ETSI TR 103 445 V1.1.1 (2017-07)

Digital Enhanced Cordless Telecommunications (DECT);
DECT security technical review;
Security review and assessment 2017

Reference
DTR/DECT-00311

Keywords
DECT, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights 5
Foreword 5
Modal verbs terminology 5
Executive summary 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 6
3 Definitions, symbols and abbreviations 7
3.1 Definitions 7
3.2 Symbols and abbreviations 7
4 Security overview and assessment 7
4.1 General 7
4.2 Authentication algorithms and procedures 7
4.3 Ciphering algorithms and procedures 7
4.4 Re-keying and early encryption strategy and procedures 8
4.4.1 Re-keying strategy and procedures 8
4.4.2 Early encryption procedures 8
4.5 Operation with Wireless Relay Stations 9
4.6 Key allocation and specific issues during system registration 9
4.7 Software Upgrading Over The Air (SUOTA) 9
4.8 ULE specific security procedures 10
5 Detailed description of changes and enhancements introduced during 2017 DECT security review 10
5.1 General 10
5.2 Changes introduced in the DECT common interface (ETSI EN 300 175) 10
5.2.1 Changes introduced in ETSI EN 300 175-5 (DECT; NWK layer) 10
5.2.1.1 Improvement in {MM-INFO-REQUEST} and in {MM-INFO-SUGEST} 10
5.2.1.2 Inclusion of Default Cipher Algorithm in IE << Auth type >> 12
5.2.1.3 Improvements in <<KEY>> IE 14
5.2.1.4 Review of the Parameter retrieval procedure 15
5.2.2 Changes introduced in ETSI EN 300 175-7 (DECT; security) 17
5.2.2.1 New description for Transfer of Cipher Keys to Wireless Relay Stations (WRS) 17
5.2.2.2 New procedure for Cipher key retrieval. PT initiated 19
5.2.2.3 New MAC layer procedure for re-keying 22
5.2.2.4 New description of the re-keying procedure and new aging model to control operation with repeaters 25
5.2.2.5 New description of the early encryption procedure 27
5.2.2.6 New annex with security timers 28
5.3 Changes introduced in the Generic Access Profile (ETSI EN 300 444) 30
5.3.1 New description of the re-keying procedure and new aging model to control operation with repeaters 30
5.3.2 New description of the early encryption procedure 31
5.3.3 New clause with additional procedures for devices supporting DSC2 32
5.4 Changes proposed for the WRS standard (ETSI EN 300 700) 33
5.4.1 Overview 33
5.4.2 Changes in Bearer handover 33
5.4.2.1 General principles and open issues 33
5.4.2.2 Solution to Bearer handover requiring cipher algorithm switching: technical approach 1 34
5.4.2.3 Solution to Bearer handover requiring cipher algorithm switching: alternative technical approach 2 37
5.4.2.4 Provision of lower DefCKs "just-in-time" 40
5.5 Other recommendations for implementation of security features 40
5.5.1 Guidelines for Implementation of the key-aging model related to the re-keying procedure 40
5.5.1.1 Introduction 40

5.5.1.2 Implementation of the re-keying timers before the addition of the aging-model 41
5.5.1.3 Additional procedures required by the aging model 41
5.5.1.4 Additional implementation guidelines 41

History 42

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Digital Enhanced Cordless Telecommunications (DECT).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document documents the review of DECT security procedures done during years 2016 and 2017. It contains two parts: a security overview and assessment on DECT security techniques, addressed to the general public, and a detailed description of the main security improvements introduced in the revisions of the DECT common interface (ETSI EN 300 175 [i.1] to [i.8]) and Generic Access Profile (ETSI EN 300 444 [i.9]) released by TC DECT during year 2017.

The present document is primary addressed to TC DECT and DECT industry communities and as well, to other participants from new industry sectors that may be considering using DECT technology for new applications.

1 Scope

The scope of the present document is documenting the review of DECT security procedures done during year 2017. The present document is structured as two different parts:

- A security overview and assessment, addressed to the general public, which presents a general description of the different DECT security elements and, for each of them, an assessment with specific recommendations to implementers, including identification of possible threats (when applicable). This part of the study is covered by clause 4 of the present document.
- A detailed description of the improvements in security procedures introduced in the revisions of the DECT common interface (ETSI EN 300 175 series [i.1] to [i.8]) and the Generic Access Profile (ETSI EN 300 444 [i.9]) released in year 2017 (version 2.7.1 of ETSI EN 300 175 [i.1] to [i.8]) and version 2.5.1 of Generic Access Profile ETSI EN 300 444 [i.9]). This part of the study is covered by clause 5 of the present document and is mostly addressed to DECT manufacturers and TC DECT participants.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI EN 300 175-1: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 1: Overview".

[i.2] ETSI EN 300 175-2: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 2: Physical Layer (PHL)".

[i.3] ETSI EN 300 175-3: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 3: Medium Access Control (MAC) layer".

[i.4] ETSI EN 300 175-4: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 4: Data Link Control (DLC) layer".

[i.5] ETSI EN 300 175-5: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 5: Network (NWK) layer".

[i.6] ETSI EN 300 175-6: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 6: Identities and addressing".

[i.7] ETSI EN 300 175-7: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 7: Security features".

[i.8] ETSI EN 300 175-8: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 8: Speech and audio coding and transmission".

[i.9] ETSI EN 300 444: "Digital Enhanced Cordless Telecommunications (DECT); Generic Access Profile (GAP)".

[i.10] ETSI EN 300 700: "Digital Enhanced Cordless Telecommunications (DECT); Wireless Relay Station (WRS)".

[i.11] ETSI TS 102 939-1: "Digital Enhanced Cordless Telecommunications (DECT); Ultra Low Energy (ULE); Machine to Machine Communications; Part 1: Home Automation Network (phase 1)".

[i.12] ETSI TS 102 939-2: "Digital Enhanced Cordless Telecommunications (DECT); Ultra Low Energy (ULE); Machine to Machine Communications; Part 2: Home Automation Network (phase 2)".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI EN 300 175-1 [i.1] and in ETSI EN 300 175-7 [i.7] apply.

3.2 Symbols and abbreviations

For the purposes of the present document, the symbols and abbreviations given in ETSI EN 300 175-1 [i.1] and in ETSI EN 300 175-7 [i.7] apply.

4 Security overview and assessment

4.1 General

Clause 4 of the present document presents a general overview of the different DECT security elements. For each of them, it provides an assessment with specific recommendations to implementers, including identification of possible threats (when applicable).

4.2 Authentication algorithms and procedures

The authentication algorithm DSAA2, based on AES-128, and the associated authentication procedures are considered secure and are recommended for any new DECT product.

The processing time for a brute force attack to the DSAA2, with current computer means, is estimated in thousands of millions of years. Therefore, a change in previous assessment is not expected in the next years, unless there is a significant change in cryptography techniques or in availability of quantum computing.

The old algorithm DSAA is considered obsolete and should not be used in any new DECT product.

The implementation of DSAA2 can be done by software and does not introduce any special processing or other extra cost requirement. There are multiple suppliers able to provide software implementations according to OEM specifications. Therefore, the present document does not see any justification for not implementing DSAA2 in new DECT products.

4.3 Ciphering algorithms and procedures

The encryption algorithm DSC2, based on AES-128, and associated procedures, are considered secure and are the primary recommendation for any new DECT product.

The processing time for a brute force attack to the DSC2, with current computer means, is estimated in thousands of millions of years. Therefore, a change in previous assessment is not expected in the next years, unless there is a significant change in cryptography techniques or in availability of quantum computing.

The old algorithm DSC is considered weak with a processing time for a brute force attack in the range of minutes to hours, depending on computer means. This issue can be compensated, to some extent, with the introduction of the "re-keying" feature (see clause 4.4), which has the goal of adding additional processing requirements to a possible brute force attack.

However, in the case of the encryption, the implementation of DSC2 introduces additional requirements of implementation by hardware (recommended) or additional processing power if implemented by software (DSP). Therefore, the recommendation depends on the type of product:

- For security critical products, the use of the DSC2 cipher algorithm is recommended.
- For general low cost voice products, the use of DSC combined with enhanced security feature "re-keying" is considered enough for preventing criminal phone tapping in consumer market under most usual scenarios.

NOTE: However, it should be expected that this second assessment may change in further reviews due to the continuous increase in computer processing availability.

4.4 Re-keying and early encryption strategy and procedures

4.4.1 Re-keying strategy and procedures

The Re-keying is a mechanism consisting of the periodic and regular change of the Cipher Key of an ongoing call, service call, or virtual connection in order to improve the security. The fundamental aim of the re-keying is to increase the computer resources needed for a brute-force attack to the cipher and/or the authentication algorithms. The re-keying strategy achieves its objectives if the time required by a potential hacker to break the algorithms with its available computer resources is significantly larger than the re-keying timer.

The re-keying is fundamentally intended to protect the relatively weak cipher algorithm DSC. The protection provided by the re-keying is not comparable to the protection provided by the use of stronger ciphers (such as DSC2), and this should be the primary route for security concerned applications. Nevertheless, it is believed that DSC combined with the re-keying strategy is effective against attacks attempting real-time phone tapping of DECT communications performed by regular hackers with their expected computer resources.

Some enhancements and clarification in the "re-keying" procedures have been introduced in version 2.7.1 of the DECT common interface (ETSI EN 300 175 series [i.1] to [i.8]) and in version 2.5.1 of the Generic Access Profile (ETSI EN 300 444 [i.9]). Refer to clause 5 for detailed description of the changes.

4.4.2 Early encryption procedures

The early encryption is a combined MAC layer/NWK layer mechanism intended to ensure the fast activation of encryption at the beginning of any call, including service calls and virtual calls. To achieve that, a special type of Cipher Key called Default Cipher Keys (DefCK) are generated and stored in advance of their intended use by means of a variation of the Authentication procedure. The encryption itself is designed to be activated using only MAC layer messages. This allows the quick enabling of the encryption at the beginning of a call, encrypting even the call CC setup messages that may contain the called party number.

Some enhancements and clarification in the "early encryption" procedures have been introduced in version 2.7.1 of the DECT common interface (ETSI EN 300 175 series [i.1] to [i.8]) and in version 2.5.1 of the Generic Access Profile (ETSI EN 300 444 [i.9]). Refer to clause 5 for detailed description of the changes.

4.5 Operation with Wireless Relay Stations

Several previous flaws identified in the operation with repeaters have been corrected in version 2.7.1 of the DECT common interface (ETSI EN 300 175 series [i.1] to [i.8]). These flaws impacted mostly the operation of the features "early-encryption" and "re-keying". Previously, such features cannot be properly implemented in all segments of systems with repeaters. After version 2.7.1, it is believed that there are no special security issues for operation in systems with repeaters or even with chains of repeaters. Therefore, all security procedures may be properly used in such systems without reduction in security.

It should be noted, however, that the implementation of security procedures in systems with repeaters will increase the number of operations and processing load in the system, and therefore, may cause specific implementation issues. This is particularly relevant for the Fixed Part. It is advised that vendors of DECT systems claiming supporting of repeaters should perform the proper simulations and testing to ensure that they may address the processing load required by the supported scenarios.

4.6 Key allocation and specific issues during system registration

The procedures for key allocation used during initial stages of device pairing (PP registration in a FP) have been analysed and it has been concluded that the security procedures themselves are correct. However, there is an inherent security limitation consequence of the reduced number of bits used for the initial Authentication Codes (PIN codes) that are introduced by the user during pairing. There is a compromise between security and usability and usability has been prioritized by most vendors.

"Security procedures are correct" means that, if the proper algorithm is used (DSAA2) and the proper length of key is used (AC equivalent to 128 bits) then, the key allocation procedures are inherently secure (as secure as the standard authentication).

Obviously, if by practicality reasons the AC introduced by the user (usually a PIN code) is restricted to 4 digits, or in some cases, it is left as a default value (0000, 1234, etc.), and a hacker is observing the key allocation process, then the resulting security is compromised. The hacker may recover the UAK just by trying all possibilities of the "PIN" and analysing with of them produce suitable authentication responses and cipher keys.

For systems with strong security requirements the following alternatives are proposed:

- Introduce the UAK in the FP avoiding the key allocation procedure.
- Use 128 bit PIN introduced by the user in one (or in both peers) during the pairing process. Such 128 PIN (AC) bit can be coded as a stream of 32 Hexadecimal characters.
- Use other non-DECT mechanism for automatically exchanging the UAK or the AC (PIN) between peers. Such mechanisms may be optical (IR) or wired (i.e. via the PP power connector).
- Be sure that the pairing process is done in a radio protected or hacker-free environment (Faraday cage assumption).

It should be noted that due to how the procedure is designed, the security limitation happens only at the key allocation procedure. After this procedure the keys are automatically generated to 128 bit lengths. A potential hacker has to observe the initial key allocation procedure to take any advantage of it. If this is not the case, the fact that the keys were initially generated using the key allocation procedure does not introduce any security reduction.

4.7 Software Upgrading Over The Air (SUOTA)

The SUOTA procedure may be other mechanism to compromise the security. If a hacker may insert its own malicious software in a DECT system, then it can bypass any security. Therefore, mutual authentications between SUOTA source and DECT device are essential.

