Draft ETSI EN 300 700 V2.0.21 (2016-08)

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

Reference
REN/DECT-ULE268

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

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

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

Foreword

This draft European Standard (EN) has been produced by ETSI Technical Committee Digital Enhanced Cordless Telecommunications (DECT), and is now submitted for the combined Public Enquiry and Vote phase of the ETSI standards EN Approval Procedure.

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	18 months after doa

Modal verbs terminology

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

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

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.

The DECT WRS defined by the present document supports the DECT New Generation (NG-DECT) and DECT Ultra Low Energy (ULE) profiles.

2 References

2.1 Normative references

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

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

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

The following referenced documents are necessary for the application of the present document.

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

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

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

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

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

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

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

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

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

[10] ETSI TS 102 527-3: "Digital Enhanced Cordless Telecommunications (DECT); New Generation DECT; Part 3: Extended Wideband Speech Services".

[11] ETSI TS 102 527-4: "Digital Enhanced Cordless Telecommunications (DECT); New Generation DECT; Part 4: Light Data Services; Software Update Over The Air (SUOTA), content downloading and HTTP based applications".

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

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

[14] ETSI EN 300 176-1: "Digital Enhanced Cordless Telecommunications (DECT); Test specification; Part 1: Radio".

2.2 Informative references

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

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

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

Not applicable.

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: 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: 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: 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: 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

NOTE: 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: 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: 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

V1 WRS: Wireless Relay Station defined according to any revision before 2.1.1 of the present document.

V2 WRS: Wireless Relay Station defined according to revision 2.1.1 or later of the present document.

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: 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
ARQ	Automatic Retransmission reQuest
BCK	B-filed aCKnowledgement
BMC	Broadcast Message Control
C/L	Connection-Less
C/O	Connection-Oriented
CFRP	Is this typo and should it be CRFP?
CK	Cipher Key
CN	Carrier Number
CRC	Cyclic Redundancy Check
CRFP	Cordless Radio Fixed Part
DCK	Derived Cipher Key
DECT	Digital Enhanced Cordless Telecommunications
DefCK	Default Cipher Key
DLC	Data Link Control
DPRS	Data Packet Radio service
DSAA2	DECT Standard Authentication Algorithm #2
DSC	DECT Standard Cipher
DSC2	DECT Standard Cipher #2
ECN	Exchanged Connection Number
FMID	Fixed part MAC Identity
FP	Fixed Part
FP-WRS	Fixed Part WRS
FT	Fixed radio Termination
GAP	Generic Access Profile
GFSK	Gaussian Frequency Shift Keying
IE	Information Element
IP	Internet Protocol
IPEI	International Portable Equipment Identity
IPUI	International Portable User Identity
IWU	Inter Working Unit
KSG	Key Stream Generator
LAPC	DLC Layer C-plane upper protocol entity

LBN	Logical Bearer Number
LLME	Lower Layer Management Entity
LSB	Least Significant Bit
MAC	Medium Access Control
MBC	Multi Bearer Control
ME	Management Entity
MM	Mobility Management
MMI	Man Machine Interface
MUX	time MUltipleXor
NG-DECT	New Generation DECT
NLF	New Link Flag
NTP	Normal Transmit Power
NWK	Network
OA&M	Operation, Administration and Maintenance
PAP	Public Access Profile
PARI	Primary Access Rights Identity
PARK	Portable Access Rights Key
PHL	PHysical Layer
PHS	Personal Handy-phone System
PHY	Physical Layer
PMID	Portable part MAC Identity
PP	Portable Part
PP-WRS	Portable Part WRS
PSCN	Primary receiver Scan Carrier Number
PT	Portable radio Termination
REP	Repeater Part
RF	Radio Frequency
RFP	Radio Fixed Part
RFPI	Radio Fixed Part Identity
RMBC	Relay Multi Bearer Control
RPN	Radio fixed Part Number
RSSI	Radio Signal Strength Indicator
RX	Receive
SAP	Service Access Point
SARI	Secondary Access Rights Identity
SDU	Service Data Unit
SN	Slot pair Number
SUOTA	Software Update Over The Air
TARI	Tertiary Access Rights Identity
TBC	Traffic Bearer Control
TPUI	Temporary Portable User Identity
TX	Transmit
UAK	User Authentication Key
ULE	Ultra Low Energy
WRS	Wireless Relay station

4 Wireless Relay Station (WRS)

4.1 Introduction

A WRS is a physical grouping that contains both Fixed Termination (FT) and Portable Termination (PT) elements, and which 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/strongest 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, which means that the RFP that the WRS locks to may in fact be another WRS.

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. For example, the capacity may be too low, or there may be a need to adjust the audio echo control requirements.

Installing or adding a WRS to a DECT infrastructure is not possible outside the control of the system operator/installer/owner, which provides the required system identities, access rights and authentication/encryption keys.

NOTE 1: Previous versions of the present document defined two different WRS concepts, the Cordless Radio Fixed Part (CRFP) and the Repeater Part (REP). The present document only defines the requirements for the CRFP. The REP had several aspects that made it complex to implement, and it is no longer supported in the present document.

NOTE 2: Since only one type of repeater is defined in the present document, the terms "repeater", "WRS" and "CRFP" are somewhat synonymous. The precise technical term is "CRFP", but the terms "WRS" and simply "repeater" can also be used more generally.

4.2 Description

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

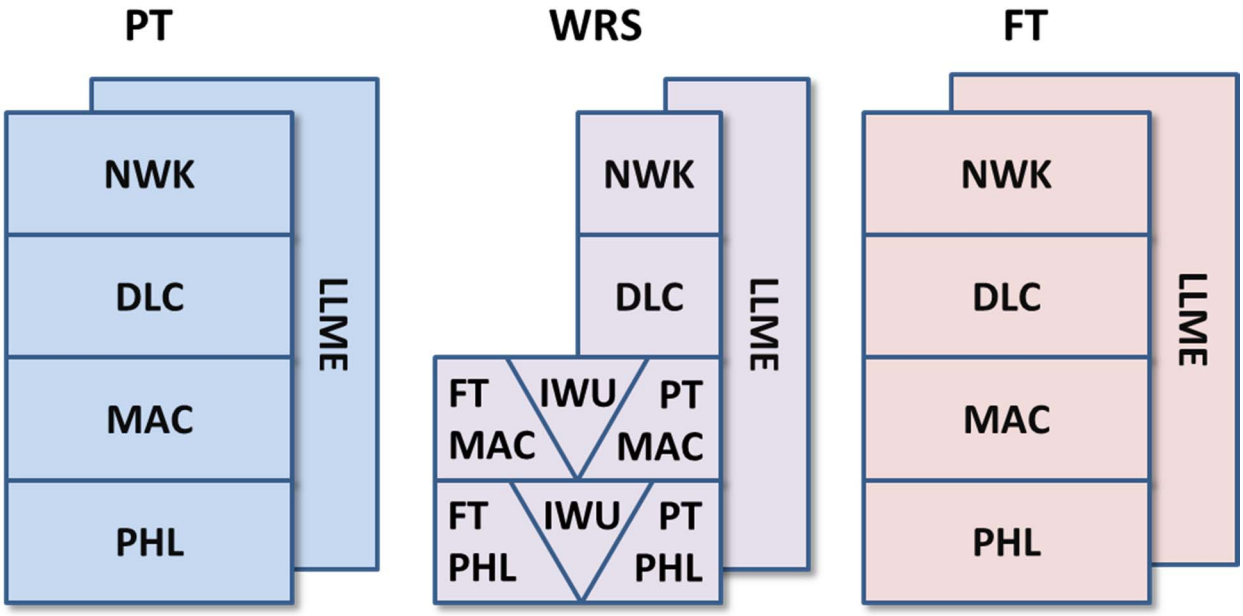

Figure 1: WRS Protocol Stack Reference Model

The PT may also be the PT side of another WRS in a multi-hop scenario. The FT may also be the FT side of another 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 ETSI EN 300 175, Parts 1 [1] to 8 [8].
- Interworking with FTs as defined by ETSI EN 300 175, Parts 1 [1] to 8 [8], with additions defined in the present document (Annex A).
- 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 protocol transparent. In general the PT cannot distinguish the WRS from any other RFP within an FT. As a consequence the WRS puts no additional mandatory requirements on the PT.

4.3 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.

The following functions are required for the CRFP based on ETSI EN 300 175, Parts 1 [1] to 8 [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 required 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.
- Cipher Key (CK) uploading and initialization for CRFP_FT MAC (including DCK and/or DefCK).

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

- MAC layer: access control of CRFP (for specific information transfer to CRFPs).
- NWK layer: Cipher Key (CK) transfer to CRFP (including DCK and/or DefCK).

The CRFP can support a number of simultaneous relayed connections (to different PPs). Each PP is handled by a separate "virtual entity" of the CRFP, also referred to as a "CRFP user" (see clause 7.6.3).

4.4 Terminology

This clause defines and clarifies some common terminology which is used in the present document:

- **Node:** A node is a component of a repeater system. For example, in a system comprising an FP, two WRS and a PP, all 4 of these entities are nodes (see Figure 2).
- **Segment:** The term segment is used to refer to the link (either uplink or downlink) between two adjacent nodes (see Figure 2).
- **Upper segment:** The segment in the upwards direction (i.e. towards the FP).
- **Lower segment:** The segment in the downwards direction (i.e. towards the PP).
- **Leg:** The term leg is synonymous with segment in this context.
- **Following node:** This term relates to the direction of travel of a message being relayed by a WRS. The following node is the one which the WRS is transmitted the relayed message to (see Figure 3).
- **Preceding node:** This term relates to the direction of travel of a message being relayed by a WRS. The following node is the one which the WRS is transmitted the relayed message to (see Figure 3).

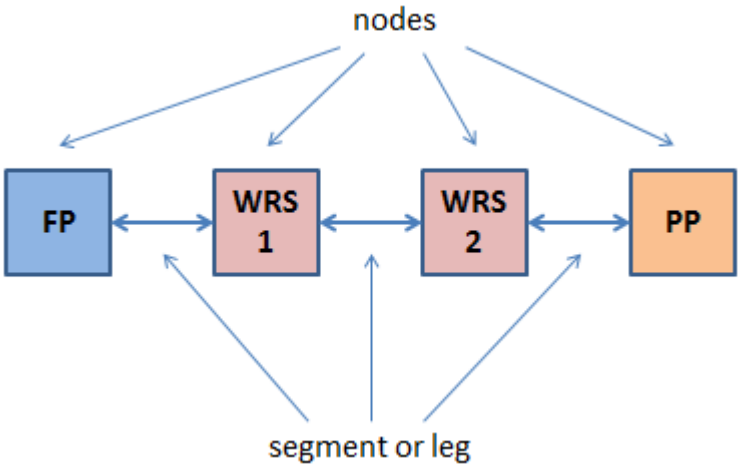

Figure 2: Components of repeater system

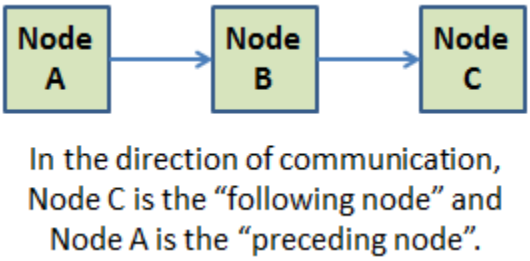

Figure 3: Following and preceding nodes

5 Service and feature definitions

5.1 System-level feature definitions

The following service definitions apply:

GAP/NG-DECT voice relay [WRS.SL.1]: Ability to provide relay of GAP/NG-DECT voice services addressed to any PP connected to the repeater.

