc:e830 -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    17 ce b4 44
6e 75 ac 39 bc 60 45 11 01 42 a7 93 67 ca c4 b7 36 dc 68 22 38 21 c5
58 55 82 33 45 37 74 e6
```

```
phone  : addr:8a ctrl:06 len:2b crc:5d01 -> 0100 CISS
(Call Independent Supplementary Services) messages :(null)    24 59
b9 64 2a b2 74 a3 19 34
station: addr:f4 ctrl:4c len:c6 crc:5854 -> reserved     c1 d7 b7 cd
85 55 c4 a9 92 2e c4 00 1e ce 10 22 7f 8f c9 f7 54 68 e6 f4 d6 d0 3b
86 d5 12 85 09 1b d1 5f c9 c9 76 f1 05 b7 36 f8 89 05 aa 57 d0 cf
station: addr:50 ctrl:38 len:62 crc:5c3a -> 0000 LCE
(Link Control Entity) messages :NULL    c0 fd 4b 18 d3 70 c4 a8 16
ef 0f 18 a8 cd 82 58 79 ff ff ff ff ff 48 29
station: addr:f6 ctrl:54 len:bf crc:9a4c -> 0011 CC
(Call Control) messages :(null)    03 4a 8d e6 75 4b 7a a4 3a 81 10
34 7a 1a b9 cc 38 c6 46 95 8f d5 fb 69 54 01 3c f6 59 6c e7 cb 01 b2
1d 83 8a ff 7d c1 96 54 4b 41 36 4b 40
station: addr:72 ctrl:14 len:a1 crc:7d91 -> 0000 LCE
(Link Control Entity) messages :NULL    70 bd 27 5b eb bb 56 ff d7
47 39 26 d8 3d db b8 56 32 14 a2 51 69 c1 a7 41 0f 1b aa e8 ac 17 61
76 65 04 77 62 86 64 d4
station: addr:6a ctrl:5f len:67 crc:d9dc -> 0110 CLMS
(ConnectionLess Message Service) messages :NULL    76 30 4c 9a f4 6c
35 ea e7 f4 59 97 0e 42 03 b4 50 ff 80 6c 7c 0c b6 e1 a5
phone  : addr:ac ctrl:cf len:e8 crc:1ac1 -> reserved     09 10 50 5e
d2 f5 b2 4d 4e f4 28 07 c5 c4 a2 91 71 73 c9 2f 8d b0 1d 57 4f 01 c8
ee 6a a1 e4 e8 0a 6e fa 7e e9 38 59 f8 bd 05 5d b6 55 13 bb 9c 0b f3
00 ec f2 ad b3 2f 6d f3
station: addr:12 ctrl:ee len:9d crc:0b19 -> reserved     9a 5f 77 e2
d5 bc 06 af 0f 27 a2 11 5b 39 f7 f6 5b c5 21 01 79 2a f8 5e 8a 2d b0
59 70 2d ea a4 15 31 c3 c3 2e 0a 7e
station: addr:69 ctrl:6a len:4b crc:ee48 -> reserved     1f 83 31 00
cd e9 07 a6 fe c6 01 52 61 82 b4 ac 4c 19
```

T-Home Sinus 101

```
phone  : addr:11 ctrl:02 len:8d crc:23b3 -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 01 25 91 fa
31 06 07 a0 a5 01 25 9a d2 98 e0 80 63 0b 44 00 08 00 1a 01 0c 80 a2
01 81
station: addr:11 ctrl:01 len:01 crc:b637
station: addr:13 ctrl:00 len:19 crc:5830 -> 0101 MM
(Mobility Management) messages :{CIPHER-REQUEST}    05 4c 19 02 81
98
phone  : addr:5c ctrl:ec len:5c crc:58cf -> reserved     aa 4d 12 b8
2a f1 a8 a2 6c 69 0b 70 74 43 71 55 3b 6b 8e 59 c8 bf 76
station: addr:72 ctrl:ec len:7f crc:fffe -> reserved     cb 56 81 5c
8d c8 2e a1 ac 01 0f 7d ec 06 49 0c 21 0d 9d 66 fd 30 5e 72 fe 0c 56
86 fd 75 bb
phone  : addr:f6 ctrl:45 len:d6 crc:2ab6 -> 0101 MM
(Mobility Management) messages :{LOCATE-ACCEPT}    25 55 1d 81 f7 04
88 25 1d 0a 4a 0b 01 08 1d 30 96 c0 6c 33 b3 e5 c3 5b 10 16 a6 5e 3e
0d 1b 34 46 85 4a b6 ce 24 58 1b 74 02 1a f0 8e b7 3c e5 57 c2 3a 9c
a8
```

T-Home Sinus 102

```
phone  : addr:91 ctrl:00 len:01 crc:b7b4
phone  : addr:11 ctrl:02 len:8d crc:23b3 -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 01 25 91 fa
31 06 07 a0 a5 01 25 9a d2 98 e0 80 63 0b 44 00 08 00 1a 01 0c 80 a2
01 81
station: addr:11 ctrl:01 len:01 crc:b637
```

```
station: addr:13 ctrl:00 len:19 crc:5830 -> 0101 MM
(Mobility Management) messages :{CIPHER-REQUEST}    05 4c 19 02 81
98
station: addr:e3 ctrl:5f len:20 crc:08c6 -> reserved     ce 87 54 e5
6d 38 e6 d9
```

T-Home Sinus 212

```
phone  : addr:91 ctrl:00 len:01 crc:b7b4
phone  : addr:11 ctrl:02 len:8d crc:1926 -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 00 80 02 cb
35 06 07 a0 a5 00 80 0e fa b8 e0 80 63 0b 44 00 08 00 1a 01 0c 80 82