The transport of SUOTA over the DECT link is secure. The mandatory encryption performs a mutual authentication role between FP and PP.

However, it is not possible to guarantee the security of the connections between the FP and the SUOTA source. These connections are typically implemented via the Internet. In most cases, the device manufacturer is the legitimate SUOTA source. Specific proprietary security solutions should be implemented by the device vendor in order to ensure that the SUOTA mechanism cannot be compromised at the Internet paths and that a hacker cannot use the mechanism to introduce malicious software in a DECT system.

4.8 ULE specific security procedures

The security procedures used in ULE (DECT Ultra Low Energy, see [i.11] and [i.12]) are considered correct and fundamentally secure with no specifics flaws:

The CCM encryption used by ULE is based on AES-128 and is therefore secure (as secure as DSAA2 and DSC2).

Procedures for service channels (encryption of Service call parameters and data in ancillary channels transported by service calls) share the same security concerns of general DECT. Basically, the security depends on the authentication and encryption procedures. Optimal security is achieved by using DSAA2 and DSC2.

Encryption of multicast channel is based on CCM and is therefore secure. However, the keys themselves are transported via the service channel (encrypted by DSC or DSC2). Therefore the multicast protection inherits the security level of general DECT. The best results are achieved by using DSC2.

The concerns on Key allocation and specific issues during system registration are also applicable to ULE. Therefore, the same recommendations for security critical products are given.

Due to the expected specification of ULE PPs (i.e. sensors without any keyboard), the strategy of supplying the device with a "label" including its UAK and introducing such number in the FP (by any human or automatic mechanism) seems to be correct and advisable from security perspective. Usability aspects have to be analysed. Note that the "label" with the "key" should be detached from the device and stored separately.

5 Detailed description of changes and enhancements introduced during 2017 DECT security review

5.1 General

Clause 5 of the present document describes the main changes related to security introduced in the revision of DECT common interface (ETSI EN 300 175 series [i.1] to [i.8]) and Generic Access Profile (ETSI EN 300 444 [i.9]) of year 2017 (release 2.7.1 of ETSI EN 300 175 [i.1] to [i.8]) and release 2.5.1 of Generic Access Profile ETSI EN 300 444 [i.9]). It also documents the proposed changes to be introduced in the next release of DECT: Wireless Relay Station (ETSI EN 300 700 [i.10]) specification.

5.2 Changes introduced in the DECT common interface (ETSI EN 300 175)

5.2.1 Changes introduced in ETSI EN 300 175-5 (DECT; NWK layer)

5.2.1.1 Improvement in {MM-INFO-REQUEST} and in {MM-INFO-SUGEST}

The MM messages {MM-INFO-REQUEST} and in {MM-INFO-SUGEST} have been updated to include the transport of the <<KEY>> IE in {MM-INFO-REQUEST}. This is required to properly handle the request of Default Cipher Keys.

"6.3.6.22 {MM-INFO-REQUEST}

This message is sent by the PT to the FT to request information (e.g. regarding external handover) to be sent in a subsequent {MM-INFO-ACCEPT} message.

It is also used to request the exchange of the encryption key and/or the CCM sequence number for multicast channels in the PT initiated multicast encryption parameter retrieval procedure (see ETSI EN 300 175-7 [i.7], clause 6.3.8).

Table 59: {MM-INFO-REQUEST}

Message Type	Format	Directions
{MM-INFO-REQUEST}	S	P=>F

Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	-	M	1/2
Transaction Identifier	7.3	-	M	1/2
Message Type	7.4	-	M	1
Info type	7.7.20	-	M	≥ 3
Portable identity	7.7.30	-	O	7 to 20
Repeat indicator	7.6.3	-	O	1
Fixed identity	7.7.18	-	O	5 to 20
KEY (see note 1)	7.7.24	-	O	3 to 5
Location area	7.7.25	-	O	≥ 3
NWK assigned identity	7.7.28	-	O	5 to 20
Call Identity	7.7.6	-	O	3 to 4
Network parameter	7.7.29	-	O	≥ 3
Segmented info (see note 2)	7.7.37	O	O	4
IWU-TO-IWU	7.7.23	-	O	≥ 4
Escape to proprietary	7.7.45	-	O	≥ 4

M = Mandatory.
O = Optional.
- = Not applicable.

NOTE 1: <<KEY>> when used in this message shall only carry the <Key type> and optionally the Default Cipher Key index. (L) shall be coded to 1 if only carries the <Key type> and to 3 if it also carries a Default Cipher Key index.

NOTE 2: The <<Segmented Info>> information element shall be included in front of the <<IWU-TO-IWU>> information element whenever the <<IWU-TO-IWU>> is segmented over a number of consecutive messages.

6.3.6.23 {MM-INFO-SUGGEST}

This message is sent by the FT to provide information to the PT or to suggest an action to the PT, e.g. to perform location updating or access rights modification or an external handover.

It is also used to exchange the encryption key for CRFPs (see ETSI EN 300 175-7 [i.7], clause 7.3) and to exchange the encryption key and the CCM sequence number for multicast channels (see ETSI EN 300 175-7 [i.7], clause 6.3.8).

Table 60: {MM-INFO-SUGGEST}

Message Type	Format	Directions
{MM-INFO-SUGGEST}	S	F=>P

Information Element	Clause	F to P message	P to F message	Length octets
Protocol Discriminator	7.2	M	-	1/2
Transaction Identifier	7.3	M	-	1/2
Message Type	7.4	M	-	1
Info type	7.7.20	M	-	≥ 3
Fixed identity	7.7.18	O	-	5 to 20
Location area	7.7.25	O	-	≥ 3
NWK assigned identity	7.7.28	O	-	5 to 20
RS	7.7.36	O	-	8
Call Identity	7.7.6	O	-	3 to 4
Network parameter	7.7.29	O	-	≥ 3
Ext h/o indicator	7.7.51	O	-	3
KEY	7.7.24	O	-	≥ 4
Setup capability	7.7.40	O	-	4
Segmented info (see note)	7.7.37	O	O	4
IWU-TO-IWU	7.7.23	O	-	≥ 4
Escape to proprietary	7.7.45	O	-	≥ 4
M = Mandatory. O = Optional. - = Not applicable.				
NOTE 1: The <<Segmented Info>> information element shall be included in front of the <<IWU-TO-IWU>> information element whenever the <<IWU-TO-IWU>> is segmented over a number of consecutive messages. NOTE 2: The <<RS>> information element may be used to exchange the CCM sequence number for multicast channels (see ETSI EN 300 175-7 [i.7], clauses 6.6.2.7 and 6.3.8). NOTE 3: <<KEY>> when used in this message shall carry the <Key type> and the <Key>. If the key is a Default Cipher Key, <Key> shall include two additional bytes coding the Default Cipher Key index (see clause 7.7.24).				

"

5.2.1.2 Inclusion of Default Cipher Algorithm in IE << Auth type >>

This change allows the inclusion of the Default Cipher Algorithm in IE << Auth type >>. This is required to properly set the algorithm associated to a Default Cipher Key.

"7.7.4 Auth type

The purpose of the <<AUTH-TYPE>> information element is to define the authentication algorithm and the authentication key. In addition it may be used to send a ZAP increment command and/or to indicate if the cipher key shall be updated and/or sent.

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< AUTH-TYPE >>							1
	Length of Contents (L)								2
	Authentication algorithm identifier								3
	Proprietary algorithm identifier								3a
	Authentication key type				Authentication key number				4
	INC	DEF	TXC	UPC	Cipher key number				5
	Default Cipher Key Index (high byte)								5a
	Default Cipher Key Index (low byte)								5b
	reserved						Default Cipher Key algorithm		5c (optional)

Figure 28: AUTH-TYPE information element

Authentication algorithm identifier coding (octet 3):

Bits	8 7 6 5 4 3 2 1	Meaning
	0 0 0 0 0 0 0 1	DECT standard authentication algorithm (DSAA)
	0 0 0 0 0 0 1 0	DECT standard authentication algorithm #2 (DSAA2)
	0 1 0 0 0 0 0 0	GSM authentication algorithm
	0 0 1 0 0 0 0 0	UMTS authentication algorithm
	0 1 1 1 1 1 1 1	Escape to proprietary algorithm identifier

All other values reserved.

Proprietary algorithm identifier (octet 3a):

This octet shall only be sent, when the authentication algorithm identifier coding (octet 3) indicates "escape to proprietary algorithm identifier".

Authentication Key (AK) type coding (octet 4):

Bits	8 7 6 5	Meaning
	0 0 0 1	User authentication key
	0 0 1 1	User personal identity
	0 1 0 0	Authentication code

All other values reserved.

NOTE 1: The User Personal Identity (UPI) is always used in combination with a User Authentication Key (UAK), therefore the key type UPI identifies always a pair of keys (UPI plus UAK).

Authentication Key (AK) number (octet 4):

Bits	4 3 2 1	Meaning
	Contains the binary coded number of the selected Authentication Key (AK) If the MSB (bit 4) is set to 0, then the key shall be related to the active IPUI If the MSB (bit 4) is set to 1, then the key shall be related to the active IPUI/PARK pair	

INC bit coding (octet 5):

Bits	8	Meaning
	0	Leave value of the ZAP field unchanged
	1	Increment value of the ZAP field

DEF bit coding (octet 5):

Bits	7	Meaning
	0	generated derived cipher key shall not be used as default cipher key for early encryption
	1	generated derived cipher key shall only be used as default cipher key stored under the given default cipher key index for early encryption (octet 5a, b, c)

TXC bit coding (octet 5):

Bits	6	Meaning
	0	Do not include the derived cipher key in the {AUTHENTICATION-REPLY} message
	1	Include the derived cipher key in the {AUTHENTICATION-REPLY} message

UPC bit coding (octet 5):

Bits	5	Meaning
	0	Do not store the derived cipher key
	1	Store the derived cipher key under the given cipher key number

Cipher key number (octet 5):

Bits 4 3 2 1 Meaning
If the UPC bit is set to 1, then this field contains the binary coded number which is given to the newly derived Cipher key
If the MSB (bit 4) is set to 0, then the key shall be related to the active IPUI
If the MSB (bit 4) is set to 1, then the key shall be related to the active IPUI/PARK pair
If the UPC bit is set to 0, then this field is not applicable and should be set to 0

NOTE 2: A derived cipher key is always related to the active IPUI and can be uniquely identified by the following three parameters, IPUI, cipher key type "derived" and cipher key number. A derived cipher key is not related to any specific cipher algorithm.

Default cipher key index (octet 5a,b):

These octets shall be sent if and only if the DEF bit coding in octet 5 is set, indicating that the generated derived cipher key shall be used as default cipher key for early encryption. When sent, these octets shall contain the index of the default cipher key.

NOTE 3: Two octets are used for this purpose, in order to allow that even in office/public environments each PP has a default cipher key with a system wide unique index.

The index shall be system wide unique so that the related MAC procedures can rely on this uniqueness to identify the requested default cipher key index.

octet 5c (optional):

This octet is optional amd may only be used if the DEF bit coding in octet 5 is set.

This octet, when used, carries the following extended information to the Default Cipher key index:

- Default cipher key algorithm (2 bits in bit position 2-1)
- Bits 3-8 are reserved for further standardization. They shall be coded to '0'.

Default cipher key algorithm (2 bits in bit position 2-1): These two bits specify the cipher algorithm that shall be used when Default encryption with the generated Default Cipher Key (with index carried in octets 5a, 5b) is requested.

The coding of these bits is as following:

Bits	**8 7 6 5 4 3 2 1**	**Meaning**
	x x x x x x 0 0	DSC
	x x x x x x 0 1	DSC2
	all other values	reserved

If the octet 5c is omitted, then it shall be understood that the algorithm to be used with the generated Default cipher key is DSC.

NOTE 4: These bits impact only to the generated Default Cipher Key whose index is carried in octets 5a and 5b. Different algorithms may be used with different default Cipher keys. This octet should not be used with and does not have any impact on Derived Cipher Keys (DCK)."

5.2.1.3 Improvements in <<KEY>> IE

The IE <<KEY>> has been updated to include two important information parameters: identification of if the key is a Default Cipher Key and identification of the Cipher Algorithm.

"7.7.24 Key

The purpose of the <<KEY>> information element is to transfer a key. When sending the <<KEY>> information element a ciphered connection shall be used.

This IE is used to exchange the encryption key for CRFPs (see ETSI EN 300 175-7 [i.7], clause 7.3) and to exchange the encryption key for CCM encryption of multicast channels (see ETSI EN 300 175-7 [i.7], clause 6.3.8).

Bit:	8	7	6	5	4	3	2	1	Octet:
	0	<< KEY >>							1
	Length of Contents (L)								2
	Key type								3
									4
	Key								
									L+2

Figure 54: KEY information element

Key type coding (octet 3):

Bits	8 7 6 5 4 3 2 1	Meaning
	1 0 0 1 0 0 0 0	Derived Cipher Key (DCK) for DSC
	1 0 0 1 0 0 0 1	Derived Cipher Key (DCK) for DSC2
	1 0 0 1 0 0 1 0	Cipher Key for CCM encryption of multicast channels
	1 0 0 1 0 1 0 0	Default Cipher Key (DefCK) for DSC
	1 0 0 1 0 1 0 1	Default Cipher Key (DefCK) for DSC2
	All other values reserved.	