NG-DECT 4 SUOTA relay [WRS.SL.2]: Ability to provide relay of the NG-DECT part 4 SUOTA service addressed to any PP connected to the repeater.

ULE C/O service relay [WRS.SL.3]: Ability to provide relay of ULE C/O services addressed to any PP connected to the repeater.

ULE C/L dummy bearer relay [WRS.4]: Ability to provide relay of the ULE C/L dummy bearer or bearers, and operation of such bearers in the WRSs.

ULE C/L multicast service relay [WRS.SL.5]: Ability to provide relay of ULE C/L multi-cast services addressed to any PP connected to the repeater.

5.2 PHL service definitions

For the purposes of the present document, all definitions of ETSI TS 102 527-3 [10], clause 5.5, ETSI TS 102 527-4 [11], clause 5.1.1, ETSI TS 102 939-2 [13], clause 5.1.1 and the following apply:

General PHL [WRS.P.1]: General Physical layer procedures applicable to all WRS systems.

Fast hopping radio [WRS.P.2]: Radio transceiver able to perform frequency change during the interval between two consecutive Physical Packets P32 (full slot).

Antenna diversity [WRS.P.3]: Physical layer procedures defining the operation of WRS devices with respect to antenna diversity.

Transmitted power [WRS.P.4]: Physical layer procedures defining the transmitted power applicable to all WRS devices.

5.3 MAC service definitions

For the purposes of the present document, all definitions of ETSI EN 300 444 [9], clause 5.2, ETSI TS 102 527-3 [10], clause 5.4, ETSI TS 102 527-4 [11], clause 5.1.2, ETSI TS 102 939-2 [13], clause 5.1.2 and the following apply:

General MAC [WRS.M.1]: General MAC layer procedures applicable to all WRS systems.

Logical channel mapping [WRS.M.2]: Rules defining how logical channels are mapped (between FT and PT) by the WRS.

CRFP connection-orientated procedures [WRS.M.3]: Various connection-orientated procedures defining the operation between the FT and WRS.

CRFP suspend/resume [WRS.M.4]: Procedures to allow switching between relay/local state of the MAC connection between FT and WRS.

Bearer handover [WRS.M.5]: Internal MAC process whereby data transfer (C channel and I channel) is switched from one duplex bearer to another in the domain of the same cell while maintaining the service to the DLC layer.

Relay of higher layer data [WRS.M.6]: Procedures defining how higher layer data (C channel and I channel) is relayed at the MAC layer between FT and PT via the WRS.

NG-DECT/DPRS I_P_error_detect relay [WRS.M.7]: Ability to provide relay of the I_P_error_detect service used in SUOTA and other DPRS services.

ULE Ip_error_correct relay [WRS.M.8]: Ability to provide relay of the Ip_error_correct service as used in ULE. The feature includes end-to-end integrity and flow control via the BCK bit.

C/O procedures for relay of ULE connections [WRS.M.9]: Ability to support the MAC C/O mode procedures required for the relay of ULE C/O communications.

ULE G_{FA} channel relay [WRS.M.10]: Ability to provide transparent relay of the G_{FA} channel used in ULE. This may include translation between different MAC messages.

ULE C/L dummy bearer relay and operation [WRS.M.11]: WRS-specific handling for the B-field component of the dummy bearer (or bearers) used by ULE systems.

C_S higher layer signalling [WRS.M.12]: Low rate connection-oriented data service with ARQ using the C_S channel to transfer higher layer signalling data. The feature includes both relay of the channel to other nodes and end-system termination when the WRS is in local mode.

C_F higher layer signalling [WRS.M.13]: High rate connection-oriented data service with ARQ using the C_F channel to transfer higher layer signalling data. The feature includes both relay of the channel to other nodes and end-system termination when the WRS is in local mode.

WRS local mode [WRS.M.14]: Special WRS mode, enabled by means of MAC signalling, that allows the exchange of higher layer signalling (C_S and C_F) and certain MAC signalling, directly between the FP and a WRS.

"No emission" mode [WRS.M.15]: WRS-specific handling for the NG-DECT "No emission" mode feature.

ULE C/L multicast procedures [WRS.M.16]: Procedures used in WRSs for relaying the ULE C/L downlink multicast service over the dummy or over other C/L bearers.

WRS security procedures [WRS.M.17]: Specific procedures for WRSs providing security features.

5.4 DLC service definitions

For the purposes of the present document, all definitions of ETSI EN 300 444 [9], clause 5.1, ETSI TS 102 527-3 [10], clause 5.3, ETSI TS 102 527-4 [11], clause 5.1.3, ETSI TS 102 939-2 [13], clause 5.1.3 and the following apply:

General DLC [WRS.D.1]: General DLC layer procedures applicable to all WRS systems.

Connection handover [WRS.D.2]: Internal handover process provided and initiated by the DLC layer (e.g. as a result of continued poor quality of service from the MAC layer), whereby one set of DLC entities (C-plane and U-plane) can re-route data from one MAC connection to a second new MAC connection while maintaining the service provided to the NWK layer.

Lc Frame delimiting and sequencing service [WRS.D.3]: Service providing channel dependant fragmentation, recombination, frame synchronization and frame delimiting transparency. Fragmentation is obtained by means of dividing a LAPC data unit into more than one service data units for delivery to the MAC layer C logical channel, whilst recombination is obtained by means of joining several service units received from the MAC layer C logical channel into a LAPC data unit.

5.5 NWK feature definitions

For the purposes of the present document, all definitions of ETSI EN 300 444 [9], clause 4.1, ETSI TS 102 527-3 [10], clause 5.2, ETSI TS 102 527-4 [11], clause 5.1.4, ETSI TS 102 939-2 [13], clause 5.1.4 and the following apply:

General NWK [WRS.N.1]: General NWK layer procedures applicable to all WRS systems.

Over-the-air maintenance [WRS.N.2]: Operation, Administration and Maintenance (OA&M) procedures to facilitate management of the WRS, including (but not limited to) setting of WRS's RPN and transfer of PP Cipher Keys.

WRS security procedures [WRS.N.3]: Specific procedures for WRSs providing security features.

5.6 Management Entity definitions

For the purposes of the present document, all definitions of ETSI TS 102 527-4 [11], clause 5.1.6, ETSI TS 102 939-2 [13], clause 5.1.6 and the following apply:

General ME [WRS.ME.1]: General ME layer procedures applicable to all WRS systems.

6 General requirements

6.1 General

The following tables define the status of all protocol elements (i.e. features, services, and procedures), which can be: mandatory, optional, conditional under the provision of another protocol element, outside the scope of the present document, or not applicable.

Elements defined as mandatory, optional or conditional in this clause are further defined in the referenced DECT specification, or, if needed, in clause 7 of the present document.

6.2 Specific conventions

6.2.1 Use of symbols in support status tables

The symbols defined in this clause are applied for procedures, features, and services in the present document if not explicitly otherwise stated. The interpretation of status columns in all tables is as follows:

C	conditional to support
I	out-of-scope
M	mandatory to support
N/A	not applicable
O	optional to support

6.3 System-level feature requirements

6.3.1 System-level features

A WRS supports the features described by table 1.

Table 1: System-level feature support

Item	Name of service	Reference	Status
WRS.SL.1	GAP/NG-DECT voice relay	5.1	M
WRS.SL.2	NG-DECT 4 SUOTA relay	5.1	M
WRS.SL.3	ULE C/O service relay	5.1	M
WRS.SL.4	ULE C/L dummy bearer relay	5.1	M
WRS.SL.5	ULE C/L multicast service relay	5.1	M
NOTE: The reference column refers to the relevant clause in the present document unless a specific reference document is noted.			

6.3.2 System-level feature to procedure mapping

The system-level feature to procedure mapping described by table 2 shall apply.

Table 2: System-level feature to procedure mapping

Feature	Procedure	Reference	Status
This table is intentionally left blank in order to facilitate future modification.			
NOTE: The reference column refers to the relevant clause in the present document unless a specific reference document is noted.			

6.4 PHL requirements

6.4.1 PHL services

A WRS supports the PHL services described by table 3.

As described in clause 4.2, the WRS contains both an FT component and a PT component at the PHL layer. The status column in table 3 relates to both FT and PT components.

Table 3: PHL service support

Item	Name of service	Reference	Status
NG1.P.1	2 level GFSK modulation	5.5 [10]	M
NG1.P.2	Physical packet P32	5.5 [10]	M
NG1.P.3	Physical packet P64	5.5 [10]	M
NG1.P.4	Physical packet P67	5.5 [10]	O
NG1.P.5	Physical packet P80	5.5 [10]	O
ULE1-P.3	Physical Packet P00	5.1.1 [13]	M
WRS.P.1	General PHL	5.2	M
WRS.P.2	Fast hopping radio	5.2	O
WRS.P.3	Antenna diversity	5.2	M
WRS.P.4	Transmitted Power	5.2	M
NOTE: The reference column refers to the relevant clause in the present document unless a specific reference document is noted.			

6.4.2 Modulation schemes

The modulation schemes described by table 4 and defined by ETSI EN 300 175-2 [2], Annex D shall be supported.

Table 4: Allowed combinations of modulation schemes

Modulation scheme	S-field	A-field	B + Z-field	Support status
1a	GFSK	GFSK	GFSK	M

6.4.3 PHL service to procedure mapping

The PHL service to procedure mapping described by table 5 shall apply.

In addition, those PHL services that are defined in clause 6.4.1 that do not have explicit procedure mapping described by table 5 below, shall have identical procedure mapping to that defined in their referenced documents.

As described in clause 4.2, the WRS contains both an FT component and a PT component at the PHL layer. The status column in the table below relates to both FT and PT components.