01 81
station: addr:11 ctrl:01 len:01 crc:b637
station: addr:13 ctrl:00 len:19 crc:5830 -> 0101 MM
(Mobility Management) messages :{CIPHER-REQUEST}    05 4c 19 02 81
98
```

T-Home Sinus 501

```
phone  : addr:13 ctrl:21 len:01 crc:4e7c
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:00 len:09 crc:6422 -> 0011 CC
(Call Control) messages :{CC-CONNECT}    83 07
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:02 len:2d crc:4d81 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 07 81 00 02 1a 02 09
01
phone  : addr:13 ctrl:01 len:01 crc:ae3c
station: addr:13 ctrl:00 len:b1 crc:9668 -> 0011 CC
(Call Control) messages :(null)    63 62 7b 28 81 00 02 58 20 03 1e
0c 91 02 02 11 1b 2d 41 4c 65 69 74 75 6e 67 20 62 65 6c 65 67 74 0a
91 02 02 03 1b 2d 41 5b 01 8f
phone  : addr:13 ctrl:21 len:01 crc:4e7c
phone  : addr:11 ctrl:20 len:4d crc:b7d3 -> 0100 CISS
(Call Independent Supplementary Services) messages :{CISS-REGISTER}
64 64 05 07 90 a8 00 b6 0e 04 3f 7b 06 81 00 02 59 01 8f
station: addr:13 ctrl:02 len:b9 crc:f101 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 28 2a 0c 9c 0e 00 02 01
00 02 00 03 00 04 00 05 00 06 00 0d 1a 91 02 02 06 57 e4 68 6c 65 6e
0a 0a 0d 1a 0a 0d 1a 0a 0d 1a 02 0a 0a
station: addr:11 ctrl:21 len:01 crc:5676
phone  : addr:13 ctrl:01 len:01 crc:ae3c
phone  : addr:11 ctrl:02 len:09 crc:80d1 -> 0100 CISS
(Call Independent Supplementary Services) messages :{CISS-RELEASE-
COM}    64 5a
station: addr:13 ctrl:20 len:91 crc:4c4b -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 20 81 00 02 03 04 20
22 43 02 26 08 b0 b0 00 8f 03 a9 b9 c9 26 0b b1 b1 00 4f 70 74 69 6f
6e 65 6e
station: addr:11 ctrl:01 len:01 crc:b636
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:02 len:a1 crc:ef86 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 24 81 00 02 26 08 b0
b0 00 8f 03 a9 b9 c9 26 0b b1 b1 00 4f 70 74 69 6f 6e 65 6e 03 08 20
22 43 02 15 25 71 3f
phone  : addr:13 ctrl:01 len:01 crc:ae3c
station: addr:13 ctrl:00 len:6d crc:f392 -> 0101 MM
```

```
(Mobility Management) messages :{AUTHENTICATION-REQUEST}    05 40 0a
03 01 18 18 0c 08 8f d7 04 48 51 b5 4e 46 0e 08 a3 ae 19 84 4f 19 40
90
phone  : addr:13 ctrl:21 len:01 crc:4e7c
phone  : addr:11 ctrl:20 len:21 crc:0500 -> 0101 MM
(Mobility Management) messages :{AUTHENTICATION-REPLY}    85 41 0d
04 51 1a 65 1e
station: addr:11 ctrl:21 len:01 crc:5676
station: addr:13 ctrl:22 len:19 crc:9cca -> 0101 MM
(Mobility Management) messages :{CIPHER-REQUEST}    05 4c 19 02 81
98
phone  : addr:13 ctrl:01 len:01 crc:ae3c
station: addr:d8 ctrl:d0 len:73 crc:8d1e -> reserved     ae 68 0f 0b
37 e2 15 78 e4 68 21 0a a7 02 26 74 b4 db 30 6a 47 dc 50 25 9c 22 e9
43
station: addr:07 ctrl:85 len:3b crc:85d6 -> reserved     b2 5a 95 54
a0 76 68 1e ad b8 4a b2 47 6c
station: addr:f5 ctrl:b8 len:ae crc:251a -> 0101 MM
(Mobility Management) messages :(null)    85 7b 47 55 ec 9c f9 50 f6
4f 13 09 fb 4b 21 71 ff 85 60 c2 ca 03 4e d1 a0 06 1c 59 18 0f fb 20
b4 19 b7 43 41 04 5e b7 f3 19 01
station: addr:e4 ctrl:5a len:e0 crc:eda8 -> 0100 CISS
(Call Independent Supplementary Services) messages :(null)    a4 59
1a 11 c7 c3 4c 83 71 44 7a bf c0 00 a2 df 15 42 40 a9 3b 72 2b 40 be
a5 42 ba 53 d2 30 a6 a6 b9 a2 f7 d8 71 53 10 53 4d 6a e2 b1 0d 50 6d
6a 0e 65 a9 10 e5 f2 e4
station: addr:ef ctrl:ce len:00 crc:853e
phone  : addr:65 ctrl:c4 len:98 crc:d7fa -> 0111 COMS
(Connection Oriented Message Service) messages :NULL    e7 d9 bf f3