Key data field: the key data field contains the numeric value of the key. The length of the key data field is (L-1) octets as defined by the length indicator (octet 2). For a multi-octet field, the order of bit values progressively decreases as the octet number increases.

NOTE: A key K1 with L1 > N bits can be mapped into a key K with N bits by taking the lower N bits of K1. A key K2 with L2 < N bits can be mapped into a key K with N bits by using: K(i) = K2 (i modulo L2), $0 \leq i \leq N-1$.

In the specific case of Key type code specifying a Default Cipher Key (code 10010100'B and 10010101'B) the Key data field is extended by 2 octets to include the Default Cipher Key Index that it is associated with the key. These 2 octets are appended to the end of the key, and the whole Key data field is encoded as follows:

octet 3 to octet L: key data (actual key length is L - 2)
octet L+1: Default Cipher Key Index (high byte)
octet L+2: Default Cipher Key Index (low byte)

In certain cases (message {MM-INFO-REQUEST}) , the IE <<KEY>>, when included, only carries the <key type> and may also include a Default Cipher key index. No real Key is transported by the message."

5.2.1.4 Review of the Parameter retrieval procedure

The Parameter retrieval procedure (clause 13.7) has been updated to include the current Key allocation and retrieval procedures. Such procedures are used with Wireless Relay Stations.

"13.7 Parameter retrieval procedure

This procedure is used to exchange information between the FT and the PT. This information could be necessary for example for an external handover, where after having obtained this information the actual handover is done by the interworking unit via the call control entity and is not described in this clause. The procedure can be initiated by the FT or by the PT.

Procedure for parameter retrieval initiated by the FT (one way procedure):

Upon receiving a MM_INFO-req primitive the FT initiates the procedure by sending a {MM-INFO-SUGGEST} message. This message contains the <<INFO-TYPE>> information element which defines the suggested action. The coding "locate suggest" is used in the case of the location updating procedure which is described in clause 13.4.3. One of the codings "external handover parameters", "location area", "hand over reference", "external handover candidate", "synchronized external handover candidate" and "non synchronized external handover candidate" is used for the external handover procedure which is described in clause 15.7.

The {MM-INFO-SUGGEST} message can optionally also contain the following information elements:

<<FIXED-IDENTITY>>	with the ARI of a proposed new FT;
<<LOCATION-AREA>>	with the identification of the current location area (extended location information);
<<SETUP-CAPABILITY>>	communicating some dynamic parameters;
<<NWK-ASSIGNED-IDENTITY>>	with a network assigned identity;
<<NETWORK-Parameter>>	with the value of a handover reference;
<<IWU-TO-IWU>>	with application specific information.
<<KEY>>	with encryption specific information.

Upon receipt of the {MM-INFO-SUGGEST} message the PT issues this information directly to the IWU by issuing a MM_INFO-ind primitive.

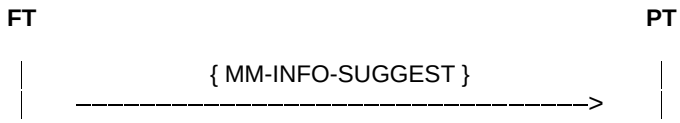

Figure 123: FT parameter retrieval procedure (one way)

Procedure for parameter retrieval initiated by the FT (two way procedure):

In certain cases a two message procedure may be used. The two way procedure allows sending confirmation to the FT of the reception and acceptance of the information. A rejection message may also be used as reply.

The sequence shall be as follows:

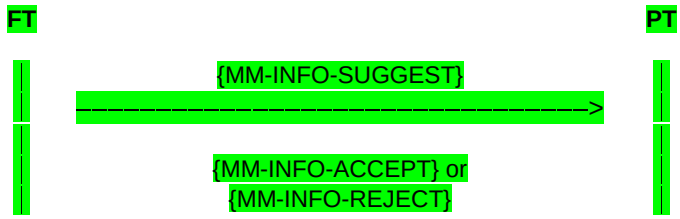

Figure 123a: FT parameter retrieval procedure (two way)

NOTE 1: A variation of the FT parameter retrieval two-way procedure is used, for instance, for transferring of keys for the CCM encryption of multicast channels (see ETSI EN 300 175-7 [i.7], clause 6.3.8).

Procedure for parameter retrieval initiated by the PT:

Upon receiving a MM_INFO-req primitive the PT initiates the procedure by sending a {MM-INFO-REQUEST} message, which contains an <<INFO-TYPE>> information element which defines the requested parameter(s) and can contain a <<PORTABLE-IDENTITY>> information element with the IPUI or individual assigned TPUI, an optional <<FIXED-IDENTITY>> information element containing ARI or PARKs identifying candidate FPs, an optional <<LOCATION-AREA>> information element with a new location area identification (extended location information), an optional <<NWK-ASSIGNED-IDENTITY>> information element with a network assigned identity, an optional <<NETWORK-Parameter>> information element with the value of a handover reference and an optional <<IWU-TO-IWU>> information element.

Upon receiving a {MM-INFO-REQUEST} message the FT issues a MM_INFO-ind primitive. Upon receiving a MM_INFO-res primitive indicating "accept" the FT shall respond by sending a {MM-INFO-ACCEPT} or a {MM-INFO-SUGGEST} message, which can include an <<INFO-TYPE>> information element which gives some more information about specific requested parameter(s), an optional <<FIXED-IDENTITY>> information element with the ARI of a new FT, an optional <<LOCATION-AREA>> information element with the current location area identification (extended location information), an optional <<NWK-ASSIGNED-IDENTITY>> information element with a network assigned identity, an optional <<NETWORK-Parameter>> information element with the value of a handover reference and an optional <<IWU-TO-IWU>> information element. Upon receiving a MM_INFO-res primitive indicating "reject" the FT shall respond by sending a {MM-INFO-REJECT} message containing the optional <<REJECT-REASON>> information element.

Upon receiving a {MM-INFO-ACCEPT} or a {MM-INFO-SUGGEST} message or a {MM-INFO-REJECT} message the PT issues a MM_INFO-cfm primitive.

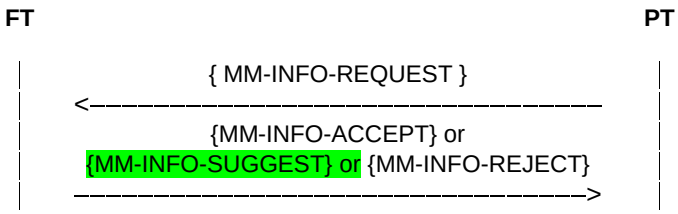

Figure 124: PT parameter retrieval procedure

NOTE 2: The inclusion of {MM-INFO-SUGGEST} as response is used in some security procedures. See for instance ETSI EN 300 175-7 [i.7], clause 6.3.8.3.

The parameter retrieval procedure is supervised by the timer <MM_info.1> in the PT. At the first expiry of the timer <MM_info.1> the PT should retransmit the {MM-INFO-REQUEST} message. If the timer <MM_info.1> expires a second time, the PT shall abort the procedure and release the transaction. Timer <MM_info.1> may be restarted by the FT at any time by sending a <<TIMER-RESTART>> information element in a {MM-NOTIFY} message.

NOTE 3: Restarting of the timer may be required if the Parameter retrieval procedure involves communication with external networks or protocols before accepting or rejecting it."

5.2.2 Changes introduced in ETSI EN 300 175-7 (DECT; security)

5.2.2.1 New description for Transfer of Cipher Keys to Wireless Relay Stations (WRS)

A New description for Transfer of Cipher Keys to Wireless Relay Stations (WRS), FT initiated, is provided:

"6.3.9 Transfer of Cipher Keys to Wireless Relay Stations (WRS)

6.3.9.1 General

The encryption model used by CRFP type Wireless Relay Stations (WRS) (see ETSI EN 300 700 [i.10]) requires the transfer to the WRS of the encryption key used by the lower segment (see ETSI EN 300 700 [i.10], clause 4.4). Two procedures are defined to allow this transfer, FT initiated and WRS initiated procedures. FT initiated is assumed to be used in most cases. WRS initiated may be used in special cases when a PP (or another WRS) initiates a connection towards a WRS, and this last does not have a valid cipher key for the operation.

Both procedures may also be used to transfer Derived Cipher Keys (DCK) and Default Cipher Keys (DefCK).

Both procedures shall be initiated in local mode to the concerned WRS (with "local mode" meaning as defined in ETSI EN 300 700 [i.10], clause 7.4.17.1.2 and concerned WRS" meaning the WRS whose key is to be transferred). Before initiating the procedure, the initiating node shall check that the link between the FP and the concerned WRS is in already in local mode, or otherwise, it shall initiate the transfer to local mode as defined in ETSI EN 300 700 [i.10], clause 7.4.17.2.

Only CRFP type WRSs are supported. Therefore the terms "WRS" and "CRFP" are synonymous for the purposes of clause 6.3.9.

6.3.9.2 Security considerations

In order not to undermine the security protection given by the present document the following provision applies:

The link where a cipher key is exchanged shall be encrypted. This encryption shall be done:

- If the transferred key is a DCK, by a DCK.
- If the transferred key is a DefCK, by either a DCK or by another DefCK.

If the security procedure "re-keying" (see clause 6.3.5) is used, then the provisions regarding the aging of the cipher keys described in clause 6.7.2.3.2 and the calculation of the initial age of the transferred key shall be observed.

6.3.9.3 Indication of cipher key. FT initiated procedure

The procedure FT initiated is named "Indication of cipher key" procedure. This procedure may be initiated by the FP as soon as it knows that a WRS needs a cipher key (DCK or DefCK) for a given node.

NOTE 1: This will be the normal key transfer procedure and should be used when the FP updated a key (DCK or DefCK) into a PP (or in another WRS) by means of an authentication procedure and knows that such PP (or WRS) is connected to the FP by means of (an) intermediate WRS(s).

Procedure is FT initiated.

The sequence shall be as follows:

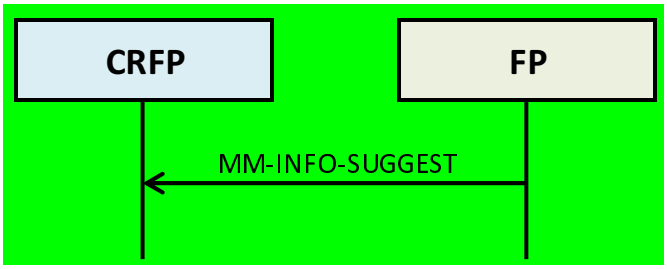

Figure 6.1e: FT initiated Indication of WRS cipher key procedure

NOTE 2: This procedure is a particular case of the "Parameter retrieval procedure" defined in ETSI EN 300 175-5 [i.5], clause 13.7. The provisions given in ETSI EN 300 175-5 [i.5] regarding primitives and timers can be observed as design guidelines.

The following parameters shall be used in the {MM-INFO-SUGGEST} message.

Table 6.6a: Values used within the {MM-INFO-SUGGEST} message

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<Info-type>>			
	<ext>	0	
	<Parameter type>	0100010'B	CK transfer
<<KEY>>			
	<Key type>	10010000 10010001 10010100 10010101	DCK for DSC DCK for DSC2 Default Cipher Key for DSC Default Cipher Key for DSC2
	<Key>	Any	In the case of Default Cipher Key (<Key type> 10010100'B or 10010101'B) the <Key> data field also includes the associated Default Cipher Key Index in 2 byte format. See ETSI EN 300 175-5 [i.5], clause 7.7.24.

The <Key type> field indicates the ciphering algorithm to be used with the transferred key (either DSC or DSC2). This is important because the WRS does not know what ciphering algorithms are supported by the PT or indeed which ciphering algorithm the FP will select in its {CIPHER-REQUEST}. When using the key, the WRS shall use the specified ciphering algorithm (see clause 7.7.6).

Multiple <<KEY>> Information Elements may be included in the {MM-INFO-SUGGEST} message by utilizing the repeat mechanism (see ETSI EN 300 175-5 [i.5], clause 7.5.6), i.e. by the inclusion of the <<REPEAT-INDICATOR>> specifying coding 1 "non-prioritized list" prior to the list of <<KEY>> Information Elements. This allows multiple keys to be transferred in the same message.

NOTE 3: This mechanism may be used for transferring to the same WRS a DCK plus a DefCK, or for transferring multiple DefCK.

When multiple <<KEY>> Information Elements are used, care should be taken to ensure that the maximum supported message length is not exceeded. If necessary, more cipher keys can be transferred by sending additional {MM-INFO-SUGGEST} messages."

5.2.2.2 New procedure for Cipher key retrieval. PT initiated

A new procedure for Cipher key retrieval, PT initiated, has been added to the standard:

"6.3.9.4 Cipher key retrieval procedure. PT initiated

The PT initiated procedure may be used when a WRS has not received or "misses" a cipher key that it needs for a security procedure. This could happen, for instance, by failure of the previous FT initiated procedure (which is one-way and not acknowledged).

NOTE 1: It is foreseen that the execution route may include an interleaved PT authentication procedure in order to check the legitimacy of the requesting PT. Messages for both MM processes are different and should not be any ambiguity.

Procedure is PT initiated.