Table 5: MAC layer service to procedure mapping

Service	Procedure	Reference	Status
WRS.P.1 General PHL		5.2	M
	General	7.3.1	M
	Timing	7.3.2	M
	Z-field mapping	7.3.3	M
	Sliding collision detection	7.3.6	M
	Synchronization window	7.3.7	M
WRS.P.2 Fast hopping radio		5.2	O
	Fast hopping radio	7.3.4	M
WRS.P.3 Antenna diversity		5.2	M
	Antenna diversity	7.3.5	M
WRS.P.4 Transmitted power		5.2	M
	Minimum Normal Transmit Power (NTP)	7.3.8	M
	Transmitted power management	7.3.9	O
NOTE: The reference column refers to the relevant clause in the present document unless a specific reference document is noted.			

6.5 MAC layer requirements

6.5.1 MAC layer services

A WRS supports the MAC layer services described by table 6.

As described in clause 4.2, the WRS contains both an FT component and a PT component at the MAC layer. The status column in table 6 relates to both FT and PT components.

Table 6: MAC layer service support

Item	Name of service	Reference	Status
NG1.M.1	$I_{N_}$minimum delay symmetric MAC service type	5.4 [10]	M
NG1.M.2	$I_{N_}$normal delay symmetric MAC service type	5.4 [10]	O
NG1.M.3	$I_{PQ_}$error_detection symmetric MAC service type	5.4 [10]	O
NG1.M.4	Advanced connections	5.4 [10]	M
GAP.M.1	General	5.2 [9]	M
GAP.M.2	Continuous broadcast	5.2 [9]	M
GAP.M.3	Paging broadcast	5.2 [9]	M
GAP.M.4	Basic connections	5.2 [9]	M
GAP.M.6	Quality control	5.2 [9]	M
GAP.M.7	Encryption activation	5.2 [9]	M
GAP.M.8	Extended frequency allocation	5.2 [9]	M
GAP.M.9	Bearer Handover, intra-cell	5.2 [9]	M
GAP.M.10	Bearer Handover, inter-cell	5.2 [9]	M
GAP.M.11	Connection Handover, intra-cell	5.2 [9]	M
GAP.M.12	Connection Handover, inter-cell	5.2 [9]	M
GAP.M.13	SARI support	5.2 [9]	M
GAP.M.14	Encryption deactivation	5.2 [9]	O
GAP.M.15	Re-keying	5.2 [9]	M
GAP.M.16	Early encryption	5.2 [9]	M
GAP.M.17	AES/DSC2 encryption	5.2 [9]	O
DPRS-M.6	$I_{PM_}$error_detection	5.1.2 [11]	M
DPRS-M.16	DPRS Bearer handover	5.1.2 [11]	M
DPRS-M.24	Full slot	5.1.2 [11]	O
DPRS-M.25	Long slot 640	5.1.2 [11]	M
DPRS-M.26	Long slot 672	5.1.2 [11]	O
DPRS-M.27	Double slot	5.1.2 [11]	O
DPRS-M.30	Simplified A-field advanced connection control	5.1.2 [11]	M
ULE1-M.1	General	5.1.2 [13]	M
ULE1-M.4	B-field Continuous ULE broadcast	5.1.2 [13]	M
ULE1-M.5	B-field paging broadcast	5.1.2 [13]	M
ULE1-M.8	Expedited operations (advanced connection control)	5.1.2 [13]	M
ULE1-M.9	Full slot	5.1.2 [13]	M
ULE1-M.10	Short slot	5.1.2 [13]	M
ULE1-M.11	$I_{PQR_}$error_correction MAC service type	5.1.2 [13]	M
ULE1-M.12	G_{FA} channel	5.1.2 [13]	M
ULE1-M.16	ULE Physical channel selection	5.1.2 [13]	M
ULE1-M.18	ULE Bearer replacement (intra-cell)	5.1.2 [13]	M
ULE1-M.19	Dummy Bearer replacement	5.1.2 [13]	M
ULE1-M.28	U-plane C/L downlink multicast service	5.1.2 [13]	M
ULE1-M.29	Quiet Channel Indication	5.1.2 [13]	C601
ULE1-M.30	PHS Detection Indication	5.1.2 [13]	C602
ULE1-M.32	Long slot (j = 640)	5.1.2 [13]	M
ULE1-M.36	ULE Bearer replacement (inter-cell)	5.1.2 [13]	M
ULE1-M.37	C/O procedures for FT connections with CRFP	5.1.2 [13]	M
ULE1-M.38	Repeater compatibility	5.1.2 [13]	M
WRS.M.1	General MAC	5.3	M
WRS.M.2	Logical channel mapping	5.3	M
WRS.M.3	CRFP connection-orientated procedures	5.3	M
WRS.M.4	CRFP suspend/resume	5.3	M

Item	Name of service	Reference	Status
WRS.M.5	Bearer handover	5.3	M
WRS.M.6	Relay of higher layer data	5.2	M
WRS.M.7	NG-DECT/DPRS I_P_error_detect relay	5.3	M
WRS.M.8	ULE Ip_error_correct relay	5.3	M
WRS.M.9	C/O procedures for relay of ULE connections	5.3	M
WRS.M.10	ULE G_{FA} channel relay	5.3	M
WRS.M.11	ULE C/L dummy bearer relay and operation	5.3	M
WRS.M.12	C_S higher layer signalling	5.3	M
WRS.M.13	C_F higher layer signalling	5.3	M
WRS.M.14	WRS local mode	5.3	M
WRS.M.15	"no emission" mode operation	5.3	M
WRS.M.16	ULE C/L multicast procedures	5.3	M
WRS.M.17	WRS security procedures	5.3	M
C601: IF ULE1-ME.3 THEN "M" ELSE "I". (Note: support for US operation). C602: IF ULE1-ME.4 THEN "M" ELSE "I". (Note: support for Japan operation).			
NOTE: The reference column refers to the relevant clause in the present document unless a specific reference document is noted.			

6.5.2 MAC service to procedure mapping

The MAC layer service to procedure mapping described by table 7 shall apply.

In addition, those MAC layer services that are defined in clause 6.5.1 that do not have explicit procedure mapping described by table 7 below, shall have identical procedure mapping to that defined in their referenced documents.

As described in clause 4.2, the WRS contains both an FT component and a PT component at the MAC layer. The status column in table 7 relates to both FT and PT components.

Table 7: MAC layer service to procedure mapping

Service	Procedure	Reference	Status
GAP.M.15 Re-keying		5.2 [9]	M
	Re-keying	7.7.5.1	M
GAP.M.16 Early encryption		5.2 [9]	M
	Early encryption	7.7.5.2	M
WRS.M.1 General MAC		5.3	M
	General	7.4.1	M
	Physical channel selection	7.4.2	M
	Maximum allowed system load	7.4.3	M
	Fixed part capabilities	7.4.4	M
	Hop control	7.4.5	M
	Frame multiplexing structure	7.4.6	M
	Quality Control and Flow Control	7.4.8	M
	MAC layer control messages	7.4.9	M
	Downlink broadcast	7.4.20	M
	Higher layer information FP broadcast	7.6.7	M
	A-field paging broadcast	7.4.21	M
WRS.M.2 Logical channel mapping		5.3	M
	General	7.4.7	M
	I_N_minimum_delay	7.4.7	M
	I_N_normal_delay	7.4.7	M
	I_P_error_detect	7.4.7	M
	I_P_error_correct	7.4.7	M
	C_S	7.4.7	M
	C_F	7.4.7	M
	G_{FA} channel	7.4.7	M

Service	Procedure	Reference	Status
WRS.M.3 CRFP connection orientated procedures		5.3	M
	General	7.4.10.1	M
	Creation of a Relay Multi Bearer Control (RMBC)	7.4.10.2	M
	Normal C/O bearer setup (Basic)	7.4.10.3	M
	Normal C/O bearer setup (Advanced)	7.4.10.4	M
	Dual C/O bearer setup (Basic)	7.4.10.5	M
	Dual C/O bearer setup (Advanced)	7.4.10.6	M
	C/O connection release	7.4.10.7	M
	C/O abnormal connection release	7.4.10.8	M
WRS.M.4 CRFP suspend/resume		5.3	M
	CRFP suspend and resume	7.4.11	M
WRS.M.5 Bearer handover		5.3	M
	Bearer handover	7.4.12	M
WRS.M.6 Relay of higher layer data		5.3	M
	Relay of higher layer data	7.4.13	M
WRS.M.7 NG-DECT/DPRS I_P_error_detect relay		5.3	M
	Transparent relay of I_P_error_detect service	7.4.16.1	M
	Detection and setting of the I_P_error_detect service	7.4.16.2	M
	Service change to/from I_P_error_detect service	7.4.16.3	O
	BA codes supported	7.4.16.4	M
	Handling of error cases in I_P_error_detect service	7.4.16.5	M
WRS.M.8 ULE I_P_error_correct relay		5.3	M
	Relay of I_P packets	7.4.15.1	M
	Setting the Q2 bit	7.4.15.2	M
	Use of BCK bit for flow control	7.4.15.3	M
WRS.M.9 C/O procedures for relay of ULE connections		5.3	M
	Repeater upper segment channel selection	7.4.15.4	M
	Relay of MAC expedited messages	7.4.15.5	M
	Conversion of single-burst access to multi-burst setup	7.4.15.6	M
	Use of "Wait" message	7.4.15.7	M
	C/O scenarios mandatory sequences	7.4.15.8	M
	Handling of ULE bearer replacement (inter-cell)	7.4.15.10	M
WRS.M.10 ULE G_{FA} channel relay		5.3	M
	G_{FA} channel relay	7.4.15.9	M
WRS.M.11 ULE C/L dummy bearer relay and operation		5.3	M
	ULE Dummy bearer operation: general	7.4.19.1	M
	ULE Dummy bearer generation: subfield B0 fields and NC channel	7.4.19.2	M
	ULE Dummy bearer generation: paging channel PU and paging related fields: HN, CA, SFa, SFb	7.4.19.3	M
	ULE Dummy bearer generation; subfield B2 fields: channels QU and MU	7.4.19.4	M
	B-field paging addressed to a WRS	7.4.19.5	M
WRS.M.12 C_S higher layer signalling		5.3	M
	General	7.4.18.1.1	M
	C_S channel transparent relay	7.4.18.1.2	M
	C_S channel end-system operation	7.4.18.1.3	M
	C_S channel retransmission and flow control	7.4.18.1.4	M

Service	Procedure	Reference	Status
WRS.M.13 C_F higher layer signalling		5.3	M
	General	7.4.18.2.1	M
	B-field control Multiplexer (E/U-MUX), C_F modes	7.4.18.2.2	M
	C_F channel transparent relay	7.4.18.2.3	M
	C_F channel end-system operation	7.4.18.2.4	M
	C_F channel relay service activation	7.4.18.2.5	M
	C_F channel retransmission and flow control	7.4.18.2.6	M
	C_F channel end-system specific WRS procedures: activation	7.4.18.2.7	M
	C_F channel end-system specific WRS procedures: single LAPC instance and coordination with C_S channel	7.4.18.2.8	M
WRS.M.14 WRS local mode		5.3	M
	General and managing rules	7.4.17.1	M
	Switching to local mode	7.4.17.2	M
	Switching to full-relayed mode	7.4.17.3	M
	Switching between local modes	7.4.17.4	M
	Switching point and error handling	7.4.17.5	M
	Higher layer signalling handling	7.4.17.6	M
	Effects of the local mode	7.4.17.7	M
WRS.M.15 "No emission" mode		5.3	M
	"No emission" mode operation	7.4.14	M
WRS.M.16 ULE C/L multicast procedures		5.3	M
	C/L multicast procedures: general	7.4.19.6	M
	C/L multicast procedures: multicast channel over the dummy bearer	7.4.19.7	M
	C/L multicast procedures: multicast channel over additional C/L bearers	7.4.19.8	O
WRS.M.17 WRS security procedures		5.3	M
	General	7.7.1	M
	Relay of START.GRANT message	7.7.7	M
NOTE: The reference column refers to the relevant clause in the present document unless a specific reference document is noted.			

