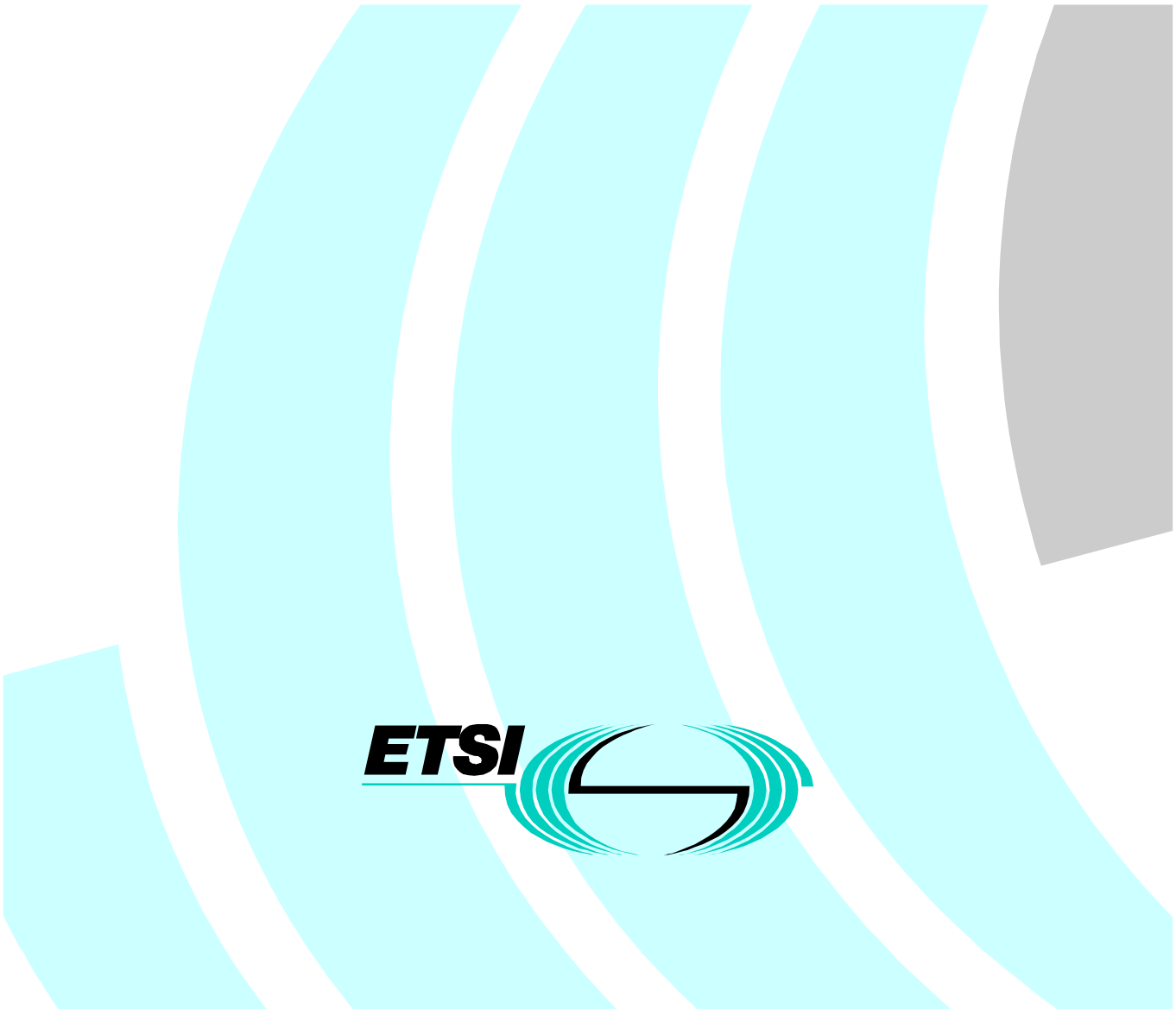
# ETSI EN 300 700 V1.2.1 (2000-09)

*European Standard (Telecommunications series)*

# Digital Enhanced Cordless Telecommunications (DECT); Wireless Relay Station (WRS)



Reference
REN/DECT-050145

Keywords
DECT, repeater

***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 ..... 6
Foreword ..... 6
1 Scope ..... 7
2 References ..... 7
3 Definitions and abbreviations ..... 8
3.1 Definitions ..... 8
3.2 Abbreviations ..... 9
4 Wireless Relay Station (WRS) ..... 10
4.1 Introduction ..... 10
4.2 Description ..... 10
4.2.1 PHY layer functions ..... 11
4.2.2 MAC layer functions ..... 11
4.2.3 DLC layer functions ..... 11
4.2.4 NWK layer functions ..... 11
4.2.4.1 Over-the-air maintenance ..... 11
4.2.5 Identities ..... 12
4.3 Services ..... 12
4.4 Procedures ..... 12
4.4.1 PHY layer ..... 12
4.4.2 MAC layer ..... 12
4.4.2.1 Extended fixed part capabilities ..... 12
4.4.2.2 Hop control ..... 12
5 Cordless Radio Fixed Part (CRFP) ..... 13
5.1 Description ..... 13
5.1.1 General ..... 13
5.1.2 Reference model ..... 13
5.1.3 MAC layer functions ..... 13
5.1.3.1 General ..... 13
5.1.3.2 Frame multiplexing structure ..... 14
5.1.3.3 Logical channel mapping ..... 15
5.1.3.4 Quality Control and Flow Control ..... 15
5.1.4 NWK layer functions ..... 15
5.1.5 Identities ..... 16
5.1.5.1 Identities and addressing ..... 16
5.1.5.2 Subscription data ..... 16
5.2 Messages ..... 16
5.2.1 MAC layer control ..... 16
5.3 Procedures ..... 17
5.3.1 MAC layer ..... 17
5.3.1.1 Connection Oriented mode (C/O) procedures at CRFP ..... 17
5.3.1.1.1 Creation of a Relay Multi Bearer Control (RMBC) ..... 17
5.3.1.1.2 Normal C/O bearer setup ..... 17
5.3.1.1.3 Dual C/O bearer setup ..... 18
5.3.1.1.4 C/O connection release ..... 19
5.3.1.1.5 C/O abnormal connection release ..... 20
5.3.1.2 CRFP connection suspend and resume ..... 21
5.3.1.3 C/O bearer handover ..... 22
5.3.2 DLC layer ..... 24
5.3.2.1 Connection handover ..... 24
5.3.2.2 DLC variables ..... 25
5.3.3 NWK layer ..... 25
5.3.4 Security ..... 27
5.3.4.1 General ..... 27

5.3.4.2 CRFP initialization of PT cipher key ..... 30
5.3.5 Management ..... 30
5.3.5.1 CRFP MAC modes ..... 30
5.3.5.2 CRFP states and state transitions ..... 30
5.4 Example operation of CRFP ..... 31
5.4.1 Introduction ..... 31
5.4.2 Example GAP procedures ..... 31

6 Repeater Part (REP) ..... 31
6.1 Description ..... 31
6.1.1 General ..... 31
6.1.2 Reference model ..... 31
6.1.3 MAC layer functions ..... 32
6.1.3.1 General ..... 32
6.1.3.2 Frame multiplexing ..... 32
6.1.3.2.1 Quality control ..... 34
6.1.3.2.2 Bearers selection ..... 35
6.1.3.2.3 Relay of a duplex bearer ..... 35
6.1.3.2.4 Relay of a double simplex bearer ..... 35
6.1.3.3 Logical channel mapping ..... 35
6.1.4 DLC functions ..... 36
6.1.5 NWK layer functions ..... 36
6.1.6 Management functions ..... 36
6.1.6.1 Identities and addressing ..... 36
6.2 Definitions ..... 37
6.3 Messages ..... 37
6.3.1 MAC control ($M_T$) ..... 37
6.4 Procedures ..... 37
6.4.1 MAC layer ..... 37
6.4.1.1 C/O connection ..... 37
6.4.1.1.1 Complementary connection setup procedure ..... 37
6.4.1.1.2 Creation of a double duplex bearer ..... 38
6.4.1.1.3 Mapping procedure ..... 39
6.4.1.2 REP relayed C/O connection ..... 40
6.4.1.2.1 IWU ..... 40
6.4.1.2.2 REP relayed C/O single duplex bearer setup ..... 41
6.4.1.2.3 REP relayed C/O bearer release ..... 41
6.4.1.2.4 REP relayed C/O bearer handover ..... 42
6.4.2 DLC layer ..... 42
6.4.2.1 REP relayed C/O connection handover ..... 42
6.4.3 Management ..... 43
6.4.3.1 REP states ..... 43
6.4.3.2 REP actions and states transitions ..... 44
6.4.3.2.1 Actions in the Idle_Unlocked and Active_Unlocked states ..... 44
6.4.3.2.2 Actions in the Locked state ..... 44
6.4.3.2.3 Entry into the Active_Idle state ..... 44
6.4.3.2.4 Actions in the Active_Idle state ..... 44
6.4.3.2.5 Entry into the Active_Traffic state ..... 45
6.4.3.2.6 Actions in the Active_Traffic state ..... 45
6.4.3.3 Channel selection ..... 45
6.5 Example operation of REP ..... 45

**Annex A (normative): The optional CRFP interface to REP ..... 54**

A.1 Description ..... 54
A.1.1 General ..... 54
A.1.2 Frame multiplexing structure ..... 54

A.2 Messages ..... 55
A.2.1 MAC layer ..... 55
A.2.2 Hop control ..... 55

A.3 Procedures ..... 55
A.3.1 MAC layer ..... 55
A.3.2 Channel selection ..... 58

**Annex B (normative): CRFP Interworking with GAP-based Fixed Parts ..... 59**

B.1 Additions and modifications to GAP Fixed Parts ..... 59
B.1.1 Downlink broadcast for "CRFP Interworking with GAP-based Fixed Parts" ..... 59
B.1.1.1 $Q_T$ - Extended fixed part capabilities ..... 59
B.1.2 Intra-cell Bearer Handover ..... 59
B.1.3 NWK layer features/procedures support ..... 60
B.1.4 Bearer handover bit mask management ..... 60

B.2 Requirements on the CRFP ..... 60
B.2.1 General ..... 60
B.2.2 Downlink broadcast ..... 61
B.2.2.1 $N_T$ message ..... 61
B.2.2.2 $Q_T$ - static information ($Q_H = 0$) ..... 61
B.2.2.3 $Q_T$ - Extended RF carrier information ($Q_H = 2$) ..... 62
B.2.2.4 $Q_T$ - FP capabilities ($Q_H = 3$) ..... 62
B.2.2.5 $Q_T$ - Extended FP capabilities ($Q_H = 4$) ..... 63
B.2.2.6 $Q_T$ - SARI support ($Q_H = 5$) ..... 63
B.2.2.7 $Q_T$ - Multiframe number ($Q_H = 6$) ..... 63
B.2.3 Paging broadcast ..... 64
B.2.3.1 Short page, normal/extended paging ..... 64
B.2.3.2 Zero length page, normal/extended paging ..... 64
B.2.4 Quality control of relayed connections ..... 64
B.2.5 NWK layer features/procedures support ..... 65

B.3 NWK layer procedures ..... 65
B.3.1 Obtaining access rights for WRS ..... 65
B.3.2 Retrieval of WRS- RPN ..... 66
B.3.3 Indication/modification of WRS- RPN ..... 67
B.3.4 Obtaining access rights for encryption of connections relayed by WRS ..... 68
B.3.5 Indication of WRS - cipher key ..... 69
B.3.6 Dual cipher switching ..... 69
B.3.7 Location registration with TPUI assignment for WRS ..... 71

B.4 Management procedures ..... 71
B.4.1 Initialization of CRFP ..... 71
B.4.1.1 Indication/Modification of WRS/RPN ..... 71
B.4.2 Management for Encryption of relayed connections ..... 71

History ..... 72

# Intellectual Property Rights

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 (http://www.etsi.org/ipr).

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.

# Foreword

This European Standard (Telecommunications series) has been produced by ETSI Project Digital Enhanced Cordless Telecommunications (DECT).

| **National transposition dates** | |
|---|---|
| Date of adoption of this EN: | 1 September 2000 |
| Date of latest announcement of this EN (doa): | 31 December 2000 |
| Date of latest publication of new National Standard or endorsement of this EN (dop/e): | 30 June 2001 |
| Date of withdrawal of any conflicting National Standard (dow): | 30 June 2001 |

# 1 Scope

The present document defines the Digital Enhanced Cordless Telecommunications (DECT) Wireless Relay Station (WRS). A WRS is an additional building block for the DECT fixed network.

The present document defines provisions needed for a controlled and reliable application of the DECT WRS infrastructure building block. These provisions are not related to any specific profile.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] ETSI EN 300 175-1 (V1.4): "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 1: Overview".

[2] ETSI EN 300 175-2 (V1.4): "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 2: Physical Layer (PHY)".

[3] ETSI EN 300 175-3 (V1.4): "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 3: Medium Access Control (MAC) Layer".

[4] ETSI EN 300 175-4 (V1.4): "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 4: Data Link Control (DLC) Layer".

[5] ETSI EN 300 175-5 (V1.4): "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 5: Network (NWK) Layer".

[6] ETSI EN 300 175-6 (V1.4): "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 6: Identities and Addressing".

[7] ETSI EN 300 175-7 (V1.4): "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 7: Security Features".

[8] ETSI EN 300 175-8 (V1.4): "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 8: Speech Coding and Transmission".

[9] ETSI ETR 043: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Services and facilities requirements specification".

[10] ETSI ETR 246: "Digital Enhanced Cordless Telecommunications (DECT); Application of DECT Wireless Relay Stations (WRS)".

[11] ETSI EN 300 444 (V1.3): "Digital Enhanced Cordless Telecommunications (DECT); Generic Access Profile (GAP)".

# 3 Definitions and abbreviations

## 3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

**Cordless Radio Fixed Part (CRFP):** WRS that provides independent bearer control to a Portable radio Termination (PT) and Fixed radio Termination (FT) for relayed connections

**Fixed Part (DECT Fixed Part) (FP):** physical grouping that contains all of the elements in the DECT network between the local network and the DECT air interface

NOTE 1: A DECT FP contains the logical elements of at least one FT, plus additional implementation specific elements.

**Fixed radio Termination (FT):** logical group of functions that contains all of the DECT processes and procedures on the fixed side of the DECT air interface

NOTE 2: A FT only includes elements that are defined in the DECT CI standard. This includes radio transmission elements together with a selection of layer 2 and layer 3 elements.

**Handover:** process of switching a call in progress from one physical channel to another physical channel. These processes can be internal (see internal handover) or external (see external handover)

NOTE 3: There are two physical forms of handover, intra-cell handover and inter-cell handover. Intra-cell handover is always internal. Inter-cell handover can be internal or external.

**Inter Working Unit (IWU):** unit that is used to interconnect sub networks

NOTE 4: The IWU contains the interworking functions necessary to support the required sub network interworking.

**Medium Access Control (MAC) Connection (CONNECTION):** association between one source MAC Multi-Bearer Control (MBC) entity and one destination MAC MBC entity. This provides a set of related MAC services (a set of logical channels), and it can involve one or more underlying MAC bearers

**Portable Part (DECT Portable Part) (PP):** physical grouping that contains all elements between the user and the DECT air interface. PP is a generic term that may describe one or several physical pieces

NOTE 5: A DECT PP is logically divided into one PT plus one or more Portable Applications (PAs).

**Portable radio Termination (PT):** logical group of functions that contains all of the DECT processes and procedures on the portable side of the DECT air interface

NOTE 6: A PT only includes elements that are defined in the DECT CI standard. This includes radio transmission elements (layer 1) together with a selection of layer 2 and layer 3 elements.

**Radio Fixed Part (RFP):** one physical sub-group of a FP that contains all the radio end points (one or more) that are connected to a single system of antennas

**Repeater Part (REP):** WRS that relays the information within the half frame time interval

**Wireless Relay Station (WRS):** physical grouping that combines elements of both PTs and FTs to relay information on a physical channel from one DECT termination to a physical channel for another DECT termination

NOTE 7: The DECT termination can be a PT or an FT or another WRS.

## 3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

| | |
|---|---|
| AC | Authentication Code |
| ARI | Access Rights Identity |
| BMC | Broadcast Message Control |
| C/O | Connection Oriented mode |
| CK | Cipher Key |
| CN | Carrier Number |
| CRFP | Cordless Radio Fixed Part |
| DCK | Derived Cipher Key |
| DECT | Digital Enhanced Cordless Telecommunications |
| DLC | Data Link Control |
| FMID | Fixed part MAC Identity |
| FP | Fixed Part |
| FT | Fixed radio Termination |
| GAP | Generic Access Profile |
| IPUI | International Portable User Identity |
| IWU | Inter Working Unit |
| KSG | Key Stream Generator |
| LLME | Lower Layer Management Entity |
| LSB | Least Significant Bit |
| MAC | Medium Access Control |
| MBC | Multi Bearer Control |
| MMI | Man Machine Interface |
| NWK | Network |
| OA&M | Operation, Administration and Maintenance |
| PA | Portable Application |
| PARI | Primary Access Rights Identity |
| PARK | Portable Access Rights Key |
| PHY | Physical Layer |
| PMID | Portable part MAC Identity |
| PP | Portable Part |
| PT | Portable radio Termination |
| REP | Repeater Part |
| RFP | Radio Fixed Part |
| RFPI | Radio Fixed Part Identity |
| RMBC | Relay Multi Bearer Control |
| RPN | Radio fixed Part Number |
| RX | Receive |
| SAP | Service Access Point |
| SN | Slot pair Number |
| TBC | Traffic Bearer Control |
| TPUI | Temporary Portable User Identity |
| TX | Transmit |
| UAK | User Authentication Key |
| WRS | Wireless Relay station |

# 4 Wireless Relay Station (WRS)

## 4.1 Introduction

A WRS is a physical grouping that contains both Fixed radio Termination (FT) and Portable radio Termination (PT) elements, and that transfers information between a Radio Fixed Part (RFP) and a Portable Part (PP). The FT element acts towards a PP exactly as an ordinary RFP. The PT element acts like a PP towards the RFP, and is locked to the closest RFP. The WRS contains interworking between its FT and its PT, including transparent transfer of the higher layer DECT services. WRS links may be cascaded.

Compared to an RFP, a WRS may introduce capacity restrictions to the services offered. The restrictions may increase with the number of cascaded WRS links (hops). Single WRS link applications can be generally applied. However, special precautions are needed when applying cascaded WRS links. The capacity may be too low, or there may be a need to adjust the echo control requirements.

A WRS shall comply with the general FT identities requirements for RFPs. Installing or adding a WRS to a DECT infrastructure is not possible outside the control of the system operator/installer/owner, who provides the required system identities, access rights and authentication/encryption keys.

The present document defines two different WRS concepts, the CRFP and the REP, which are detailed in clauses 5 and 6 respectively.

## 4.2 Description

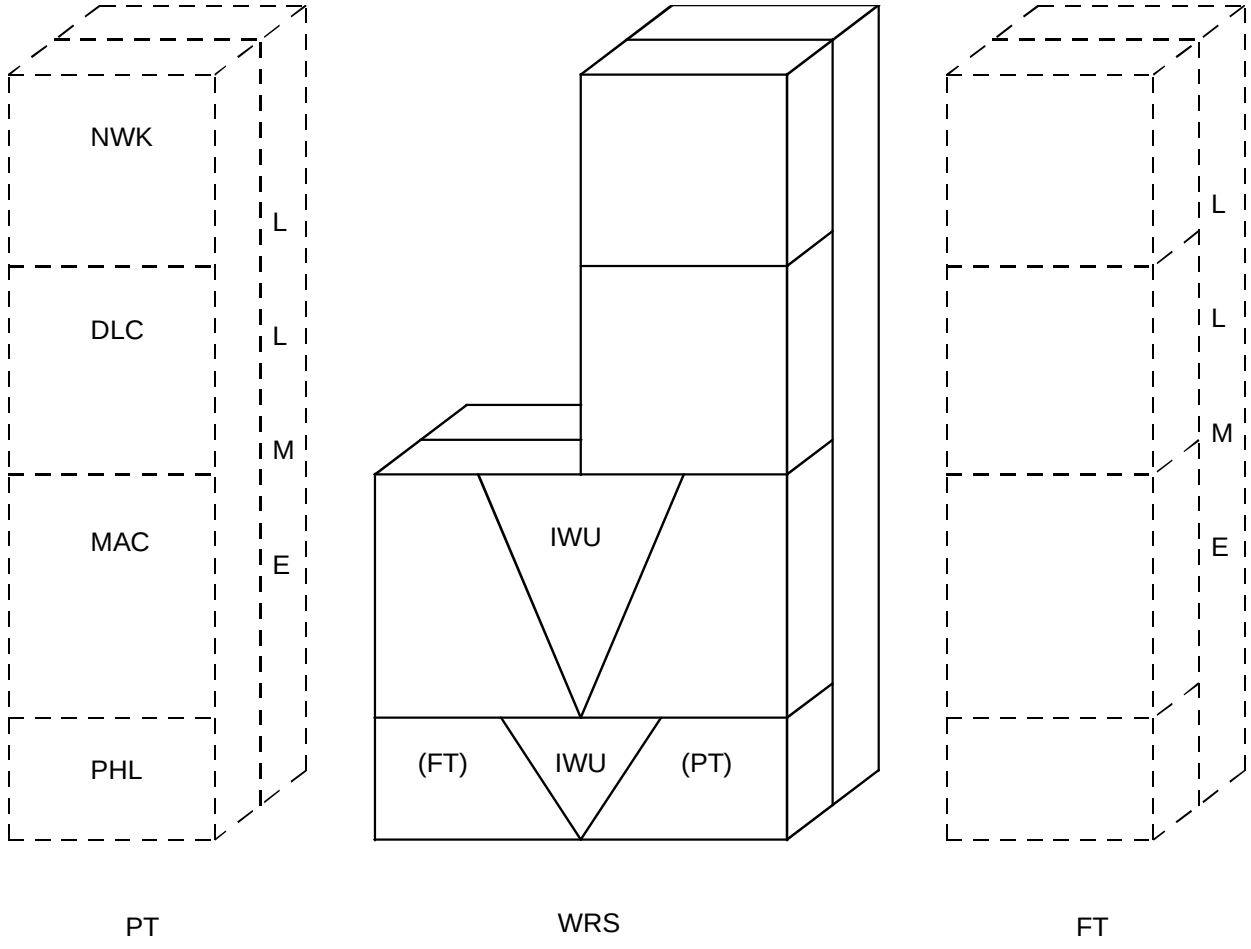



**Figure 1: WRS reference model, Protocol stack model**

The WRS, as shown in figure 1, provides interworking on the DECT air interface between a PT and an FT as described in EN 300 175, Parts 1 to 8, [1] to [8].

The PT may also be the PT side of a WRS in a multi-hop scenario.

The reference model of figure 1 establishes the following basic principles of the WRS:

- interworking with PTs as defined by EN 300 175, Parts 1 to 8, [1] to [8];
- interworking with FTs as defined by EN 300 175, Parts 1 to 8, [1] to [8], with additions defined in the present document;
- interworking between PT and FT side is provided at Medium Access Control (MAC) layer and Physical (PHY) layer;
- a logical grouping of PT and WRS operates as a PT;
- a logical grouping of FT and WRS operates as a FT.

Looking towards the PT the WRS is fully protocol transparent. The PT cannot distinguish the WRS from any other RFP within an FT. Therefore, the WRS puts no additional requirements on the PT.

### 4.2.1 PHY layer functions

The WRS shall fulfil the following PHY layer requirements:

- the WRS shall for the relevant packet type meet the PP requirements in EN 300 175-2 [2] when it is acting as a PP, and meet the RFP requirements in EN 300 175-2 [2] when it is acting as an RFP, except that the timing requirements in EN 300 175-2 [2], subclause 4.2.4 shall be met by all WRS transmissions and that the requirement in EN 300 175-2 [2], subclause 4.2.5 on difference between reference timers shall be disregarded;
- Z-field mapping as defined in EN 300 175-2 [2], subclause 4.8 shall be supported.

### 4.2.2 MAC layer functions

The WRS provides interworking at the MAC layer. The WRS incorporates PT and FT functions as defined in EN 300 175-3 [3].

The WRS shall fulfil the obligatory requirements of EN 300 175-3 [3], subclauses 11.4 and 11.6, with the modifications as defined in the present document.

### 4.2.3 DLC layer functions

The WRS may incorporate DLC layer PT functionality to support communication with the FT according to EN 300 175-4 [4].

### 4.2.4 NWK layer functions

The WRS may incorporate NWK layer PT functionality to support communication with the FT according to EN 300 175-5 [5].

#### 4.2.4.1 Over-the-air maintenance

If Operation, Administration and Maintenance (OA&M) information transfer is supported, it may use the <<IWU-TO-IWU>> information element (see EN 300 175-5 [5], subclause 7.7.23) in NWK layer messages. This element can accommodate unstructured user specific data. For over the air maintenance, a link towards the WRS is created using the PP identity of the WRS.

### 4.2.5 Identities

The WRS shall have a specific Radio fixed Part Number (RPN) identity and Portable Access Rights Key (PARK). The RPN may be transferred by over-the-air maintenance procedures. For transferring the RPN to the WRS, the Fixed Identity information element with identity type "ARI + RPN for WRS" should be used.

The WRS may have additional specific PT identities when PT DLC and NWK layer functionality is included.

## 4.3 Services

The WRS may be used in all applications as defined in ETR 043 [9]. Typical WRS applications are presented in ETR 246 [10].

The WRS shall provide a relay service for MAC layer connection oriented, broadcast and connectionless services as defined in EN 300 175-3 [3], subclauses 5.6 and 5.7.

The WRS shall provide the services as given in table 1.

**Table 1: WRS services**

| | Offered service | Support | Comment |
|---|---|---|---|
| S.1 | Transparency between PT and FT | Yes | |
| S.2 | MAC services | Yes | All, see EN 300 175-3 [3] |
| S.3 | Over the air maintenance | Optional | |
| S.4 | PT services<br>(e.g. authentication) | Optional | As applicable for a certain application (e.g. based on a profile) |

## 4.4 Procedures

### 4.4.1 PHY layer

The WRS shall conform to the PT and FT procedures as defined by EN 300 175-2 [2].

### 4.4.2 MAC layer

The WRS shall conform to the PT and FT procedures as defined by EN 300 175-3 [3].

#### 4.4.2.1 Extended fixed part capabilities

The FP can control the hop configuration and indicate the admitted WRS scenarios by means of the extended fixed part capabilities message (see EN 300 175-3 [3]).

The extended fixed part capabilities message shall be sent by all WRSs at least once every 8 multiframes, and all WRSs shall understand this message. The WRS shall assume all WRS support bits being set to '0' when the FT does not transmit the message.