eb 25 55 3d 1f 06 29 ec 96 99 c5 69 25 bb 4e 11 e5 95 92 fd 3d 3d 8c
e5 36 87 08 4f 12 be 55 8b 83 7e
```

T-Home Sinus 710 Komfort

```
phone  : addr:91 ctrl:00 len:01 crc:b7b5
phone  : addr:11 ctrl:02 len:79 crc:f1f9 -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 00 1d 45 00
08 06 07 a0 a5 00 4d 60 9c 80 e0 80 7b 06 81 00 02 18 01 42
station: addr:11 ctrl:01 len:01 crc:b636
station: addr:13 ctrl:00 len:09 crc:6422 -> 0011 CC
(Call Control) messages :{CC-CONNECT}    83 07
phone  : addr:13 ctrl:21 len:01 crc:4e7c
phone  : addr:11 ctrl:20 len:25 crc:15f0 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 05 32 35 37 31 33
station: addr:13 ctrl:02 len:85 crc:62a3 -> 0011 CC
(Call Control) messages :(null)    63 62 7b 1d 81 00 02 58 15 03 13
0c 91 02 02 0e 4c 65 69 74 75 6e 67 20 62 65 6c 65 67 74 5b 01 9b
station: addr:11 ctrl:21 len:01 crc:5676
phone  : addr:13 ctrl:01 len:01 crc:ae3c
phone  : addr:11 ctrl:02 len:25 crc:8e95 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 7b 05 81 00 02 30 00
station: addr:13 ctrl:20 len:29 crc:c6d5 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 06 81 00 02 01 01 01
station: addr:11 ctrl:01 len:01 crc:b636
phone  : addr:13 ctrl:21 len:01 crc:4e7c
phone  : addr:11 ctrl:20 len:4d crc:bb61 -> 0100 CISS
(Call Independent Supplementary Services) messages :{CISS-REGISTER}
64 64 05 07 90 a8 00 1d 45 00 08 7b 06 81 00 02 59 01 9b
station: addr:13 ctrl:02 len:65 crc:bb54 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 28 15 0c 9c 08 00 02 01
00 02 00 03 00 91 02 02 06 57 e4 68 6c 65 6e
```

```
station: addr:11 ctrl:21 len:01 crc:5676
phone  : addr:13 ctrl:01 len:01 crc:ae3c
phone  : addr:11 ctrl:02 len:09 crc:80d1 -> 0100 CISS
(Call Independent Supplementary Services) messages :{CISS-RELEASE-
COM}    64 5a
station: addr:13 ctrl:20 len:6d crc:9e44 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 17 81 00 02 26 08 b0
b0 00 8f 03 a9 b9 c9 26 08 b1 b1 00 8f 03 a5 b5 c5
station: addr:11 ctrl:01 len:01 crc:b636
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:02 len:29 crc:6f0d -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 06 81 00 02 32 01 0e
phone  : addr:13 ctrl:01 len:01 crc:ae3c
station: addr:13 ctrl:00 len:65 crc:f31e -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 28 15 0c 9c 08 00 02 01
00 02 00 03 00 91 02 02 06 57 e4 68 6c 65 6e
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:02 len:6d crc:8080 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 17 81 00 02 26 08 b0
b0 00 8f 03 a9 b9 c9 26 08 b1 b1 00 8f 03 a5 b5 c5
phone  : addr:13 ctrl:01 len:01 crc:ae3c
station: addr:13 ctrl:00 len:45 crc:e46b -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 0d 81 00 02 03 08 20
22 40 01 15 25 71 3f
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:02 len:39 crc:275e -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 0a 81 00 02 2b 05 32
35 37 31 33
phone  : addr:13 ctrl:01 len:01 crc:ae3c
station: addr:13 ctrl:00 len:11 crc:fabc -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b e4 4f
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:02 len:29 crc:18c1 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 28 06 02 1a 9c 02 00 00
phone  : addr:13 ctrl:01 len:01 crc:ae3c
station: addr:13 ctrl:00 len:75 crc:3c37 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 19 81 00 02 26 0a b0
b0 00 52 fc 63 6b 66 72 2e 26 08 b1 b1 00 8f 03 a5 b5 c5
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:02 len:2d crc:8c4b -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 07 81 00 02 1a 02 00