6.6 DLC layer requirements

6.6.1 DLC layer services

A WRS supports the DLC layer services described by table 8.

As described in clause 4.2, the WRS contains both an FT component and a PT component at the lower layers. However, in the higher layers, including the DLC, only the PT component is present.

Table 8: DLC layer service support

Item	Name of service	Reference	Status
GAP.D.1	LAPC class A service and Lc	5.1 [9]	M
GAP.D.3	Broadcast Lb service	5.1 [9]	M
GAP.D.4	Intra-cell voluntary connection handover	5.1 [9]	M
GAP.D.5	Inter-cell voluntary connection handover	5.1 [9]	M
GAP.D.6	Encryption activation	5.1 [9]	M
GAP.D.9	Encryption deactivation	5.1 [9]	O
WRS.D.1	General DLC	5.4	M
WRS.D.2	Connection handover	5.4	O
WRS.D.3	Lc Frame delimiting and sequencing service	5.4	M
NOTE: The reference column refers to the relevant clause in the present document unless a specific reference document is noted.			

6.6.2 DLC service to procedure mapping

The DLC layer service to procedure mapping described by table 9 shall apply.

In addition, those DLC layer services that are defined in clause 6.6.1 that do not have explicit procedure mapping described by table 9, shall have identical procedure mapping to that defined in their referenced documents.

As described in clause 4.2, the WRS contains both an FT component and a PT component at the lower layers. However, in the higher layers, including the DLC, only the PT component is present.

Table 9: DLC layer service to procedure mapping

Service	Procedure	Reference	Status
GAP.D.1 LAPC class A service and Lc		5.1 [9]	M
	Class A link establishment	7.5.5	M
	Class A acknowledged informationtransfer	9.2 [9]	M
	Class A link release	9.3 [9]	M
	Class A link re-establishment	9.4 [9]	M
WRS.D.1 General DLC		5.4	M
	General	7.5.1	M
	DLC variables	7.5.2	M
WRS.D.2 Connection handover		5.4	O
	Connection handover	7.5.3	M
WRS.D.3 Lc Frame delimiting and sequencing service		5.4	M
	General	7.5.4.1	M
	C_S channel fragmentation and recombination	7.5.4.2	M
	C_F channel fragmentation and recombination	7.5.4.3	M
	Selection of logical channels (C_S and C_F)	7.5.4.4	M
NOTE: The reference column refers to the relevant clause in the present document unless a specific reference document is noted.			

6.7 NWK layer requirements

6.7.1 NWK features

A WRS supports the NWK layer features described by table 10.

As described in clause 4.2, the WRS contains both an FT component and a PT component at the lower layers. However, in the higher layers, including the NWK, only the PT component is present.

Table 10: NWK layer feature support

Item	Name of feature	Reference	Status
GAP.N.9	Authentication of PP	4.1 [9]	M
GAP.N.11	Location registration	4.1 [9]	M
GAP.N.12	On air key allocation	4.1 [9]	M
GAP.N.13	Identification of PP	4.1 [9]	M
GAP.N.14	Service class indication/assignment	4.1 [9]	M
GAP.N.16	ZAP	4.1 [9]	M
GAP.N.17	Encryption activation FT initiated	4.1 [9]	M
GAP.N.18	Subscription registration procedure on-air	4.1 [9]	M
GAP.N.19	Link control	4.1 [9]	M
GAP.N.20	Terminate access rights FT initiate	4.1 [9]	M
GAP.N.26	Authentication of FT	4.1 [9]	O
GAP.N.27	Encryption activation PT initiated	4.1 [9]	O
GAP.N.28	Encryption deactivation FT initiated	4.1 [9]	O
GAP.N.19	Encryption deactivation PT initiated	4.1 [9]	O
GAP.N.35	Enhanced security	4.1 [9]	M
GAP.N.36	AES/DSAA2 authentication	4.1 [9]	M

Item	Name of feature	Reference	Status
WRS.N.1	General NWK	5.5	M
WRS.N.2	Over-the-air maintenance	5.5	M
WRS.N.3	WRS security procedures	5.5	M
NOTE: The reference column refers to the relevant clause in the present document unless a specific reference document is noted.			

6.7.2 NWK features to procedures mapping

The NWK layer feature to procedure mapping described by table 11 shall apply.

In addition, those NWK layer features that are defined in clause 6.7.1 that do not have explicit procedure mapping described by table 11 below, shall have identical procedure mapping to that defined in their referenced documents.

As described in clause 4.2, the WRS contains both an FT component and a PT component at the lower layers. However, in the higher layers, including the NWK, only the PT component is present.

Table 11: NWK layer feature to procedure mapping

Feature	Procedure	Reference	Status
GAP.N.35 Enhanced security		4.1 [9]	M
	Encryption of all calls	8.45.1 [9]	N/A
	Re-keying during a call	7.7.5.1	M
	Early encryption	7.7.5.2	M
	Subscription requirements	8.45.4 [9]	N/A
	Behaviour against legacy devices	8.45.5 [9]	N/A
WRS.N.1 General NWK		5.5	M
	General	7.6.1	M
	Identities and addressing	7.6.3	M
	Subscription data	7.6.4	M
	Obtaining access rights for WRS	7.6.5	M
	Location registration for WRS	7.6.6	M
WRS.N.2 Over-the-air maintenance		5.5	M
	General	7.6.2.1	M
	Retrieval of WRS RPN	7.6.2.2	M
	Indication/Modification of WRS RPN	7.6.2.3	M
WRS.N.3 WRS security procedures		5.5	M
	General	7.7.1	M
	CRFP initialization of PT cipher key	7.7.2	M
	Management for encryption of relayed connections	7.7.3	M
	Indication of cipher key	7.7.4	M
	DSC2 operation	7.7.6	C1101
C1101: IF GAP.M.17 then M else N/A.			
NOTE: The reference column refers to the relevant clause in the present document unless a specific reference document is noted.			

6.8 Management Entity requirements

6.8.1 Management Entity services

A WRS supports the Management Entity (ME) services described by table 12.

Table 12: ME service support

Item	Name of service	Reference	Status
ULE1-ME.1	ULE phase 1 Management	5.1.6 [13]	M
ULE1-ME.2	ULE Physical Channel Selection	5.1.6 [13]	M
ULE1-ME.3	ULE Physical Channel Selection for US region	5.1.6 [13]	O
ULE1-ME.4	ULE Physical Channel Selection for Japan region	5.1.6 [13]	O
WRS.ME.1	General ME	5.6	M
NOTE: The reference column refers to the relevant clause in the present document unless a specific reference document is noted.			

6.8.2 Management Entity service to procedures mapping

The Management Entity (ME) service to procedure mapping described by table 13 shall apply.

Table 13: ME layer service to procedure mapping

Service	Procedure	Reference	Status
WRS.ME.1 General ME		5.6	M
	CRFP initialization	7.8.1	M
	CRFP MAC modes	7.8.2	M
	CRFP state transitions	7.8.3	M
NOTE: The reference column refers to the relevant clause in the present document unless a specific reference document is noted.			

7 Procedures description

7.1 General

Clause 7 defines various procedures for the WRS. Some of these procedures also form part of the interworking requirements for a Fixed Part, and these are referenced from tables and clauses in Annex A.

7.2 System-level procedures

This clause is intentionally left blank in order to facilitate future modification.

7.3 PHL procedures

7.3.1 General

The WRS shall incorporate PT and FT PHL functions as defined in ETSI EN 300 175-2 [2].

7.3.2 Timing

For the supported packet types, the WRS shall meet the PP requirements in ETSI EN 300 175-2 [2] when it is acting as a PP, and meet the RFP requirements in ETSI EN 300 175-2 [2] when it is acting as an RFP, except that the timing requirements in ETSI EN 300 175-2 [2], clause 4.2.4 shall be met by all WRS transmissions and that the requirement in ETSI EN 300 175-2 [2], clause 4.2.5 on difference between reference timers shall be disregarded.

7.3.3 Z-field mapping

The Z-field mapping as defined in ETSI EN 300 175-2 [2], clause 4.8 shall be supported.

7.3.4 Fast hopping radio

The radio transceiver shall be able to perform any frequency change during the interval between two consecutive Physical Packets P32 (full slot).

7.3.5 Antenna diversity

7.3.5.1 General

A WRS shall provide at least two antennas.

7.3.5.2 Antenna diversity at CRFP_PT

With respect to the FT's "prolonged preamble" capability and the CRFP_PT's own capability the requirements defined in table 14 shall apply.

Table 14: Antenna diversity at CRFP_PT

FT "prolonged preamble"	CRFP_PT "prolonged preamble"	Action
No	Yes/No	CRFP_PT shall transmit on one preferred antenna FT will perform antenna diversity according to ETSI EN 300 444 [9], clause 10.11, for both uplink and downlink.
Yes	No	CRFP_PT may perform fast antenna selection base on prolonged preamble according to ETSI EN 300 175-3 [3], clause 7.2.5.5.1.2. CRFP_PT shall transmit on one preferred antenna. FT will perform antenna diversity according to ETSI EN 300 444 [9], clause 10.11 for both uplink and downlink.
Yes	Yes	CRFP_PT may perform fast antenna selection based on prolonged preamble according to ETSI EN 300 175-3 [3], clause 7.2.5.5.1.2. FT will perform fast antenna selection based on prolonged preamble according to ETSI EN 300 175-3 [3], clause 7.2.5.5.1.1.

7.3.5.3 Antenna diversity at CRFP_FT

With respect to the PT's "prolonged preamble" capability and the CRFP_FT's own capability the requirements defined in table 15 shall apply.