The sequence shall be as follows:

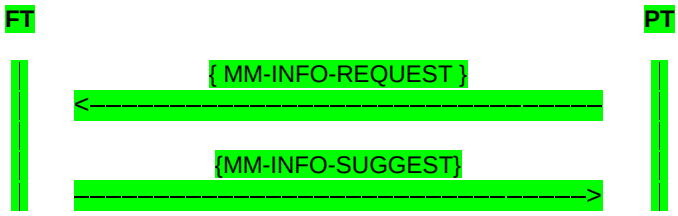

Figure 6.1f: PT initiated cipher key retrieval procedure

NOTE 2: This procedure is a particular case of the "Parameter retrieval procedure" defined in ETSI EN 300 175-5 [i.5], clause 13.7. The provisions given in ETSI EN 300 175-5 [i.5] regarding primitives and timers can be observed as design guidelines.

The following parameters shall be used in the {MM-INFO-REQUEST} message.

Table 6.6b: Values used within the {MM-INFO-REQUEST} message

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<Info-type>>			
	<ext>	0	
	<Parameter type>	0100010'B	CK transfer
<<KEY>>			
	<Key type>	10010000 10010001 10010100 10010101	DCK for DSC DCK for DSC2 Default Cipher Key for DSC (or unknown algorithm) Default Cipher Key for DSC2
	<Key>	Carries only the Default Cipher Key index (2 octets)	See ETSI EN 300 175-5 [i.5], clause 7.7.24.
NOTE: To request a default cipher key, the requesting node should include the requested Default Cipher Key Index. The <Key type> shall be coded indicating the Ciphering algorithm, when known. However this discrimination shall be ignored by the other peer that shall always code the algorithm type as the real algorithm associated to the given key. The recommended practice when the algorithm is unknown is coding the <Key type> in the request message with the DSC or unknown value ('10010100'B).			

Multiple <<KEY>> Information Elements may be included in the {MM-INFO-REQUESTT} message by utilizing the repeat mechanism (see ETSI EN 300 175-5 [i.5], clause 7.5.6), i.e. by the inclusion of the <<REPEAT-INDICATOR>> specifying coding 1 "non-prioritized list" prior to the list of <<KEY>> Information Elements. This allows multiple keys to be requested in the same message.

NOTE 3: This mechanism may be used for requesting to the FP a DCK plus a DefCK, or for requesting multiple DefCK.

The following parameters shall be used in the {MM-INFO-SUGGEST} message.

Table 6.6c: Values used within the {MM-INFO-SUGGEST} message

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<Info-type>>			
	<ext>	0	
	<Parameter type>	0100010'B	CK transfer
<<KEY>>			
	<Key type>	10010000 10010001 10010100 10010101	DCK for DSC DCK for DSC2 Default Cipher Key for DSC Default Cipher Key for DSC2
	<Key>	Any	In the case of Default Cipher Key (<Key type> 10010100'B or 10010101'B) the <Key> data field also includes the associated Default Cipher Key Index in 2 byte format. See ETSI EN 300 175-5 [i.5], clause 7.7.24.

The <Key type> field indicates the ciphering algorithm to be used with the transferred key (either DSC or DSC2). This is important because the WRS does not know what ciphering algorithms are supported by the PT or indeed which ciphering algorithm the FP will select in its {CIPHER-REQUEST}. When using the key, the WRS shall use the specified ciphering algorithm (see clause 7.7.6).

Multiple <<KEY>> Information Elements may be included in the {MM-INFO-SUGGEST} message by utilizing the repeat mechanism (see ETSI EN 300 175-5 [i.5], clause 7.5.6), i.e. by the inclusion of the <<REPEAT-INDICATOR>> specifying coding 1 "non-prioritized list" prior to the list of <<KEY>> Information Elements. This allows multiple keys to be transferred in the same message.

NOTE 4: This mechanism may be used for transferring to the same WRS a DCK plus a DefCK, or for transferring multiple DefCK.

When multiple <<KEY>> Information Elements are used, care should be taken to ensure that the maximum supported message length is not exceeded. If necessary, more cipher keys can be transferred by sending additional {MM-INFO-SUGGEST} messages.

The parameter retrieval procedure is supervised by the timer <MM_info.1> in the PT. At the first expiry of the timer <MM_info.1> the PT should retransmit the {MM-INFO-REQUEST} message. If the timer <MM_info.1> expires a second time, the PT shall abort the procedure and release the transaction. Timer <MM_info.1> may be restarted by the FT at any time by sending a <<TIMER-RESTART>> information element in a {MM-NOTIFY} message.

NOTE 5: The timer value for <MM_info.1> is defined in the NWK standard (ETSI EN 300 175-5 [i.5], clause A.5).

6.3.9.5 Error cases

6.3.9.5.1 PT initiated cipher key retrieval procedure - FT reject

In the PT initiated procedure, there is the option for the FT for rejecting the procedure. This may happen either due to error/inconsistency in the parameters supplied by the PP in the messages, or by error in a PP authentication that the FP may have executed interleaved with the procedure. The error is notified to the PT by sending a {MM-INFO-REJECT} as response.

The sequence shall be as follows:

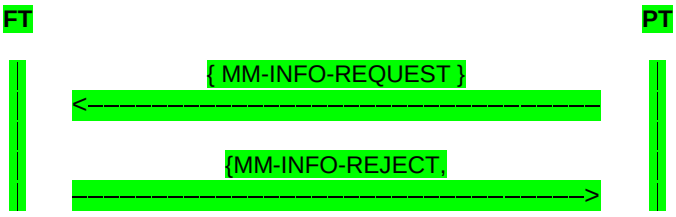

Figure 6.1g: PT initiated cipher key retrieval procedure - FT reject

The following parameters shall be used in the {MM-INFO-REJECT} message.

Table 6.6d: Values used within the {MM-INFO-REJECT} message

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<Info-type>>			
	<ext>	0	
	<Parameter type>	0100010'B	CK transfer

"

5.2.2.3 New MAC layer procedure for re-keying

New procedures and procedure descriptions have been added, including the case of re-keying to a DefCK:

"6.4 MAC layer procedures

6.4.6 Encryption mode control

6.4.6.5 Procedures for re-keying

6.4.6.5.1 Re-keying to a DCK

The procedure is provided to change the DCK during an encrypted call.

The procedure may also be used for changing from a Default Cipher Key (DefCK) to a DCK.

This is the re-keying procedure used in normal operation.

The procedure is similar to the procedure of clause 6.4.6.3 with the difference that there is already an encrypted call established. In order to change the DCK, the PT sends a STOP.REQ (see clause 6.4.6.4). After receiving STOP.CFM, the PT sends immediately the START.REQ to restart encryption with the newly activated DCK.

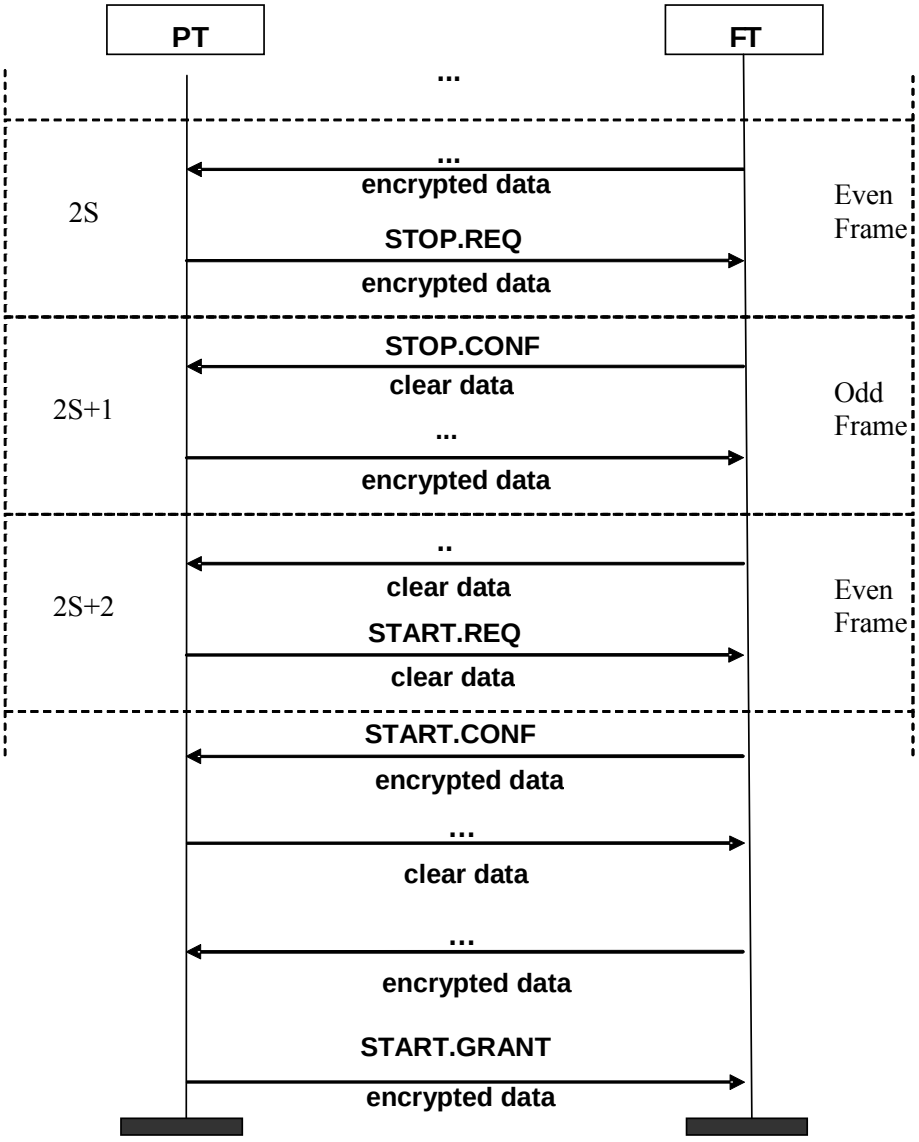

Figure 6.11: Encryption change - good link example

6.4.6.5.2 Re-keying to a DefCK

This procedure allows changing the key used in the encryption process from a DCK to a DefCK.

This is an exceptional procedure intended for some special operation cases where a fast change of cipher keys is required. It is provided to facilitate some handover cases.

NOTE 1: It should be assumed that in most cases the FT involved in this procedure will be a CRFP.

The procedure is analogous to the re-keying procedure described in clause 6.4.6.5.1 with the difference that the START messages (REQ, CFM and GRANT) will be replaced by the START with Default Cipher Key messages, including the desired cipher key index.

The Cipher Key index is generally chosen by the PT. See also the procedure described in clause 6.4.6.5.3.

The cipher algorithm to be used with the DefCK is the one predefined for the chosen DefCK (indicated by the cipher key index). Since each DefCK has a cipher algorithm predefined (defined at time of generation), this procedure can also change the encryption algorithm.

This procedure is only defined as PT initiated. A related procedure FT initiated (clause 6.4.6.5.3) may be used by the FT to trigger the PT procedure.

NOTE 2: Due to the security considerations this procedure is intended to be used only in special cases as part of specific procedures (such as handovers). Such cases should be specifically indicated in other clauses of the present document or in other DECT specifications.

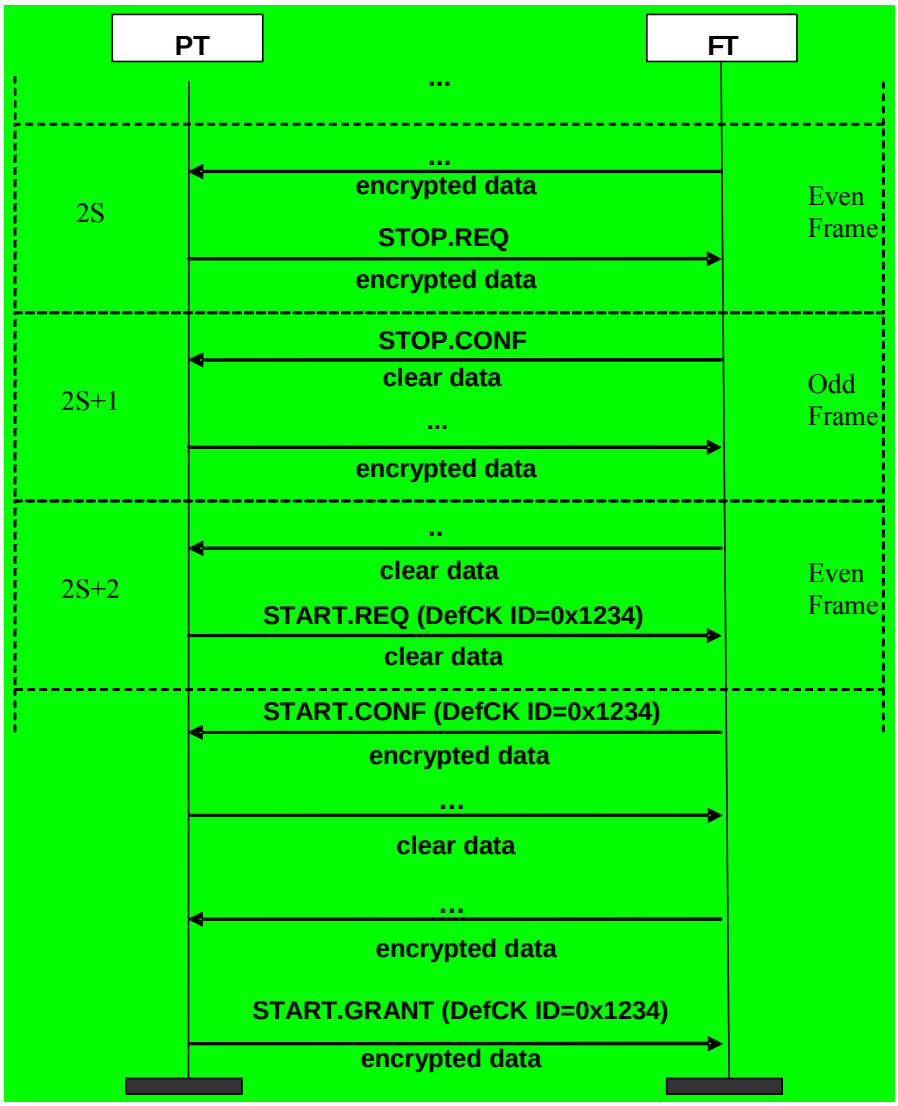

Figure 6.11a: Encryption change to a DefCK

6.4.6.5.3 FT Indication of re-keying to a DefCK

The FT may send to the PT a request to initiate the procedure of re-keying to a DefCK. This may be of interest in certain special cases. For instance, during inter-cell bearer handover (including cases with WRS) where the key was not known, and a change of cipher algorithm was required.