01
phone  : addr:13 ctrl:01 len:01 crc:ae3c
station: addr:13 ctrl:00 len:15 crc:9a13 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 28 01 02
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:02 len:29 crc:2285 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 06 81 00 02 04 01 11
phone  : addr:13 ctrl:01 len:01 crc:ae3c
station: addr:13 ctrl:00 len:45 crc:5cfa -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 0d 81 00 02 28 08 80
06 b8 32 35 37 31 33
phone  : addr:13 ctrl:21 len:01 crc:4e7c
phone  : addr:11 ctrl:20 len:29 crc:c531 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 7b 06 81 00 02 2a 01 00
station: addr:11 ctrl:21 len:01 crc:5676
```

T-Home Sinus A301

```
phone  : addr:13 ctrl:21 len:01 crc:4e7c
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:00 len:09 crc:6422 -> 0011 CC
(Call Control) messages :{CC-CONNECT}    83 07
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:02 len:2d crc:4d81 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 07 81 00 02 1a 02 09
01
phone  : addr:13 ctrl:01 len:01 crc:ae3c
station: addr:13 ctrl:00 len:a1 crc:20d9 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 28 24 0c 9c 0a 00 02 01
00 02 00 03 00 04 00 0d 1a 91 02 02 06 57 e4 68 6c 65 6e 0a 0d 1a 0a
0d 1a 0a 0d 1a 02 0a
phone  : addr:13 ctrl:21 len:01 crc:4e7c
station: addr:13 ctrl:02 len:91 crc:783e -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 20 81 00 02 03 04 20
22 43 01 26 08 b0 b0 00 8f 03 a9 b9 c9 26 0b b1 b1 00 4f 70 74 69 6f
6e 65 6e
phone  : addr:13 ctrl:01 len:01 crc:ae3c
station: addr:13 ctrl:00 len:99 crc:44ee -> 0011 CC
(Call Control) messages :(null)    63 62 7b 22 81 00 02 58 1a 03 18
0c 91 02 02 0e 4c 65 69 74 75 6e 67 20 62 65 6c 65 67 74 0a 91 02 02
00 5b 01 ad
phone  : addr:13 ctrl:21 len:01 crc:4e7c
phone  : addr:11 ctrl:20 len:4d crc:4541 -> 0100 CISS
(Call Independent Supplementary Services) messages :{CISS-REGISTER}
64 64 05 07 90 a8 00 b6 07 3e f2 7b 06 81 00 02 59 01 ad
station: addr:13 ctrl:02 len:a1 crc:f581 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 24 81 00 02 26 08 b0
b0 00 8f 03 a9 b9 c9 26 0b b1 b1 00 4f 70 74 69 6f 6e 65 6e 03 08 20
22 43 01 15 25 71 3f
station: addr:11 ctrl:21 len:01 crc:5676
phone  : addr:13 ctrl:01 len:01 crc:ae3c
phone  : addr:11 ctrl:02 len:09 crc:80d1 -> 0100 CISS
(Call Independent Supplementary Services) messages :{CISS-RELEASE-
COM}    64 5a
station: addr:13 ctrl:20 len:6d crc:a617 -> 0101 MM
(Mobility Management) messages :{AUTHENTICATION-REQUEST}    05 40 0a
03 01 18 18 0c 08 1d 56 8a 07 bb a8 ec 19 0e 08 78 69 22 0a 8c 6d d1
d7
station: addr:11 ctrl:01 len:01 crc:b636
phone  : addr:13 ctrl:21 len:01 crc:4e7c
phone  : addr:11 ctrl:20 len:21 crc:7533 -> 0101 MM
(Mobility Management) messages :{AUTHENTICATION-REPLY}    85 41 0d
04 16 3a f4 06
station: addr:11 ctrl:21 len:01 crc:5676
station: addr:13 ctrl:22 len:19 crc:9cca -> 0101 MM
(Mobility Management) messages :{CIPHER-REQUEST}    05 4c 19 02 81
98
station: addr:35 ctrl:d7 len:c7 crc:d834 -> reserved     8b cc 43 5c
16 22 60 75 75 00 6e c4 be fd b1 7e 10 c8 53 41 30 e8 17 20 f0 a4 73
79 db e5 83 03 d2 1f d0 a8 e8 09 25 54 26 37 81 18 bb f5 ed f4 04
phone  : addr:77 ctrl:7f len:52 crc:2b13 -> reserved     62 53 47 4b
7c 59 b4 1b 1e 7f 5e d0 4e 8c 2e 6e 07 8e 50 8d
station: addr:10 ctrl:c2 len:fc crc:18dd -> reserved     bc 4b 34 14
cf e4 9c bc 09 a3 a8 c8 df c2 09 c3 20 c4 3f 2f 08 67 fa 6f 16 d4 3c