Table 15: Antenna diversity at CRFP_FT

CRFP_FT "prolonged preamble"	PT "prolonged preamble"	Action
No	Yes/No	PT will transmit on one preferred antenna CRFP_FT shall perform antenna diversity according to ETSI EN 300 444 [9], clause 10.11, for both uplink and downlink.
Yes	No	PT may perform fast antenna selection base on prolonged preamble according to ETSI EN 300 175-3 [3], clause 7.2.5.5.1.2. PT will transmit on one preferred antenna. CRFP_FT shall perform antenna diversity according to ETSI EN 300 444 [9], clause 10.11 for both uplink and downlink.
Yes	Yes	PT may perform fast antenna selection based on prolonged preamble according to ETSI EN 300 175-3 [3], clause 7.2.5.5.1.2. CRFP_FT shall perform fast antenna selection based on prolonged preamble according to ETSI EN 300 175-3 [3], clause 7.2.5.5.1.1.

7.3.6 Sliding collision detection

The WRS shall be able to detect sliding collision on received packets.

Minimum criteria for sliding collision are defined as S-field or Z-field failure. Early sliding collision detection may also be supported by other means e.g. signal strength measurements in the guard band.

The Z-field is defined to have failed if the received X-field and Z-fields are not identical.

S-field failure is defined with some tolerance in order not to restrict the physical implementation of the word synchronization detector. S-field failure may be indicated if there are 1 or more bit errors in bits s12 to s31 (errors in bits s0 to s11 shall be ignored). In all cases, S-field failure shall be indicated if 3 or more bit errors occur in bits s16 to s31.

When protected B-field format is used, B field CRC criteria may also be used for detecting sliding collisions.

7.3.7 Synchronization Window

Related to its reference timer, the CRFP_PT synchronization window shall be at least ±4 bits for bearers to the FT to which the reference timer is synchronized. The difference between reference timer of the CRFP_FT and the reference timer of FT shall be less than 4 µs.

NOTE: The FT could be the CRFP_FT of another WRS.

7.3.8 Minimal Normal Transmit Power

The nominal NTP shall be greater than 80 mW per simultaneously active transmitter as shown by the test verdict criteria and declaration of ETSI EN 300 176-1 [14], clause 10.2.3.

7.3.9 Transmitted Power Management

To fight mutual interference between data terminals operating in different local DECT networks when using for the transmission most of the slots from a frame, control of the transmission power is recommended.

If transmission power control procedure is implemented, the requirements in ETSI EN 300 175-2 [2], Annex E shall fully apply.

7.4 MAC procedures

7.4.1 General

The WRS incorporates PT and FT MAC functions as defined in ETSI EN 300 175-3 [3].

7.4.2 Physical channel selection

The WRS shall fulfil the mandatory requirements of ETSI EN 300 175-3 [3], clause 11.4, with the modifications as defined in the present document.

7.4.3 Maximum allowed system load

The WRS shall fulfil the mandatory requirements of ETSI EN 300 175-3 [3], clause 11.6, with the modifications as defined in the present document.

7.4.4 Fixed part capabilities

7.4.4.1 General

The WRS shall relay the fixed part capability messages that it receives from the RFP. The MAC standard defines 3 such messages: Fixed Part Capabilities, Extended Fixed Part Capabilities, and Extended Fixed Part Capabilities (Part 2).

The WRS shall relay these Q_T messages at least once every 8 multi-frames. See ETSI EN 300 175-3 [3], clause 7.2.3.1.

These Q_T messages consist of PHL and MAC layer capabilities and some Higher Layer Information.

The WRS shall assume the capability bits pertaining to a particular message as being set to '0' when the FT does not transmit that message. The WRS does not have to relay a capability message that is not being transmitted by the RFP.

The WRS shall understand the received PHL and MAC layer capabilities bits. These shall be relayed on its own dummy bearer(s). However, some bits may be modified according to the following rules:

- The relayed capability message shall not indicate support of any feature that is not supported by the WRS itself, i.e. the transmitted message shall indicate "no support" for such a feature.
- The relayed capability message shall not indicate support of any feature that is not supported by the RFP to which the WRS is attached, i.e. if the received message indicates "no support" for a particular feature, then the transmitted message shall also indicate "no support" (even if the WRS itself was capable of supporting it).

Exceptions or additions to the above rules are defined in the following clauses which provide more information on the individual capability messages.

The Higher Layer Information component of these messages shall be handled as defined in clause 7.6.7.

7.4.4.2 Fixed Part Capabilities

The definitions of ETSI EN 300 175-3 [3], clause 7.2.3.4 apply.

7.4.4.3 Extended Fixed Part Capabilities

The definitions of ETSI EN 300 175-3 [3], clause 7.2.3.5 apply.

The FP can control the hop configuration and indicate the permitted WRS scenarios by means of the CRFP Hops field in the Extended Fixed Part capabilities message (bits a12-a14). This field is not broadcast transparently, but is modified to reduce the number of permitted hops for each subsequent hop, see ETSI EN 300 175-3 [3], clause 7.2.3.5.2.1.

NOTE: The present document underwent a major overhaul for revision 2.1.1, including the definition and modification of several features. In order to address compatibility and interoperability issues and to distinguish between support of "V1" repeaters (i.e. before revision 2.1.1) and "V2" repeaters (i.e. revision 2.1.1 or later), a capability bit was introduced into the FP's Extended Fixed Part Capabilities broadcast message.

If the WRS receives the pattern '001'B in bits a15-a17 of the Extended Fixed Part capabilities message, this shall be understood to mean that the FP supports "V2" WRSs.

If the WRS receives the pattern '000'B in bits a15-a17, this shall be understood to mean that the FP does not support "V1" WRSs.

Whatever the received value of bits a15-a17, they shall be relayed directly in the WRS's own downlink broadcast.

7.4.4.4 Extended Fixed Part Capabilities (Part 2)

The definitions of ETSI EN 300 175-3 [3], clause 7.2.3.11 apply.

The WRS does not support "no emissions" mode. Therefore, the WRS shall always use bit $a_{23} = 0$ for the "Extended Fixed Part Capabilities (Part 2)" message (see ETSI EN 300 175-3 [3], clause 7.2.3.11.2) on its own downlink broadcast. See clause 7.4.16.

7.4.5 Hop control

A WRS that is locked to an FT (including the FT component of another WRS) shall decrease its received value of CRFP Hops (when > 0) see ETSI EN 300 175-3 [3], clause 7.2.3.5.2.1, when sending its own Extended Fixed Part Capabilities broadcast (see clause 7.4.4.3).

7.4.6 Frame multiplexing structure

Figure 4 shows the typical frame multiplexing structure for a CRFP that supports full slots with I_N_minimum_delay.

NOTE: The use of I_N_minimum_delay and full-slots shown in this example is for descriptive purposes, and is not intended to restrict the use of other slot types or services.

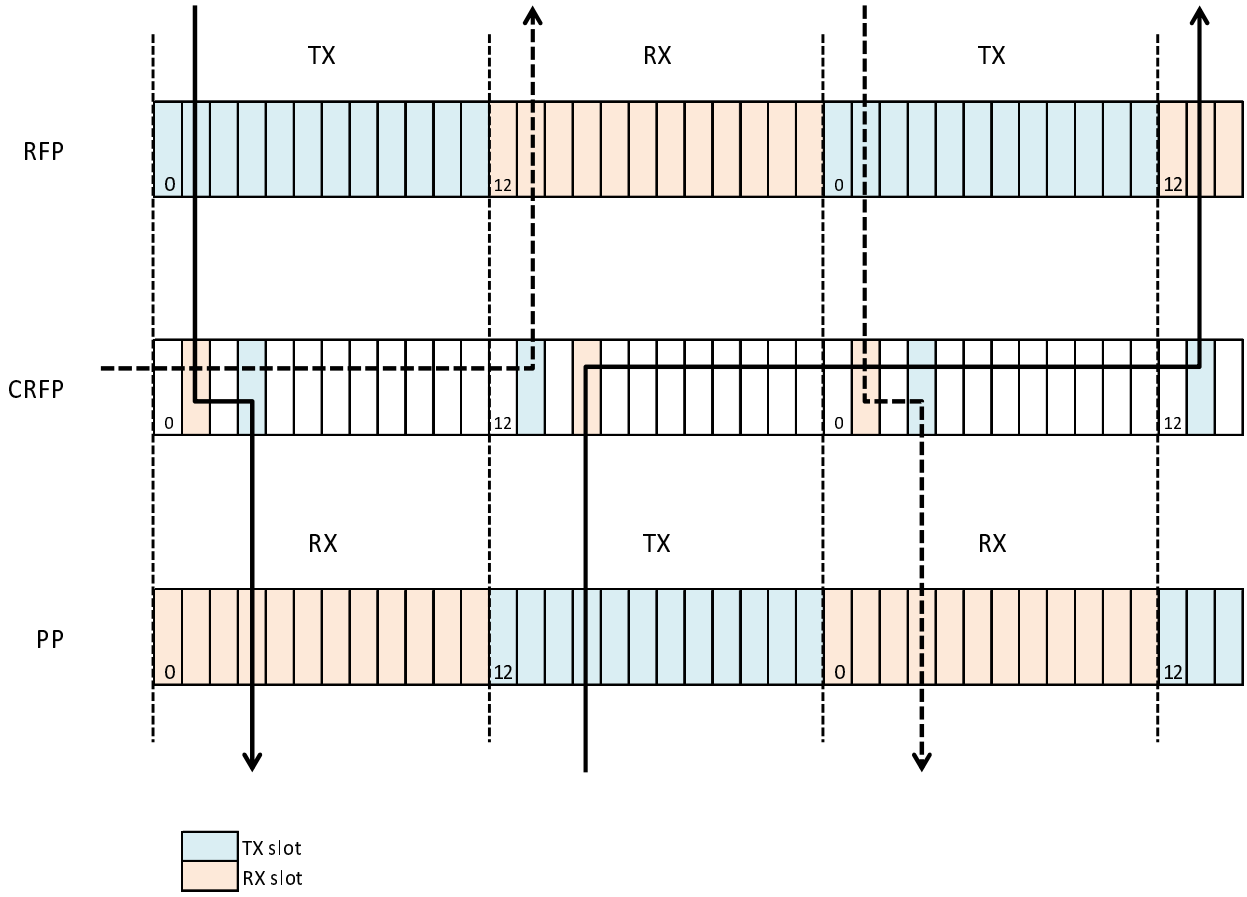

Figure 4: Typical frame multiplexing structure of the CRFP

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 ETSI 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 ETSI 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.