NOTE: It should be assumed that in most cases the FT will be a WRS.

The procedure is implemented by sending FT to PT the message START.REQ with default cipher key.

The expected PT response is either the initiation of the procedure for re-keying to a DefCK (clause 6.4.6.5.2) in the next frame, or simply ignoring the procedure.

Due to the security considerations of the procedure, it is intended that PT will only obey the command in certain cases related to operations (such as handovers) where the procedure may have sense. Such cases should be specifically indicated in other clauses of the present document or in other DECT specifications. In any other case the PT shall ignore the command.

If the FT does not receive reply to the START.REQ message (STOP.REQ sent by the PT), it shall repeat the message in all successive odd numbered frames until 2S + 11 or until it receives the STOP.REQ from the PT.

The field cipher key index in the START message may be used to code the desired DefCK or may be coded with a conventional value in cases where it is intended that the PT choose the key. The conventional value may also be used for discriminating the intended cipher algorithm. The convention for such coding will be defined in other DECT specifications.

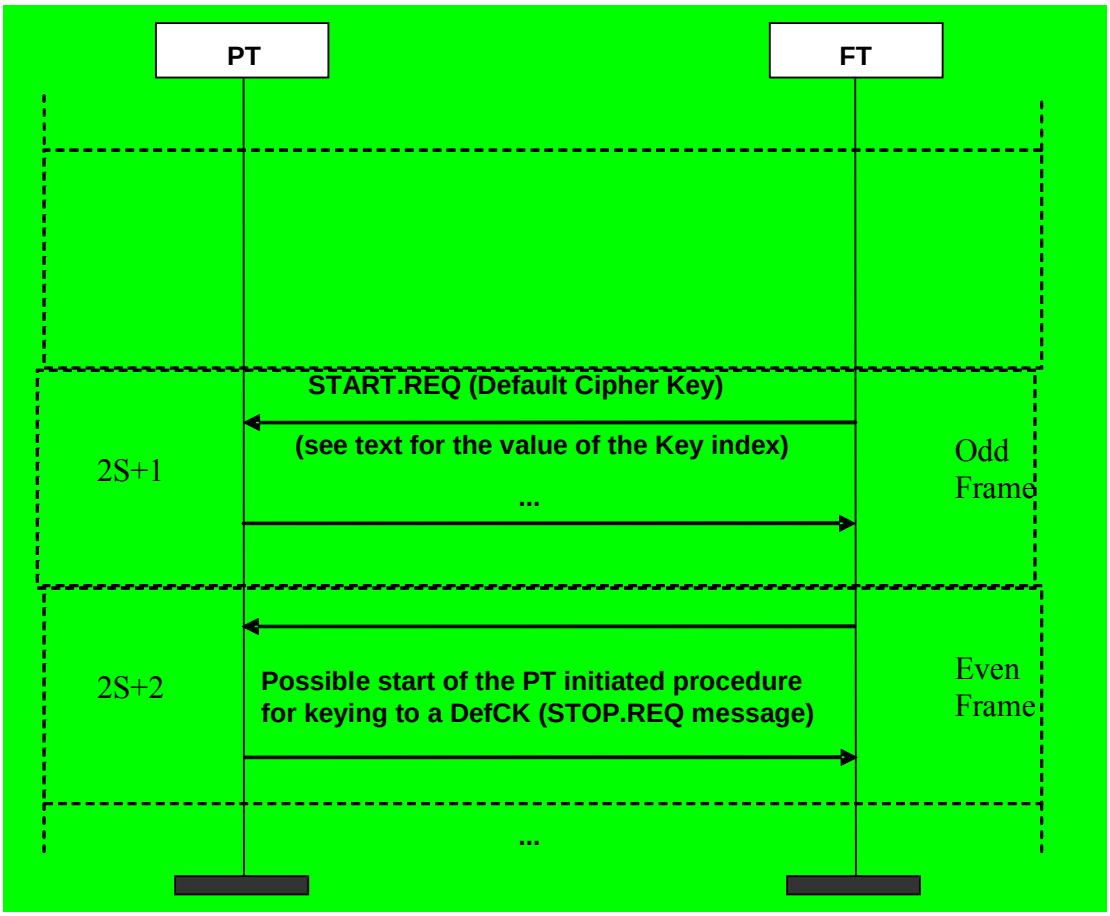

Figure 6.11b: FT indication of encryption change to a DefCK"

5.2.2.4 New description of the re-keying procedure and new aging model to control operation with repeaters

A new description of the re-keying procedure and a new aging model to control operation in systems with repeaters have been added to the standard:

"6.7 Security meta-procedures

6.7.1 General

By "security meta-procedures" it is meant procedures related to system security that are fundamentally controlled at Management Entity (ME) level. These meta-procedures make use of MAC and NWK procedures invoked in the proper way and sequence, and normally include timers and strategies to be performed by the ME.

6.7.2 Re-keying

6.7.2.1 Aim and strategy

The Re-keying is a mechanism consisting on the periodic and regular change of the Cipher Key of an ongoing call, service call, or virtual connection in order to improve the security. The fundamental aim of the re-keying is to increase the computer resources needed for a brute-force attack to the cipher and/or the authentication algorithms. The re-keying strategy achieves its objectives if the time required by a potential hacker to break the algorithms with its available computer resources is significantly larger than the re-keying timer.

The re-keying is fundamentally intended to protect the relatively weak cipher algorithm DSC. The protection provided by the re-keying is not comparable to the protection provided by the use of stronger ciphers (such as DSC2), and this should be the primary route for security concerned applications. Nevertheless, it is believed that DSC combined with the re-keying strategy is effective against attacks attempting real-time phone tapping of DECT communications performed by regular hackers with their expected computer resources.

6.7.2.2 Re-keying procedure

This re-keying ME procedure consists on the periodic modification of the cipher key used for encryption during an ongoing call and within a maximum time defined by a timer. The call may be a voice call, a service call, a virtual call or any other virtual connection.

To implement the re-keying procedure, the FP shall perform periodically authentication of PP procedures with generation and storage of a new DCK followed by Cipher switching procedures, in a way that between the generation and the last use of such DCK there is never a longer time than a given timer.

The timers <MM_re-keying.1> and <MM_re-keying.2> provided in annex I.1 are given as recommendations. The timer <MM_re-keying.2> is only intended to be used only in combination with DSAA2 and DSC2 (in case of repeaters, only if all segments use these algorithms). With DSC or in any other case the timer <MM_re-keying.1> is the recommended choice.

In absence of specific provisions on the matter in the applicable application profile, or if such profile does not exist, or only contains a reference to the present document, then it shall be understood that timers <MM_re-keying.1> and <MM_re-keying.2> shall be used.

For the purposes of <MM_re-keying.1> and <MM_re-keying.2>, the generation of the key is assumed to happen at the FT sending of the {AUTHENTICATION-REQUEST} message, and the last use of the key is assumed to happen at the FT sending of a {CIPHER-REQUEST} message that is confirmed by the reception of a MAC START.GRANT message.

The authentication procedure shall be executed using either DSAA (as clause 6.3.3.1, see also ETSI EN 300 444 [i.9], clause 8.27) or DSAA2 (as clause 6.3.3.3, see also ETSI EN 300 444 [i.9], clause 8.45) algorithms. DSAA2 procedure shall only be used if DSAA2 is supported by both peers.

The encryption algorithm may be either DSC (see annex J) or DSC2 (see annex M).

After receiving the {AUTHENTICATION-REPLY} message, the FP shall perform the Cipher switching initiated by FT. This procedure shall be performed as described in ETSI EN 300 175-5 [i.5], clause 13.8. See also clause 6.5.3 in the present document and ETSI EN 300 444 [i.9], clause 8.33.

The PP will respond with the initiation of the MAC procedure "re-keying to a DCK" as described in clause 6.4.6.5.1 of the present document. This procedure contains a final message "START.grant" that allows the FT to know the completion of the procedure in all cases.

NOTE: This is true even in cases when there are WRSs. See ETSI EN 300 700 [i.10], clause 7.7.

In case of no completion of the re-keying procedure before the expiration of the timer, the procedure has failed. The application profile may specify the action to be performed in this case. These actions may range from additional security measures to simply dropping the call.

6.7.2.3 Re-keying procedure with Wireless Relay Stations (WRSs)

6.7.2.3.1 General

In cases of systems with repeaters (Wireless Relay Station, see ETSI EN 300 700 [i.10]), several additional rules shall be followed:

- Re-keying should be applied to all communication segments in the system (i.e. segments from FP to WRSs, from WRSs to PP and potentially from WRSs to other WRSs).
- Transfer of keys to WRSs shall be only done over encrypted "re-keyed" links (additional requirement to the general rule of "encrypted links") and the key for such links should be "fresh" according to the aging model.
- The key aging model described in clause 6.7.2.3.2 shall be used to control the age of the key and the evaluation of the re-keying timer.

The FP shall perform the re-keying operations for all nodes and segments, in the proper sequence and initiated early enough, to guarantee that no key in the connection path has an age higher than the re-keying timer.

NOTE 1: Not following these rules may result in a reduction of security (due to the exposure of a key over a vulnerable link).

NOTE 2: The re-keying procedure, even in systems with WRSs, is under control of the FP. Note that the FP has all elements to control the evolution of the procedure.

NOTE 3: The message "START.grant" of the re-keying MAC procedure (see 6.4.6.5.2 "Re-keying to a DefCK") is always relayed by the repeaters towards the FP (see ETSI EN 300 700 [i.10], clause 7.7.7). Therefore, the FP may be aware of the completion of any re-keying in any segment.

6.7.2.3.2 Key aging model

The underlying aim of re-keying is to minimize the exposure and use of a cipher key, in order to mitigate the threat of brute-force attacks for recovering the cipher key. In order to control the expiration of the re-keying timer in systems with repeaters, the following key aging model shall be used:

1) Any DCK in the system can be considered to have an "age" which starts aging as soon as the key is first exposed or used, and will continue to age thereafter (regardless of whether the key continues to be used or not).

2) The age of a DCK is considered to start at the moment of key generation (i.e. by means of the Authentication procedure). The exact starting point is taken to happen at the FT sending of the {AUTHENTICATION-REQUEST} message.

3) When any DCK is provisioned to an upper node of a segment (e.g. to a WRS) by means of the {MM-INFO-SUGGEST} message, then that DCK inherits the age value of the key used to protect that {MM-INFO-SUGGEST} message, if that value is older than the age as calculated from the key generation (see note). The key continues aging from this value.

NOTE: It should be assumed that the most usual case is that key inherits the value of the key used for transporting the {MM-INFO-SUGGEST} message."

5.2.2.5 New description of the early encryption procedure

A new description of the early encryption procedure has been added to the standard:

"6.7.3 Early encryption

6.7.3.1 Aim and strategy

The early encryption is a combined MAC layer/NWK layer mechanism intended to ensure the fast activation of encryption at the beginning of any call, including service callas and virtual calls. To achieve that, a special type of Cipher Key called Default Cipher Keys (DefCK) are generated and stored in advance of their intended use by means of a variation of the Authentication procedure. The encryption itself is designed to be activated using only MAC layer messages. This allows the quick enabling of the encryption at the beginning of a call, encrypting even the called party number.

6.7.3.2 The Default Cipher Keys (DefCK)

The Default Cipher Keys are a special type of encryption keys intended for use in the early encryption feature. They are characterized by the following:

- Cryptographically, they are identical to the DCKs and may have 64 or 128 bits depending on the cipher algorithm to be used.
- The cipher algorithm to be used is identical to the one used with the DCKs and may be DSC or DSC2.
- They are generated by the same authentication procedure used to generate DCK (but a different execution). A set of parameters in the authentication messages indicates that the key to be generated and stored will be a DefCK.
- Each DefCK has an associated system level parameter called "Default Cipher Key Index". This parameter is allocated by the FP at the time of generation (by the NWK layer) and will be used by the PP at the time of execution of the MAC procedure.