73 94 89 46 76 73 b9 3a e9 5d ca 35 c7 43 5e 0e ae b4 bd 51 52 60 ea
ed 7e 35 ee 52 04 f4 fe da ff d7 e8 d3
station: addr:58 ctrl:ea len:45 crc:1d54 -> reserved     ac f6 0b 96
5f 48 34 6a 97 a5 59 b7 04 4d 1f a8 b5
```

```
phone  : addr:6e ctrl:df len:78 crc:8904 -> reserved     fd 99 af 10
5d cd e6 57 52 b7 83 04 19 d3 5d cc 19 1f ea 2e 78 f0 f8 b6 ca b6 f3
e4 63 d2
station: addr:59 ctrl:7c len:b6 crc:4588 -> 0000 LCE
(Link Control Entity) messages :NULL    f0 f6 6e 84 f9 97 6d a4 8c
81 cf 76 e8 e9 37 fb 0b cf bf ae 88 fd bb 56 39 42 4a e3 13 fc b7 11
36 79 a8 28 1c 58 7e 25 9c d9 35 23 c2
station: addr:a1 ctrl:50 len:97 crc:c84a -> reserved     79 39 6b 97
0d 7e 93 78 55 13 97 f0 29 ae dc 9f 5a d2 68 11 8a d3 92 1b fe a5 96
b0 05 67 2e f1 bf 0d 6a 48 8e
```

T-Home Sinus C31

```
phone  : addr:91 ctrl:00 len:01 crc:b714
phone  : addr:11 ctrl:02 len:59 crc:f2b2 -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 00 cc 9f 2a
31 06 07 a0 a5 00 ec f3 c7 58 e0 80
station: addr:11 ctrl:01 len:01 crc:b697
station: addr:13 ctrl:00 len:4d crc:8ad5 -> 0011 CC
(Call Control) messages :{CC-CONNECT}    83 07 7b 0f 81 03 51 0a 00
1a 00 1f 00 29 00 30 00 28 00
phone  : addr:13 ctrl:21 len:01 crc:4edd
station: addr:13 ctrl:02 len:55 crc:26cc -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 11 81 03 51 02 16 0a
00 1a 00 1f 00 29 00 30 00 28 00
phone  : addr:11 ctrl:20 len:25 crc:1551 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 05 32 35 37 31 33
phone  : addr:13 ctrl:01 len:01 crc:ae9d
station: addr:11 ctrl:21 len:01 crc:56d7
phone  : addr:11 ctrl:02 len:15 crc:9339 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 01 00
station: addr:11 ctrl:01 len:01 crc:b697
station: addr:13 ctrl:00 len:55 crc:a0a6 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 11 81 03 51 05 01 0a
00 1a 00 1f 00 29 00 30 00 28 00
phone  : addr:13 ctrl:21 len:01 crc:4edd
station: addr:13 ctrl:02 len:55 crc:689c -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 11 81 03 51 05 01 0a
00 1a 00 1f 00 29 00 30 00 28 00
phone  : addr:13 ctrl:01 len:01 crc:ae9d
station: addr:13 ctrl:00 len:55 crc:a0a6 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 11 81 03 51 05 01 0a
00 1a 00 1f 00 29 00 30 00 28 00
phone  : addr:13 ctrl:21 len:01 crc:4edd
station: addr:13 ctrl:02 len:55 crc:689c -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 11 81 03 51 05 01 0a
00 1a 00 1f 00 29 00 30 00 28 00
phone  : addr:13 ctrl:01 len:01 crc:ae9d
station: addr:13 ctrl:00 len:55 crc:a0a6 -> 0011 CC
(Call Control) messages :{CC-INFO}    83 7b 7b 11 81 03 51 05 01 0a
00 1a 00 1f 00 29 00 30 00 28 00
phone  : addr:13 ctrl:21 len:01 crc:4edd
phone  : addr:11 ctrl:20 len:11 crc:eb0c -> 0011 CC
(Call Control) messages :{CC-RELEASE}    03 4d e2 00
station: addr:11 ctrl:21 len:01 crc:56d7
station: addr:13 ctrl:22 len:11 crc:8523 -> 0011 CC
(Call Control) messages :{CC-RELEASE-COM}    83 5a e2 00
```

Tiptel Dectline

```
phone  : addr:91 ctrl:00 len:01 crc:b7b5
phone  : addr:11 ctrl:02 len:59 crc:d9c7 -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 00 19 51 a0
68 06 07 a0 a5 00 19 5d 03 40 e0 80
phone  : addr:13 ctrl:21 len:01 crc:4e7c
phone  : addr:11 ctrl:20 len:25 crc:15f0 -> 0011 CC
(Call Control) messages :{CC-INFO}    03 7b 2c 05 32 35 37 31 33
phone  : addr:11 ctrl:22 len:11 crc:dbbb -> 0011 CC
(Call Control) messages :{CC-RELEASE}    03 4d e2 00
phone  : addr:13 ctrl:01 len:01 crc:ae3c
```

TopCom Butler 800

```