#### 4.4.2.2 Hop control

The WRS that is locked to an FT shall decrease the value HOPS (when > 0) of the corresponding WRS type (CRFP or REP respectively; see clauses 5 and 6 in the received extended fixed part capabilities message (see EN 300 175-3 [3], subclause 7.2.3.5.2.1) for the transmission of its own extended fixed part capability information.

NOTE: The number of hops should be no more than one. Use of more than one hop may be subject to agreement with national radio authorities.

# 5 Cordless Radio Fixed Part (CRFP)

This clause defines requirements in addition to the general requirements for the WRS in clause 4.

## 5.1 Description

### 5.1.1 General

This description avoids defining specific implementations of the CRFP for a certain application. ETR 246 [10] clarifies the operation of the CRFP for typical applications. This description defines the architecture model of the CRFP and additional messages and procedures necessary to support the CRFPs in the DECT environment.

In this description the full slot frame multiplexing structure and IN_minimum_delay speech service are used for descriptive purposes only, and not to restrict the application of the CRFP to a specific slot structure or service.

### 5.1.2 Reference model

The reference model of figure 1 is applicable for the CRFP. The PT side of the CRFP is called CRFP_PT. The FT side of the CRFP is called CRFP_FT.

To support a CRFP, the following additional procedures are defined for the FT:

- MAC layer: access control of CRFP (for specific information transfer to CRFPs);
- NWK layer: Cipher Key (CK) transfer to CRFP.

The following functions are defined for the CRFP based on EN 300 175, Parts 1 to 8, [1] to [8]:

- FT and PT PHY and MAC layer to provide independent bearer control to PTs and FT;
- a selection of PT DLC and NWK layer to support communication between CRFP and FT.

The following additional functions and procedures are defined for the CRFP:

- IWU at MAC and PHY layer to provide interworking between CRFP_PT and CRFP_FT;
- access control procedures to support both relay and local handling of data on the same bearer;
- CK uploading and initialization for CRFP_FT MAC.

### 5.1.3 MAC layer functions

#### 5.1.3.1 General

The basic function of the CRFP is defined by its frame multiplexing structure. Procedures are defined based on this structure to allow the CRFP to support required services.

### 5.1.3.2 Frame multiplexing structure

Figure 2 shows the typical frame multiplexing structure for a CRFP that supports full slots with IN_minimum_delay.

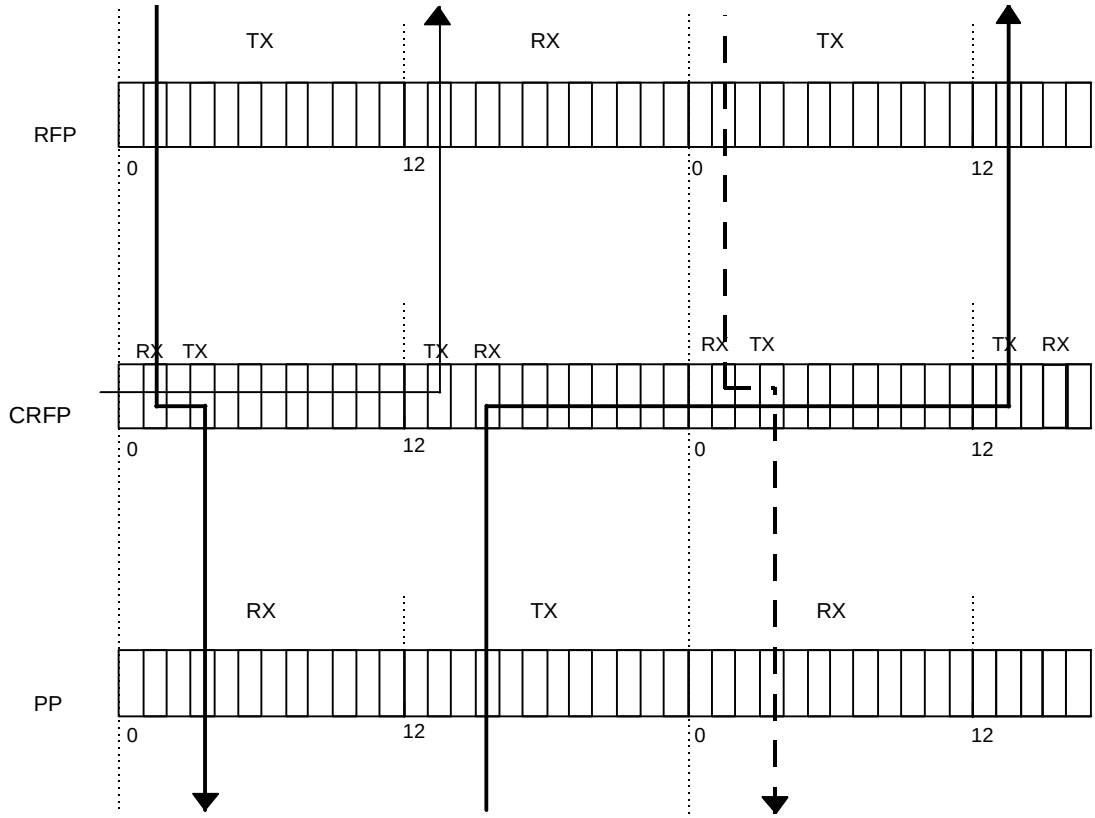



**Figure 2: Typical frame multiplexing structure of the CRFP**

Use of one hop via a CRFP will cause an additional delay of 1 frame, no matter what timeslots are used.

The frame multiplexing structure supports a combination of both links with PTs and FTs. In this dual frame multiplexing structure the CRFP may transmit or receive during any slot of a frame. A duplex bearer to either the PT or FT is still supported by a combination of a CRFP Receive (RX) and Transmit (TX) slot separated by one half frame.

The CRFP shall support the frame multiplexing structure defined as:

- CRFP-PT frames and CRFP-FT frames are synchronized to the FT frames;
- CRFP-PT and CRFP-FT bearer control complies at least with EN 300 175-3 [3] (e.g. Duplex bearers are separated by one half frame);
- relayed logical channels are buffered to support MAC multiplexing rules of CRFP-PT and CRFP-FT;
- available slots of the CRFP are marked to be either Receive (RX) or Transmit (TX) slots. A slot shall be regarded as TX slot only when it is actually used for transmission;

NOTE 1: During the first half frame (e.g. Slot 0 to 11) all RX slots listen to FT transmissions and all TX slots transmit to PTs. During the second half frame all RX slots listen to PTs and all TX slots should transmit to FT.

- RX and TX slots of one relayed bearer belong to the same half frame.

NOTE 2: In idle mode the CRFP listens to an FT during all frames, transmits at least one dummy bearer (see EN 300 175-3 [3]) to PTs and performs receiver scanning on all other slots. Idle receiver scanning is done in accordance with PT and FT idle receiver scan procedures.

#### 5.1.3.3 Logical channel mapping

The CRFP_PT and CRFP_FT shall fulfil the multiplexing rules as defined in EN 300 175-3 [3].

Handling of logical channel data received at CRFP_PT shall be as follows:

ME-SAP (Q, N, P, M): data shall be delivered to the Lower Layer Management Entity (LLME) of CRFP. The LLME of the CRFP shall also generate information for the BMC of the CRFP_FT;

MA-SAP ($B_S$): data shall be delivered to the higher layer and to the IWU of the CRFP. The IWU shall issue a MAC-PAGE.Req for the BMC of the CRFP_FT;

MB-SAP ($C_L$, $SI_N$, $SI_P$): data shall be delivered to the higher layer and to the IWU of the CRFP;

MC-SAP (C, I, $G_F$): U-plane data shall always be relayed by the IWU. Depending on the CRFP state, the C-plane data shall be delivered as follows:

- in "local state", all C-plane data is delivered to higher layers;
- in "relay state", all C-plane data is delivered to the IWU for relay at CRFP_FT.

The local and relay state of a connection are defined in subclause 5.3.1.1.

All other logical channel data is handled locally in the CRFP_PT and CRFP_FT MAC. Logical channel data received at CRFP_FT related to the MB-SAP and MC-SAP shall be delivered to the IWU for relay. ME-SAP data shall be delivered to the LLME of the CRFP.

**Delay logical channels:**

Logical channel information that is relayed in the CRFP shall bear a minimum delay within the constraints of the multiplexing rules as defined in subclause 6.2.2 of EN 300 175-3 [3]. IN_minimum_delay information, like speech, shall be relayed in the same or next frame, depending upon bearer position.

#### 5.1.3.4 Quality Control and Flow Control

The CRFP has separate quality control and flow control on the two links.

For C-channel and $I_P$ channel flow control, for antenna switch requests and sliding collision detection, the BCK and Q2 bits shall be used for each link and the procedures as described in EN 300 175-3 [3] shall be followed for each link independently.

If the CRFP receives a B-field with corrupt $I_N$ data (X-CRC failed) then it shall relay this data and change the B-field identifications ($a_4$, $a_5$ and $a_6$ bits) to '001' B.

If the CRFP receives a B-field with corrupt $I_P$ error detect data then it shall relay this data and change the B-field identifications ($a_4$, $a_5$ and $a_6$ bits) to '000' B.

### 5.1.4 NWK layer functions

Additional functionality in NWK layer and LLME of both FT and CRFP is defined to support over-the-air CK transfer (for encryption of relayed connections) and OA&M.

### 5.1.5 Identities

#### 5.1.5.1 Identities and addressing

The connections in the CRFP are identified by Portable part MAC Identities (PMIDs).

Relayed connections shall use the PMID of a PT.

Connections in local state shall use a PMID of the CRFP. To allow multiple local connections simultaneously, the CRFP shall provide multiple PMIDs. Each PMID should be related to a different International Portable User Identity (IPUI) of the CRFP. Therefore the CRFP may comprise multiple IPUIs.

Both in relay state and local state, the FMID used to address a CRFP is derived from the PARI of the FT and the RPN of the CRFP and the FMID used to address a RFP is derived from the PARI of the FT and the RPN of the RFP according to EN 300 175-3 [3].

The PARK should be the same for all IPUIs of the CRFP.

At the NWK layer the FT can address the CRFP as a PT. The CRFP may define one IPUI of the available ones, which shall be used for over-the-air maintenance. The FT may address other IPUIs of the CRFP to derive Derived Cipher Key (DCK) from a User Authentication Key (UAK).

#### 5.1.5.2 Subscription data

In order to ensure interworking of the CRFP within a FP with PTs, it is necessary to install the parameters given in table 2 into the CRFP during subscription. The installation procedure is implementation dependent and may require a Man Machine Interface (MMI). It is recommended to use over-the-air maintenance procedures to allow on-air installation of most parameters.

**Table 2: CRFP parameters**

| Parameter | Optional/ Mandatory | Value | Comment |
|---|---|---|---|
| RPN | M | All | PARI is relayed from FT and combined with RPN of CRFP to provide RFPI |
| PARK | M | All | PARK should be the same for all CRFP users |
| IPUI (1..n) | O | All | n is the number of CRFP users |
| UAK/AC (1..n) | O | All | n is the number of CRFP users |
| CK | O | All | CK may be derived from UAK |
| NOTE: The number of CRFP users is the maximum number of simultaneous connections from the CRFP that require higher layer control in the CRFP. | | | |

## 5.2 Messages

### 5.2.1 MAC layer control

The CRFP uses the messages indicated with "**" in EN 300 175-3 [3], subclauses 7.2.5.2.2, 7.2.5.3.1 and 7.3.3.1 only, with the "first PT transmission" code for the first transmission to an FT. For all other transmissions of these messages the CRFP shall use these messages without the "first PT transmission" code.

In all following message diagrams, the notation access.req indicates an access.req message with the "first PT transmission" code, and the notation *access.req indicates a message without the "first PT transmission" code.

# 5.3 Procedures

## 5.3.1 MAC layer

### 5.3.1.1 Connection Oriented mode (C/O) procedures at CRFP

The following procedures provide means to address CRFPs on one physical relayed connection of a FT with a PT. The connection with the PT is either in relay state or local state. In relay state, all higher layer C-plane signalling shall be relayed by the CRFPs between FT and PT. In local state, all higher layer C-plane signalling shall be buffered at the FT and CRFP. The local state is a temporary state to allow higher layer communication between FT and a specific CRFP.

#### 5.3.1.1.1 Creation of a Relay Multi Bearer Control (RMBC)

To perform a relay function in the CRFP, a RMBC is defined in the MAC IWU. The creation of an RMBC in the IWU of the CRFP is very similar to the creation of MBCs as specified in EN 300 175-3 [3], subclause 10.2.4.1.

To setup a relay service the RMBC can use a normal bearer setup or a dual bearer setup depending on the current mode of the CRFP (subclause 5.3.5.1).

#### 5.3.1.1.2 Normal C/O bearer setup

Using the normal bearer setup the FT does not recognize that the bearer setup is arriving from a CRFP, the CRFP_PT operates as a PT. The CRFP connection shall always be in "relay state".

Below the calling side shall be the initiating PT or FT for a bearer setup. The called side shall be the destination PT or FT. Figure 3 shows the time-message diagram for basic setup.

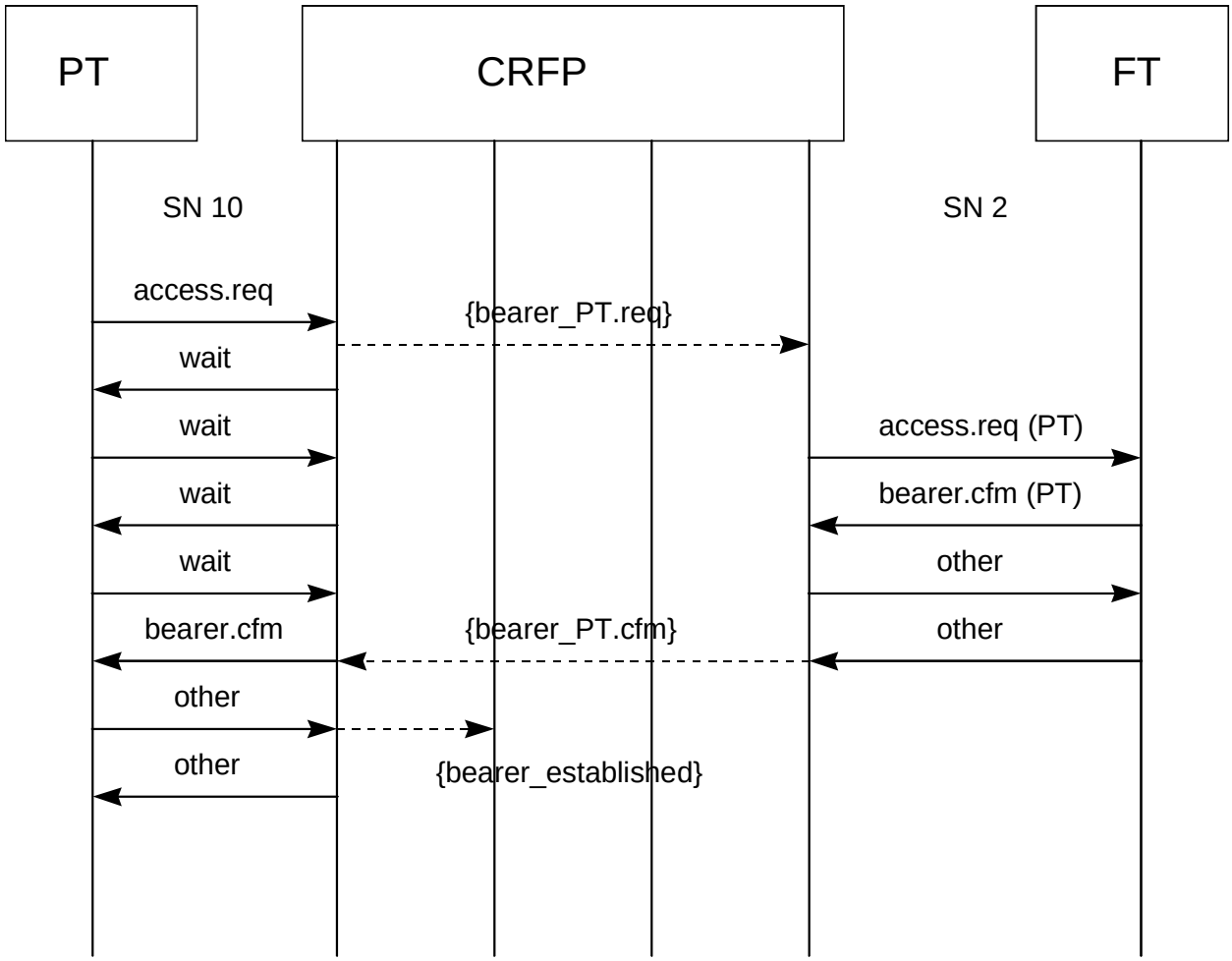



**Figure 3: Normal relay bearer setup**

During the bearer setup procedures $TBC_1$, which has been created at the CRFP due to an "access_request", requests the LLME to be connected to an MBC. If the connection does not exist, the LLME shall create an RMBC in the CRFP. In the mean time $TBC_1$ transmits "wait" messages to the calling side.

The RMBC shall create a new TBC ($TBC_2$) at the other side of the CRFP and shall issue the called address (FMID/PMID) and physical channel description to $TBC_2$. The PMID and FMID of the called and calling parties shall be used (not a CRFP PMID, FMID). The CRFP $TBC_2$ initiates a bearer setup by transmitting the corresponding "access_request" to the called side.

If the bearer setup is successful (after "other" received error free) $TBC_2$ reports "bearer_established" to the RMBC. The RMBC informs the LLME that the requested MBC is connected and $TBC_1$ is allowed to transmit "bearer_confirm" to the calling side.

#### 5.3.1.1.3 Dual C/O bearer setup

Using the dual bearer setup the FT shall recognize that the bearer setup is arriving from a CRFP. The FT can therefore control the state of the CRFP connection using the connection identity of CRFP local service (specific PMID).

Below the calling side is the initiating PT or FT for a bearer setup. The called side is the destination PT or FT. Additional access procedures for the FT are defined below. Figure 4 shows the time-message diagram for basic connections.

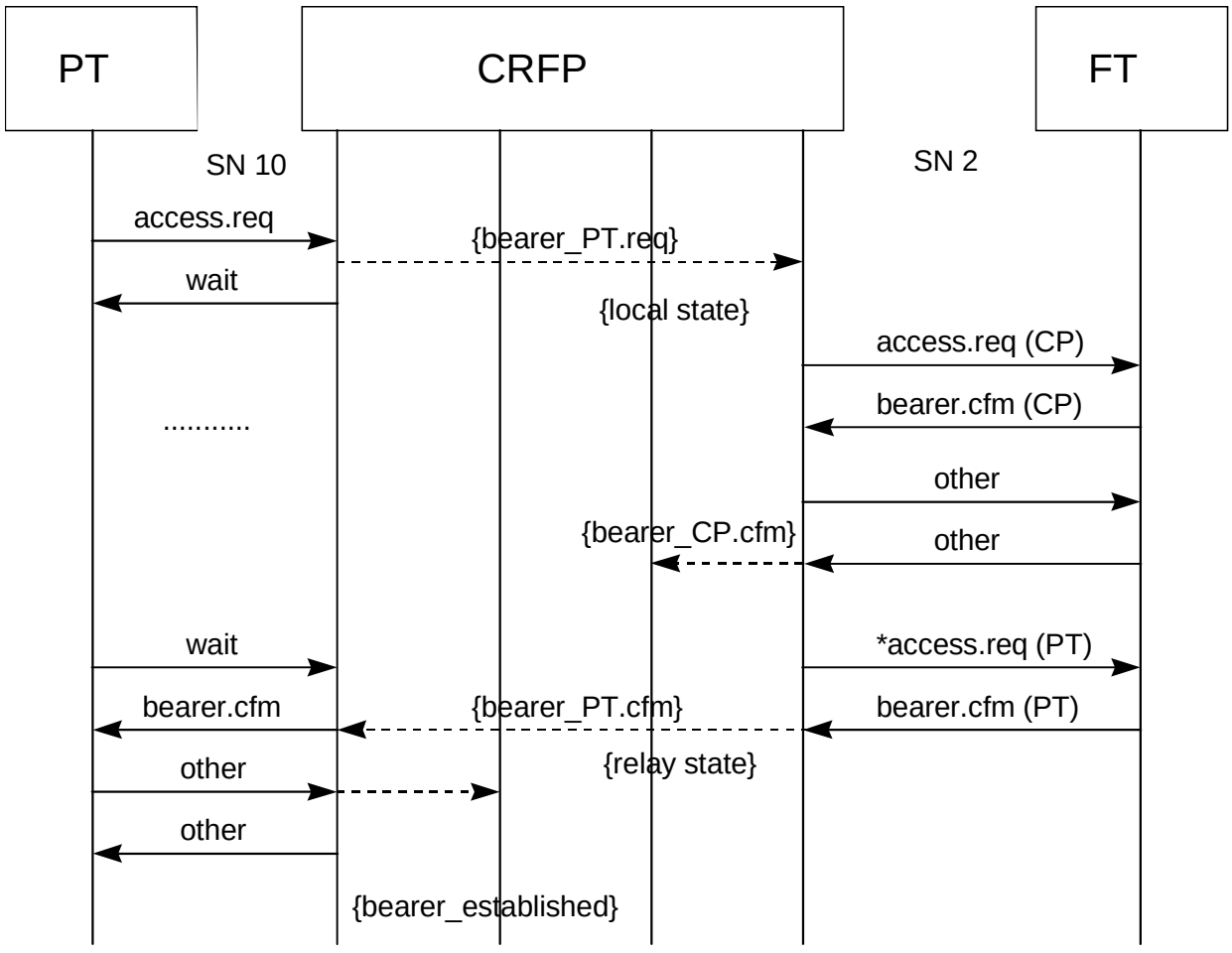



**Figure 4: Dual relay bearer setup**

**At the CRFP**

During the bearer setup procedures the TBC, which has been created at the CRFP due to an "access_request", asks the LLME to be connected to an MBC. If the RMBC related to this connection does not exist, the LLME creates an RMBC and a MBC for the CRFP_PT and CRFP is by definition in "local state". In "local state" the RMBC activities are suspended. The creation of the MBC is reported to the DLC by issuing a MAC-CON.Ind primitive after the first successful bearer setup with the FT.

The MBC creates a TBC for setup of a single duplex bearer connection (with the same slot type as requested by the PT) to an FT and issues the called address (FMID/PMID) and physical channel description to the new TBC. The PMID of the CRFP shall be used.

NOTE: This connection is necessary for CK transfer.

After the TBC has reported "bearer_established" to the MBC, the MBC reports the successful setup of the connection to the LLME, which changes the state of the CRFP for this connection to "relay state". The MBC activities are now suspended and RMBC activities are resumed.

If a TBC exists with the called side, the RMBC shall now relay the "access_request" on that TBC without the "first PT transmission" code, with the PMID and FMID of the called and calling parties (not a CRFP PMID, FMID).

If the bearer setup is successful (after "other" received error free) the TBC reports "bearer_established" to the RMBC. The RMBC informs the LLME that the requested MBC at the called side is connected and the TBC is allowed to transmit "bearer_confirm" to the calling side.

#### 5.3.1.1.4 C/O connection release

**At the CRFP**

When the CRFP receives a release message with the PMID indicating the MBC of the CRFP, the CRFP shall release that MBC.

When the CRFP RMBC is released, the CRFP shall release all corresponding TBCs and MBC at both CRFP_PT and CRFP_FT.

Figure 5 shows the procedure for basic connections.

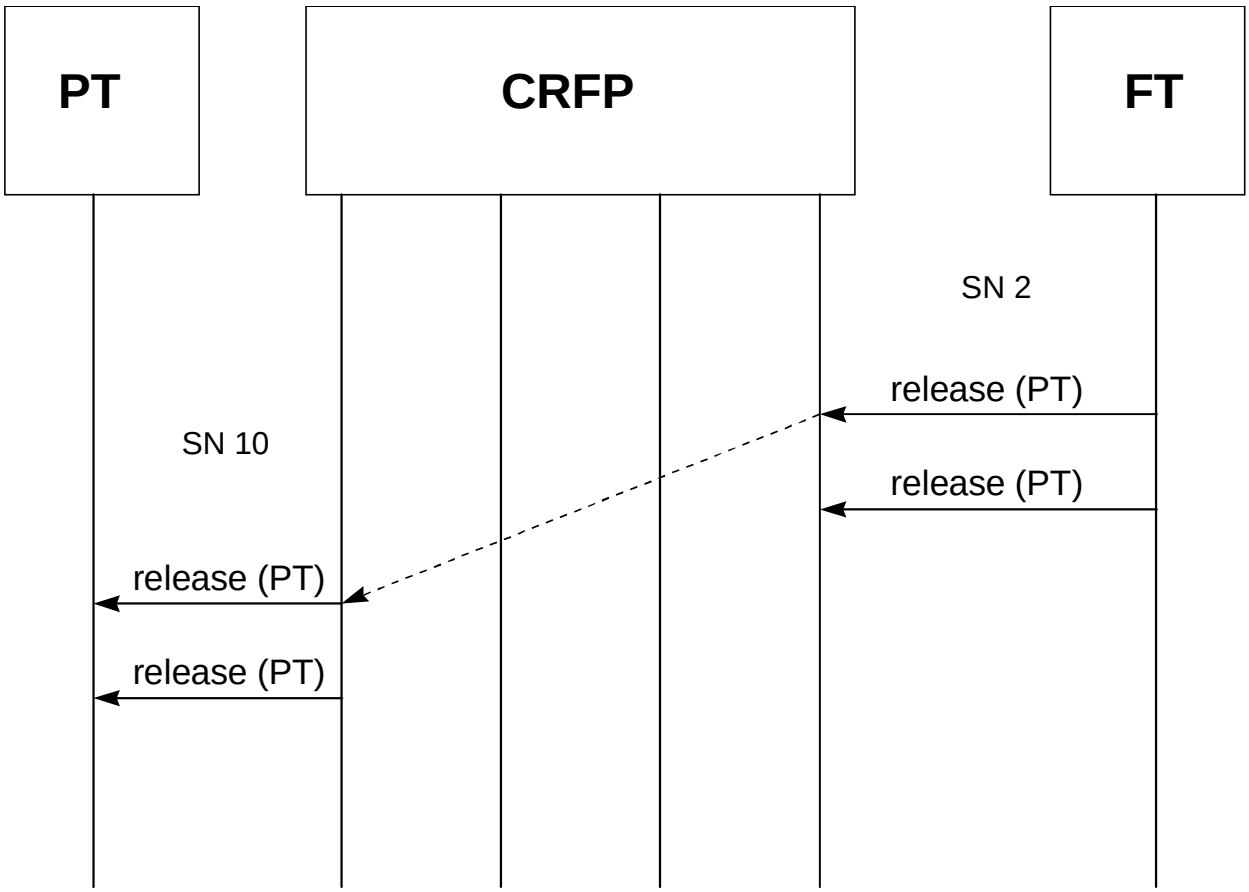



**Figure 5: Release**

#### 5.3.1.1.5 C/O abnormal connection release

If the CRFP detects an abnormal loss of signal, the CFRP shall release all corresponding TBCs, MBC and RMBC at both CRFP_PT and CRFP_FT.