6.7.3.3 The Default Cipher Key Index

The Default Cipher Key Index is a 16 bit value with the structure shown in figure 6.20.

Table 6.20: Default Cipher key index

Key-Index	Meaning
m.s.b l.s.b	
0000 0000 0000 0000	no cipher key index
0000 0000 0000 0001 to 1111 1110 1111 1111	valid cipher key index
1111 1111 0000 0000 to 1111 1111 1111 1110	reserved
1111 1111 1111 1111	invalid cipher key index

The Default Cipher Key Index is included in the MM messages used for generating or transporting it and in the MAC messages used to activate the early encryption (see ETSI EN 300 175-3 [i.3], clause 7.2.5.7).

6.7.3.4 Generation and refresh strategy

The FP may allocate multiple DefCKs to a given PP by using different key index values. In addition to it, the FP may refresh or regenerate the value of a given DefCK, by running an authentication to generate a DefCK and using the same index value.

Due to the implementations constrains consequence of the need for storage of the keys in non-volatile memory, the present document does not impose any requirement about when the keys should be generated or refreshed and on how many keys a PP should have allocated. The application profiles may establish additional provisions about both matters.

6.7.3.5 Running the procedure

To perform the early encryption procedure, the FP performs some authentication of PP procedures with generation and storage of a DefCK.

The authentication procedure shall be executed using either DSAA (as clause 6.3.3.1, see also ETSI EN 300 444 [i.9] clause 8.24 and 8.27) or DSAA2 (as clause 6.3.3.3, see also ETSI EN 300 444 [i.9] clause 8.24 and 8.27) algorithms. DSAA2 procedure shall only be used if DSAA2 is supported by both peers.

The generation and storage of Default Cipher Key is indicated by the inclusion of the flag <DEF> in the IE <<AUTHENTICATION-TYPE>> as well as two additional octets < Default Cipher Key Index> at the end of this same Information element (see ETSI EN 300 175-5 [i.5]).

Once that a PP has been provisioned with one (or more) DefCKs, the PP will be ready to run the MAC procedure for encryption with Default Cipher Keys (early encryption) when required. This procedure will be performed as described in clause 6.4.6.3.4 (PT procedure for switching from clear to encrypt mode with a Default Cipher Key (DefCK).

The encryption with Default Cipher Keys is seen as a temporary encryption mechanism. Once a call encrypted with DefCK has been setup, the FP should be in charge of performing a switch to a "regular" DCK as soon as possible. This may be done by running a further authentication with generation of a DCK followed by a Cipher switching procedure.

The present document does not impose any requirement on the timer for this transition that is left to the relevant application profiles.

NOTE: The reason of this recommendation is protecting the Default Cipher key by not exposing it unnecessarily. See clause 6.7.3.6 on security considerations.

6.7.3.6 Security considerations

Since a DefCK is generated by the same algorithm as a DCK and use potentially the same cipher algorithm, the primary security strength of a DefCK is similar to a DCK. However there are significant differences due to the potentially longer time between generation and use. Note that this time may be of the order of days in a real system.

If a DefCK has been generated with the algorithm DSAA, and this authentication exchange has been observed by a hacker, it would be in theory possible performing a brute force attack over the DSAA, if enough time is available. This threat disappears if the stronger algorithm DSAA2 is used (brute force attack time in the range of several millions of years).

For a DefCK generated using DSAA2 and using DSC, the only practical strategy would be attacking the DSC algorithm. This would be facilitated by the potential long time of use of a given key. However this would also be made difficult by the reduced exposure of the key (the connection is re-keyed from a DefCK to a fresh DCK in a very short time).

An optimal strategy when not using DSC2 ciphering, would be using DSAA2 refreshing the keys regularly. It is even possible having "fresh" keys (keys never used with the cipher) ready for use for each new call. However this strategy may be excessive in practical terms and collides with strategies or reducing emissions and extending the battery duration of the handsets.

A DefCK generated with DSAA2 and using DSC2 is considered to be not vulnerable to brute force attacks and is therefore the recommended solution for security concerned applications (in systems with repeaters this DSAA2/DSC2 combination should be used consistently in all segments between FP to PP)."

5.2.2.6 New annex with security timers

A new annex with security timers has been added to the standard:

"Annex I (normative):
Security system parameters

I.1 Security timers

<MM_re-keying.1>

Description: FT re-keying timer.

FT value: 60 seconds.

Start: A {AUTHENTICATION-REQUEST} message for re-keying is sent.

Stop: Next { AUTHENTICATION-REQUEST } for re-keying message is sent. The timer is restarted.

<MM_re-keying.2>

Description: FT re-keying timer.

FT value: 3 600 seconds.

Start: A {AUTHENTICATION-REQUEST} message for re-keying is sent.

Stop: Next { AUTHENTICATION-REQUEST } for re-keying message is sent. The timer is restarted.

NOTE: Timer <MM_re-keying.2> is intended to be used only when cipher algorithm DSC2 is used in all segments between FT and PT.

<MM_early_encryption.1>

Description: FT early encryption timer within which a default cipher key has to be generated.

FT value: 30 seconds.

Start: Encryption activation of the first call after end of obtaining access rights procedure, in case no default cipher key was generated until this point in time.

Stop: Default cipher key is generated (Authentication of PP with DEF-bit = 1).

<MM_encryption_check.1>

Description: FT timer within which a call has to be encrypted.

FT value: 15 seconds.

Start: Send/receive of {CC-SETUP}.

Stop: Encryption is activated.

<MM_encryption_check.2>

Description: PT timer within which a call has to be encrypted.

PT value: 15 seconds.

Start: Send/receive of {CC-SETUP}, respectively {CC-CONNECT}.

Stop: Encryption is activated.

<MM_registration.1>

Description: FT timer within which the registration mode is active (Extended Fixed Part capability bit a44 = 1).

FT value: 120 seconds.

PT value: Not used.

Start: Subscription mode has been requested by the user: set a44 "access rights supported" bit.

Stop: As soon as on-air subscription procedure is successful, clear a44 "access rights supported"."

5.3 Changes introduced in the Generic Access Profile (ETSI EN 300 444)

5.3.1 New description of the re-keying procedure and new aging model to control operation with repeaters

A new description of the re-keying procedure and rules for use of the new aging model to control operation with repeaters have been added to the standard:

"8.45.2 Re-keying during a call

This procedure consists on the periodic modification of the cipher key used for encryption during an ongoing call and thus improving the security of the call.

When implementing the procedure, the FP shall set bit a_{42} of the "Extended higher layer capabilities (part 2)" (see ETSI EN 300 175-5 [i.5], clause F.3).

The PP shall support the re-keying and indicate this in the <<Terminal Capability>> information element both in the {ACCESS-RIGHTS-REQUEST} message and in the {LOCATE-REQUEST} message. It is however allowed not to indicate this capability in case the FP does not itself indicate the same capability in the extended FP Capabilities part 2.

NOTE 1: This exception is allowed with respect to existing GAP Protocol test equipment which is not able to test PPs indicating newly defined terminal capability bits.

This procedure shall be used as described in ETSI EN 300 175-7 [i.7], clause 6.4 and ETSI EN 300 175-5 [i.5], clause 13.8 for each call, i.e. voice calls as well as service calls and List Access service calls (when supported).

The FP shall periodically perform 'authentication of PP' procedures with generation and storage of a new DCK (clause 8.27) followed by Cipher switching (clause 8.33) procedures, in a way that between the generation of a and the last use of such DCK there is never a longer time than timer <MM_re-keying.1>.

For the purposes of the timer <MM_re-keying.1>, the generation of the key is assumed to happen at the FT sending of the {AUTHENTICATION-REQUEST} message, and the last use of the key is assumed to happen at the FT sending of a {CIPHER-REQUEST} message that is confirmed by the reception of a MAC START.GRANT message.

The authentication procedure shall be executed using either DSAA (as clause 8.24) or DSAA2 (as clause 8.45.7) algorithms. DSAA2 procedure (clause 8.45.7) shall be used if DSAA2 is supported by both peers.

The encryption algorithm may be either DSC (see ETSI EN 300 175-7 [i.7], annex J) or DSC2 (see service M.17 and ETSI EN 300 175-7 [i.7], annex M).

Refer to ETSI EN 300 175-7 [i.7], clause I.1 for the value of timer <MM_re-keying.1>.

After receiving the {AUTHENTICATION-REPLY} message, the FP shall immediately perform the Cipher switching initiated by FT as described in clause 8.33.

The FP may retry the messages {AUTHENTICATION-REQUEST} and {CIPHER-REQUEST} in case of no proper answers from the PP (reception of {AUTHENTICATION-REPLY} and MAC START messages respectively).

In case of expiration of the timer associated to the authentication procedure (timer -<MM_auth.1> defined in ETSI EN 300 175-5 [i.5], clause A.5) or if the PP rejects the authentication, or answers with a wrong authentication result, the FP shall perform abnormal release of the call and shall indicate the release reason [Re-keying failed] within the <<Release Reason>> information element in the {CC-RELEASE-COM}message.

In case of no completion of the re-keying procedure (reception of the START.GRANT after switching to the new key), the FP shall perform abnormal release of the call and shall indicate the release reason [Re-keying failed] within the <<Release Reason>> information element in the {CC-RELEASE-COM} message.

In case the re-keying fails on MAC layer, the connection shall be released on MAC layer as specified in ETSI EN 300 175-7 [i.7], clause 6.4.6.

Specific for systems with Wireless Relay Stations (WRS)

In cases of systems with repeaters (Wireless Relay Station, see ETSI EN 300 700 [i.10]), the rules on aging of the key described in ETSI EN 300 175-7 [i.7], clause 6.7.2.3, shall apply. The requirement on re-keying shall be understood as that no key in use may have an age (in the meaning of ETSI EN 300 175-7 [i.7], clause 6.7.2.3.2) longer than timer <MM_re-keying.1>.

NOTE 2: Based on ETSI EN 300 175-7 [i.7], clause 6.7.2.3.2, the life of a key for a segment directly connected to the FP starts with its generation. The life of a key for any other segment inherits the previous age of the key used for protecting the message {MM-INFO-SUGGEST} that carries the key when it is provided to the WRS upper peer of the segment. The life of a key terminates when a Cipher Switching procedure is run and a new key is set in use.

NOTE 3: In general, the FP may control the re-keying rule by performing rekeying to both WRSs and PPs in the right sequence, and by starting a timer with the generation of the DCK in the segment directly connected to the FP and stopping it when it gets confirmation that key is replaced by a new one at the PP segment. Such timer should never exceed <MM_re-keying.1>.

Specific for DSC2

When the Cipher Algorithm in use is DSC2, the more relaxed timer <MM_re-keying.2> (defined in ETSI EN 300 175-7 [i.7], clause I.1) shall be used instead of <MM_re-keying.1>, allowing longer intervals between re-keying. In the case of systems with repeaters, DSC2 should be used in all segments of the connection. In any other case, the timer <MM_re-keying.1> shall apply.

NOTE 4: DSC2 is always used with Authentication Algorithm DSAA2."

5.3.2 New description of the early encryption procedure

A new description of the early encryption procedure has been added to the standard:

"8.45.3 Early encryption

This procedure allows to encrypt all CC messages in a call and thus, to protect the early stages of the signalling such as dialling or CLIP information sending, that may be sensitive.

This procedure shall be used for each call, i.e. voice calls, service calls and List Access service calls (when supported).

When implementing the procedure, the FP shall set bit a_{42} of the "Extended higher layer capabilities (part 2)" (see ETSI EN 300 175-5 [i.5], clause F.3).

The PP shall support the early encryption and indicate this in the <<Terminal Capability>> information element both in the {ACCESS-RIGHTS-REQUEST} message and in the {LOCATE-REQUEST} message. It is however allowed not to indicate this capability in case the FP does not itself indicate the same capability in the extended FP Capabilities part 2.

NOTE 1: This exception is allowed with respect to existing GAP Protocol test equipment which is not able to test PPs indicating newly defined terminal capability bits.

In case the PP indicated support of early encryption, the FP shall perform an 'Authentication of PP' procedure in order to generate a default cipher key after successful subscription registration. For this purpose the {AUTHENTICATION-REQUEST} message shall indicate that a default cipher key is being generated (DEF bit=1) and shall also contain a default cipher key index.

It is recommended that the FP should perform this 'Authentication of PP' procedure as soon as possible after successful subscription. In any case, this procedure shall be completed at the very latest before expiration of timer <MM_early_encryption.1> after start of encryption of the first call.

The FP may perform further 'Authentication of PP' procedures generating default cipher keys at any time. This may be done either to update a previous default cipher key, or to provision additional default cipher keys.

The authentication procedure shall be executed using either DSAA (as clause 8.24) or DSAA2 (as clause 8.45.7) algorithms. DSAA2 procedure (clause 8.45.7) shall be used if DSAA2 is supported by both peers.

The encryption algorithm may be either DSC (see ETSI EN 300 175-7 [i.7] annex J) or DSC2 (see service M.17 and ETSI EN 300 175-7 [i.7], annex M).