phone  : addr:91 ctrl:00 len:01 crc:b7b7
phone  : addr:11 ctrl:02 len:8d crc:d8f1 -> 0011 CC
(Call Control) messages :{CC-SETUP}    03 05 05 07 80 a8 00 fd a0 e3
9d 06 07 a0 a5 00 fd a2 9f d8 e0 80 63 0b 44 00 08 00 1a 01 0c 80 82
01 81
station: addr:11 ctrl:01 len:01 crc:b634
station: addr:13 ctrl:00 len:19 crc:5833 -> 0101 MM
(Mobility Management) messages :{CIPHER-REQUEST}    05 4c 19 02 81
98
phone  : addr:6f ctrl:8c len:21 crc:36f2 -> reserved     da 7d bd ed
a2 04 1b 9f
station: addr:16 ctrl:a0 len:5a crc:a1ca -> 0101 MM
(Mobility Management) messages :(null)    c5 ab a5 9f 92 1f bc 30 2d
e7 a9 b9 98 92 ba 3c b4 29 88 05 fe 19
```

8 Message Summaries [2]

Summary of Call Control (CC) messages

Table 15: CC message summary according to [2]

	Direction
Call establishment messages	
{CC-SETUP}	Both
{CC-INFO}	Both
{CC-SETUP-ACK}	F=>P
{CC-CALL-PROC}	F=>P
{CC-ALERTING}	Both
{CC-NOTIFY}	F=>P
{CC-CONNECT}	Both
{CC-CONNECT-ACK}	Both
Call information phase messages	
{CC-INFO}	Both
{CC-SERVICE-CHANGE}	Both
{CC-SERVICE-ACCEPT}	Both
{CC-SERVICE-REJECT}	Both
{IWU-INFO}	Both
Call related supplementary services	
{FACILITY}	Both
{HOLD}	Both
{HOLD-ACK}	Both
{HOLD-REJECT}	Both
{RETRIEVE}	Both
{RETRIEVE-ACK}	Both
{RETRIEVE-REJECT}	Both
Call release messages	
{CC-INFO}	Both
{CC-RELEASE}	Both
{CC-RELEASE-COM}	Both

Summary of Call Independent Supplementary Services (CISS) messages

Table 16: CISS message summary according to [2]

	Direction
CISS establishment messages	
{CISS-REGISTER}	Both
CISS information phase messages	
{FACILITY}	Both
CISS release messages	
{CISS-RELEASE-COM}	Both

Summary of Connection Oriented Message Services (COMS) messages

Table 17: COMS message summary according to [2]

	Direction
COMS establishment messages	
{COMS-SETUP}	Both
{COMS-CONNECT}	Both
{COMS-NOTIFY}	F=>P
COMS information phase messages	
{COMS-INFO}	Both
{COMS-ACK}	Both
COMS release messages	
{COMS-RELEASE}	Both
{COMS-RELEASE-COM}	Both

Summary of ConnectionLess Message Services (CLMS) messages

Table 18: CLMS message summary according to [2]

	Direction
CLMS information phase messages	
{CLMS-VARIABLE}	Both
{CLMS-FIXED}	F=>P
NOTE: {CLMS-FIXED} is a B-Format message.	

Summary of Mobility Management (MM) messages

Table 19: MM message summary according to [2]

	Direction
Identity messages	
{TEMPORARY-IDENTITY-ASSIGN}	F=>P
{TEMPORARY-IDENTITY-ASSIGN-ACK}	P=>F
{TEMPORARY-REJ}	P=>F
{IDENTITY-REQUEST}	F=>P
{IDENTITY-REPLY}	P=>F
Authentication messages	
{AUTHENTICATION-REQUEST}	Both
{AUTHENTICATION-REPLY}	Both
{AUTHENTICATION-REJECT}	Both
Location messages	
{LOCATE-REQUEST}	P=>F
{LOCATE-ACCEPT}	F=>P
{LOCATE-REJECT}	F=>P
{DETACH}	P=>F
Access rights messages	
{ACCESS-RIGHTS-REQUEST}	P=>F
{ACCESS-RIGHTS-ACCEPT}	F=>P
{ACCESS-RIGHTS-REJECT}	F=>P
{ACCESS-RIGTHS-TERMINATE-REQUEST}	Both
{ACCESS-RIGHTS-TERMINATE-ACCEPT}	Both
{ACCESS-RIGHTS-TERMINATE-REJECT}	Both
Key allocation messages	
{KEY-ALLOCATE}	F=>P
Parameter retrieval messages	
{MM-INFO-SUGGEST}	F=>P
{MM-INFO-REQUEST}	P=>F
{MM-INFO-ACCEPT}	F=>P
{MM-INFO-REJECT}	F=>P
Ciphering messages	
{CIPHER-SUGGEST}	P=>F
{CIPHER-REQUEST}	F=>P
{CIPHER-REJECT}	Both
External protocol messages	
{MM-IWU}	Both
Internal protocol information messages	
{MM-NOTIFY}	F=>P

Summary of Link Control Entity (LCE) messages

Table 20: LCE message summary according to [2]

	Direction

LCE establishment messages
{LCE-REQUEST-PAGE}
{LCE-PAGE-RESPONSE}
{LCE-PAGE-REJECT}
	F=>P
	P=>F
	F=>P

NOTE: {LCE-REQUEST-PAGE} is a B-Format message.	