For the release messages generated by the CRFP the PMID of the CRFP shall be used in difference to the normal release cases.

Figures 5a and 5b show the procedures for abnormal connection release.

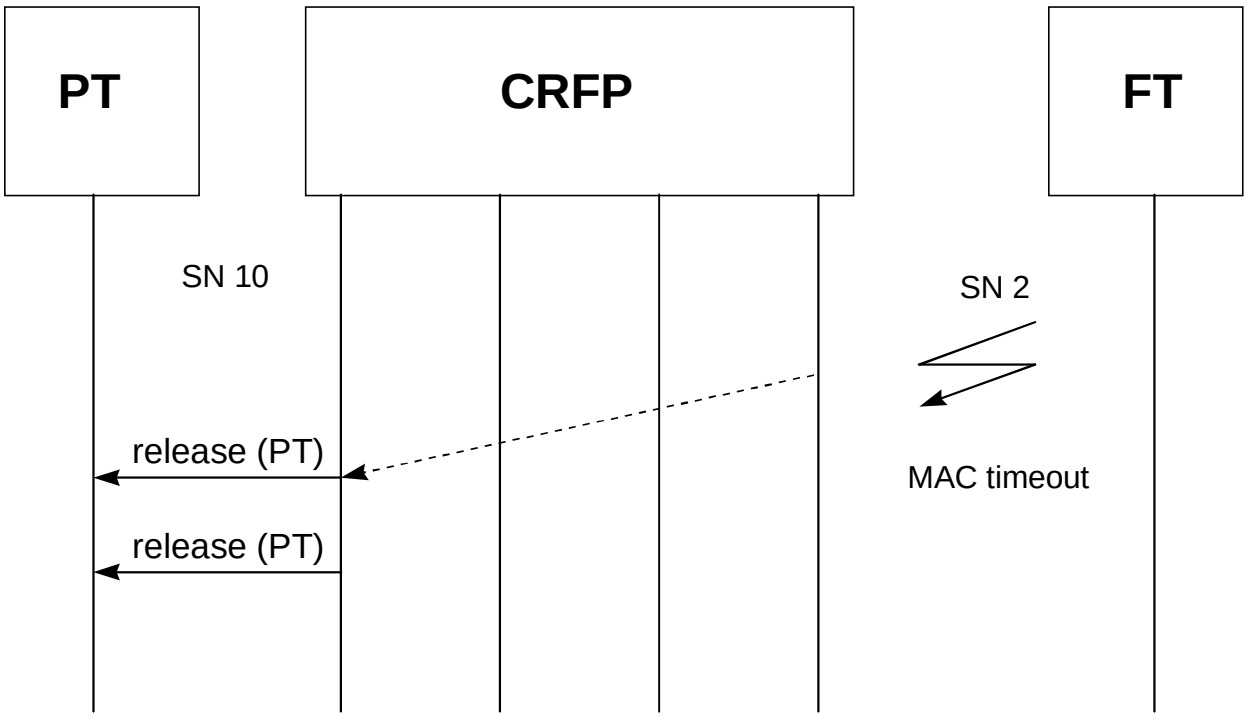



**Figure 5a: Abnormal release at CRFP_PT**

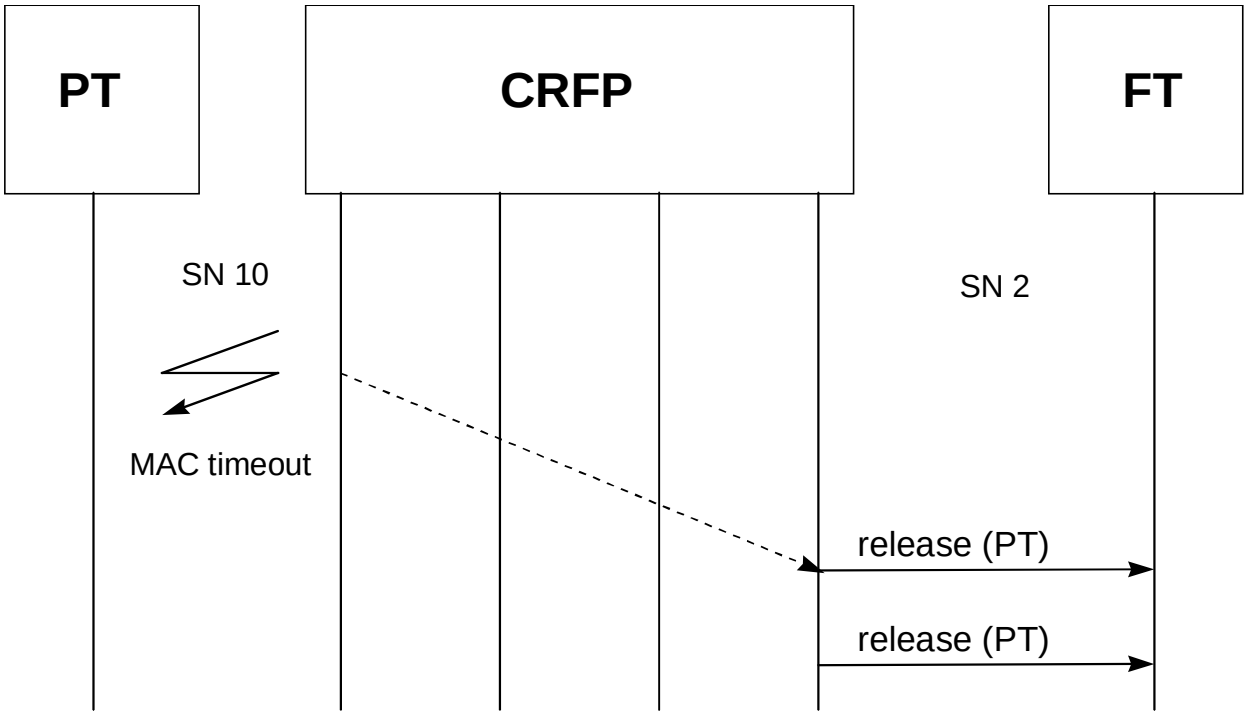



**Figure 5b: Abnormal release at CRFP_FT**

### 5.3.1.2 CRFP connection suspend and resume

**At the CRFP**

When an existing TBC at the CRFP_PT receives an "access_request", the TBC shall ask the LLME to connect to the (R)MBC indicated by the PMID in the message. If the connection with the (R)MBC is possible, the LLME shall suspend the connection with the old (R)MBC. The LLME shall not activate the connection with another (R)MBC, until all outstanding C-channel data in the TBC is successfully transmitted to the FT. Then the LLME shall ask the TBC to transmit "bearer_confirm" and resume the connection with the assigned (R)MBC.

If the access.req is not answered, then the access.req message may be repeated twice.

The CRFP is in "local state", when the TBC is connected with an MBC. The CRFP is in "relay state" when the TBC is connected to an RMBC.

In case of a basic connection, the access request and bearer confirm messages belong to the basic connection control set and in case of an advanced connection, the access request and bearer confirm messages belong to the advanced control set.

In order to establish a CRFP state transition, the FT NWK layer (MM entity) issues a DL-CRFP-STATE-SWITCH primitive to the FT DLC layer. The FT DLC layer issues a MAC-CRFP-STATE-SWITCH primitive to the FT MAC layer. After receiving this primitive, the FT MAC layer requests for a CRFP state transition.

DL-CRFP-STATE-SWITCH {req} primitive parameter list:

| Parameter | req |
|---|---|
| Direction | X |
| X = parameter exists | |

MAC-CRFP-STATE-SWITCH {req} primitive parameter list:

| Parameter | req |
|---|---|
| Direction | X |
| X = parameter exists | |

NOTE 1: Direction = {local to relay, relay to local}

The FT MAC layer can inform the DLC layer about the CRFP state by means of a MAC-CRFP-STATE primitive. The FT DLC layer informs the FT NWK layer (MM entity) about the CRFP state by means of a DLC-CRFP-STATE primitive.

DL-CRFP-STATE-SWITCH {ind} primitive parameter list:

| Parameter | ind |
|---|---|
| State | X |
| X = parameter exists | |

MAC-CRFP-STATE-SWITCH {ind} primitive parameter list:

| Parameter | ind |
|---|---|
| State | X |
| X = parameter exists | |

NOTE 2: State = {local, relay}

Figure 6 shows time-message diagrams for basic connections.

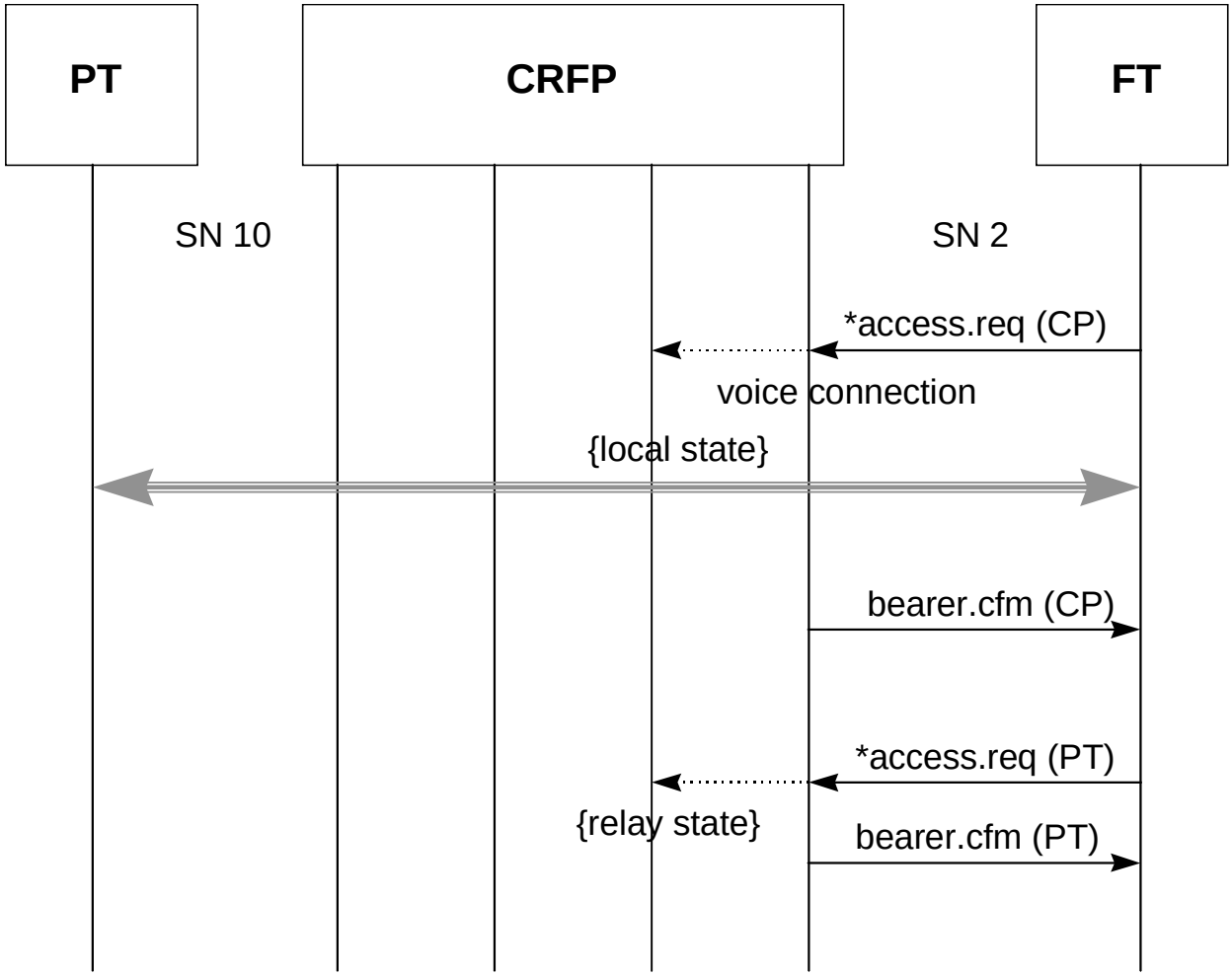



**Figure 6: CRFP connection suspend and resume**

### 5.3.1.3 C/O bearer handover

Bearer handover procedures may be used to perform:

1) intra-cell handover of the PT within the CRFP;
2) intra-cell handover of the CRFP within one RFP;
3) inter-cell handover of the CRFP from one RFP to an RFP belonging to the same cluster;
4) inter-cell handover of the PT from an CRFP to an RFP belonging to the same cluster;
5) inter-cell handover of the PT from an RFP to a CRFP belonging to the same cluster;
6) inter-cell handover of the PT from one CRFP to a CRFP belonging to the same cluster;
7) inter-cell handover of the CRFP from one CRFP to a CRFP belonging to the same cluster.

The CRFP may be defined as a separate cluster or as part of the cluster of the RFP(s) that it is connected to.

The specific bearer handover procedures shall be handled as follows:

1) completely handled at CRFP_FT using procedures as defined in EN 300 175-3 [3];
2) completely handled at CRFP_PT using procedures as defined in EN 300 175-3 [3];
3) completely handled at CRFP_PT using procedures as defined in EN 300 175-3 [3];

4) completely handled by RFP. The connection via the CRFP is released (see figure 7);

5) this handover requires the setup of an RMBC (and MBC) in the CRFP to handle the new bearer. The procedure is identical to the handling of the setup of a new connection via the CRFP as defined by subclause 5.3.1.1, replacing the "access.req" from the PT with a "bearer_handover.req" (see figure 8);

6) this handover is identical to 5) for the CRFP;

7) this handover is a combination of case 3) and 6).

During bearer handover, it is subject of the implementation to avoid loss of signalling and user data. Due to re-arrangement of usage of slots in the CRFP frame multiplexing structure, relay of data may be changed.

NOTE: Due to the extra one frame delay introduced by CRFP, in case of bearer handover it could not be possible to have the same I-channel data (In normal delay and Ip data) on both the new and the old bearer.

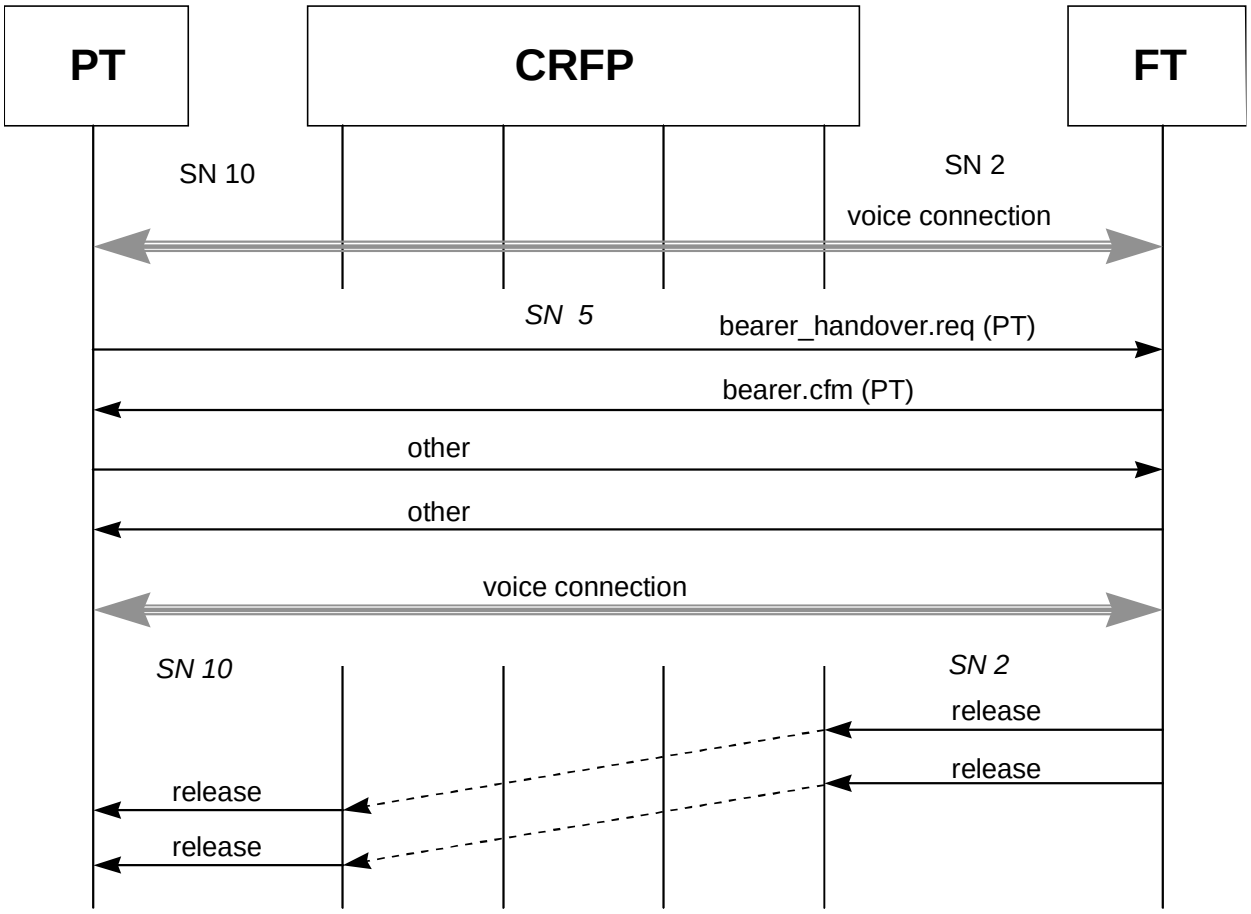



**Figure 7: Bearer handover from CRFP to RFP**

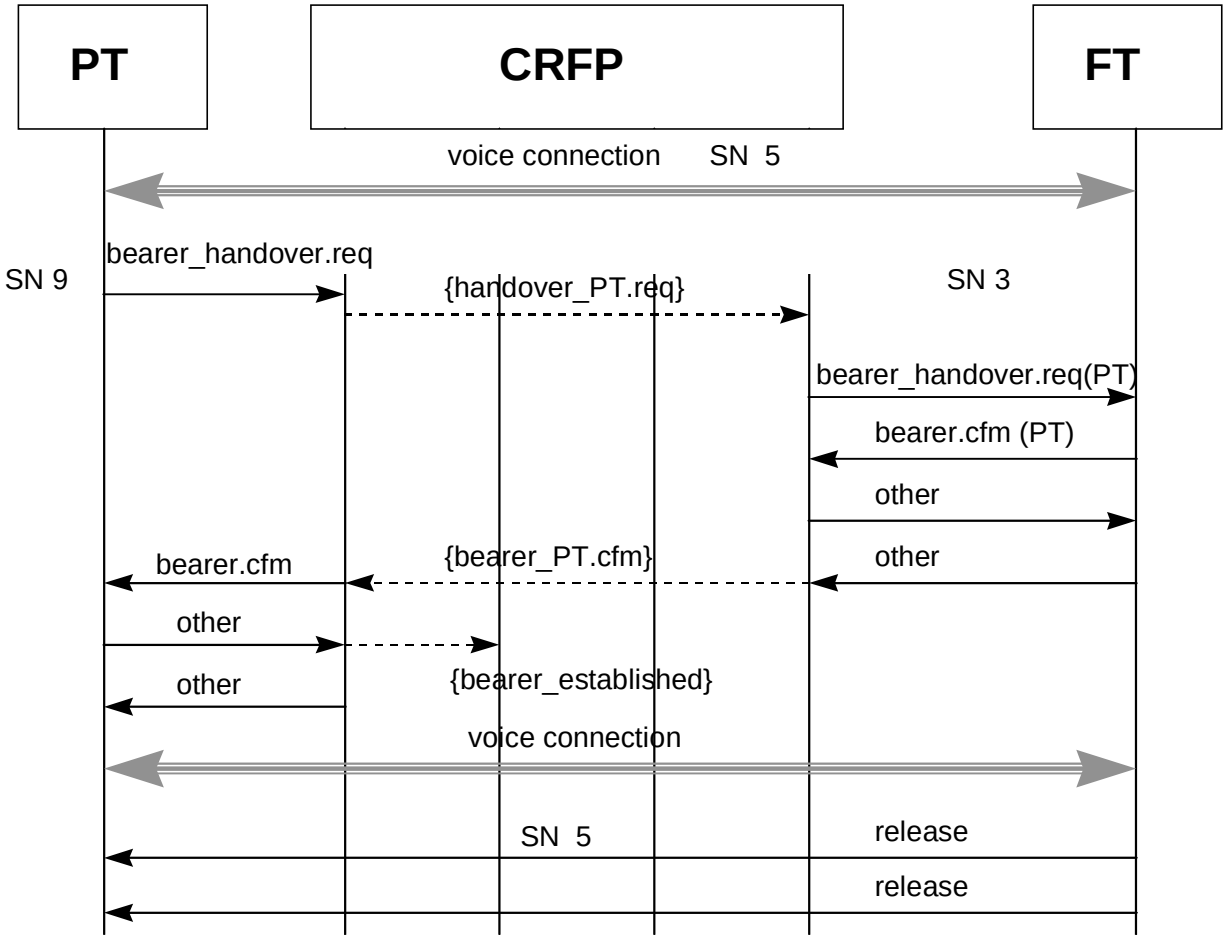



**Figure 8: Bearer handover from a RFP to CRFP (normal setup)**

## 5.3.2 DLC layer

### 5.3.2.1 Connection handover

Connection handover procedures may be used to perform:

1) inter-cell handover of the CRFP from one RFP to an RFP;
2) inter-cell handover of the PT from an CRFP to an RFP;
3) inter-cell handover of the PT from an RFP to a CRFP;
4) inter-cell handover of the PT from one CRFP to a CRFP;
5) inter-cell handover of the CRFP from one CRFP to a CRFP;
6) inter-cell handover of the CRFP from one CRFP (or RFP) to an RFP (or CRFP).

The specific connection handover procedures shall be handled as follows:

1) completely handled at CRFP_PT using procedures as defined in EN 300 175-4 [4];
2) completely handled by RFP. The connection via the CRFP is released;
3) this handover requires the setup of an RMBC (and MBC) in the CRFP to handle the new connection. The procedure is identical to the handling of the setup of a new connection via the CRFP, replacing the "access_req" from the PT with a "connection_handover.req";
4) this handover is identical as 3) for the CRFP;

5) this handover is a combination of 4) and 1).

#### 5.3.2.2 DLC variables

Switching over from local mode to relay mode includes an implicit release of the DLC-link used for the local mode.

### 5.3.3 NWK layer

All PT network and higher layer information is relayed through the CRFP. As an example, figure 11 shows a typical outgoing encrypted call setup with MAC and NWK layer messages via the CRFP.

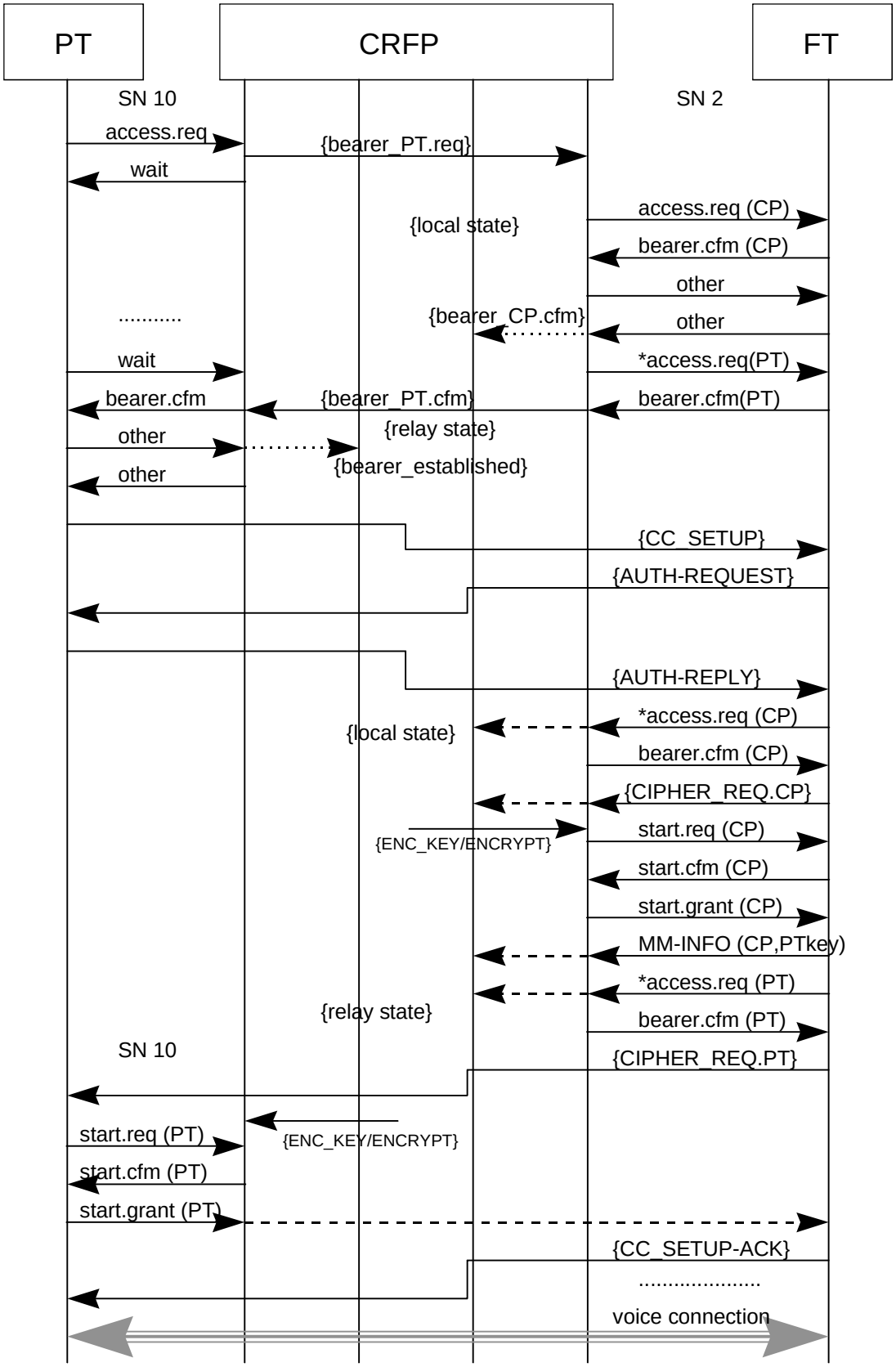



**Figure 9: Typical call setup message diagram (with encryption)**

## 5.3.4 Security

### 5.3.4.1 General

To support encryption for relayed connections via the CRFP, a PT CK needs to be loaded in the CRFP that provides access to the PT (see EN 300 175-7 [7]).