7.4.7 Logical channel mapping

The CRFP_PT and CRFP_FT shall fulfil the multiplexing rules as defined in ETSI 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. The data shall be delivered to the DLC layer as a MAC_PAGE-ind primitive via the MA-SAP (see note 4).

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. C-plane data requires special handling depending on the CRFP state (depending on relayed or local state), see clause 7.4.10.1 (also clauses 7.4.17.7.2 and 7.4.17.7.3).

NOTE 1: Some channels require special handling depending on relayed or local state, see clause 7.14.17.7 for more details.

NOTE 2: For the handling of ULE data (including G_{FA} channel) see clause 7.4.15.1 (and related clauses).

NOTE 3: For the handling of the I_P_error_detect service data see clause 7.4.16.

NOTE 4: Page messages directed towards the WRS itself are handled by the higher layers, and can result in the establishment of a link (by indirect link establishment procedures). This may be required for various WRS maintenance procedures.

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 clause 6.2.2 of ETSI EN 300 175-3 [3]. I_N_minimum_delay information, like speech, shall be relayed in the same or next frame, depending upon bearer position.

NOTE: ETSI EN 300 175-3 [3], Annex F describes additional rules for processing I_N_minimum_delay, in order to achieve "seamless handover" operation. These rules prescribe a slot-specific offset to take into account the behaviour of the minimum delay data. However, this rule is not applicable to frame-based codecs, such as G.729.1. In general, the WRS cannot know the codec currently in-use, although non-frame-based codecs, G.726, G.722 and G.711 are the most common. The decision to use (or not) the additional rules described in Annex F is optional, and left to the implementer.

7.4.8 Quality Control and Flow Control

7.4.8.1 General

The CRFP shall have separate quality control and flow control on each of the two links relating to a single relayed connection.

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 ETSI EN 300 175-3 [3] shall be followed for each link independently.

7.4.8.2 I_N data handling

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

NOTE: The use of B-field identification '001'B code is not mandated by GAP/NG-DECT profiles. As such, many handsets will not understand it, and might possibly ignore the code. This could lead to the corrupt audio being output by the handset (since the relayed data will have its X-CRC is corrected). In this case, the use of mitigation strategies such as filling the B-field with "mute" pattern data could be employed. However, the use of such mitigation strategies is not standardized, and is left to the implementer.

7.4.8.3 I_P data handling

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

7.4.9 MAC layer control messages

The CRFP uses the messages indicated with "**" in ETSI EN 300 175-3 [3], clauses 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.

7.4.10 CRFP Connection-oriented mode procedures

7.4.10.1 General

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 non-local 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.

7.4.10.2 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 ETSI EN 300 175-3 [3], clause 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 (see clause 7.8.2).

7.4.10.3 Normal C/O bearer setup (Basic)

When using the normal bearer setup the FT cannot recognize that the bearer setup is arriving from a CRFP, the CRFP_PT operates as a PT. The resulting 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 5 shows the message sequence diagram for basic setup.

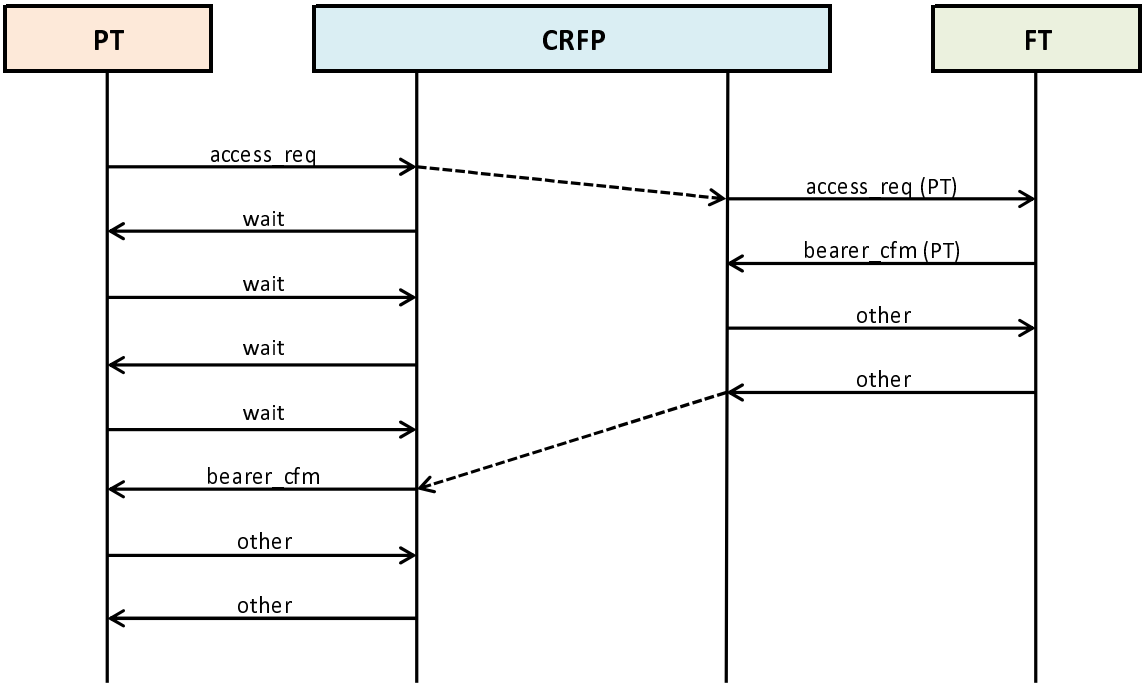

Figure 5: Normal bearer basic setup

At the CRFP:

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 meantime 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.

NOTE: Normal bearer setup procedures do not allow the use of the DECT security procedures, and so this procedure is only normally used with older FPs that do not support encryption.

7.4.10.4 Normal C/O bearer setup (Advanced)

The process of normal bearer setup for advanced connections is very similar to the basic connection (see clause 7.4.10.3), except for the use of the equivalent advanced connection control set of messages, and the requirement to exchange the ATTRIBUTES_T request/confirm messages in accordance with ETSI EN 300 175-3 [3], clause 10.5.1.2.

Figure 6 is a typical message sequence for normal bearer setup using advanced connections. The exact sequence and timing of message may vary due to implementation differences and the time-slots used. However, the following points are emphasized:

- WAIT messages may be required at various stages in the sequence, including between the ACCESS-REQ and ATTRIBUTES_T-REQ , between the ATTRIBUTES_T-REQ and ATTRIBUTES_T-CFM messages and between the ATTRIBUTES_T-CFM and the "other" messages.

- The trigger for sending the ATTRIBUTES_T-CFM to the PT is the receipt of the 2nd "other" message from the FT. This ensures that the bearer between the CRFP and the FT is established before completing the process with the PT.

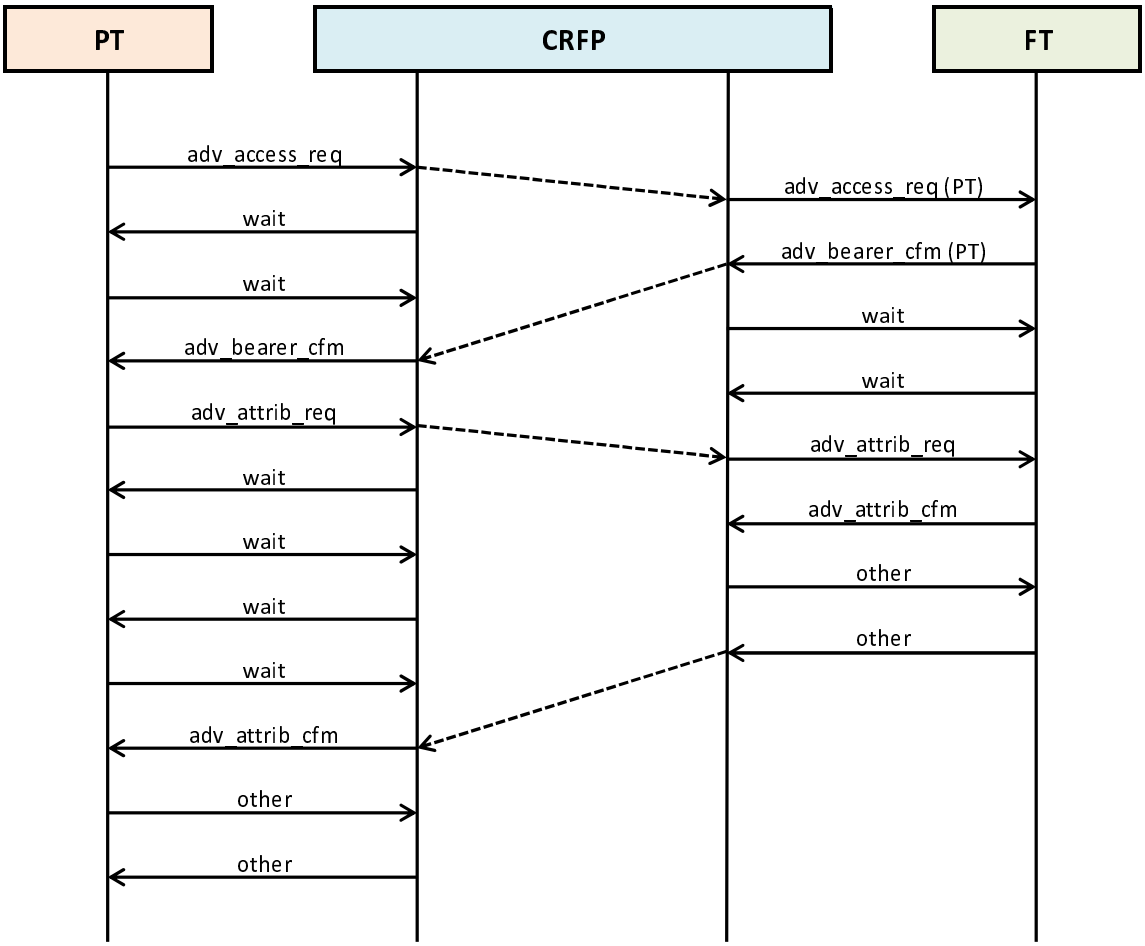

Figure 6: Normal bearer advanced setup

NOTE: Normal bearer setup procedures do not allow the use of the DECT security procedures, and so this procedure is only normally used with older FPs that do not support encryption.

7.4.10.5 Dual C/O bearer setup (Basic)

When 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 7 shows the message sequence diagram for basic connections.