Refer to ETSI EN 300 175-7 [i.7], clause I.1 for the value of timer <MM_early_encryption.1>.

The generated default cipher key shall remain valid for the whole remaining validity of the current subscription or until the same default cipher key index is re-used in another 'Authentication of PP' procedure.

The FP may repeat the procedure in order to assign a new default cipher key at any time. It is recommended to do this not too often, since the default cipher key needs to be stored in non-volatile memory. The PP shall remember at least the last assigned default cipher key and the corresponding default cipher key index during the validity of the subscription. The FP shall remember all previously assigned default cipher keys and their corresponding default cipher key indices during the validity of the subscription.

If the PP supports DSC2, then it shall be able to remember at least 2 DefCKs: one for DSC2 and one for DSC (see clause 8.45.12.3). That is to say, the PP shall remember at least the last assigned DefCK for DSC2, and at least the last DefCK for DSC.

NOTE 2: The DefCK for DSC is only used in special cases (see clause 8.45.12.3).

When the FP assigns a DefCK, it may do so using a new default cipher key index, in which case it is considered as a new DefCK (i.e. requiring allocation of non-volatile storage). Alternatively, the FP may re-use an existing default cipher key index, in which case the new key shall over-write the old key.

NOTE 3: The FP is responsible for assigning the DefCKs, and so it is capable of managing the number of keys assigned to any device. For example, if non-volatile memory is limited it can re-use an existing default cipher key index, which will cause the old key to be over-written.

When a PP has multiple DefCK assigned, it may choose to use any of them that are appropriate. The PP algorithm for selecting the key to be used is left to the implementer.

As soon as a default cipher key is available, the PP shall activate encryption with one of the valid default cipher keys (as described in ETSI EN 300 175-7 [i.7], clause 6.4) immediately (at least before the first NWK C-Plane message is sent) after each MAC connection establishment. The PP shall indicate the chosen default cipher key by use of the corresponding default cipher key index. The PP shall not establish connections without immediately following early encryption activation as long as a valid default cipher key is available. The PP shall release the connection within 10 seconds from the start of the connection in case that the connection is not encrypted successfully (e.g. the FP repeatedly rejects early encryption activation attempts or the early encryption activation fails on MAC layer).

The PP shall encrypt the beginning of a call by using the default cipher key. The FP shall start the 'Authentication of PP' procedure in order to generate a new derived cipher key and shall use it for this call (as described in clauses 8.45.1 and 8.45.2) within timer <MM_re-keying.1>.

Refer to ETSI EN 300 175-7 [i.7] clause I.1 for the value of timer <MM_re-keying.1>.

The timer <MM_re-keying.1>.shall be started:

- for incoming calls, after receiving the first NWK message, after a {CC_SETUP} message has been sent;
- for outgoing calls, after receiving a {CC_SETUP} message."

5.3.3 New clause with additional procedures for devices supporting DSC2

A new clause with additional procedures for devices supporting DSC2 has been added to the standard:

"8.45.12 Additional procedures for devices supporting DSC2

8.45.12.1 General

Clause 8.45.12 describes the additional compatibility procedures to be supported by PP and FP implementing the encryption algorithm DSC2.

NOTE: See ETSI EN 300 700 [i.10] for the additional procedures for CRFPs.

8.45.12.2 Support of additional octet in <<AUTH-TYPE>>

PPs and FPs supporting DSC2 shall support the inclusion of the optional octet 5c in IE <<AUTH-TYPE>> as defined in ETSI EN 300 175-5 [i.5], clause 7.7.4. Such octet shall be inserted by the FP if the PP supports DSC2 and the authentication operation generates a Default Cipher Key.

FPs supporting DSC2 shall support the exchange and request of Default Cipher Keys by CRFPs using the <Key-type> "Default Cipher Key (DefCK) for DSC2" and the associated <<Key>> format as described in ETSI EN 300 175-5 [i.5], clause 7.7.24. This procedure is only used in operations between FPs and CRFP.

8.45.12.3 Support of Default Cipher Keys

If the PP supports DSC2, then it shall be able to remember at least 2 DefCKs: one for DSC2 and one for DSC (see clause 8.45.12.3). That is to say, the PP shall remember at least the last assigned DefCK for DSC2, and at least the last DefCK for DSC.

The following rule apply:

- PP shall always use DefCKs for DSC2 and DSC2 algorithm unless the exceptional case when the FT peer does not support DSC2.

NOTE 1: The reason of keeping the DefCK for DSC in systems supporting DSC2 is for compatibility with CRFPs not supporting DSC2.

NOTE 2: It should be expected that the FP will only normally assign a DefCK for DSC if there are devices not supporting DSC2 (such as CRFPs) in the system.

8.45.12.4 Procedure for cipher algorithm switching at bearer handover

A PP supporting DSC2 shall support the procedures "Re-keying to a DefCK" and "FT Indication of re-keying to a DefCK" described in ETSI EN 300 175-7 [i.7], clauses 6.4.6.5.2 and 6.4.6.5.3. The PP shall be able to follow the sequence given in ETSI EN 300 700 [i.10], clause 7.4.12 ("Bearer handover"), figure 15a ("Handover with cipher algorithm switching").

NOTE: This case can only happen when the PP is connected to a CRFP.

The FP shall be able to perform its role in the bearer handover process described in ETSI EN 300 700 [i.10], clause 7.4.12, figure 15a. Such role consist on the generation of a DCK and re-keying to that after reception of a related START.GRANT."

5.4 Changes proposed for the WRS standard (ETSI EN 300 700)

5.4.1 Overview

Some modifications for inclusion in the next revision of ETSI EN 300 700 (DECT; Wireless Relay Station, [i.10]) have been drafted. The status of these modifications is "OPEN" and may be subject to changes and revisions before inclusion in the next revision of ETSI EN 300 700 [i.10].

5.4.2 Changes in Bearer handover

5.4.2.1 General principles and open issues

The known issue of handovers to WRSs requiring cipher algorithm switching has been addressed. An original solution based on a quick switching to a DefCK followed of a further switching to a DCK has been proposed and accepted by TC DECT.

The exact point of initiation of the procedure "FT Indication of re-keying to a DefCK" (start.req (DefCK) message) is open to further debate. Two possible flowcharts have been created depending on the point of initiation of the procedure.

The "conventional value" of the index in the FT start w/DefCK message may be used to insert a "suggested value" chosen by the FT. If the PT accepts this value, this would guarantee that the FT has the key and would avoid any further delay due a to a key retrieval procedure. However, the security implications need to be analysed.

5.4.2.2 Solution to Bearer handover requiring cipher algorithm switching: technical approach 1

"7.4.12 Bearer handover

...

Handover with cipher algorithm switching

In certain rare cases the handover may require a cipher algorithm switching. For instance, this case may happen e.g. when both the PP and the RFP supports cipher algorithm DSC2 and the CRFP does not. In such a case the CRFP has to perform a change in the cipher algorithm. This will be performed in two phases; in a first phase CRFP and PP shall invoke the procedures "FT Indication of re-keying to a DefCK" and "Re-keying to a DefCK" described in ETSI EN 300 175-7 [i.7], clauses 6.4.6.5.3 and 6.4.6.5.2. In a second phase the RFP shall perform a re-keying to changing the CK to a DCK with an algorithm supported by the CRFP.

Figure 15a shows the sequence of operations to handle this case. The starting point is identical to figure 15. PP and RFP are assumed to have an active connection encrypted with DSC2 or other algorithm supported by both. The CRFP does not support such algorithm.

The procedure sequence shall be identical to the flowchart described in figure 15 with the following differences.

The CRPF shall be in charge of detecting the cipher algorithm mismatch and initiating the switching procedure. The CRFP might detect it at the reception of the NWK message {MM-INFO-SUGGEST} sent from the RFP, that contains the key in use by the PP an indication of the Key Cipher Algorithm carried in the field <KEY-TYPE> within IE <<KEY>> (see ETSI EN 300 175-5 [i.5], clause 7.7.24). In normal cases, the key algorithm is supported and no action is needed. Should the CRFP detect a key mismatch the following actions shall be taken:

- MAC handover procedure shall progress exactly as the normal case given in figure 15.
- The CRFP shall initiate the procedure "FT Indication of re-keying to a DefCK" as described in ETSI EN 300 175-7 [i.7], clause 6.4.6.5.3.
- The CRFP shall send the MAC cipher.start w/DefCK message (as described in ETSI EN 300 175-7 [i.7], clause 6.4.6.5.3) within a time window of three frames that starts with the one following the bearer.cfm message (this is the frame shown in figure 15a). If the first frame was used, this message also performs the role of the "other" message in the setup.
- For security reasons, the PP shall be ready to receive and accept the message only in the time window of three frames after the bearer.cfm. In any other cases, the PP shall ignore the start.req w/DefCK message.
- The CRFP shall code the Default cipher key index fields in the start.req w/DefCK message with the following conventional value:
  - A conventional value: Default Cipher Key index = '1111 1111 0000 1000'B. In that case the PT will choose the index value.
  - Or, alternatively, the FT may code the field with a valid Default Cipher Key index value. This value will have the nature of a suggested value. The PT may use it or choose it or another one.
  - NOTE; the advantage of using the suggested value is that the PT may be sure that the FT has already this DefCK, avoiding further retrieval procedures and speeding up the completion of the operation.
- The PP shall reply to the received MAC message by initiating the sequence "Re-keying to a DefCK" as described in ETSI EN 300 175-7 [i.7] clause 6.4.6.5.2. The first STOP.req message shall be sent in the half-frame immediately following the start.req w/DefCK sent by the CRFP:
  - PP shall take the decision on which DefCK shall be used (within the pool already allocated to such PP).

- In certain cases, the CRFP might not have the requested DefCK. Then, it shall use a Key retrieval procedure (see ETSI EN 300 175-7 [i.7], clause 6.3.9.4) to retrieve such key. This would typically require a new local state. The procedure and timing for this process will be identical to the equivalent case in an initial keying with a DefCK at call setup.

- If the CRFP does not receive the STOP.req showing that the PP has initiated the "Re-keying to a DefCK" procedure, it shall repeat the message start.req w/DefCK and may do it an additional time (up to a total of three frames).

- Once that the MAC procedure of "re-keying to a DefCK" between PP and CRFP has been finished, the CRFP shall relay the message "Start.grant (w/DefCK) to the RFP. The RFP shall then perform a PP authentication procedure to generate a new DCK compatible with the CRFP supported algorithm. This will follow by a rekeying to such DCK:

  - The procedure and timers for this re-keying process shall be identical to the normal re-keying to a DCK after call establishment.

  - This procedure will normally involve a new local state between RFP and CRFP and a transmission of the new DCK to the CRFP.

The described detection and switching procedure shall be supported by all CRFP implementations. They should assume that all PP implementations supporting DSC2 shall be able to react to the procedure. However PPs only supporting DSC may not implement the procedure and will typically not react to the "FT Indication of re-keying to a DefCK" procedure initiated by the CRFP.

All RFP implementations supporting repeaters shall be able to react to a received relayed start.grant (with DefCK) by initiating a subsequent re-keying procedure to a DCK. Note that this case will also happen after initial call setup.

Figure 15a: Bearer handover from RFP to CRFP (dual C/O bearer setup, basic connection) requiring cipher algorithm switching - original option (w/ message sequence corrected)"

5.4.2.3 Solution to Bearer handover requiring cipher algorithm switching: alternative technical approach 2

"Handover with cipher algorithm switching

In certain rare cases the handover may require a cipher algorithm switching. For instance, this case may happen e.g. when both the PP and the RFP supports cipher algorithm DSC2 and the CRFP does not. In such a case the CRFP has to perform a change in the cipher algorithm. This will be performed in two phases; in a first phase CRFP and PP shall invoke the procedures "FT Indication of re-keying to a DefCK" and "Re-keying to a DefCK" described in ETSI EN 300 175-7 [i.7], clauses 6.4.6.5.3 and 6.4.6.5.2. In a second phase the RFP shall perform a re-keying to changing the CK to a DCK with an algorithm supported by the CRFP.

Figure 15a shows the sequence of operations to handle this case. The starting point is identical to figure 15. PP and RFP are assumed to have an active connection encrypted with DSC2 or other algorithm supported by both. The CRFP does not support such algorithm.

The procedure sequence shall be identical to the flowchart described in figure 15 with the following differences.

The CRPF shall be in charge of detecting the cipher algorithm mismatch and initiating the switching procedure. The CRFP might detect it at the reception of the NWK message {MM-INFO-SUGGEST} sent from the RFP, that contains the key in use by the PP an indication of the Key Cipher Algorithm carried in the field <KEY-TYPE> within IE <<KEY>> (see ETSI EN 300 175-5 [i.5], clause 7.7.24). In normal cases, the key algorithm is supported and no action is needed. Should the CRFP detect a key mismatch the following actions shall be taken:

- The CRFP shall initiate the procedure "FT Indication of re-keying to a DefCK" as described in ETSI EN 300 175-7 [i.7], clause 6.4.6.5.3.
- The CRFP shall send the MAC cipher.start w/DefCK message (as described in ETSI EN 300 175-7 [i.7], clause 6.4.6.5.3) within a time window of three frames that starts with the one following the reception of the last segment of the {MM-INFO-SUGGEST} message (see figure 15a1).
- For security reasons, the PP shall be ready to receive and accept the message only in the time window of TEN frames after the initiation of the handover procedure (message bearer_handover.req sent by the PT). In any other cases, the PP shall ignore the start.req w/DefCK message.
- The CRFP shall code the Default cipher key index fields in the start.req w/DefCK message with the following conventional value:
  - A conventional value: Default Cipher Key index = '1111 1111 0000 1000'B. In that case the PT will choose the index value.
  - Or, alternatively, the FT may code the field with a valid Default Cipher Key index value. This value will have the nature of a suggested value. The PT may use it or choose it or another one.