For encryption on a relayed FT-PT connection, different CKs shall be used for links between FT and CRFP and between CRFP and PT. A CRFP CK shall be used for encryption of the FT-CRFP connection and a PT CK shall be used for encryption of the CRFP-PT connection. The PT CK shall be transferred to the CRFP on a ciphered link. Different keys shall be used for different connections between FT and a CRFP.

Figure 10 shows the protocol diagram for the CRFP supporting encryption on these relayed connections.

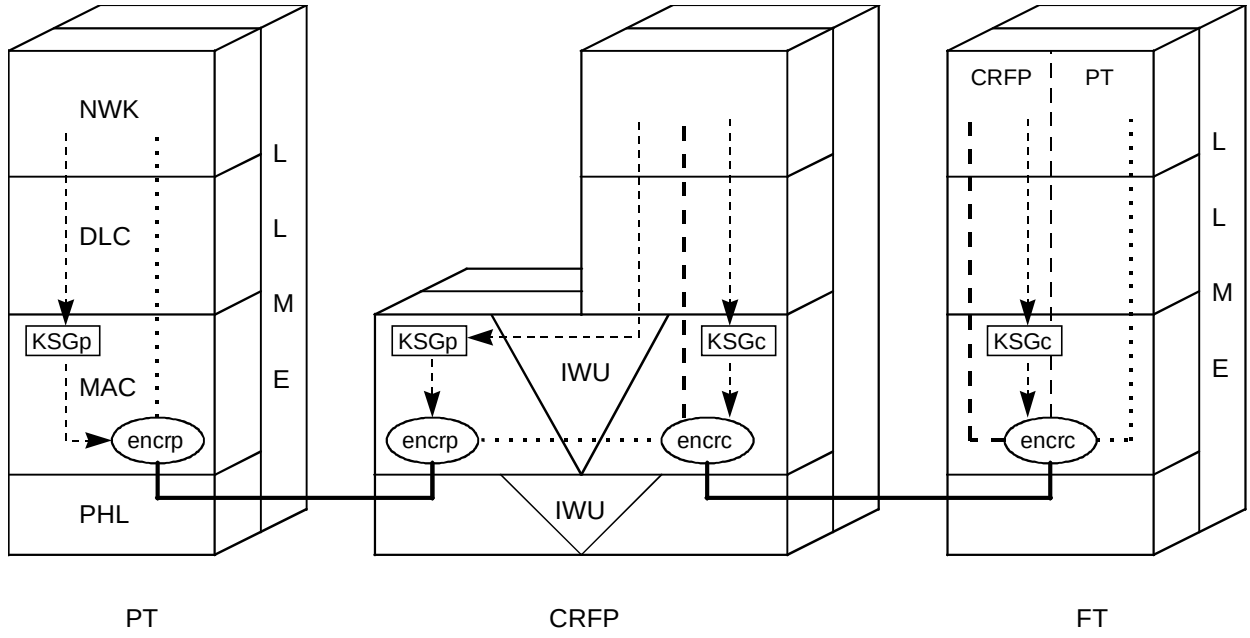



**Figure 10: Protocol stack for encryption**

Figure 10 shows how the principle for ciphering is supported. Separate encryption engines are used to encrypt FT-CRFP and CRFP-PT connections.

The FT shall initiate the procedure for cipher key transfer given in EN 300 175-7 [7] subclause 7.3.2 when the CRFP requires a cipher key:

- when FT need to send a NWK layer {CIPHER-REQUEST} message to a PT that is relayed via a CRFP;
- during bearer or connection handover when the FT receives a relayed handover request.

These procedures with the PT shall be temporarily frozen until the cipher key is transferred to the CRFP or until time-out of the connection.

The CRFP shall use the received DCK for ciphering the connection to the PT.

The CRFP shall relay a received from the PT start.grant message to the FT.

NOTE: The received PMID is kept and the FMID is replaced by the relevant one.

At the FT side the receipt of the START_GRANT message at this stage shall not be treated as an unexpected message even though the MAC FT has already started ciphering for the connection between the FT and CRFP_PT. The event of reception of START_GRANT shall be signalled to the FT NWK layer to indicate the successful completion of the NWK layer FT initiated cipher-on procedure if such is running. For this the defined in EN 300 175 part 3 [3] and 4 [4] primitives may be used: MAC_ENC_EKS and DL_ENCRYPT respectively. For the behaviour of the FT in case of successful completion of ciphering procedure the requirements in EN 300 175-5 [5] shall apply. If there is no NWK layer ciphering procedure running, e.g. ciphering was due to handover of a ciphered connection, NWK layer shall ignore the indication.

When initiating a NWK layer procedure for ciphering with a PT over a relayed connection the FT shall not signal this to the DLC/MAC layer and shall not deliver the DCK.

During bearer handover and connection handover with encryption from a RFP to a CRFP, it is allowed that the FT and CRFP exchange higher layer messages and start messages between the bearer_handover.req message (PT PMID) and the $M_T$ bearer.cfm message.

Figures 9 and 11 show typical examples of the procedures for basic connections.

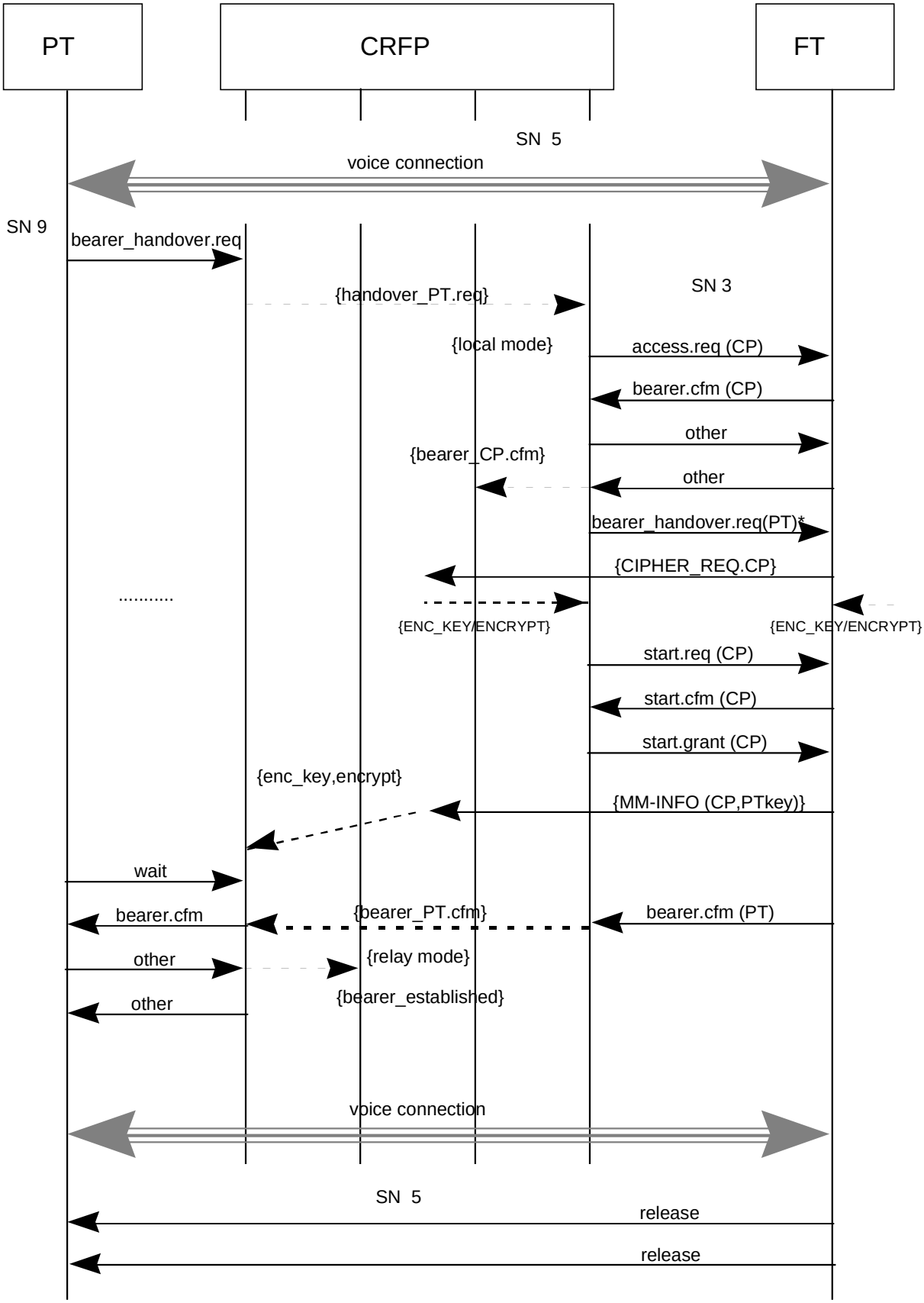



**Figure 11: Bearer handover from a RFP to CRFP (dual setup with encryption)**

In the case of a bearer handover the new bearer between PT and CRFP shall switch to the appropriate encryption mode of the connection without exchange of any further MAC messages immediately after bearer established.

In case of connection handover the encryption activation on the new connection has to be done immediately after it has been established using the corresponding MAC procedure.

#### 5.3.4.2 CRFP initialization of PT cipher key

The FT will initiate ciphering between FT and CRFP that requires a PT CK using {CIPHER-REQUEST} message with a CRFP CK (see subclause 5.1.5).

When the connection between the FT and the destination CRFP is completely ciphered, the FT sends the PT CK to the CRFP_PT using the {MM-INFO-SUGGEST} message.

The CRFP shall download the received CK to the appropriate KSG for the CRFP_FT. The CRFP shall relate the PT CK to the relayed connection at the MAC layer.

After downloading the CK in the KSG, the CRFP is ready for encryption to be enabled at the MAC layer with the PT whenever needed.

NOTE: The procedure is repeated in multi-hop scenarios. In that case the PT may be the CRFP_PT of a relayed CRFP setup or handover.

### 5.3.5 Management

#### 5.3.5.1 CRFP MAC modes

Two MAC modes are defined for operation of the CRFP with an FT:

- normal MAC mode (PT MAC procedures as defined in EN 300 175-3 [3]);
- dual MAC mode (defined in this subclause).

To support encryption the CRFP shall be able operate in Dual MAC mode towards a FT. This mode shall only be used by the CRFP, when the FT has indicated that it supports CRFP with encryption.

NOTE: The FT may also be the FT side of another CRFP.

#### 5.3.5.2 CRFP states and state transitions

The CRFP combines states of both PT and RFP as defined in EN 300 175-3 [3].

**CRFP_FT:**

The CRFP_FT shall be inactive when the CRFP cannot provide any service to any PTs (i.e. CRFP_PT is unlocked). After the CRFP_PT has entered the unlocked state, the CRFP_FT shall enter the inactive state within T205.

NOTE: The CRFP does not transmit any dummies when it cannot provide a service to PTs.

**CRFP_PT:**

In addition to the PP requirement for locking, the CRFP shall receive the extended fixed part capabilities message if the FT supports this message. The CRFP_PT may only enter the locked state when the FT supports the CRFP with HOPS > 0.

If the FT supports encryption, the CRFP_PT may only enter the locked state when the CRFP supports encryption and the FT supports the CRFP with encryption.

## 5.4 Example operation of CRFP

### 5.4.1 Introduction

This subclause is informative and refers to the time-message diagrams for typical General Access Profile (GAP) protocol procedures.

### 5.4.2 Example GAP procedures

In the diagrams the (PT) refers to the PMID of the PT. The (CP) refers to the PMID of the CRFP.

For normal relay bearer setup see figure 3.

For dual relay bearer setup see figure 4.

For release see figure 5.

For CRFP connection suspend and resume see figure 6.

For bearer handover from CRFP to RFP see figure 7.

For bearer handover from a RFP to CRFP (normal setup) see figure 8.

For typical call setup message diagram (with encryption) see figure 9.

For bearer handover from a RFP to CRFP (dual setup with encryption) see figure 11.

In each of the figures SN indicates the slot pair (0;11) (see EN 300 175-3 [3], subclause 7.2.3.2.3).

# 6 Repeater Part (REP)

This clause defines requirements in addition to the general requirements for the WRS, (see clause 4).

## 6.1 Description

### 6.1.1 General

This subclause describes the reference model of the REP and the additional messages and procedures required to support this WRS concept, in respect to an FT-PT direct connection.

Non-restrictive examples of frame structure and slots allocation when relaying a connection are given. For a description of the specific application scenarios, reference has to be made to ETR 246 [10].

### 6.1.2 Reference model

The reference model of figure 1 is applicable for the REP. The PT side of the REP is called REP_PT. The FT side of the REP is called REP_FT.

REP_FT shall have MAC and PHY layer functionalities to interface a PT (or another REP) like an FT; REP_PT shall have MAC and PHY layer functionalities to interface an FT (or another WRS) like a PT. REP_PT can also have a selection of PT DLC and NWK layer functionalities to access directly to the network services (i.e. to exchange on air OA&M messages; to subscribe etc.).

An Inter Working Unit (IWU) is required to allow interworking between the REP_PT and the REP_FT at PHY and MAC layers.

At the REP_FT and PT air interface, the REP does not require any additions.

At the REP_PT and FT air interface, the REP requires the following additions:

- **at the MAC layer:**
  - the complementary connection setup procedure and the relevant $M_T$ messages to establish a complementary connection;
  - the Mapping procedure and the relevant $M_T$ messages to setup a double duplex bearer;
  - the procedure to release relayed bearers;
  - quality control and flow control on the relayed bearers;
  - channel selection rules for the relayed bearers.

  The additional MAC functionalities can be logically located within the Multi-Bearer_control (MBC) entity (see EN 300 175-3 [3]).

- **at LLME:**
  - configuration control (number of allowed cascaded REPs; type of repeater supported ea.) with the use of the Q message "Extended Fixed Part Capabilities" (see EN 300 175-3 [3], subclause 7.2.3.5.2).

## 6.1.3 MAC layer functions

### 6.1.3.1 General

REP shall be compliant with both the PT and the FT MAC layer requirements according to EN 300 175-3 [3]. Additions are required when interfacing an FT or another WRS and are given in the following subclauses.

### 6.1.3.2 Frame multiplexing

REP can switch from transmit to receive mode on a time slot base. REP, once locked to a suitable FT (other WRS), is listening for bearer set up attempts on the idle time slots (i.e. slots where REP does not transmit nor receive) of the second half frame while, on the idle time slots of the first half frame, it is scanning for suitable channels and listening for suitable FTs (other WRSs) to get synchronized to. REP shall scan the radio environment in the second half frame synchronously with the locked FT (other WRS).

REP relays the information received from one radio termination to another radio termination, combining Physical and MAC layer functionalities both of a PT and of an FT, with some improvements when interfacing the FT (another WRS). The relay of the information between the two radio terminations is completed within the half frame time interval.

Figure 12 describes an example of frame structure and slot allocation within REP, RFP and PP when relaying one duplex bearer connection through a single hop; figure 13 describes the frame multiplexing structure when relaying one duplex bearer connection through two hops.

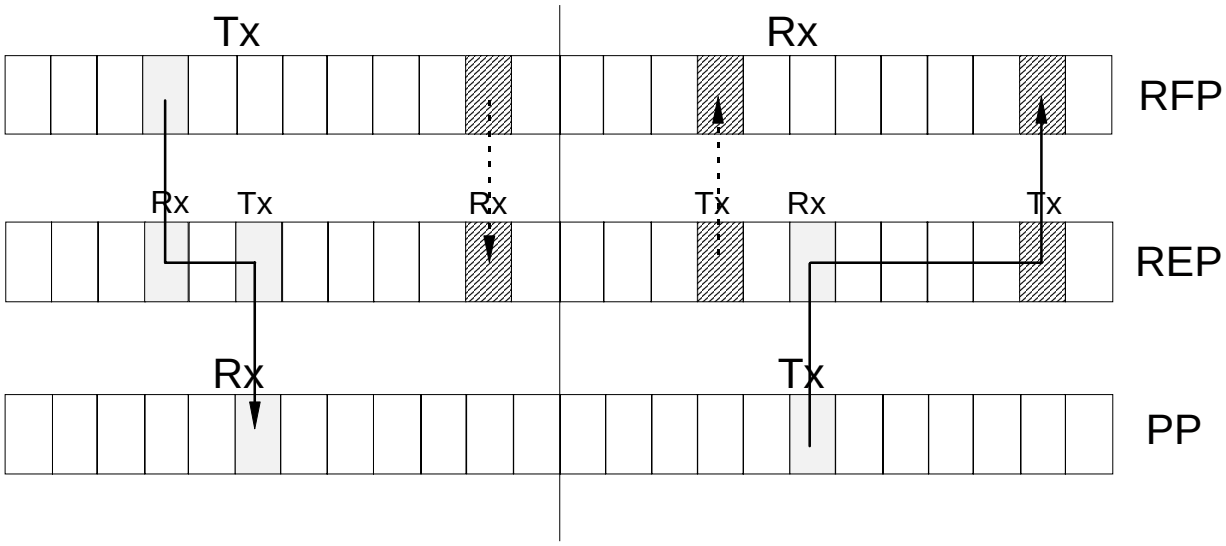



**Figure 12: Frame multiplexing structure when relaying one duplex bearer connection through a single hop**

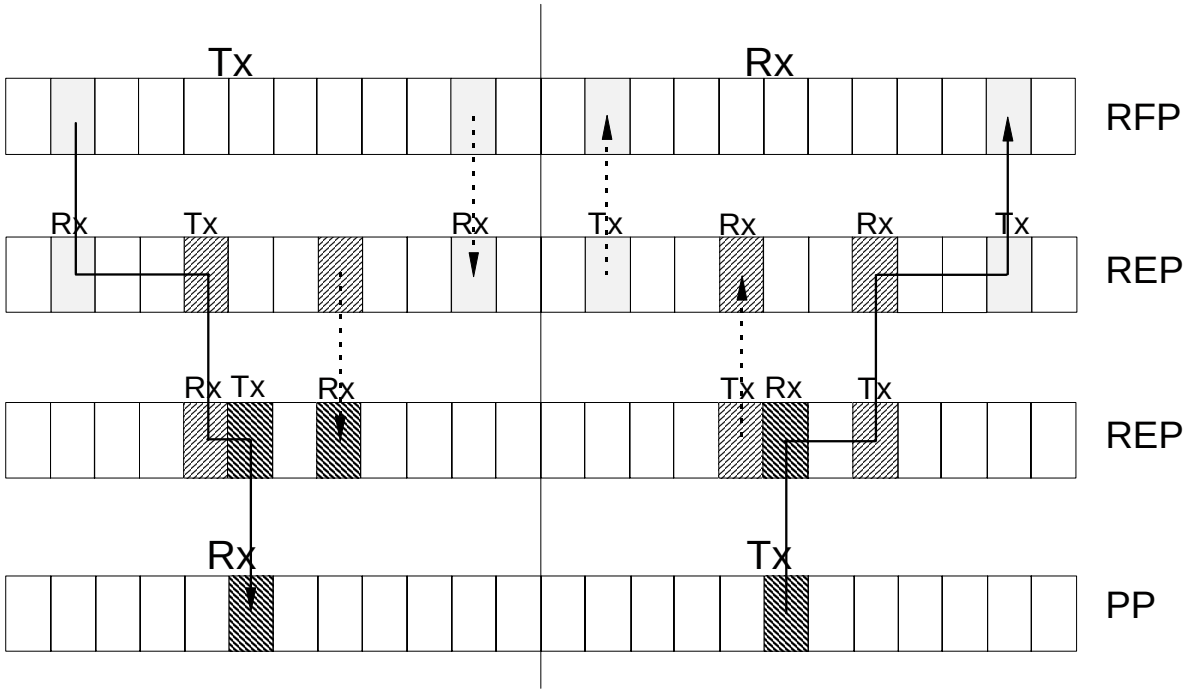



**Figure 13: Frame multiplexing structure when relaying one duplex bearer connection through two hops**

In figure 14 an example of two single duplex bearer connections, REP relayed with an interlacing procedure (see subclause 6.4.1.1.3) is presented; PP1 and PP2 connections share on REP the slot pair (i.e. the duplex bearer) marked with "S".

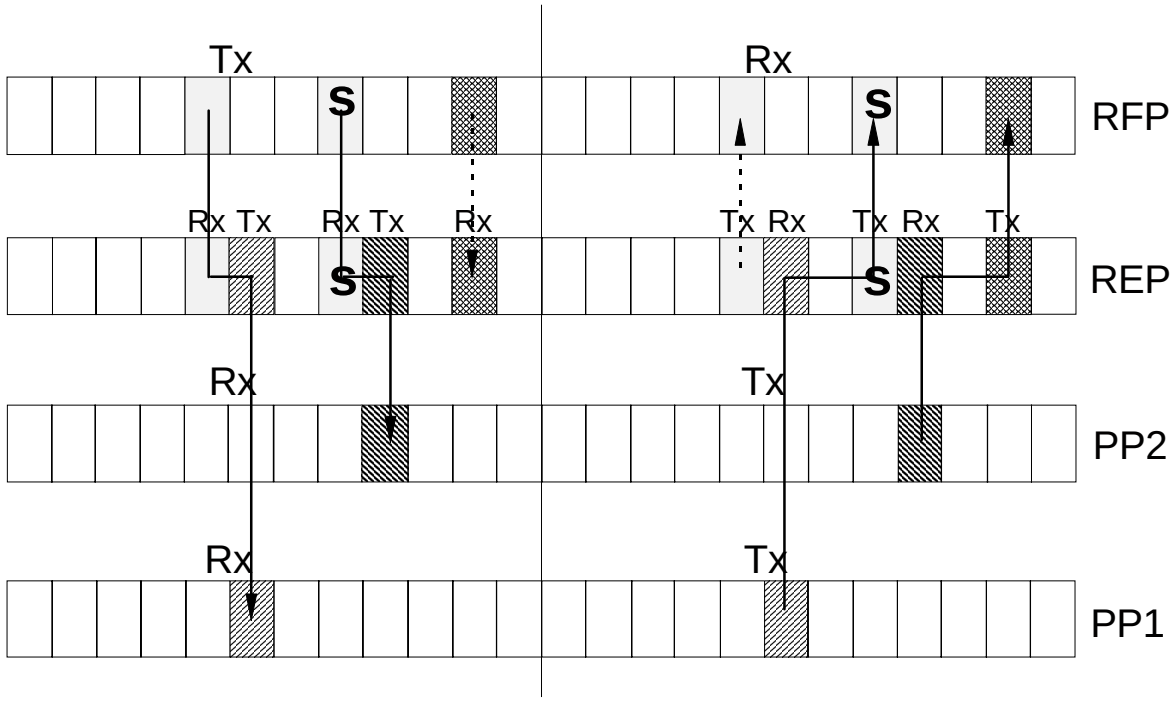



**Figure 14: Two single duplex bearer connections, REP relayed with interlacing**

### 6.1.3.2.1 Quality control

REP repeater shall release a bearer and all the related bearers, both in downlink and in uplink direction, if it has not received the correct RFPI with a correct CRC on that bearer in the last T201 seconds.

"Related bearers" are all the bearers, which are required for transferring the same data burst between an FT and a PT.

In a duplex bearer the Q2 bit is used for C channel flow control and, together with the BCK bit, for Ip channel flow control (see EN 300 175-3 [3]).

In a duplex bearer belonging to a double duplex bearer (see subclause 6.4.1.1.3) the Q2 and BCK bits shall be set in response to the last received data burst from the other duplex bearer of the pair.

In a duplex bearer the Q1 bit can be used in downlink direction to indicate a detected sliding collision and in uplink direction to request a switch of antenna (see EN 300 175-3 [3]).

In a duplex bearer belonging to a double duplex bearer the Q1 bit always refers to the duplex bearer where it has been set.

**Q2 bit setting for duplex bearers:**

- REP shall not store the received C or $I_P$ channel data from duplex bearers of a relayed connection. The re-transmission of unacknowledged segments shall be done only by the source transmitter (FT or PT);
- in response to the last received data burst, REP shall set the Q2 bit to '0' if A-CRC failed or $C_F$ segments rejected or the destination receiver (PT or FT) of C segments has set the Q2 bit to '0';
- if A-CRC failed, REP shall send to the destination receiver a data burst where the A-field shall contain a whatever allowed internal MAC channel information (N; P; Q) and, if B-field rejected, the B-field may contain In or Ip user data depending on the connection service type;

- in case of $I_P$ error detect service, if REP receives a B-field with corrupt $I_P$ data then it shall relay this data and change the B-field identifications ($a_4$, $a_5$ and $a_6$ bits) to '000'B;
- in case of $I_N$ service, if REP receives a B-field with corrupt $I_N$ data (X-CRC failed) then it shall relay this data and change the B-field identifications ($a_4$, $a_5$ and $a_6$ bits) to '001'B.

**Q1 bit setting for duplex bearers:**

- both in reception and in transmission, REP can independently manage the Q1 bit.

#### 6.1.3.2.2 Bearers selection

To setup bearers the REP shall follow the channel selection rules as described in subclause 6.4.4.3.

#### 6.1.3.2.3 Relay of a duplex bearer

Each duplex bearer to be relayed requires the setup of an additional double duplex bearer at the REP_PT air interface.

One duplex bearer composing the double duplex bearer shall be set up by the same procedure as required for the duplex bearer to be relayed. The other duplex bearer can be already established (if interlacing is applicable; see subclause 6.4.1.1.3) or shall be setup by a complementary connection setup procedure (see subclause 6.4.1.1.1).

A complementary connection set up has not to be notified to the DLC, and the established bearer has no properties, it is just a duplex bearer.

As an example, figure 14 shows that for the second in time relayed duplex bearer connection (PP2) the required double duplex bearer is setup by establishing one duplex bearer only on the time slot pair (10;22); the other constituent duplex bearer is shared with PP1 on the time slot pair (7;19).

#### 6.1.3.2.4 Relay of a double simplex bearer

Each double simplex bearer to be relayed at the REP_FT (REP_PT) air interface requires the setup of an additional double simplex bearer at the REP_PT (REP_FT) air interface.

REP does not allow a change of the transmission direction for the relayed double simplex bearers (see EN 300 175-3 [3]).