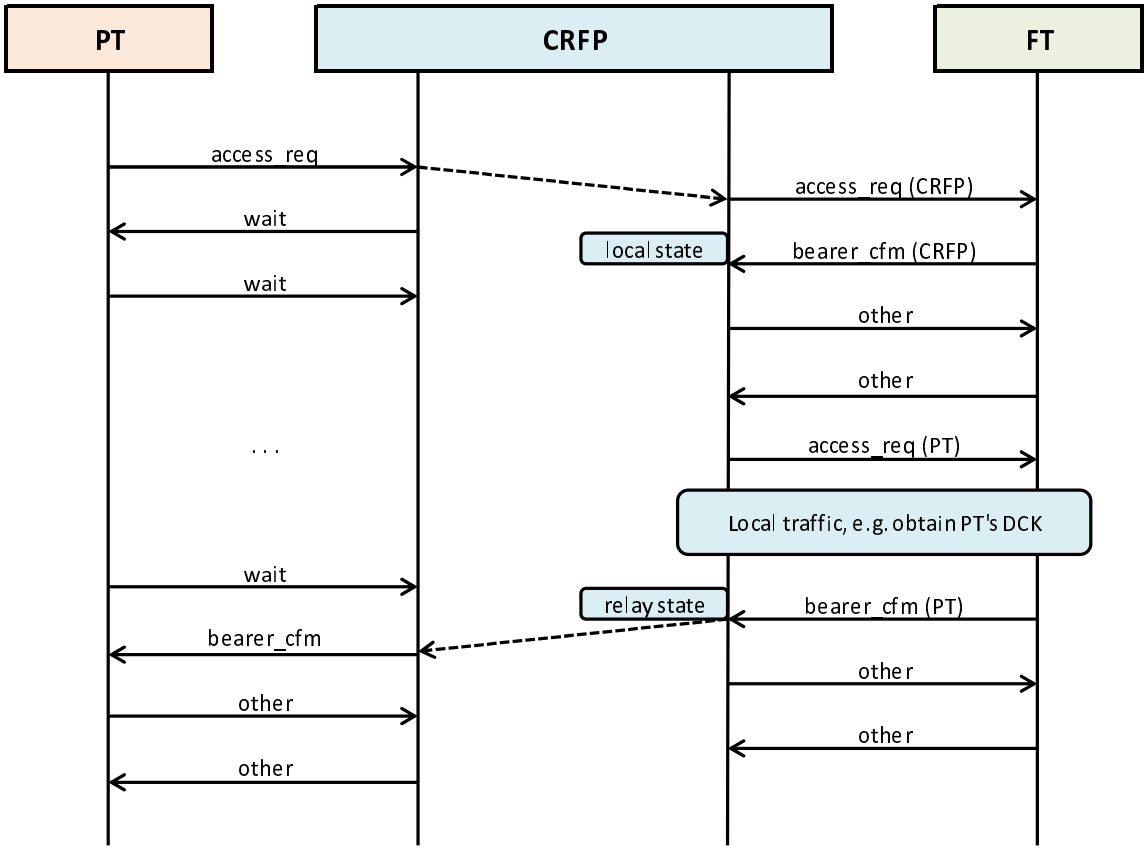

Figure 7: Dual bearer basic setup

At the CRFP:

During the bearer setup procedures the TBC, which has been created at the CRFP due to an "access_request", requests 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 Cipher Key (CK) transfer (e.g. DCK and/or DefCK).

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.

7.4.10.6 Dual C/O bearer setup (Advanced)

The process of dual bearer setup for advanced connections is very similar to the basic connection (see clause 7.4.10.5), except for the use of the equivalent advanced connection control set of messages, and the requirement to exchange the ATTRIBUTES_T request/confirm messages in accordance with ETSI EN 300 175-3 [3], clause 10.5.1.2.

Figure 8 is a typical message sequence for dual bearer setup using advanced connections. The exact sequence and timing of message may vary due to implementation differences and the time-slots used.

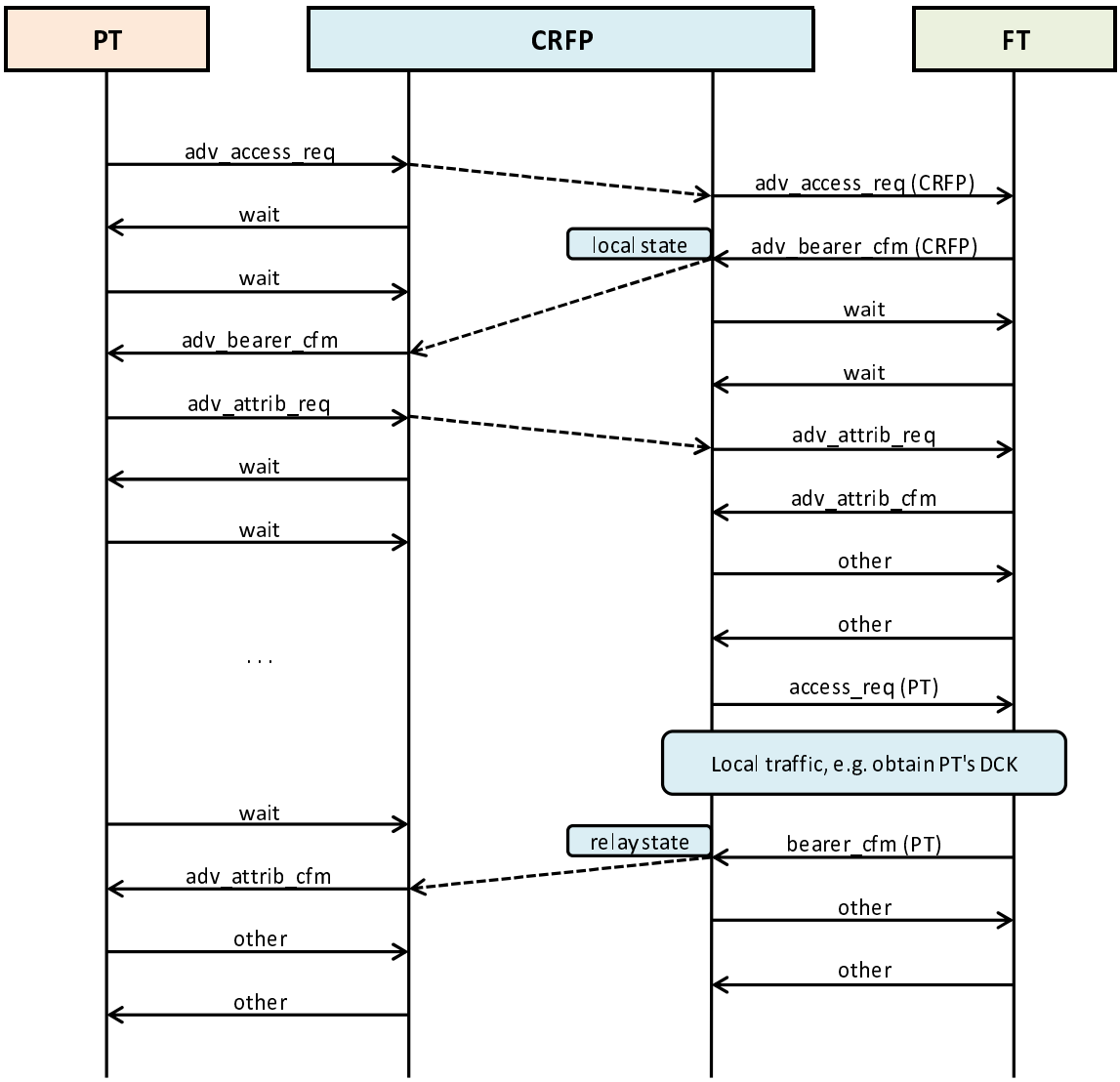

Figure 8: Dual bearer advanced setup

7.4.10.7 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.

The procedure is identical for basic or advanced connections, except for the appropriate coding (either basic or advanced) of the release messages.

Figure 9 shows the FT-initiated procedure for basic connections.

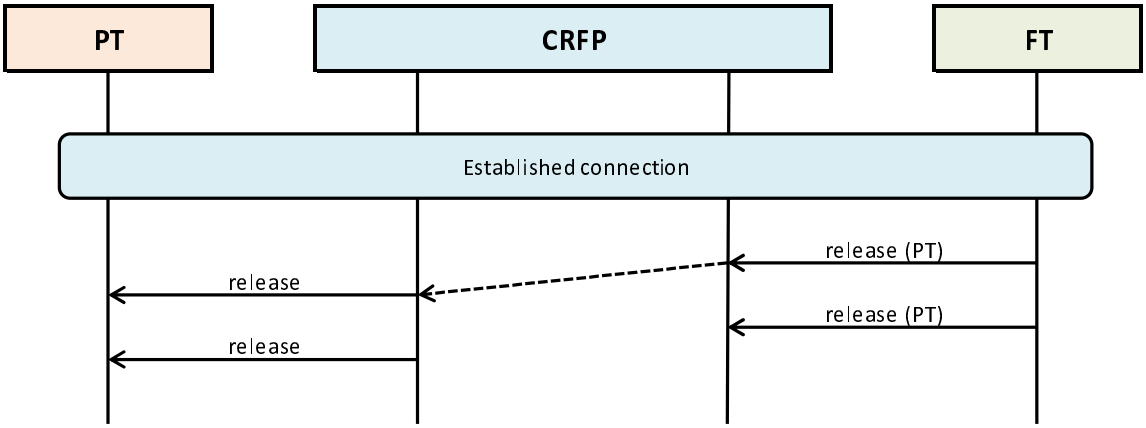

Figure 9: Release (FT-initiated)

Figure 10 shows the FT-initiated procedure for basic connections.

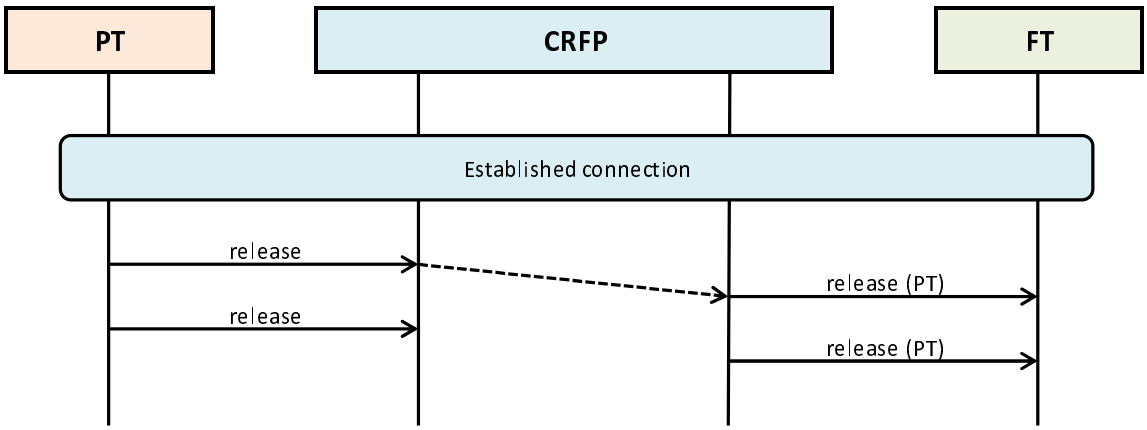

Figure 10: Release (PT-initiated)

7.4.10.8 C/O abnormal connection release

If the CRFP detects an abnormal loss of signal, the CRFP 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.