NOTE 1: The advantage of using the suggested value is that the PT may be sure that the FT has already this DefCK, avoiding further retrieval procedures and speeding up the completion of the operation.

- The PP shall reply to the received MAC message by initiating the sequence "Re-keying to a DefCK" as described in ETSI EN 300 175-7 [i.7], clause 6.4.6.5.2. The first STOP.req message shall be sent in the half-frame immediately following the start.req w/DefCK sent by the CRFP:
  - PP shall take the decision on which DefCK shall be used (within the pool already allocated to such PP). It may consider the suggested value, if used by the FPT, but this is not mandatory.
- If the CRFP does not receive the STOP.req showing that the PP has initiated the "Re-keying to a DefCK" procedure, it shall repeat the message start.req w/DefCK and may do it an additional time (up to a total of three frames).
- The CRFP shall reply to the STOP.req message with a STOP.cfm send in the next half frame (as described in ETSI EN 300 175-7 [i.7], clause 6.4.6.5.2). The sending of this message has preference over a possible message bearer.cfm related to the confirmation of the handover.

- The CRFP may have received meanwhile a 'bearer.cfm' sent by the FP related to the completion of the handover. However the CRFP shall not relay this message towards the PT until having sent first the message STOP.CFM related to the re-keying process. Once the CRFP has sent the STOP.REQ, it shall send the bearer.cfm at soon as possible (after reception from the FT), even if it is interleaved in the continuation of the re-keying process. This may lead to repetition of some encryption control messages (see figure 15a1).

- The release procedure of the old bearers (messages 'release' PT - FT in figure 15a) shall progress normally as a normal bearer handover procedure.

- The re-keying procedure shall continue with a start.req w/DefCK sent by the PT containing the finally chosen key:

  - In certain cases, the CRFP might not have the requested DefCK. Then, it shall use a Key retrieval procedure (see ETSI EN 300 175-7 [i.7], clause 6.3.9.4) to retrieve such key. This would typically require a new local state. The procedure and timing for this process will be identical to the equivalent case in an initial keying with a DefCK at call setup.

NOTE 2: If this case happens, it will result in a delay in between the message start.req w/DefCK sent by the PT and the start.cfm w/DefCK sent by the FT, due to the time required for completing the retrieval procedure. Regarding the U-plane date, note that these frames will be transmitted in clear, so no interruption will be perceived by the used.

- Once that the MAC procedure of "re-keying to a DefCK" between PP and CRFP has been finished, the CRFP shall relay the message "Start.grant (w/DefCK) to the RFP. The RFP shall then perform a PP authentication procedure to generate a new DCK compatible with the CRFP supported algorithm. This will follow by a rekeying to such DCK:

  - The procedure and timers for this re-keying process shall be identical to the normal re-keying to a DCK after call establishment.

  - This procedure will normally involve a new local state between RFP and CRFP and a transmission of the new DCK to the CRFP.

The described detection and switching procedure shall be supported by all CRFP implementations. They should assume that all PP implementations supporting DSC2 shall be able to react to the procedure. However PPs only supporting DSC may not implement the procedure and will typically not react to the "FT Indication of re-keying to a DefCK" procedure initiated by the CRFP.

All RFP implementations supporting repeaters shall be able to react the a received relayed start.grant (with DefCK) by initiating a subsequent re-keying procedure to a DCK. Note that this case will also happen after initial call setup.

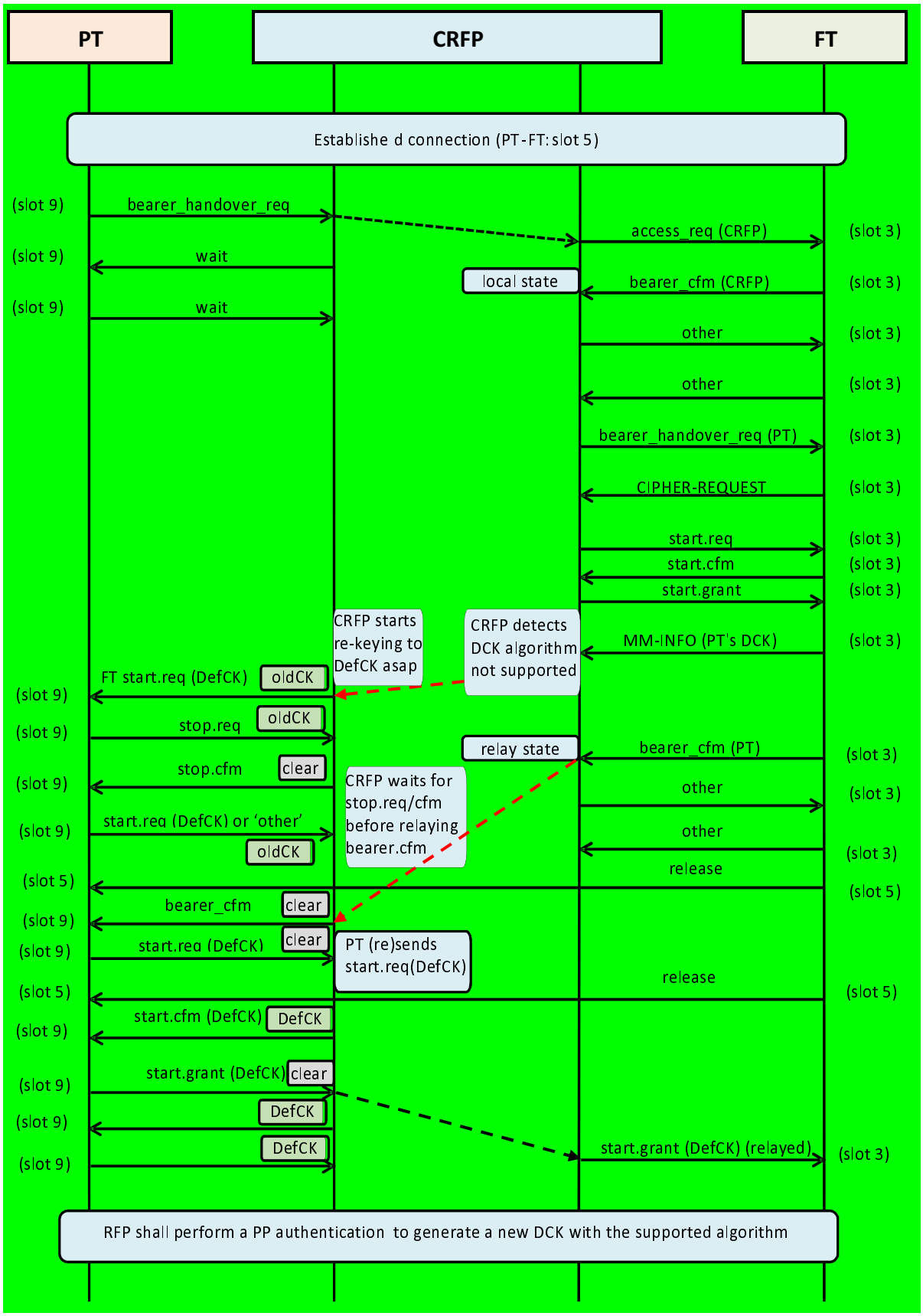

Figure 15a1: Bearer handover from RFP to CRFP (dual C/O bearer setup, basic connection) requiring cipher algorithm switching - alternative option after DECT#72

NOTE 3: The procedures for the encryption of the upper segment and transfer of the cipher key for the lower segment are described in detail in clause 7.7."

5.4.2.4 Provision of lower DefCKs "just-in-time"

"7.7.5.2.5 Provision of lower DefCKs "just-in-time"

The FP may provide a WRS with a PT's DefCK during the connection establishment procedure. This is only possible during the dual C/O bearer setup procedure (see clauses 7.4.10.5 and 7.4.10.6).

During dual C/O bearer setup, the connection between FP and WRS is set to local state, and the "access_request" of the PT is passed to the FP. At this point, the FP may provide the WRS with the PT's DefCK, as described below:

- The FP shall use the PT's PMID to find the associated DefCK and index (see note 1).
- In the event that no associated DefCK is found (for example the PT does not support Early Encryption), then clearly no key can be provided.
- In the event that an associated DefCK is found, and the key **has not** been previously provided in advance (e.g. by an earlier invocation of the procedure defined in clause 7.7.5.2.4 or the present clause), then the FP shall provide the key to the WRS now, by use of the Indication of cipher key procedure (clause 7.7.4) (see note 2).
- In the event that an associated DefCK is found, then the FP may provide the key to the WRS now, by use of the Indication of cipher key procedure (clause 7.7.4) procedure (see note 3).
- If necessary, multiple DefCKs can be provided to the WRS by "just-in-time provision" by use of the Indication of cipher key procedure (clause 7.7.4) procedure (see note 4).

NOTE 1: The FP maintains an association between PMID and DefCK index for this purpose.

NOTE 2: This includes the case where the FP has generated a new DefCK re-using an existing key index, and this newly generated version of the key has not yet been provided to the WRS.

NOTE 3: Always supplying the DefCK in this way is redundant when it has already been provided in advance. However, doing it this way is simpler (since the FP does not have to remember which keys it has provided) and so the implementation is allowed to do it.

NOTE 4: Multiple DefCKs could be assigned to a PT. However, it is recommended that only one DefCK per PT is assigned in order to reduce overhead and complexity (see clause 7.7.5.2.3).

Figure 38 shows a scenario involving early encryption of upper segment (marked "A"), re-keying of upper-segment (marked "B"), just-in-time key provision (marked "C") and early encryption of lower segment (marked "D")."

5.5 Other recommendations for implementation of security features

5.5.1 Guidelines for Implementation of the key-aging model related to the re-keying procedure

5.5.1.1 Introduction

The key-aging model described in ETSI EN 300 175-7 [i.7], clause 6.7.2.3 has been created to properly model the re-keying timer in a generalized way suitable for any DECT system. This includes systems with repeaters, including complex combinations such as multiple levels of repeaters (chained repeaters). Despite this generalization, the model has been designed to be of very simple implementation, as the following clauses show.

5.5.1.2 Implementation of the re-keying timers before the addition of the aging-model

In a complex system, i.e. a system with repeaters, the FP is required to maintain a timer for each active individual PP or active WRS in the system. In the case of WRS, each active connection causes an independent MM entity and thus an independent timer. In case of chained WRSs, each of them will have separate timers and will be re-keyed separately. Such timers are started at the key generation (authentication request message as described in ETSI EN 300 175-7 [i.7], clause 6.7.2). It may be assumed that a routine detects when such timers are approaching the limit value and performs the proper action (running the re-keying sequence to refresh the key). Such action should be initiated with the proper anticipation to avoid timer expiration. The choice of how much is the "anticipation" and also the exact sequence of events is an implementation choice. If a re-keying timer finally expires a more drastic action has to be implemented. GAP (ETSI EN 300 444 [i.9]) prescribes dropping the call.

The implementation of the timers may be done in multiple ways. It can be done by real counters (the obvious way) or simply by storing a time stamp with the absolute time of timer start. This is irrelevant for the next discussion.

5.5.1.3 Additional procedures required by the aging model

To properly implement the aging model, the only additional operation that the FP has to implement is the following:

- When the FP sends a cipher key towards a WRS (sending of the message {MM-INFO-SUGGEST}, it should compare the value of the timers of the *protecting key* and the *transmitted key* and, if the first is older than the second, it will update the *transmitted key* timer with this value.

This operation can be added to the routine in charge of the {MM-INFO-SUGGEST} submission. The procedure would be the same irrespective of the implementation of the timers (if the timers are implemented with a time-stamp, the operation would be coping the value of the time-stamp).

For the purposes of the previous rule the following definitions apply:

- ***Protecting key timer*** is the timer associated to the cipher key that is protecting the transmission of the {MM-INFO-SUGGEST} message in the immediate upper segment (segment between the WRS and the FP or previous WRS).
- ***Transmitted key timer*** is the timer associated to the key included in the {MM-INFO-SUGGEST} message (key to be used in the segment between the WRS and the PP or next WRS).

5.5.1.4 Additional implementation guidelines

ETSI EN 300 175-7 [i.7] does not impose any specific sequencing regarding how the different re-keyings are done. This is left up to the implementer. This allows the implementer to perform them according to i.e. the situation of the link regarding local/relayed state (see ETSI EN 300 700 [i.10]) towards the different repeaters.

However, after analysis, it can be said that the most efficient operation is achieved by doing the re-keyings exactly in sequence, starting with the segment directly connected to the FP continuing (immediately) with the re-keying of the next segment, ending with the segment reaching the PP.

History

Document history		
V1.1.1	July 2017	Publication