### 6.1.3.3 Logical channel mapping

REP shall be compliant both with the PT and with the FT multiplexing rules as defined in EN 300 175-3 [3].

The multiplexing rules can introduce a delay in the REP re-transmission at the air interface of the paging messages as received from the locked FT (other WRS).

It may be impossible for REP to re-transmit on all the downlink active bearers the received paging messages within the same time frame interval.

Handling of logical channel data received at REP:

MA-SAP ($B_S$):

REP_PT:

- data shall be delivered to the higher layer and to the IWU of REP for relay; IWU shall issue a MAC-PAGE.req (for those paging messages not addressing to REP) to the MBC of the REP_FT;

MB-SAP (CL; $SI_N$; $SI_P$):

REP_PT:

- data shall be delivered to the higher layer and to the IWU of REP for relay;

REP_FT:

- C channel data shall be delivered to IWU of REP for relay;

MC-SAP (C; $G_F$; I):

REP_PT:

- U-plane data shall be delivered to the IWU of REP for relay;
- C-plane data shall be delivered to higher layer in case of a REP-FT direct connection otherwise to IWU of REP for relay;

REP_FT:

- U-plane and C-plane data shall be delivered to IWU of REP for relay;

ME-SAP (Q; N; P; M):

REP_PT:

- data shall be delivered to the LLME of REP; LLME of REP shall also generate information for the MBC of the REP_FT;

REP_FT:

- data shall be delivered to the LLME of REP.

### 6.1.4 DLC functions

REP can incorporate DLC layer PT functionalities to support communication with the FT according to EN 300 175-4 [4].

### 6.1.5 NWK layer functions

REP can incorporate NWK layer PT functionalities to support communication with the FT according to EN 300 175-5 [5].

### 6.1.6 Management functions

#### 6.1.6.1 Identities and addressing

REP shall have an assigned Radio Fixed Part Identity (RFPI), which shall broadcast as REP_FT once it has entered the Active_Idle/Active_Traffic state (see subclause 6.4.3.1).

The REP RFPI is composed by the PARI, the same as broadcast by the locked FT (other WRS), and by the RPN, which has been assigned to REP during the subscription phase, according to EN 300 175-6 [6].

The MAC identity of REP_FT (FMID) as an FT is derived as follows:

- FMID = least significant 12 bits of REP RFPI (see EN 300 175-3 [3]).

REP should have at least one IPUI to have direct access to the system (e.g. for on air subscription, on air OA&M etc.).

To setup direct connections with the locked FT, REP shall use an assigned PMID or a default one (see EN 300 175-3 [3]).

For relayed connections, REP shall use the same PMID as required for the calling/called PT, while for a complementary connection (see subclause 6.4.1.1.1) it shall use a PMID (e.g. randomly generated) which unambiguously identifies the associated bearer.

# 6.2 Definitions

REP requires the definition of a new type of bearer, the "Double duplex bearer".

# 6.3 Messages

## 6.3.1 MAC control ($M_T$)

REP requires the messages of the "REP control set", defined in EN 300 175-3 [3], for the procedures in the following subclauses.

# 6.4 Procedures

## 6.4.1 MAC layer

### 6.4.1.1 C/O connection

#### 6.4.1.1.1 Complementary connection setup procedure

A complementary connection setup shall always be REP initiated and allows setting up one duplex bearer without any interaction/notification with/to the higher layers, as explained in the following overview. An existing REP_PT MBC entity shall setup a complementary connection with the locked FT (another WRS).

**Calling side:**

The IWU of the initiating side shall have knowledge of at least one available physical channel. The IWU shall also know the address (FMID) of the called part (FT or another WRS). The IWU shall create the TBC and issue the called part address, the calling part address (PMID) and the physical channel description to the new TBC. The IWU shall also indicate if the wanted bearer is used for bearer handover or for a new setup and shall specify that a complementary connection setup procedure has to be used. After this, a setup timer, T200, shall be started (see EN 300 175-3 [3]). A successful complementary connection setup shall be completed before this timer expires. Otherwise, the complementary connection setup fails.

To establish the bearer the TBC shall use the complementary connection setup procedure.

At the end of a setup procedure the TBC shall report to the IWU either:

- "bearer_established" (the procedure succeeded); or
- "bearer_setup_failed".

If a bearer setup attempt failed the TBC shall be released (see EN 300 175-3 [3], subclause 10.7.2.1). The calling IWU can re-attempt with the same procedure up to N200 times, subject to using a new available channel each time (see EN 300 175-3 [3]).

NOTE 1: In the case of a successful complementary connection setup there exists a common identification for the connection known both at the calling and at the called side. It consists of the ARI + PMID. A duplication of the identification is possible only during bearer handover.

NOTE 2: It is assumed that the PMID does not change during one connection (e.g. from an arbitrary PMID to a PMID derived from the assigned individual TPUI (see EN 300 175-3 [3], subclause 11.7.2)).

**Called side:**

At the called side a new TBC is created by receiving a "REP_bearer_request" message, including the MAC addresses PMID and FMID on the scanned physical channel. The message type also contains the information that the new bearer belongs to a complementary connection.

**MBC identification**

The calling side does not require the creation of a new MBC at the called side; the TBC of the complementary connection will be connected to an existing MBC.

The TBC has to receive all necessary parameters to identify the MBC.

The MBC is fully identified after:

a) receiving with "REP_bearer_request" message either a REP_access request or a REP_bearer_handover request (see EN 300 175-3 [3], subclause 7.2.5.11), including the calling address PMID and defining the connection type as complementary; and

b) receiving the REP_channel_map_request message (see EN 300 175-3 [3], subclause 7.2.5.11), which indicates the duplex bearer (the Master channel) to which the complementary connection has to be linked. This message is necessary only for a new bearer setup, as in case of a bearer handover request, the previous mapping still remains effective.

The MBC shall be the one, which controls the TBC of the master channel.

The TBC issues a PMID, ARI and the REP_channel_map message to the LLME and indicates the purpose of the wanted connection (i.e. bearer handover or a new setup).

The LLME can now decide:

a) to release the TBC;

b) to connect the TBC to the identified MBC.

**Procedure:**

The procedure for the complementary connection setup is identical to the basic bearer setup procedure as described in EN 300 175-3 [3], subclause 10.5.1, where:

- the PT is REP and the FT could also be a WRS;
- the exchanged $M_T$ messages belong to the REP control set (see EN 300 175-3 [3], subclause 7.2.5.11);
- the bearer_request message can be either a REP_access_request or a REP_bearer_handover.request message.

#### 6.4.1.1.2 Creation of a double duplex bearer

To relay one duplex bearer between a PT and an FT, REP_PT shall establish towards the FT (other WRS) a double duplex bearer. A double duplex bearer is composed by a pair of duplex bearers, which have been mapped/interlaced together (see subclause 6.4.1.1.3). One of the two duplex bearers shall always be setup by using the same bearer setup procedure as requested for the duplex bearer to be relayed; while the second one can either:

a) be already established; or

b) shall be setup by using the complementary connection setup procedure (see subclause 6.4.1.1.1).

If it is case (b), it is this duplex bearer of the pair, which has to be established at first.

Case (a) applies if an available duplex bearer already exists which is suitably time positioned in respect to the rules as defined in subclause 6.4.4.3.

#### 6.4.1.1.3 Mapping procedure

The mapping procedure shall always be REP initiated. This procedure allows setting up a double duplex bearer, after two duplex bearers have been set up between two far ends. When one of the two duplex bearers already belongs to a double duplex bearer, the procedure is called "interlacing".

**Procedure:**

- the sending side:
  - REP_PT shall send to the far end onto a duplex bearer the REP_channel_map.request message (see EN 300 175-3 [3], subclause 7.2.5.11), indicating the two duplex bearers, which have to be mapped together, i.e. to be linked to the same connection. The first SN and CN fields (bits $a_{16}$ to $a_{25}$) within this message, shall identify the "master" channel: it is the channel controlled by that MBC which, after the mapping, shall also control the other channel (said "slave") indicated by the following SN and CN fields (bits $a_{38}$ to $a_{47}$). After successful completion of the mapping procedure, the two linked channels shall then belong to the same MAC connection;
  - The REP_channel_map.request message can be repeated until the REP_channel_map.confirm (see EN 300 175-3 [3]) message is detected or a connection release is recognized. After reception without errors (see note 1) of the REP_channel_map.confirm message with A/R flag set to "Accepted", the double duplex bearer is setup. After reception without errors of the REP_channel_map.confirm message with A/R flag set to "Rejected", a new REP_channel_map.request message may be forwarded but selecting a more suitable duplex bearer (i.e. a duplex bearer which does not already belong to a double duplex bearer).
- the receiving side:
  - after receiving without errors (see note 1) the REP_channel_map.request message onto a duplex bearer, the receiving side can decide:
    a) to accept to map together the indicated channels; or
    b) to reject to map together the indicated channels (see note 2).

As soon as it is ready, the receiving side shall answer by sending onto the same duplex bearer the REP_channel_map.confirm message with the A/R flag set to "Accepted" if it is case (a), otherwise to "Rejected".

NOTE 1: Receiving without errors means A-field CRC holds and message recognized (message type decoded).

NOTE 2: Case (b) may apply when interlacing of the two duplex bearers is requested but the receiving side does not support "interlacing".

Within the double duplex bearer the two duplex bearers shall exchange their simplex bearers such that the information flow (i.e. higher layer signalling and user data) shall use, for the uplink transmission direction the uplink simplex bearer of one duplex bearer and, for the downlink transmission direction, the downlink simplex bearer of the other duplex bearer.

The release of one of the two duplex bearers composing the double duplex bearer shall cancel the link, given with the mapping procedure, between the surviving duplex bearer and the released one.

A duplex bearer can be paired with two different duplex bearers (i.e. in case of interlacing) on condition that in one double duplex bearer it represents the master channel and in the other double duplex bearer it is the slave channel.

A new mapping request as a master (slave) channel for a duplex bearer, which is already the master (slave) channel in another double duplex bearer, shall overwrite the previous mapping.

The REP_channel_map.req message may over-ride the T-Mux algorithm (see EN 300 175-3 [3]), subclause 6.2.2.1) when transmitted as a first "other" message (see EN 300 175-3 [3], subclause 10.5) during a bearer setup procedure. The first response (REP_channel_map.confirm message) shall occur in the TDMA half frame following the successful reception of the REP_channel_map.request from the receiving side and may also over-ride the T-Mux algorithm. The TBC shall report "bearer established" after the mapping procedure is successfully completed (i.e. the double duplex bearer has been setup).

### 6.4.1.2 REP relayed C/O connection

#### 6.4.1.2.1 IWU

The relay of a connection through REP involves, within REP, the MAC and the PHY layers, and the IWU which co-ordinates the REP_FT side and the REP_PT side.

Figure 15 shows how the IWU controls and co-ordinates between the two REP sides the TBCs of a relayed connection.

IWU shall also update the channels table and shall decide to map/interlace together duplex bearers.

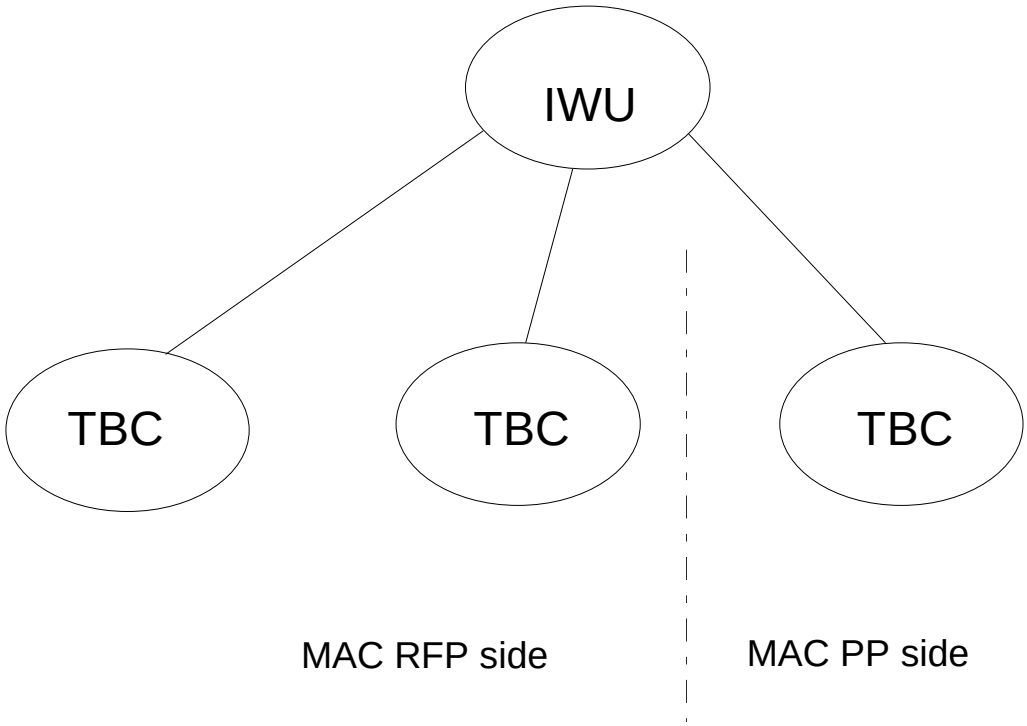



**Figure 15: IWU functionality in co-ordinating the TBCs of a relayed connection**

At the REP_FT (REP_PT) a new TBC is created by receiving a "bearer_request" message which contains the calling and called address (PMID;FMID) and the information if the new bearer belongs to a basic or an advanced or a complementary connection.

The TBC has then received all necessary parameters to be unambiguously identified and to identify the required service, that is:

1) receiving with the "bearer_request" message either an access request or a handover request, including the calling address and the connection type; and

2) for basic connection and only in case of handover request, an indication if bearer or connection handover is wanted.

The TBC issues the received parameters to IWU, which can now decide:

a) to release the TBC;

b) to keep the TBC; and

**IF** the requested connection **IS NOT** of the complementary type **THEN:**

**b1)** if required (refer to subclause 6.4.1.1.2 for definition), IWU shall request to the REP_PT to initiate towards the locked FT (other WRS) a complementary connection setup procedure, by also indicating the called and calling addresses to be used;

**b2)** if required (e.g. in case of a new access) it shall request to the REP_PT (REP_FT) to initiate towards the locked FT the specific PT a bearer setup procedure of the same type as requested for the connection to be relayed, by also indicating the called and calling addresses to be used;

**b3)** if required (e.g. in case of a new access), it shall request to the REP_PT to initiate towards the locked FT (or WRS) the mapping procedure, by also indicating the two duplex bearers to be linked together;

**b4)** IWU shall then control and co-ordinate together all the involved TBCs.

#### 6.4.1.2.2 REP relayed C/O single duplex bearer setup

**Procedure:**

as soon as REP_FT (REP_PT) receives from a peer entity a "Bearer_request" (access or handover request) message error free (see note), a new TBC ($TBC_1$) is created and between the two peer entities a bearer setup procedure of the requested type (Basic or A-field advanced or B-field or complementary; refer to subclause 6.4.1.1 and to EN 300 175-3 [3], subclause 10.5) is engaged.

NOTE: Error free means A-field CRC holds and message recognized (message type decoded).

**IF** the relay of the requested bearer requires to setup additional bearers **THEN**:

- **if** a duplex bearer (i.e. the TBC1 pending procedure is an intra-cell handover) or a double duplex bearer only is required, this is set up at first and after the TBC1 pending procedure can be concluded. In the meantime, TBC1 and the peer entity exchange "wait" messages;

- **else** both a duplex and a double duplex bearer (i.e. the TBC1 pending procedure is a fast bearer setup) are required; then the double duplex bearer should be set up at first, after it is the duplex bearer and finally the TBC1 pending procedure can be concluded. In the meantime, TBC1 and the peer entity exchange "wait" message.

**ELSE** TBC1 and the peer entity can conclude the pending procedure.

Whenever a complementary connection setup is required, it shall be setup at first.

For each further duplex bearer to be relayed, the procedure is repeated.

Figures 17 and 18 show examples of relayed basic bearer connection setups.

#### 6.4.1.2.3 REP relayed C/O bearer release

The release of a bearer, which belongs to a REP relayed connection, implies the release of all the related bearers, that is of all the bearers, which transfer the same data, burst.

In case of unacknowledged release procedure (see EN 300 175-3 [3], subclause 10.7.2.1) of a bearer which has been mapped to another bearer (see subclause 6.4.1.1.3):

- at the REP as a transmitting side:

  the bearer and the associated TBC shall not be released after sending the RELEASE messages, if it is an MBC decision to release that bearer and if the bearer is also interlaced with another channel (see subclause 6.4.1.1.3 for definitions).

- at the REP as a receiving side:

  the bearer and the associated TBC shall not be released after successful reception of a RELEASE message if that bearer is also interlaced with another channel.

#### 6.4.1.2.4 REP relayed C/O bearer handover

Bearer handover procedures may be used to perform:

1) intra-cell handover of the PT within REP;
2) intra-cell handover of the REP within one RFP;
3) inter-cell handover of the REP from one RFP to an RFP belonging to the same cluster;
4) inter-cell handover of the PT from a REP to an RFP belonging to the same cluster;
5) inter-cell handover of the PT from an RFP to a REP belonging to the same cluster;
6) inter-cell handover of the PT from one REP to a REP belonging to the same cluster;
7) inter-cell handover of one REP to another WRS belonging to the same cluster.

REP can be defined as a separate cluster or as part of the cluster of the RFP(s) that it is locked to.

These handover procedures are handled as follows:

1) completely handled at REP as an FT (example in figure 25);
2) handled between REP and the FT (other WRS), with the procedure described in subclause 6.4.1.2.2 (example in figure 26);
3) as for 2);
4) completely handled at FT (examples in figures 27 and 28);
5) as for 2);
6) as for 2);
7) as for 2).

### 6.4.2 DLC layer

#### 6.4.2.1 REP relayed C/O connection handover

Connection handover procedures may be used to perform:

1) handover of REP from an RFP (or REP or CRFP) to another RFP (or REP or CRFP);
2) handover of the PT from a REP to an RFP;
3) handover of the PT from an RFP to a REP;
4) handover of the PT from a REP to another REP.

These handover procedures are handled as follow:

1) completely handled at REP as a PT;
2) completely handled at RFP;

3), 4) handled between REP and RFP (other WRS) with the same procedure described in subclause 6.4.1.2.2.

## 6.4.3 Management

### 6.4.3.1 REP states

REP combines states of both an FT and a PT, as defined in EN 300 175-3 [3].

The diagram of figure 16 reports the transitions between all the allowed REP states.

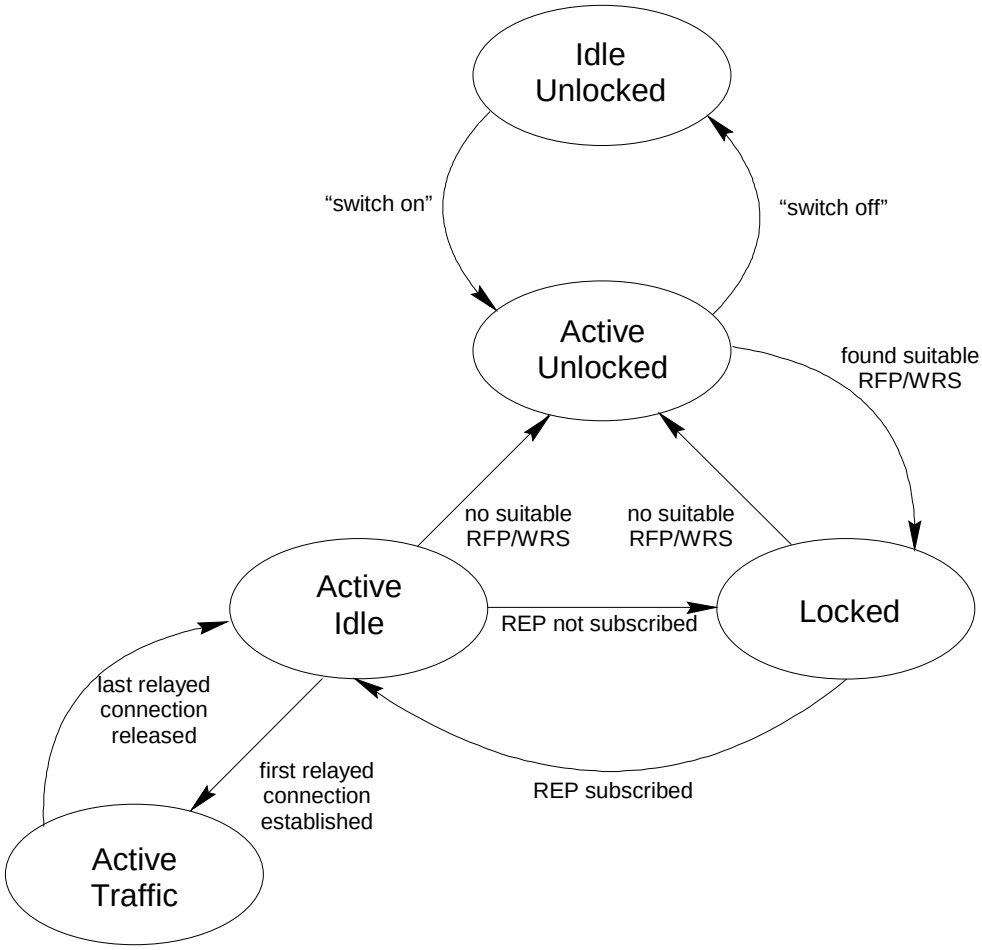



**Figure 16: REP state diagram**

1) Idle_Unlocked: where the REP is not synchronized and does not attempt to get synchronized to an RFP or WRS. In this state REP is not receiving nor transmitting.

2) Active_Unlocked: where the REP is not synchronized to any RFP or WRS and is unable to make/receive direct connections, or to relay connections. REP makes attempts to detect a suitable RFP or another WRS and enter the Locked state.

3) Locked: where the REP is synchronized to at least one RFP or WRS. It is able to make/receive direct connections, and may have direct connections in progress, but it is still unable to relay connections.

4) Active_Idle: where the REP has been subscribed to the system and has received a consistent MAC identity. The REP has either at least one dummy bearer or at least one connectionless downlink bearer, and a receiver that is scanning the physical channels in a known sequence. In this state REP is able to make/receive direct connections and to relay connections, but has no relayed connection in progress.

5) Active_Traffic: where REP relays at least one connection. In this state REP can have direct connections in progress and may have a dummy or connectionless downlink bearer.

### 6.4.3.2 REP actions and states transitions

#### 6.4.3.2.1 Actions in the Idle_Unlocked and Active_Unlocked states

In the Idle_Unlocked state, REP shall do nothing.

In the Active_Unlocked state, REP tries to get synchronized to a suitable RFP or other WRS and enter the Locked state, with the same modality as described in EN 300 175-3 [3] subclause 11.3.2, where a DECT FP can be either an FT or another WRS.

#### 6.4.3.2.2 Actions in the Locked state

In the Locked state, REP shall maintain frame and multiframe synchronism with the FP or other WRS and may occasionally scan for RFPs (WRSs) with a stronger signal strength. If a stronger RFP (WRS) is found, then the REP may lock to this RFP (WRS) instead.

In order to remain in the Locked state the REP shall:

- re-synchronize its timing with the FPs (WRSs) timing at least every T216 multiframes (refer to EN 300 175-2 [2]);
- receive in frame 0 at least one A-field with correct CRC every T207 seconds; and
- receive at least one $N_T$ type tail containing the PARI every T208 seconds.

If any of these conditions is not met, REP shall enter the Active_Unlocked state.

At any time REP can leave the Locked state and enter the Active_Unlocked state.

Once REP has been subscribed to the system, it enters the Active_Idle state.

#### 6.4.3.2.3 Entry into the Active_Idle state

Once REP has been subscribed to the system, it enters the Active_Idle state.

#### 6.4.3.2.4 Actions in the Active_Idle state

In the Active_Idle state, REP shall:

- still get synchronized to an RFP (WRS) as it does in the Locked state;
- broadcast in downlink direction the N channel information with its own RPN value, assigned in the subscription phase onto an established dummy or connectionless downlink bearer;
- broadcast in downlink direction the Q channel information onto an established dummy or connectionless downlink bearer.

The fixed part capabilities system information i.e. SARI list contents system information and multi-frame number system information, shall reflect the same system information broadcast by the RFP (WRS) locked to. It shall also reflect its own extended fixed part capabilities system information to control the number of allowed cascaded REPs, if this information is broadcast by the RFP (other WRS) locked and the number of allowed HOPS is greater than 0. It shall answer to the paging messages referring to itself and broadcast in the downlink direction the not referring ones onto an established dummy or connectionless downlink bearer.

REP shall fill out the MAC layer information field both of short and of zero length page messages with its own MAC information and shall fill out the 20 least significant bits of RFPI field within zero length page messages with its RFPI value.

At any time an Active_Idle state REP may leave this state and enter the Active_Unlocked state, as soon as the synchronism gets lost.

In Active_Idle state, REP shall receive all the RFP (WRS) locked to broadcast messages.

#### 6.4.3.2.5 Entry into the Active_Traffic state

REP enters the Active_Traffic state at the first relayed connection.

#### 6.4.3.2.6 Actions in the Active_Traffic state

In the Active_Traffic state REP shall do the same actions as in Active_Idle state and shall relay at least one connection.

### 6.4.3.3 Channel selection

Once in one of the states, i.e. Active_Idle or in Active_Traffic or in Active_Locked, REP may start transmission on a physical channel according to EN 300 175-3 [3], subclause 11.4 with the following additions:

a) double duplex bearers:

   The relay of a duplex or of a double duplex bearer requires, at the REP_PT air interface, the setup of a double duplex bearer. Said $((y;y+12);f_y)$ and $((z;z+12);f_z)$ the two time slot pairs of the double duplex bearer to be setup and respectively $((x;x+12);f_x)$ or $((x1;x1+12);f_{x1})$ and $((x2;x2+12);f_{x2})$ the time slot pair or the two time slot pairs of the associated duplex bearer or double duplex bearer to be relayed, the following further restriction has to be respected:

   $0=<Y<X$ (where X = min (X1;X2)); and

   $X<Z<=11$ (where X = max (X1;X2)).

b) double simplex bearer:

   The relay of a double simplex bearer requires, at the REP_PT (REP_FT) air interface, the setup of another double simplex bearer.

   Said (x;x+12) the time slot pair of the double simplex bearer to be setup and (y;y+12) the time slot pair of the double simplex bearer to be relayed, the following further restriction has to be respected:

   $X>Y$..

## 6.5 Example operation of REP

This subclause contains example time-message diagrams for a REP relayed basic connections.