9 S-Format messages functional contents

Table 21: {CC-Setup} according to [2]

Information Element	F to P message	P to F message	Length octets
Protocol Discriminator	M	M	½
Transaction Identifier	M	M	½
Message Type	M	M	1
Portable Identity	M	M	7 to 20
Fixed Identity	M	M	5 to 20
NWK assigned identity	N	O	5 to 20
Basic service	M	M	2
Repeat indicator	O	O	1
IWU attributes	M/N	M/N	6 to 12
Repeat Indicator	O	O	1
Call attributes	O	O	6 to 8
Repeat Indicator	O	O	1
Connection attributes	O	O	7 to 12
Cipher Info	O	O	4 to 5
Connection identity	O	O	>=3
Repeat indicator	O	O	1
Facility	O	O	>=4
Repeat indicator	O	N	1
Progress indicator	O	N	4
"Display"	O	N	>=2
"Keypad"	N	O	>=2
Signal	O	N	2
Feature Activate	N	O	3 to 4
Feature Indicate	O	N	>=4
Network parameter	O	O	>=3
Ext h/o indicator	O	N	3
Terminal capability	N	O	6 to 19
End-to-end compatibility	O	O	3 to 6
Rate parameters	O	O	6 to 9
Transit Delay	O	O	4
Window size	O	O	4 to 10
Calling Party Number	O	O	>=3
Called Party Number	O	O	>=4
Called Party Subaddr	O	O	>=4
Sending Complete	O	O	1
Repeat indicator	O	O	1

Segmented Info	O	O	4
IWU-TO-IWU	O	O	>=4
IWU-PACKET	O	O	>=4
Calling Party Name	O	O	>=2
Codec List	O	O	>=6
Call information	O	O	>=2
Escape to proprietary	O	O	>=4

Table 22: {CC-INFO} according to [2]

Information Element	F to P message	P to F message	Length octets
Protocol Discriminator	M	M	½
Transaction Identifier	M	M	½
Message Type	M	M	1
Location area	N	O	>=3
NWK assigned identity	N	O	5 TO 20
Repeat indicator	O	O	1
Facility	O	O	>=4
Repeat indicator	O	N	1
Progress Indicator	O	N	4
"Display"	O	N	>=2
"Keypad"	O	O	>=2
Signal	O	N	2
Feature Activate	N	O	3 TO 4
Feature Indicate	O	N	>=4
Network Parameter	O	O	>=3
Ext h/o indicator	O	N	3
Calling Party Number	O	O	>=3
Called Party Number	O	O	>=4
Called Party Subaddr	O	O	>=4
Sending Complete	O	O	1
Test Hook Control	O	N	2
Repeat indicator	O	O	1
IWU-TO-IWU	O	O	>=4
IWU-PACKET	O	O	>=4
Calling Party Name	O	O	>=2
Codec List	O	O	>=6
Call information	O	O	>=2
Escape to proprietary	O	O	>=4

Table 23: {CC-CONNECT} according to [2]

Information Element	F to P message	P to F message	Length octets
Protocol Discriminator	M	M	½
Transaction Identifier	M	M	½
Message Type	M	M	1
IWU attributes	O	O	6 to 12
Call attributes	O	O	6 to 8
Connection attributes	O	O	7 to 12
Connection identity	O	O	>=3
Repeat indicator	O	O	1
Facility	O	O	>=4
Repeat indicator	O	N	1
Progress Indicator	O	N	4
“Display”	O	N	>=2
Signal	O	N	2
Feature Indicate	O	N	>=4
Network parameter	O	N	>=3
Ext h/o indicator	O	N	3
Terminal capability	N	O	6 to 19
Transit Delay	O	O	4
Window size	O	O	4 to 10
Repeat indicator	O	O	1
Segmented Info	O	O	4
IWU-TO-IWU	O	O	>=4
IWU-PACKET	O	O	>=4
Codec List	O	O	>=6
Escape to proprietary	O	O	>=4

Table 24: {CC-RELEASE} according to [2]

Information Element	F to P message	P to F message	Length octets
Protocol Discriminator	M	M	½
Transaction Identifier	M	M	½
Message Type	M	M	1
Release Reason	O	O	2
Repeat indicator	O	O	1
Facility	O	O	>=4
Repeat indicator	O	O	1
Progress Indicator	O	O	4
“Display”	O	N	>=2
Feature Indicate	O	N	>=4
Repeat indicator	O	N	1

Segmented Info	O	O	4
IWU-TO-IWU	O	O	>=4
IWU-PACKET	O	O	>=4
Escape to proprietary	O	O	>=4

Table 25: {CC-RELEASE-COM} according to [2]

Information Element	F to P message	P to F message	Length octets
Protocol Discriminator	M	M	½
Transaction Identifier	M	M	½
Message Type	M	M	1
Release Reason	O	O	2
Identity Type	O	N	4
Location area	O	N	>=3
IWU attributes	O	O	6 to 12
Connection attributes	O	O	7 to 12
Repeat indicator	O	O	1
Facility	O	O	>=4
"Display"	O	N	>=2
Feature Indicate	O	N	>=4
Network parameter	O	N	>=3
Repeat indicator	O	O	1
Segmented Info	O	O	4
IWU-TO-IWU	O	O	>=4
IWU-PACKET	O	O	>=4
Escape to proprietary	O	O	>=4

Table 26: {IWU-INFO} according to [2]