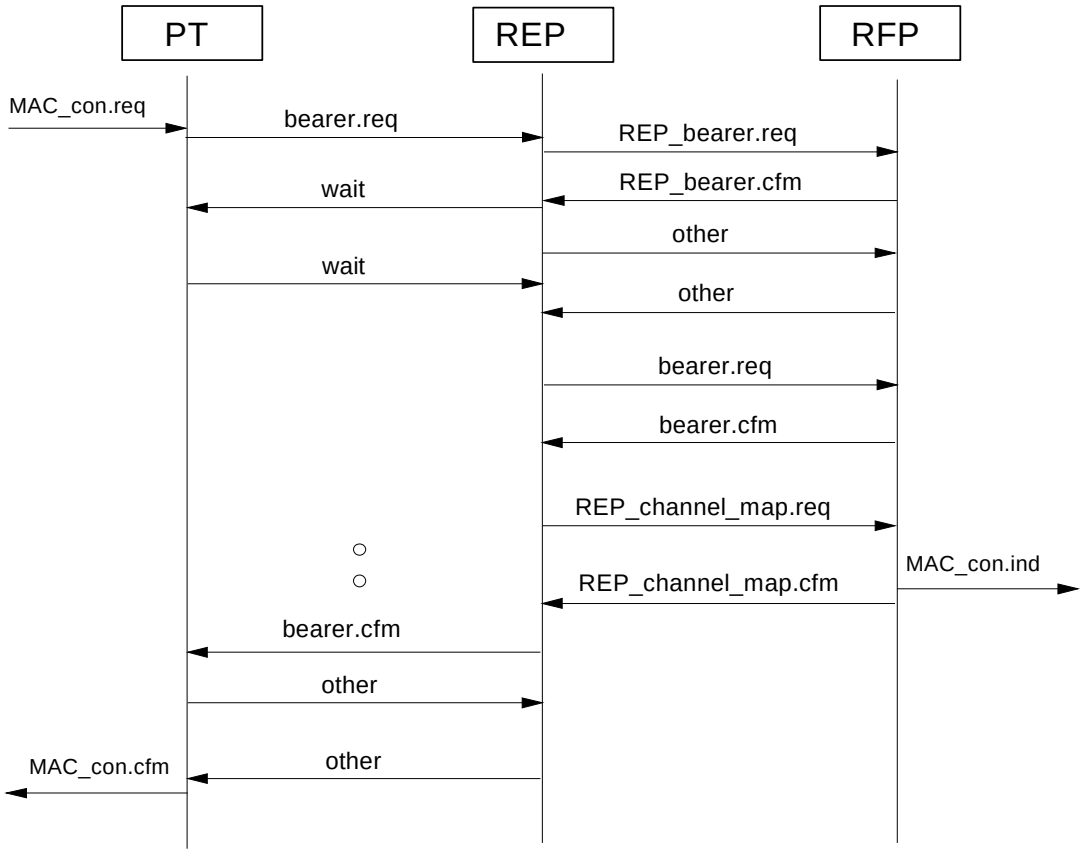



**Figure 17: Bearer setup scenario**

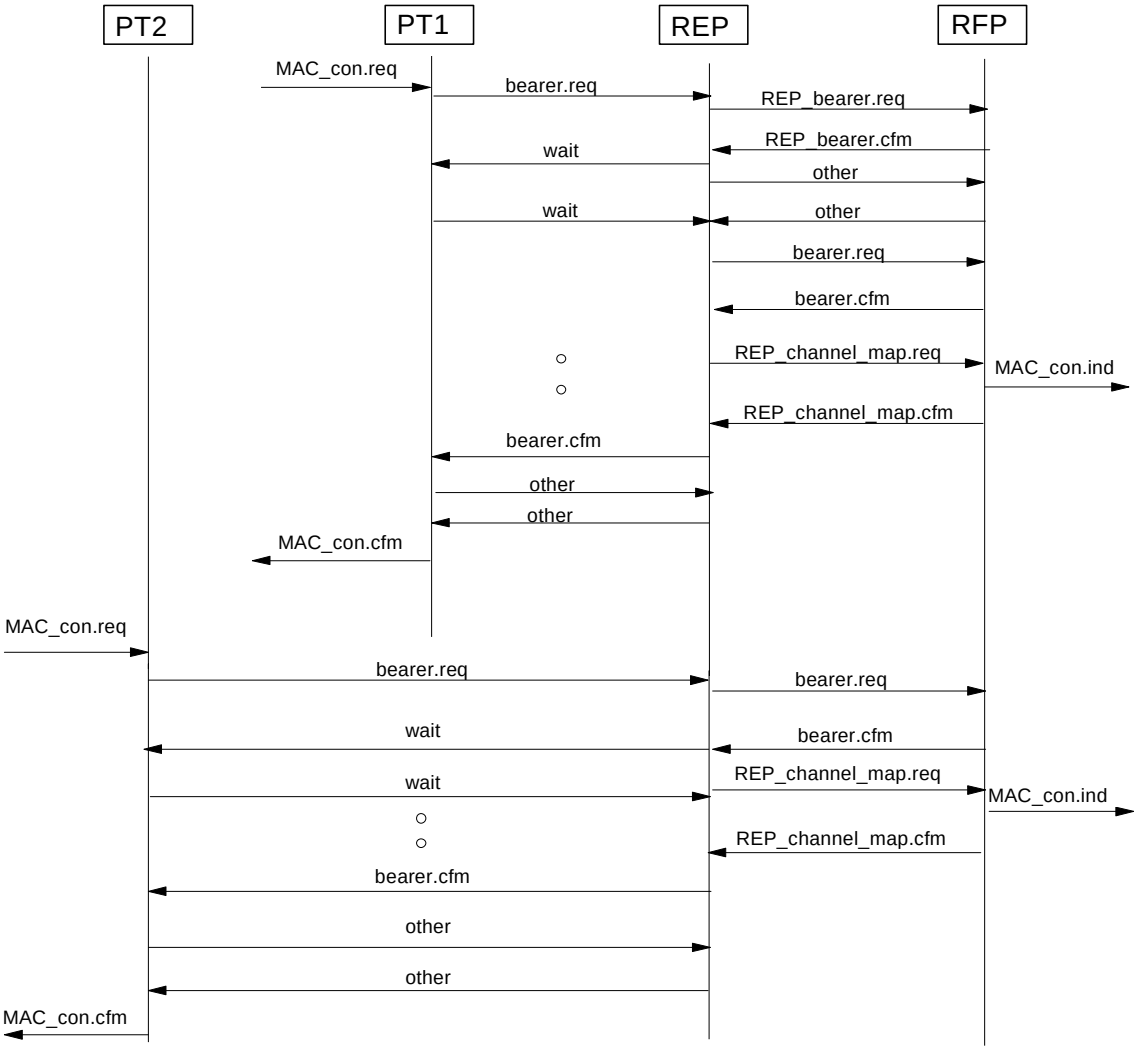



**Figure 18: Interlaced bearer setup scenario**

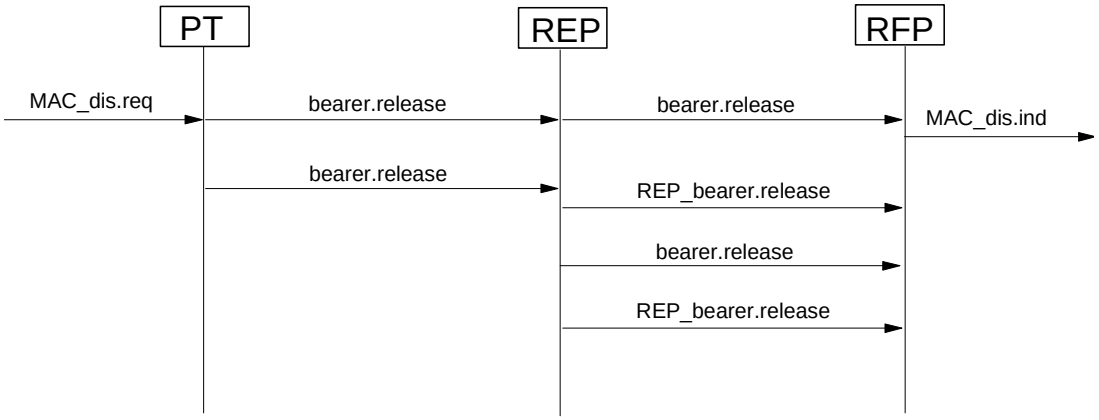



**Figure 19: PP initiated bearer release scenario**

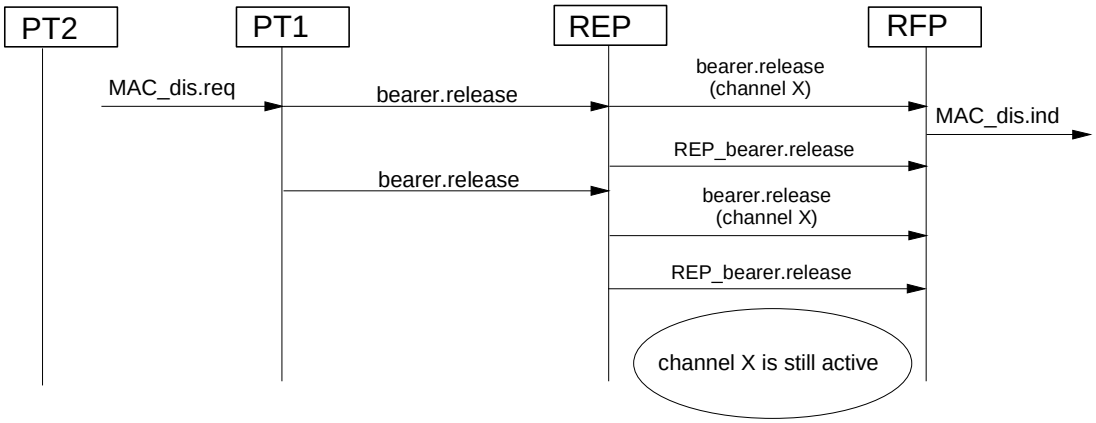



**Figure 20: PP initiated interlaced bearer release scenario**

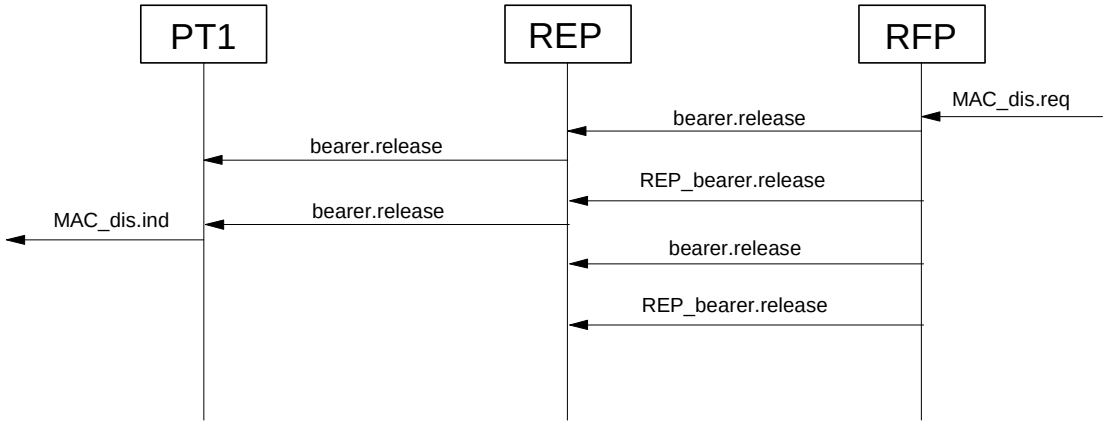



**Figure 21: FP initiated bearer release scenario**

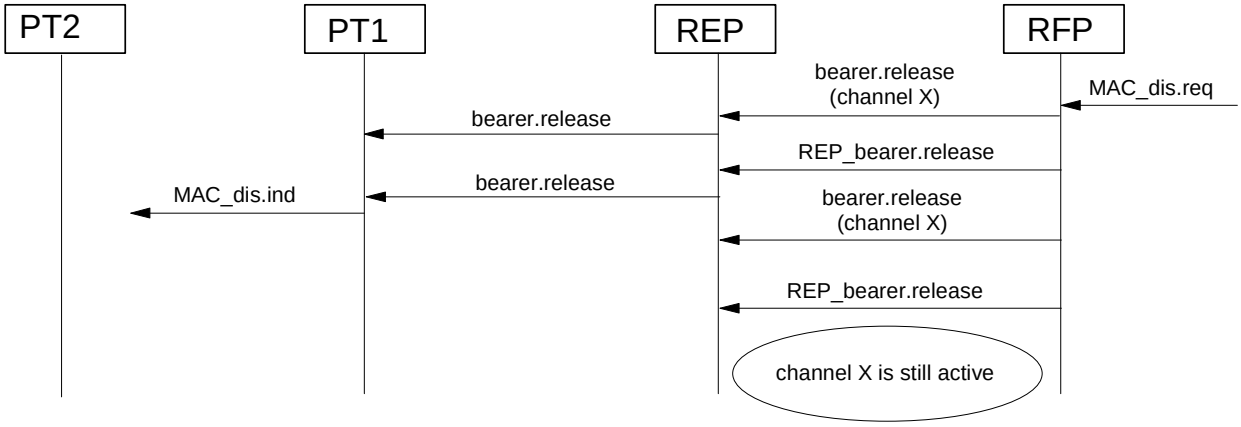



**Figure 22: FP initiated interlaced bearer release scenario**

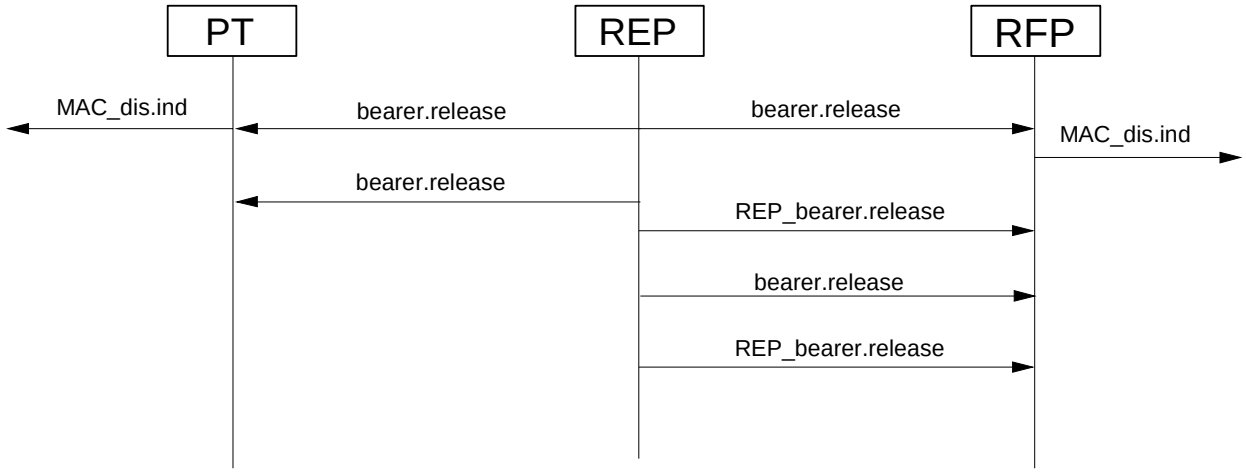



**Figure 23: REP initiated bearer release scenario**

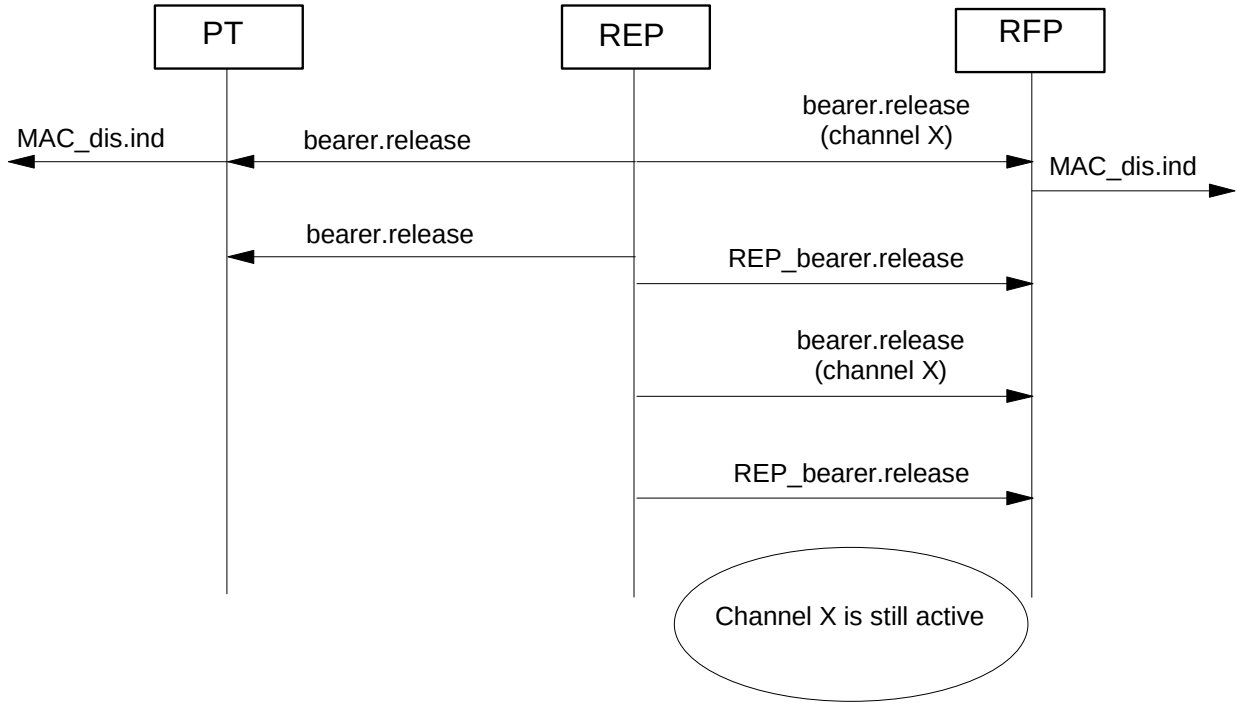



**Figure 24: REP initiated interlaced bearer release scenario**

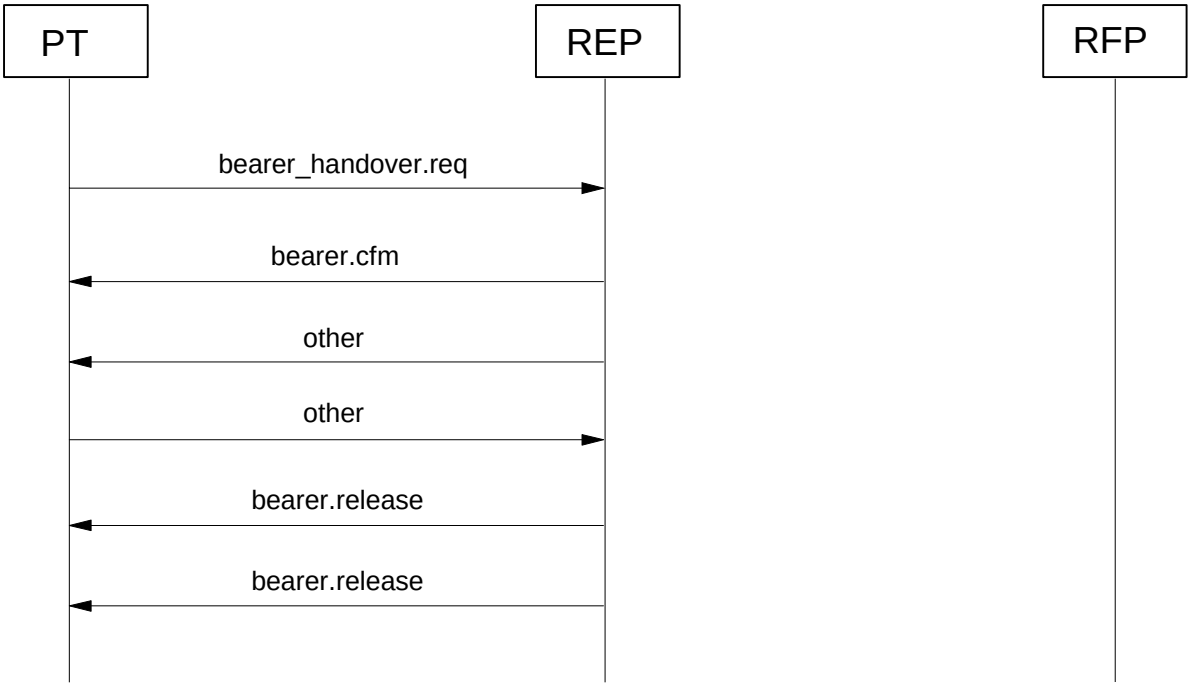



**Figure 25: PP-REP bearer handover scenario; the new PP-REP setup bearer still lies between the two REP-RFP established channels (subclause 6.4.4.3 is still fulfilled)**

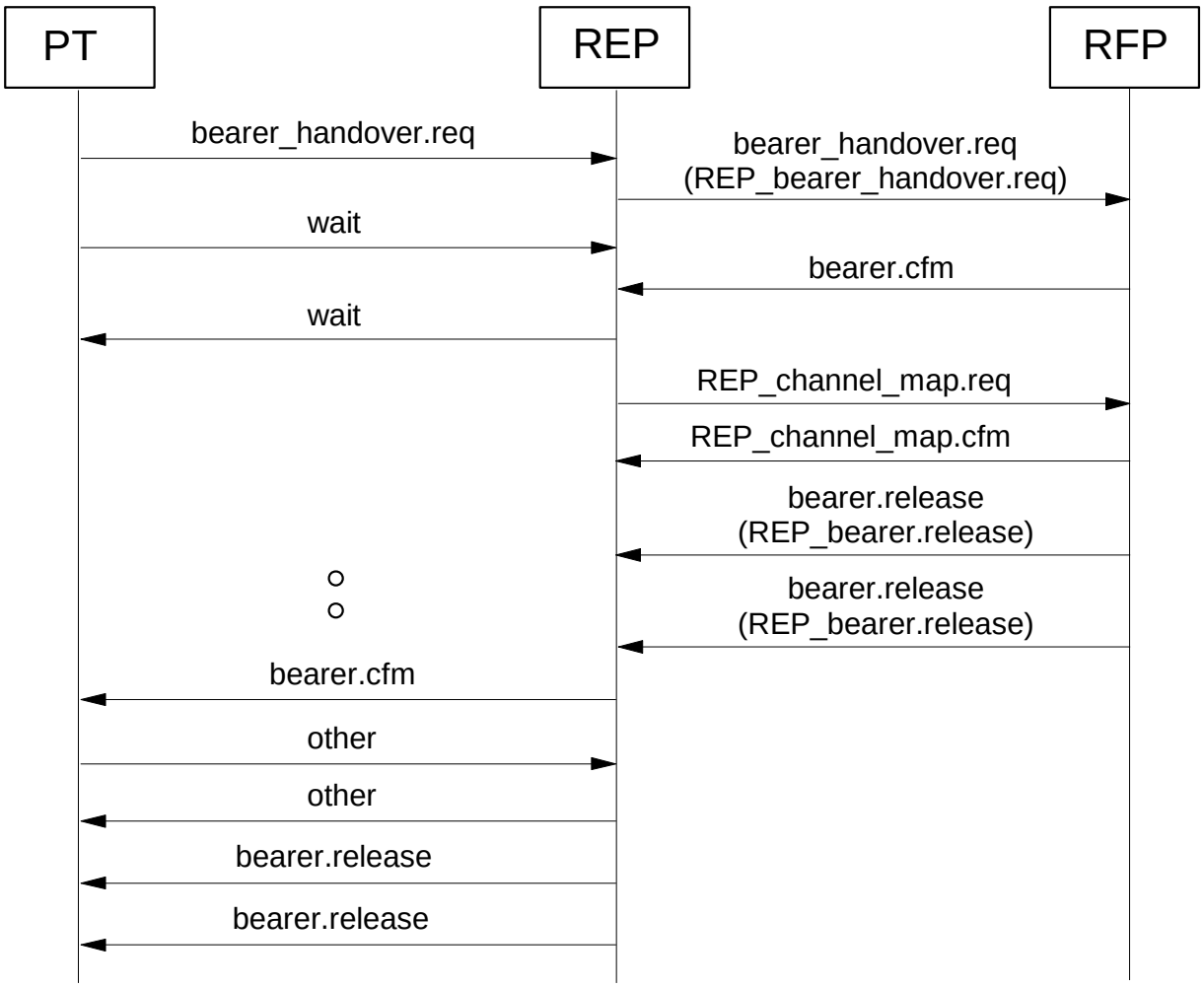



**Figure 26: PP-REP bearer handover scenario; a REP-RFP bearer handover is required (i.e. subclause 6.4.4.3 is no longer fulfilled)**

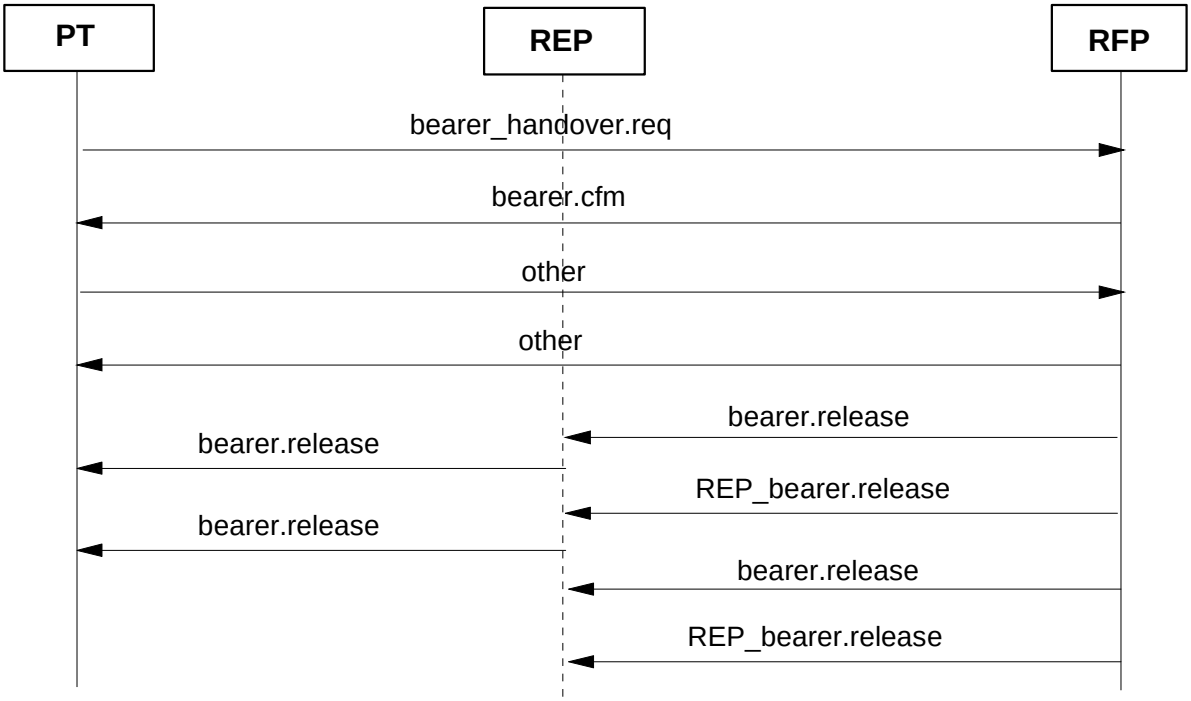



**Figure 27: PP-RFP basic bearer handover scenario**

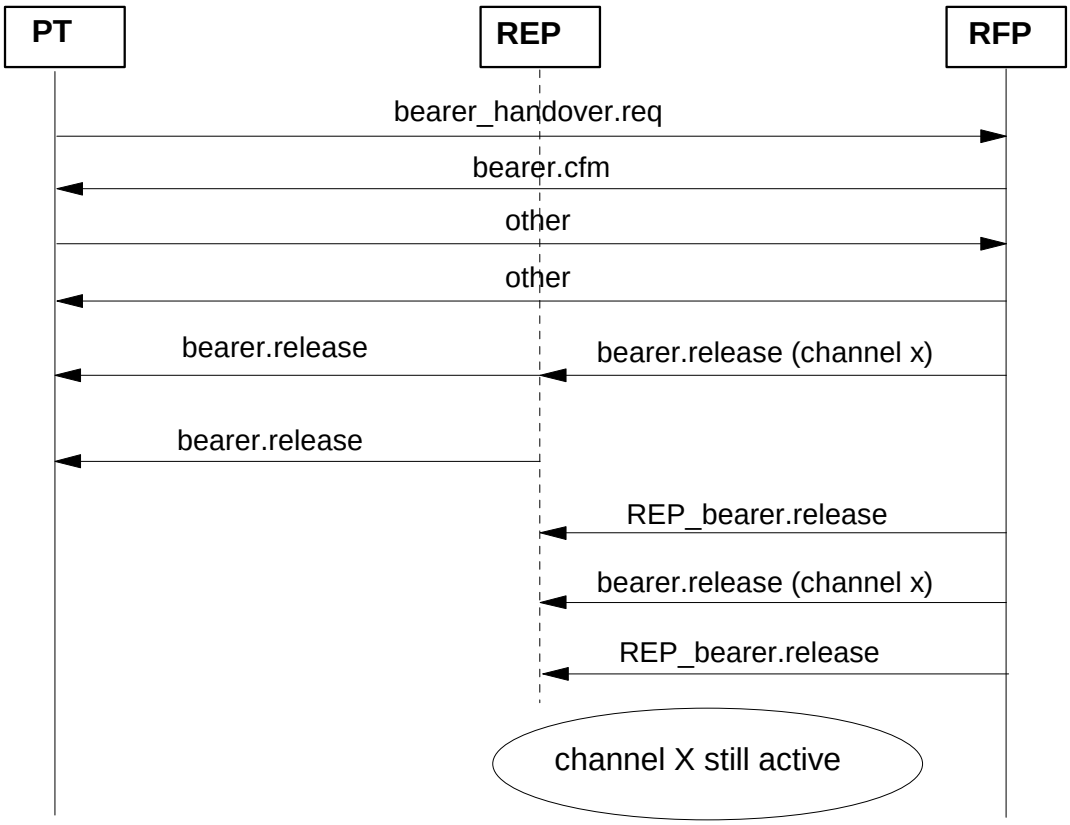



**Figure 28: PP-RFP interlaced bearer handover scenario**

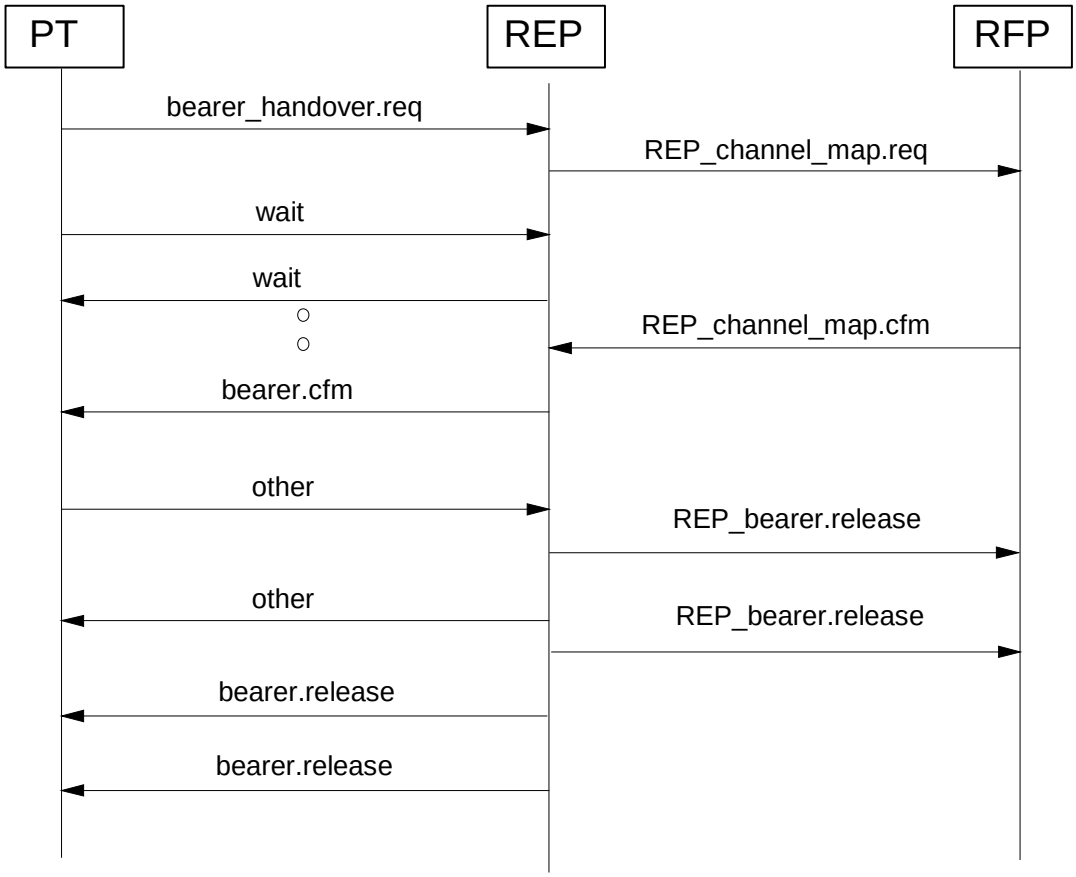



**Figure 29: PP-REP bearer handover scenario; the new setup bearer allows the interlacing with an existing bearer**

# Annex A (normative): The optional CRFP interface to REP

This annex defines optional requirements to the CRFP, which allows a CRFP to interface to a REP. These requirements specify the optional CRFP feature **"REP interface"**.

The CRFP provided with this enhanced interface may perform an adapter function between an FT supporting a CRFP interface, and a REP, in a multihop WRS chain.

## A.1 Description

### A.1.1 General

The CRFP with the optional "REP interface" shall fulfil - in addition to the requirements to the CRFP in clause 5 - the requirements to an FT stated in subclause 6.1.2 and in EN 300 175-3 [3], to support the REP in place of the PT. This means that the CRFP_FT will be able to communicate to a REP_PT.

### A.1.2 Frame multiplexing structure

When performing the adapter function between an FT (or CRFP) and the REP, the CRFP shall perform a mapping between a REP double duplex bearer at the FT side and a duplex bearer at the PT side. This support of a duplex bearer and a double duplex bearer in parallel results in a frame multiplexing structure which combines the CRFP (see subclause 5.1.3.2) and the REP (see subclause 6.1.3.2) frame multiplexing structure.

Figure A.1 shows an example of the frame structure at the CRFP within a two-hop WRS chain built with a CRFP and a REP.

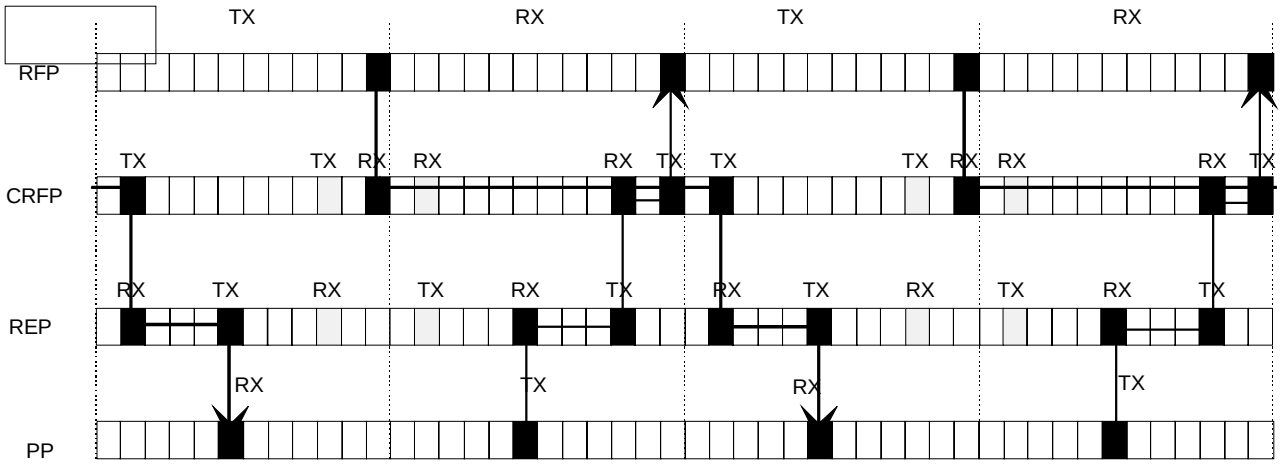



**Figure A.1: Example of frame multiplexing structure in a chain of a CRFP and a REP**

NOTE 1: The minimum incremental round-trip delay for B-field user data caused by a mixed-type WRS chain of one CRFP and one or more REPs is one DECT frame (10 ms) if the bearer allocation rule of subclause A.3.2 is applied by the CRFP and two DECT frames (20 ms) otherwise. Even in the latter case, the delay is not more than that of a 2 hop CRFP chain.

NOTE 2: For a 2 hop WRS chain composed by a REP cascaded to a CRFP, the maximum number of offered connections (full slot duplex bearers) by the last hop of the chain is 4. This corresponds to 0,85 E at the Grade of Service (GoS) 0,5 %. Under the same assumptions, the maximum number of connections cleared by the last hop of a 2 hop CRFP chain is 6, which corresponds to 1,5 E.

# A.2 Messages

## A.2.1 MAC layer

When interfacing to a REP, the CRFP shall use the MAC messages defined for REP at the interface between CRFP and REP. At the interfaces to other units (FT, CRFP, PP) the MAC messages required by CRFP shall be used.

## A.2.2 Hop control

The FP can allow chains of WRSs of the same or different type by means of the extended fixed part capabilities message (see subclause 4.4.2.1) and may control the WRS attachment by means of the $a_{13}$ bit of the Physical and MAC layer capabilities in the fixed part capabilities message (see EN 300 175-3 [3]).

# A.3 Procedures

## A.3.1 MAC layer

When interfacing a REP, the CRFP shall use the procedures defined for REP, and when interfacing the FT (or CRFP) it shall still use the procedures required by CRFP.

Figure A.2 shows an example of time-messages diagram exchanged to establish a Basic connection between an FT and a PT, through a two hops chain of a CRFP and a REP. Figure A.3 widens the example for the case of encryption supported.

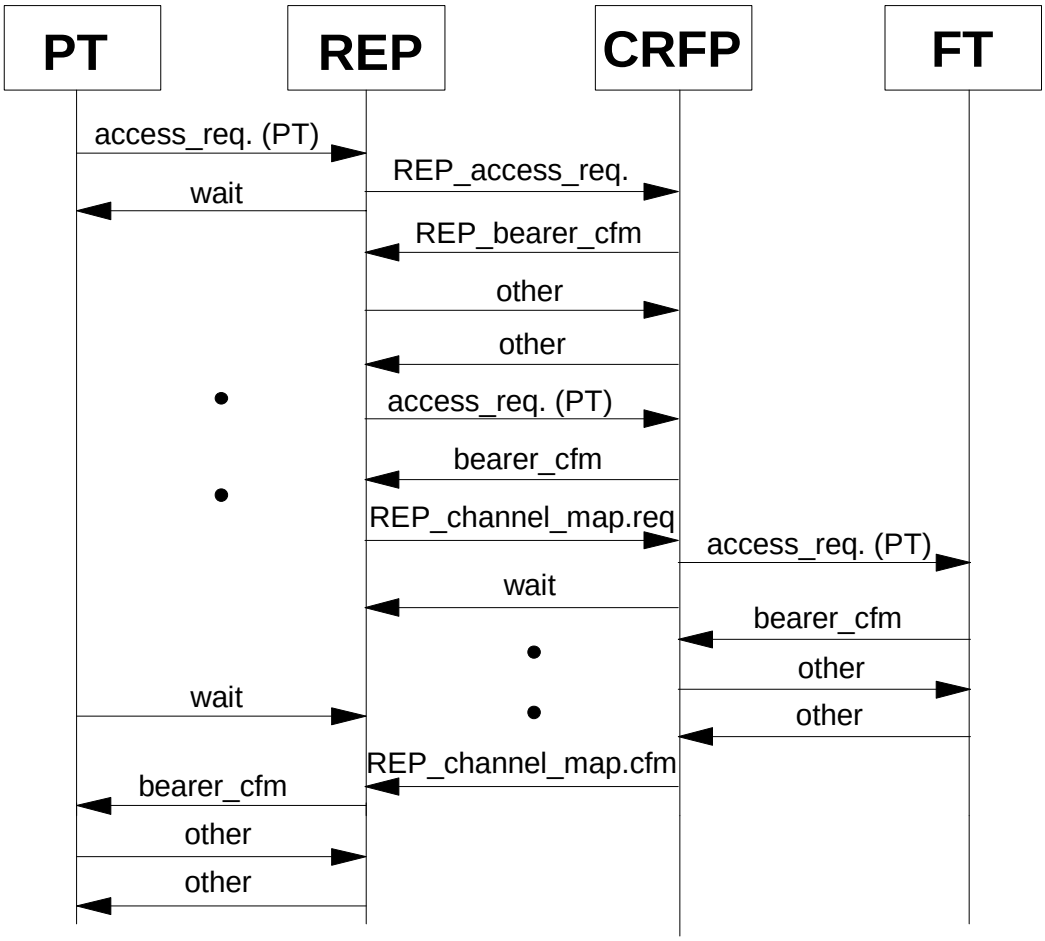



**Figure A.2: Example of basic bearer setup through a chain of CRFP and REP**

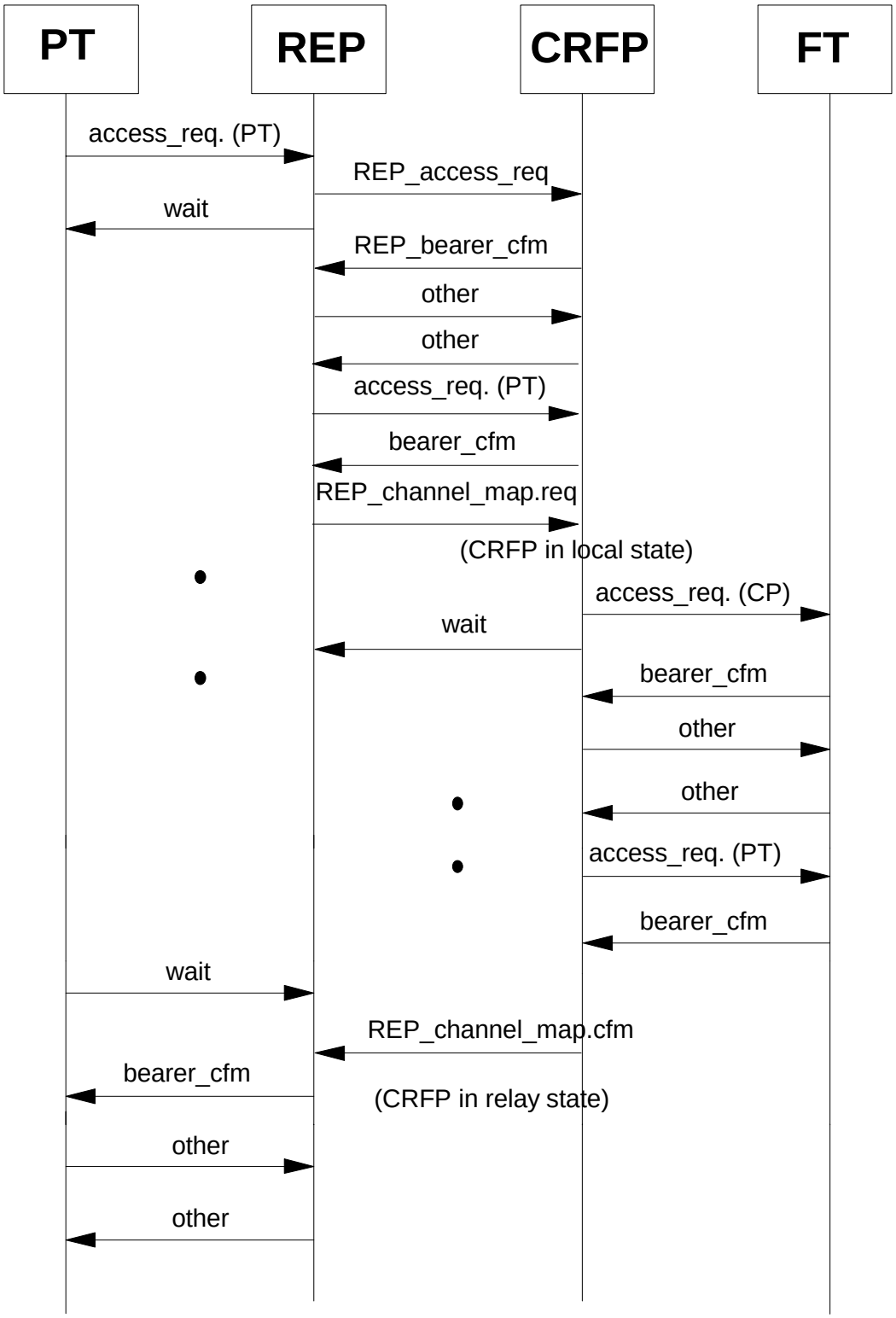



**Figure A.3: Example of basic bearer setup through a chain of CRFP and REP, when encryption is supported**

## A.3.2 Channel selection

In principle, the bearer positions at the CRFP_PT side and the CRFP_FT side to relay a connection are independent from each other except that the bearer positions (time slots) at the PT side and the FT side cannot be identical. This also holds for the case where the CRFP interfaces to a REP, and REP double duplex bearers are used at the CRFP_FT side, which are interworked to single duplex bearers at the CRFP_PT side.

However in the latter case the incremental round-trip delay depends on the relative positions of the double duplex bearers and the single duplex bearers. The delay is reduced by one DECT frame if the following condition is met.

Let (x1; x1+12) and (x2; x2+12) be the two time slot pairs of a double duplex bearer at the REP-CRFP interface (with $0 \leq x1 < x2 \leq 11$), and (y; y+12) with $0 \leq y \leq 11$ be the time slot pair of the associated (single) duplex bearer to be established at the CRFP-FT interface, then the following restriction to obtain minimum delay applies:

$$(y < x1) \text{ OR } (y > x2)$$

This means that the duplex bearer should be positioned **outside the interval** (x1, x2) spanned by the double duplex bearer, either to the left of (before) or to the right of (behind) the interval, to achieve the delay reduction indicated in subclause A.1.3.

# Annex B (normative): CRFP Interworking with GAP-based Fixed Parts

## B.1 Additions and modifications to GAP Fixed Parts

### B.1.1 Downlink broadcast for "CRFP Interworking with GAP-based Fixed Parts"

This subclause describes additions for the FT to the downlink broadcast procedure of EN 300 444 [11], subclause 10.2.

#### B.1.1.1 $Q_T$ - Extended fixed part capabilities

The FT shall be capable of sending and the CRFP shall be capable of receiving and processing the $Q_t$ message as defined in EN 300 175-3 [3], subclause 7.2.3.5.

**Table B.1: Values used within FP capabilities sent by the FP**

| MAC message | Field within the message | Standard values within the MAC message | Normative action/comment |
|---|---|---|---|
| << extended fixed part capabilities >> | | | |
| | <$Q_H$> | 4 | |
| | <a12, a13> | '00' B | 1 CRFP is allowed |
| | <a14> | 0, 1 | 0: CRFP encryption not supported<br>1: CRFP encryption supported |

The CRFP shall not accept intercell handover attempts from a PT if the FP broadcasts to support encryption and does not support CRFP encryption (i.e. having set <a14> equal 0).

### B.1.2 Intra-cell Bearer Handover

A FP supporting "CRFP Interworking with GAP-based Fixed Parts" shall support the GAP-feature (see EN 300 444 [11]): M.9 Bearer Handover intra-cell.

### B.1.3 NWK layer features/procedures support

In addition to the GAP NWK layer features as indicated in EN 300 444 [11] the support as indicated into the following table is required:

**Table B.2**

| No | Feature | Procedure | Ref. | FT r/b | FT pub |
|---|---|---|---|---|---|
| 1 | WRS subscription on air | | | c201 | c201 |
| | | Obtaining access rights for WRS | B.3.1 | M | M |
| 2 | Assignment of WRS- RPN | | | c201 | c201 |
| | | Retrieval of WRS- RPN | B.3.2 | O | O |
| | | Indication/Modification of WRS- RPN | B.3.4 | M | M |
| 3 | Encryption of relayed connections | | | c202 | c202 |
| | | Obtaining access rights for encryption of connections relayed by WRS | B.3.5 | M | M |
| | | Indication of WRS- cipher key | B.3.6 | M | M |
| | | Dual cipher switching | B.3.7 | M | M |
| 4 | Management | | | c201 | c201 |
| | | Initialization of CRFP | B.4.1 | M | M |
| | | Management for Encryption of relayed connections | B.4.2 | M | M |
| 5 | Location registration with TPUI | | | c203 | c203 |
| | | Location registration with TPUI assignment | B.3.7 | M | M |

c201: If CRFP supported THEN M ELSE I.

c202: If CRFP supported THEN O ELSE I.

c203: If CRFP supported AND Encryption supported THEN M ELSE (As in GAP).

### B.1.4 Bearer handover bit mask management.

This subclause is relates to FPs, which use the bit mask inside the MAC layer information "bearer handover info" (see subclause 7.2.4.3.8 of EN 300 175-3 [3]).

All RFPs in the same cluster shall broadcast the same bit mask.

During registration of the CRFP the FP shall assign an RPN (see B.4.1) and if necessary the FP changes the bit mask to be transmitted by all RFPs in the same cluster.

The selection of the RPN for the CRFP and the bit mask transmitted by all RFPs in the same cluster shall ensure that a PP that receives this information concludes that bearer handover is possible between all RFPs (and CRFPs) within the same cluster.

## B.2 Requirements on the CRFP

### B.2.1 General

The CRFP-PT and CRFP-FT shall support all requirements of subclause 10.1 of EN 300 444 [11] with PT replaced by CRFP-PT and FT replaced by CRFP-FT.

In addition the CRFP shall support intercell connection handover on the CRFP-FT side (see subclause 5.3.2.1 of EN 300 444 [11]). The support of connection handover is broadcasted by the FT with the Fixed Part Capabilities.

## B.2.2 Downlink broadcast

### B.2.2.1 $N_T$ message

The CRFP shall be able to receive, process and transmit the $N_T$ message as defined in the following table.

**Table B.3**

| MAC message/broadcast element | Field within the message | Standard values FP | Standard value CRFP-FT | CRFP action |
|---|---|---|---|---|
| <<RFPI>> | <E-bit> | 0 | 0 | SARI not broadcasted by CRFP |
| | | 1 | 1 | SARI broadcasted by CRFP |
| | <PARI> | All | Same PARI as FP | - |
| | <RPN> | All | Assigned RPN | - |

### B.2.2.2 $Q_T$ - static information ($Q_H$ = 0)

The CRFP shall be able to receive, process and transmit the $Q_T$ message as defined in the following table.

**Table B.4**

| Field within the message | Standard values FP | Standard value CRFP-FT | CRFP action |
|---|---|---|---|
| <NR> | 0 | 0 | Symmetric connections only |
| <SN> | 0-11 | SN of relay bearer | - |
| <SP> | 0 | 0. | Always start S-field at bit f0 |
| <ESC> | 0 | 0. | No $Q_T$ escape messages |
| <TX> | 0 | 0 | 1 transceiver |
| <Ext-car> | 0 | 0 | - |
| | 1 | 1 | See extended carriers (optional) |
| <RF-car> | 1-1023 | Same value of <RF-car> as FP | - |
| <SPR> | 0 | 0 | - |
| <CN> | 0-9 | CN of relay bearer | - |
| <SPR> | 0 | 0 | - |
| <PSCN> | 0-N | Aligned PSCN | CRFP shall align PSCN with PSCN of RFP |

### B.2.2.3 $Q_T$ - Extended RF carrier information ($Q_H$ = 2)

The CRFP shall be able to receive, process and transmit the $Q_T$ message as defined in the following table.

If extended frequencies are not supported by the CRFP, the CRFP shall not transmit the Extended RF carrier information.

If the FP supports extended carriers, CRFP shall adapt PSCN scanning to allow continued use of at least the standard DECT frequencies.

**Table B.5**

| Field within the message | Standard values FP | Standard value CRFP-FT | CRFP action |
|---|---|---|---|
| <RF carriers> | All | Copy value of RFP if extended frequencies supported by CRFP | - |
| <RF band> | All | Copy value of RFP if extended frequencies supported by CRFP | Use same RF band as RFP |
| <SPR> | 0 | 0 | - |
| <number of RF carriers> | All | Copy value of RFP if extended frequencies supported by CRFP | Use same number of RF carriers as RFP |

### B.2.2.4 $Q_T$ - FP capabilities ($Q_H$ = 3)

The CRFP shall be able to receive, process and transmit the $Q_T$ message as defined in the following table.