Information Element	F to P message	P to F message	Length octets
Protocol Discriminator	M	M	½
Transaction Identifier	M	M	½
Message Type	M	M	1
Portable Identity	O	O	7 to 20
MMS Generic Header	O	O	>=2
MMS Object Header	O	O	>=2
Repeat indicator	O	O	1
MMS Extended Header	O	O	>=2
Repeat indicator	O	O	1
Time-Date	O	O	6 to 10
Repeat indicator	O	O	1
Calling Party Number	O	O	>=3

Repeat indicator	O	O	1
Called Party Number	O	O	>=4
Called Party Subaddr	O	O	>=4
Segmented Info	O	O	4
Alphanumeric	O	O	>=4
Repeat indicator	O	O	1
Segmented Info	O	O	4
IWU-TO-IWU	O	O	>=4
Segmented Info	O	O	4
IWU-PACKET	O	O	>=4
Calling Party Name	O	O	>=2
Codec List	O	O	>=6
Escape to proprietary	O	O	>=4

Table 27: {AUTHENTICATION-REJECT} according to [2]

Information Element	F to P message	P to F message	Length octets
Protocol Discriminator	M	M	½
Transaction Identifier	M	M	½
Message Type	M	M	1
Repeat indicator	O	O	1
AUTH-TYPE	O	O	5 to 6
Reject Reason	O	O	3
Authentication Reject Parameter	N	O	>=2
Repeat indicator	O	O	1
IWU-TO-IWU	O	O	>=4
Escape to proprietary	O	O	>=4

Table 28: {AUTHENTICATION-REQUEST} according to [2]

Information Element	F to P message	P to F message	Length octets
Protocol Discriminator	M	M	½
Transaction Identifier	M	M	½
Message Type	M	M	1
RES	M	M	6
RS	M/O	N	10
ZAP field	N	M/O	3
Service class	N	M/O	3
Key	N	O	>=4
Repeat indicator	O	O	1
IWU-TO-IWU	O	O	>=4
Escape to proprietary	O	O	>=4

Table 29: {AUTHENTICATION-REPLY} according to [2]

Information Element	F to P message	P to F message	Length octets
Protocol Discriminator	M	M	½
Transaction Identifier	M	M	½
Message Type	M	M	1
AUTH-TYPE	M	M	5 to 6
RAND	M	M	10
RES	N	M/O	6
RS	M/O	N	10
Cipher Info	O	O	4 to 5
Repeat indicator	O	O	1
IWU-TO-IWU	O	O	>=4
Escape to proprietary	O	O	>=4

Table 30: {CIPHER-REJECT} according to [2]

Information Element	F to P message	P to F message	Length octets
Protocol Discriminator	M	M	½
Transaction Identifier	M	M	½
Message Type	M	M	1
Repeat indicator	O	O	1
Cipher Info	O	O	4 to 5
Reject Reason	O	O	3
Escape to proprietary	O	O	>=4

Table 31: {CIPHER-REQUEST} according to [2]

Information Element	F to P message	P to F message	Length octets
Protocol Discriminator	M	-	½
Transaction Identifier	M	-	½
Message Type	M	-	1
Cipher Info	M	-	4 to 5
Call Identity	O	-	3 to 4
Connection Identity	O	-	>=3
IWU-TO-IWU	O	-	>=4
Escape to proprietary	O	-	>=4

Table 32: {CIPHER-SUGGEST} according to [2]

Information Element	F to P message	P to F message	Length octets
Protocol Discriminator	-	M	½
Transaction Identifier	-	M	½
Message Type	-	M	1
Cipher Info	-	M	4 to 5
Call Identity	-	O	3 to 4
Connection Identity	-	O	>=3
IWU-TO-IWU	-	O	>=4
Escape to proprietary	-	O	>=4

Table 33: {KEY-ALLOCATE} according to [2]

Information Element	F to P message	P to F message	Length octets
Protocol Discriminator	M	-	½
Transaction Identifier	M	-	½
Message Type	M	-	1
Allocation Type	M	-	4
RAND	M	-	10
RS	M	-	10
Escape to proprietary	O	-	>=4

Table 34: {LOCATE-REQUEST} according to [2]

Information Element	F to P message	P to F message	Length octets
Protocol Discriminator	-	M	½
Transaction Identifier	-	M	½
Message Type	-	M	1
Portable Identity	-	M	7 to 20
Fixed Identity	-	O	5 to 20
Location area	-	O	>=3
NWK assigned identity	-	O	5 to 20
Cipher info	-	O	4 to 5
Setup capability	-	O	4
Terminal capability	-	O	6 to 19
Network parameter	-	O	>=3
Repeat Indicator	-	O	1
Segmented Info	O	O	4
IWU-TO-IWU	-	O	>=4
Model identifier	-	O	5 to 20
Codec List	-	O	>=6
Escape to proprietary	-	O	>=4

Table 35: {TEMPORARY-IDENTITY-ASSIGN-ACK} according to [2]

Information Element	F to P message	P to F message	Length octets
Protocol Discriminator	-	M	½
Transaction Identifier	-	M	½
Message Type	-	M	1
Segmented Info	O	O	4
IWU-TO-IWU	-	O	>=4
Escape to proprietary	-	O	>=4