**Table B.6**

| Field within the message | Standard values FP | Standard value CRFP-FT | CRFP action |
|---|---|---|---|
| <a12> | 1 | 1 | Process extended FP capabilities, See also B.1.1.1 and B.2.2.5 |
| <a17> | 1 | 1 | Support Full slot |
| <a23> | 1 | 1 | Support Basic A-field setup |
| <a27> | 1 | 1 | Support IN_min_delay |
| <a32> | 1 | 1 | ADPCM speech |
| <a33> | 1 | 1 | GAP basic speech |
| <a36> | 0,1 | Copy $Q_{H3}$ (a36) from RFP | Standard authentication required (Transparent for CRFP) |
| <a37> | 0,1 | Copy $Q_{H3}$ (a37) from RFP | Standard ciphering supported (Transparent for CRFP) |
| <a38> | 0,1 | Copy $Q_{H3}$ (a38) from RFP | Location registration supported (Transparent for CRFP) |
| <a40> | 0,1 | Copy $Q_{H3}$ (a40) from RFP | Non-static FP (Transparent for CRFP) |
| <a44> | 0,1 | Copy $Q_{H3}$ (a44) from RFP | Access Rights supported (Transparent for CRFP) |
| <a46> | 0,1 | Copy $Q_{H3}$ (a46) from RFP | Connection handover supported |

It cannot be guaranteed that a GAP CRFP supports the capabilities that are related to codings that are **NOT** mentioned in this table.

### B.2.2.5 $Q_T$ - Extended FP capabilities ($Q_H$ = 4)

See also B.1.1.1.

**Table B.7**

| Field within the message | Standard values FP | Standard value CRFP-FT | CRFP action |
|---|---|---|---|
| <a12, a13> | 00 | 11 | CRFP is allowed to lock to RFP. |
| | 11 | - | CRFP is not allowed to lock to RFP. |
| <a14> | 0,1 | 0 | Not relevant for the CRFP because only 1 hop is allowed |

It cannot be guaranteed that a GAP CRFP supports the capabilities that are related to codings that are **NOT** mentioned in this table.

### B.2.2.6 $Q_T$ - SARI support ($Q_H$ = 5)

The CRFP shall be able to receive, process and transmit the $Q_T$ message as defined in the following table. The CRFP shall transmit the $Q_t$ -SARI support only if the FP sends it.

**Table B.8**

| Field within the message | Standard values FP | Standard value CRFP-FT | CRFP action |
|---|---|---|---|
| <SARI list length> | All | Copy from RFP | - |
| <TARIs yes/no> | All | Optional | TARI support can not be guaranteed by GAP CRFP |
| <Black yes/no> | All | Copy from RFP | - |
| <ARI or black-ARI> | All | Copy from RFP | - |

### B.2.2.7 $Q_T$ - Multiframe number ($Q_H$ = 6)

The CRFP shall be able to receive, process and transmit the $Q_T$ message as defined in the following table. The CRFP shall transmit the $Q_t$-multiframe number only if the FP sends it.

**Table B.9**

| Field within the message | Standard values FP | Standard value CRFP-FT | CRFP action |
|---|---|---|---|
| <SPARE > | 1111 0000 1111 | 1111 0000 1111 | - |
| <multiframe number> | All | Regenerate value from RFP | - |

## B.2.3 Paging broadcast

### B.2.3.1 Short page, normal/extended paging

The CRFP shall be able to receive, process and transmit the PT message as defined in the following table.

**Table B.10**

| Field within the message | Standard values FP | Standard value CRFP-FT | CRFP-FT action |
|---|---|---|---|
| <Extended flag > | 0,1 | Copy value from RFP | - |
| <$B_s$ SDU length indication > | 1 | 1 | CRFP-FT supports short page messages |
| <20 bits of $B_s$ channel data> | All | Copy value from RFP | CRFP repeats broadcast that it received from the RFP |
| <Information type> | 1,2,5,9 | 1,2,5,9 | |
| <MAC layer information> | Corresponding local RFP MAC layer information | Corresponding local CRFP MAC layer information | 1: blind full slot<br>CRFP shall send out its local blind slot information (as defined in subclause 10.3.3 of EN 300 444 [11])<br>2: other bearer and<br>5: dummy or C/L bearer position<br>CRFP shall send out corresponding local bearer positions<br>9: bearer handover information<br>CRFP shall copy the "info type" received from the RFP |

### B.2.3.2 Zero length page, normal/extended paging

**Table B.11**

| Field within the message | Standard values FP | Standard value CRFP-FT | CRFP-FT action |
|---|---|---|---|
| <Extended flag > | 0,1 | Copy value from RFP | - |
| <$B_s$ SDU length indication > | 0 | 0 | CRFP-FT supports zero length page messages |
| <20 bits of $B_s$ channel data> | All | All | Insert 20 least significant bits of RFPI of CRFP |
| <Information type> | 1,2,5,9 | 1,2,5,9 | |
| <MAC layer information> | Corresponding local RFP MAC layer information | Corresponding local CRFP MAC layer information | 1: blind full slot<br>CRFP shall send out its local blind slot information (as defined in subclause 10.3.3 of EN 300 444 [11])<br>2: other bearer and<br>5: dummy or C/L bearer position<br>CRFP shall send out corresponding local bearer positions<br>9: bearer handover information<br>CRFP shall copy the "info type" received from the RFP |

## B.2.4 Quality control of relayed connections

See subclause 5.1.3.4 of the present document.

### B.2.5 NWK layer features/procedures support

In addition to the GAP NWK layer features as indicated in EN 300 444 [11] the support as indicated into the following table is required:

**Table B.12**

| No | Feature | Procedure | Ref. | crfp |
|---|---|---|---|---|
| 1 | WRS subscription on air | | | M |
| | | Obtaining access rights for WRS | B.3.1 | M |
| 2 | Assignment of WRS- RPN | | | M |
| | | Retrieval of WRS- RPN | B.3.2 | O |
| | | Indication/Modification of WRS- RPN | B.3.4 | M |
| 3 | Encryption of relayed connections | | | M |
| | | Obtaining access rights for encryption of connections relayed by WRS | B.3.5 | M |
| | | Indication of WRS- cipher key | B.3.6 | M |
| | | Dual cipher switching | B.3.7 | M |
| 4 | Management | | | M |
| | | CRFP Initialization | B.4.1 | M |
| | | Management for Encryption of relayed connections | B.4.2 | M |
| 5 | Location registration with TPUI | | | M |
| | | Location registration with TPUI assignment | B.3.7 | M |

## B.3 NWK layer procedures

### B.3.1 Obtaining access rights for WRS

The procedure as defined in subclause 8.30 of EN 300 444 [11] applies with the additions/modifications as defined in this subclause.

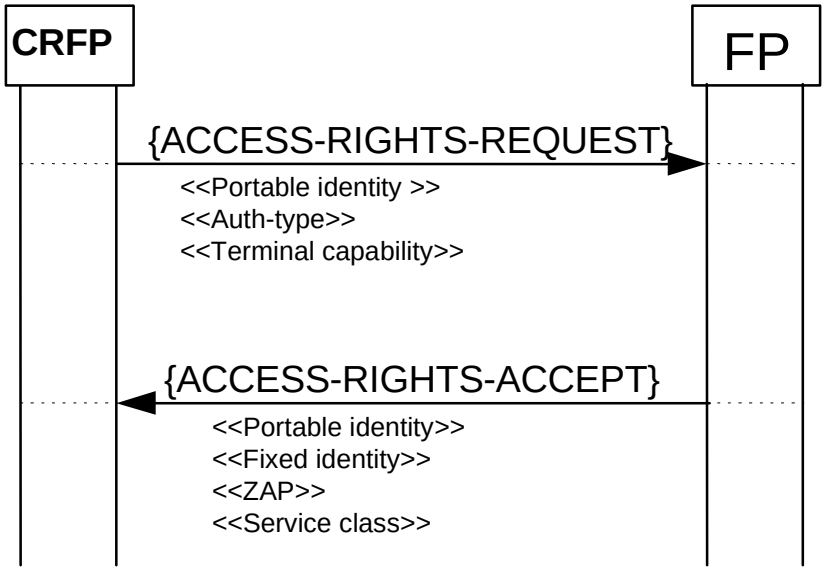



**Figure B.1: Obtain access rights for WRS**

**Table B.13: Additions/modification to the {ACCESS-RIGHTS-REQUEST} message**

| Information element | Field within the information element | Standard values within the field/IE | Normative action/comment |
|---|---|---|---|
| <<Terminal capability>> | | | |
| | <Tone capability> | All | |
| | <Display capability> | All | |
| | <Profile_Indicator_1> | 'xxxxx1x' | GAP and/or PAP supported |
| | <Profile_Indicator_2> | All | |
| | <Profile_Indicator_3> | 'xxxxx1x' | WRS supported |
| | | | |
| | <Control codes> | All | |

## B.3.2 Retrieval of WRS- RPN

The procedure shall be performed as defined in EN 300 175-5 [5], subclause 13.7, parameter retrieval initiated by PT. The following text together with the included subclauses define the minimum requirements with regard to the present document.

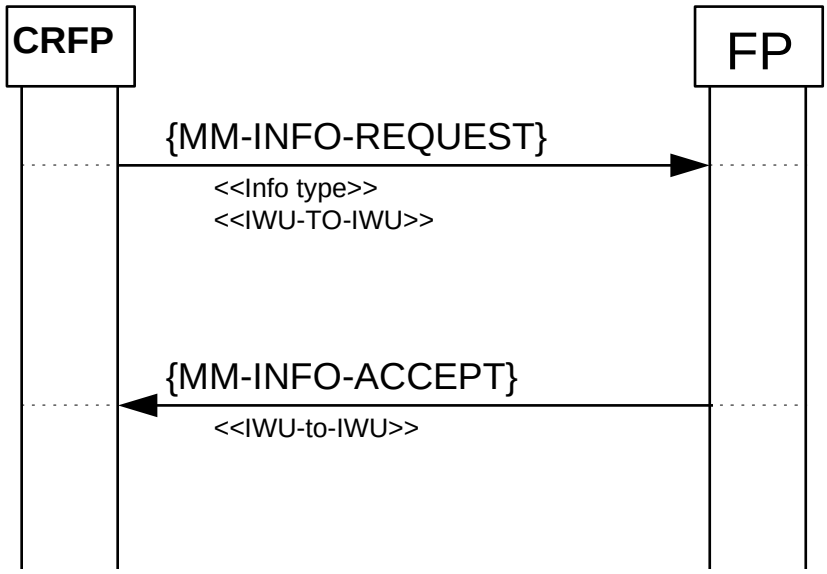



**Figure B.2: Retrieval of WRS- RPN**

**Table B.14: 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> | 24H | OA&M call |
| <<IWU- TO – IWU>> | | | |
| | <S/R> | 1 | Transmission of message |
| | <Protocol discriminator> | 16H | WRS |
| | <SC> | 001 | WRS OA&M |
| | <Service type> | 00111 | Remote configuration |
| | <Configuration information type> | 10000000 | WRS- RPN |

**Table B.15: Values used within the {MM-INFO-ACCEPT} message**

| Information element | Field within the information element | Standard values within the field/IE | Normative action/comment |
|---|---|---|---|
| <<IWU- to - IWU>> | | | |
| | <S/R> | 1 | Transmission of message |
| | <Protocol discriminator> | 16H | WRS |
| | <SC> | 001 | WRS OA&M |
| | <Service type> | 00111 | Remote configuration information |
| | <Configuration information type> | 10000000 | WRS- RPN |
| | <RPN- length> | [10000011 .. 10001000] | |
| | <RPN- value> | all | See as well management requirements |

## B.3.3 Indication/modification of WRS- RPN

The procedure shall be performed as defined in EN 300 175-5 [5], subclause 13.7, parameter retrieval initiated by FT. The following text together with the included subclauses define the minimum requirements with regard to the present document.

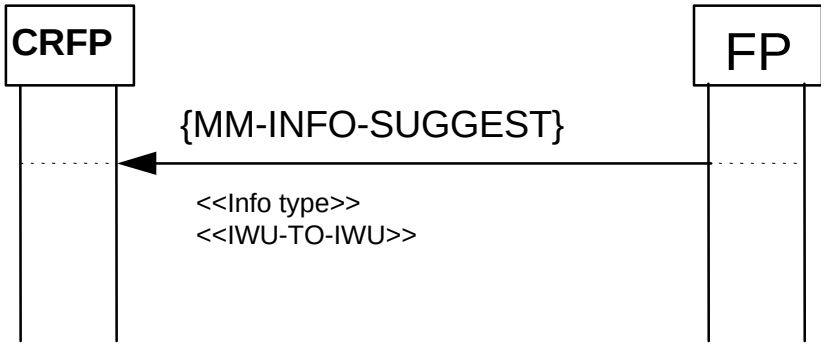



**Figure B.3: Indication/modification of WRS- RPN**

**Table B.16: 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> | 34H | OA&M call |
| <<IWU- to - IWU>> | | | |
| | <S/R> | 1 | Transmission of message |
| | <Protocol discriminator> | 16H | WRS |
| | <SC> | 001 | WRS OA&M |
| | <Service type> | 00111 | Remote configuration information |
| | <Configuration information type> | 10000000 | WRS- RPN |
| | <RPN- length> | [10000011 .. 10001000] | |
| | <RPN- value> | all | See as well management requirements |

## B.3.4 Obtaining access rights for encryption of connections relayed by WRS

The procedure as defined in subclause 8.30 of EN 300 444 [11] applies with the additions/modifications as defined in this subclause.

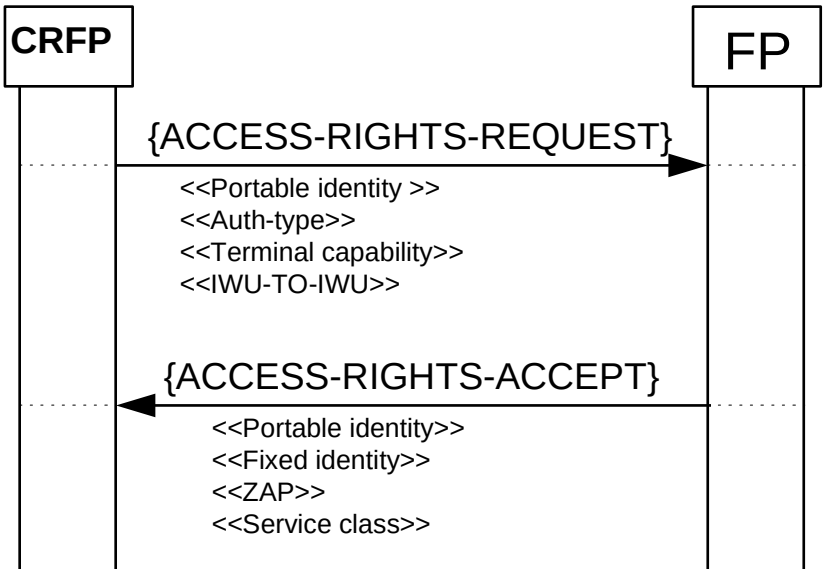



**Figure B.4: Obtaining access rights for encryption of connections relayed by WRS**

**Table B.17: Additions/modification to the {ACCESS-RIGHTS-REQUEST} message**

| Information element | Field within the information element | Standard values within the field/IE | Normative action/comment |
|---|---|---|---|
| <<IWU- to - IWU>> | | | |
| | <S/R> | 1 | Transmission of message |
| | <Protocol discriminator> | 16H | WRS |
| | <SC> | 001 | WRS OA&M |
| | <Service type> | 00111 | Remote configuration |
| | <Configuration information type> | 10000001 | WRS subscription for encryption of relayed connection |
| | <Subscription number> | Any | Indicates the number of the requested subscription. In case of failure, the PT may re- attempt the procedure with the same subscription number |

## B.3.5 Indication of WRS - cipher key

The cipher key transfer procedure is used by the FP to transfer a cipher key to the CRFP for encryption of relayed connections. The procedure shall be performed as defined in EN 300 175-5 [5], subclause 13.7, parameter retrieval initiated by FT. The following text together with the included subclauses define the minimum requirements with regard to the present document.

NOTE: Prior to the cipher key transfer, the link between FP and CRFP is switched to local mode. Upon completion of the cipher key transfer procedure, the link switches back to relayed mode. An overview of the entire procedure is provided in subclause 5.3.

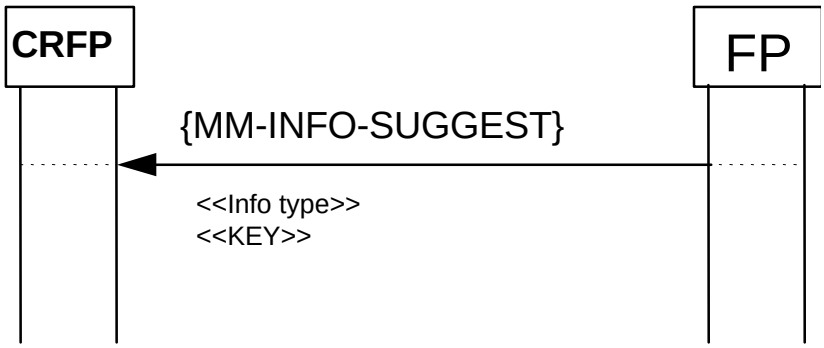



**Figure B.5: Indication of WRS- cipher key**

**Table B.18: 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> | 0 | CK transfer |
| <<KEY>> | | | |
| | <Key type> | 10010000 | DCK |
| | <Key> | Any | |

## B.3.6 Dual cipher switching

Before initiation of ciphering a reliable link shall be established between the CRFP and the FP.

On receipt of an MM_CIPHER-req primitive the FT shall request the LLME for the type of the link available, i.e. whether the Dual relay operation MAC services are being used.

If the type of link is one based on Dual relay operation underlying services the FT shall start a Dual cipher switching initiated by FT procedure.

Otherwise, i.e. if the link is directly to PT or link only to CRFP (e.g. for OA&M) it shall start a normal Cipher switching FT initiated procedure as described in EN 300 444 [11].

If the Dual cipher switching initiated by FT procedure is required, and, if the link with the CRFP is in "relay state" the FT-NWK shall send a DL-CRFP-STATE-SWITCH-req primitive to request the MAC to switch to "local state". After a DL-CRFP-STATE-SWITCH-ind is received indicating that the MAC is now in "local state" the FT shall first perform a normal Cipher switching FT initiated procedure to the CRFP as defined in EN 300 444 [11], using the parameters associated with the particular CRFP user in charge of the link.

When the link is successfully ciphered, i.e. the FP-IWU receives a MM_CIPHER-cfm primitive indicating "success" the FT-IWU shall send a MN-INFO_req primitive to the FT-NWK layer requesting the FT to provide the CRFP with the PP's DCK needed for the other end of the link, i.e. between the CRFP and PP. The FT-NWK shall send a MM-INFO-SUGGEST message.

Upon receipt of a new MM_CIPHER-req primitive from the FT-IWU the FT-NWK shall submit a DL-CRFP-STATE-SWITCH-req primitive requesting MAC to switch to "relay state".

Upon receipt of request for switching the underlying connection state DLC and MAC shall ensure that all outstanding data is successfully transmitted and only then the link shall be switched to another state.

When confirmation of the switching is received in a DL-CRFP-STATE-SWITCH-ind primitive the FT-NWK shall submit the MM-CIPHER-REQUEST message intended for the PP. The FT shall not provide the DL_ENC_KEY-req and shall not provide the DL_ENCRYPT-req primitive to DLC, it shall start timer <MM_cipher.1>.

The outcome of this procedure shall be indicated to the FT-IWU as in the normal Cipher switching FT initiated procedure as described in EN 300 444 [11].

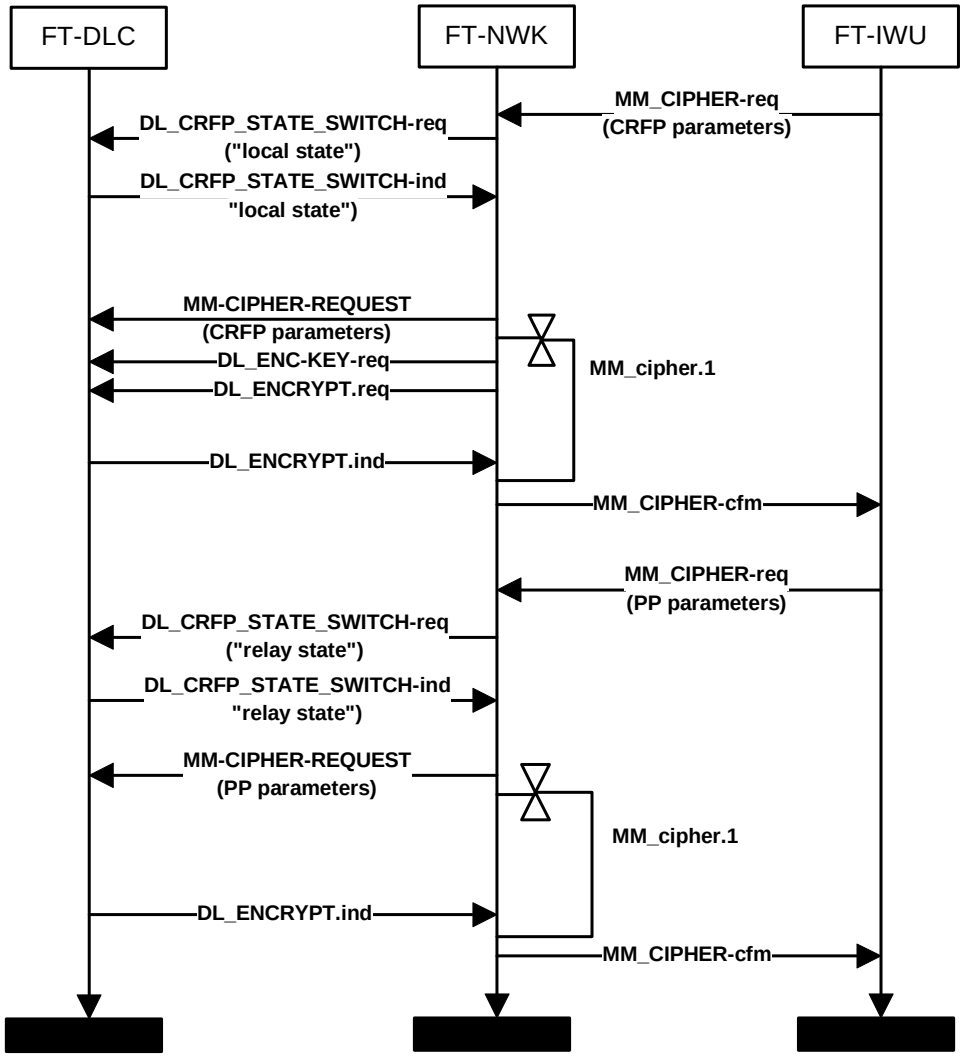



**Figure B.6: Dual cipher switching initiated by FT procedure NWK layer prospective**

If FT performs dynamic allocation of DCK to the CRFP before any attempt to cipher the link to the CRFP, as well as allocation of new DCK to the PP the FT-IWU shall ensure that the FT-NWK is able to distinguish the different addressees of the message, thereby it can request a proper change in the link state and provide/use the correct parameters, e.g. if the message is for the CRFP only the keys and numbers used with the particular CRFP user, if the message is for the PP - the keys and numbers associated with that PP.

### B.3.7 Location registration with TPUI assignment for WRS

The procedure as defined in subclause 8.28 of EN 300 444 [11] applies with the additions/modifications as defined in this subclause.

The CRFP shall perform a location registration to ensure that a TPUI ahs been assigned per user (i.e. possible relayed connection). This will allow the FT to identify, based on the received from the CRFP assigned PMID, which subscription record (in particular which DCK) to be used when a relayed connection is established on request from the CRFP.

FPs that support CRFP and Encryption shall as well support Location registration with TPUI assignment and shall always use this procedure with the CRFP initiated location registration.

## B.4 Management procedures

### B.4.1 Initialization of CRFP

The CRFP shall have installed at least one IPEI at delivery. If the CRFP supports encryption it shall be pre-installed with at least as many IPEIs as CRFP users, see subclause 5.1.5.2.

For OA&M procedures an additional IPEI may be installed.

To attach a CRFP to an existing DECT system, on user request the CRFP shall perform an Obtain Access Rights for WRS procedure as defined in subclause B.3.1 providing the OA&M IPEI if special one installed or one of the available IPEIs otherwise and indicating that this is a CRFP initiated subscription into the <<Terminal capabilities>> information element. The received PARK and IPUI shall be used for establishment of connection for OA&M purposes. Before accepting the obtain access rights the FT shall provide the CRFP with RFPI to be used when communication to the PPs - the Indication/Modification of WRS - RPN procedure shall be used as described in subclause B.3.3.

#### B.4.1.1 Indication/Modification of WRS/RPN

When a subscription of a CRFP has taken place at a FP with an ARI indicating "single cell RFPI" by having set the LSB of the RPN equal 0 (i.e. PARK-A, -C, -D), the FP shall set this LSB of its RPN equal 1. The resulting RPN shall not be assigned to a CRFP.

Additionally, when a FP assigns an RPN towards a CRFP it shall do this according to clause 5 of EN 300 175-6 [6].

### B.4.2 Management for Encryption of relayed connections

After the initialization of CRFP has been successfully accomplished the CRFP shall examine the FP "Extended FP capabilities" and shall establish whether the FP supports Ciphering towards the CRFP. If the FP supports ciphering, the CRFP shall initiate the Obtaining access rights for encryption of connections relayed by WRS procedure as defined in subclause B.4.5. The CRFP shall perform the procedure once per every CRFP user thereby establishing a CRFP user dedicated subscription record. If the FP does not support ciphering the CRFP shall not initiate this procedure.

For all Obtain access rights procedures the FT shall assign the same PARK value. The IPUI assigned value should equal the IPEI value used for initiation of the procedure with possible change of the type of portable identity.

NOTE: Usage of IPEI is required to ensure unique identity and to allow smart handling of size of subscription record.

Per each CRFP user a DCK shall be established. The Storing the Derived Cypher Key (DCK) procedure as defined in EN 300 444 [11] shall be used. For DCK derivation the FP may perform in advance a Key allocation procedure to establish a UAK, as defined in EN 300 444 [11], otherwise the AC shall be used for DCK derivation.

For location registration, see annex C clause 13.2 of EN 300 444 [11].

# History

| Document history | | | |
|---|---|---|---|
| Edition 1 | March 1997 | Publication as ETS 300 700 | |
| V0.2.1 | March 1999 | Public Enquiry | PE 9927: 1999-03-05 to 1999-07-02 |
| V0.3.3 | July 2000 | Vote | V 20000901: 2000-07-03 to 2000-09-01 |
| V1.2.1 | September 2000 | Publication | |
| | | | |