The procedure is identical for basic or advanced connections, except for the appropriate coding (either basic or advanced) of the release messages.

Figure 11 shows the procedure for abnormal connection release (initiated from FT side).

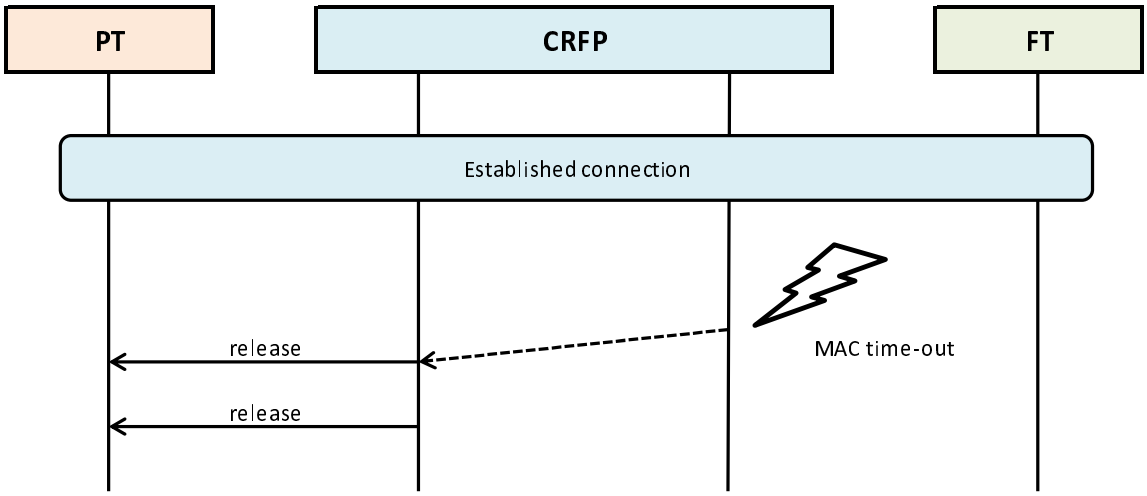

Figure 11: Abnormal release (initiated from FT side)

Figure 12 shows the procedure for abnormal connection release (initiated from PT side).

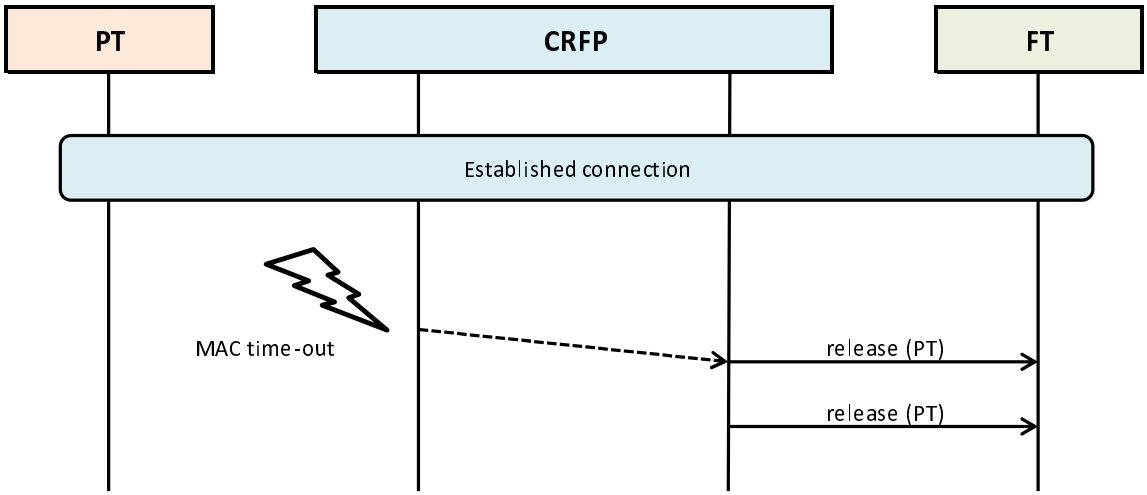

Figure 12: Abnormal release (initiated from PT side)

7.4.11 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 its destination. This means that any transmitted C-channel data has been acknowledged by the other side and there is no pending C-channel data waiting to be sent.

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 more.

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 13 shows message sequence diagrams for basic connections.

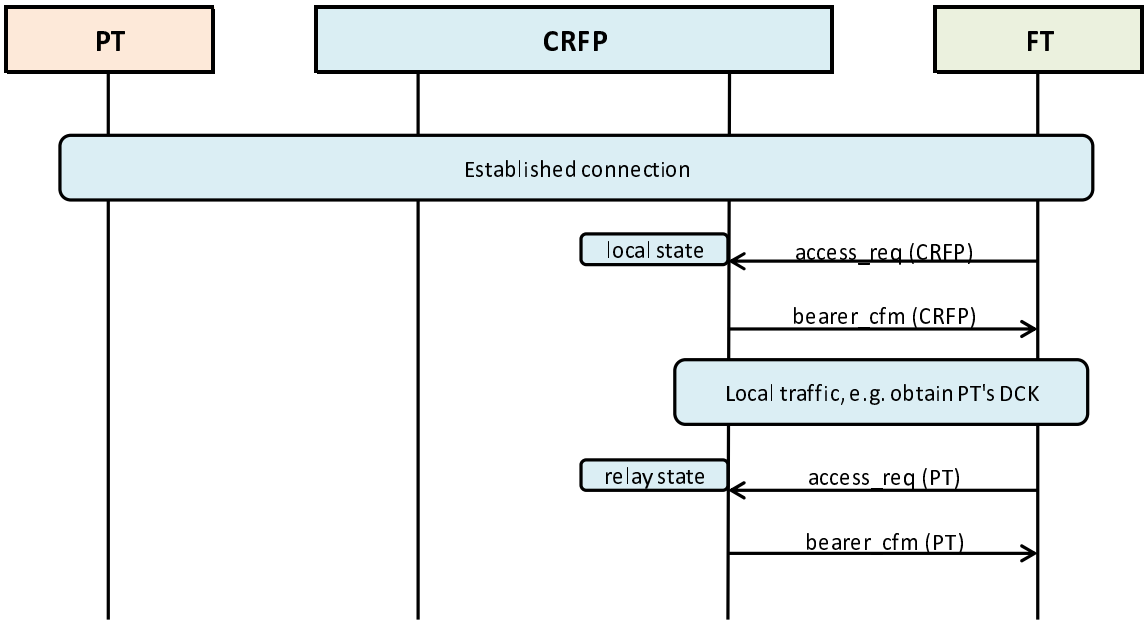

Figure 13: CRFP connection suspend and resume

Clause 7.4.17 of the present document describes in more detail the effects of switching between local/relay states, and the impact on the system operation.

7.4.12 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 ETSI EN 300 175-3 [3].
2) Completely handled at CRFP_PT using procedures as defined in ETSI EN 300 175-3 [3].
3) Completely handled at CRFP_PT using procedures as defined in ETSI EN 300 175-3 [3].
4) Completely handled by RFP. The connection via the CRFP is released (see Figure 14).
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 clause 5.3.1.1, except for replacing the "access.req" from the PT with a "bearer_handover.req" (see Figure 15).
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 1: 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 (I_N normal delay and I_P data) on both the new and the old bearer.

The examples sequences shown in Figure 14 and Figure 15 are using basic connections. However, this is just an example and similar sequences could be derived for advanced connections.

NOTE 2: In the following figures the slot numbers in the parenthesis refer to the slot pairs, e.g. "slot 5" refers to "slot pair 5 & 17".

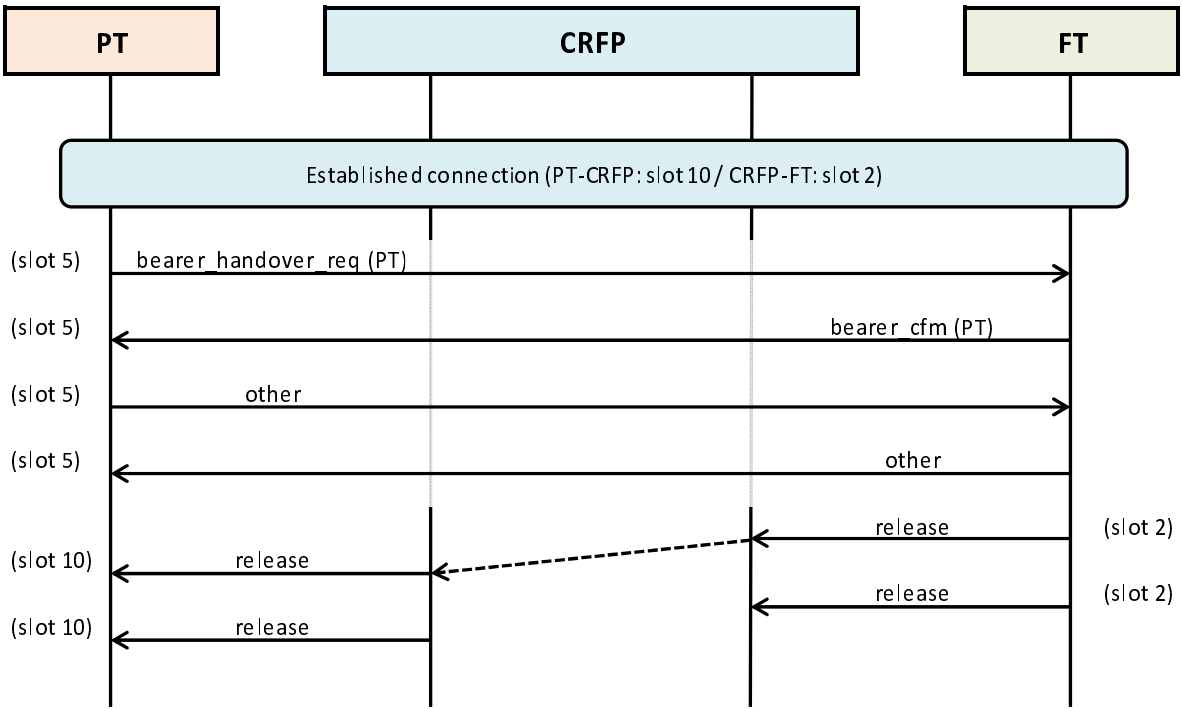

Figure 14: Bearer handover from CRFP to RFP (basic connection)

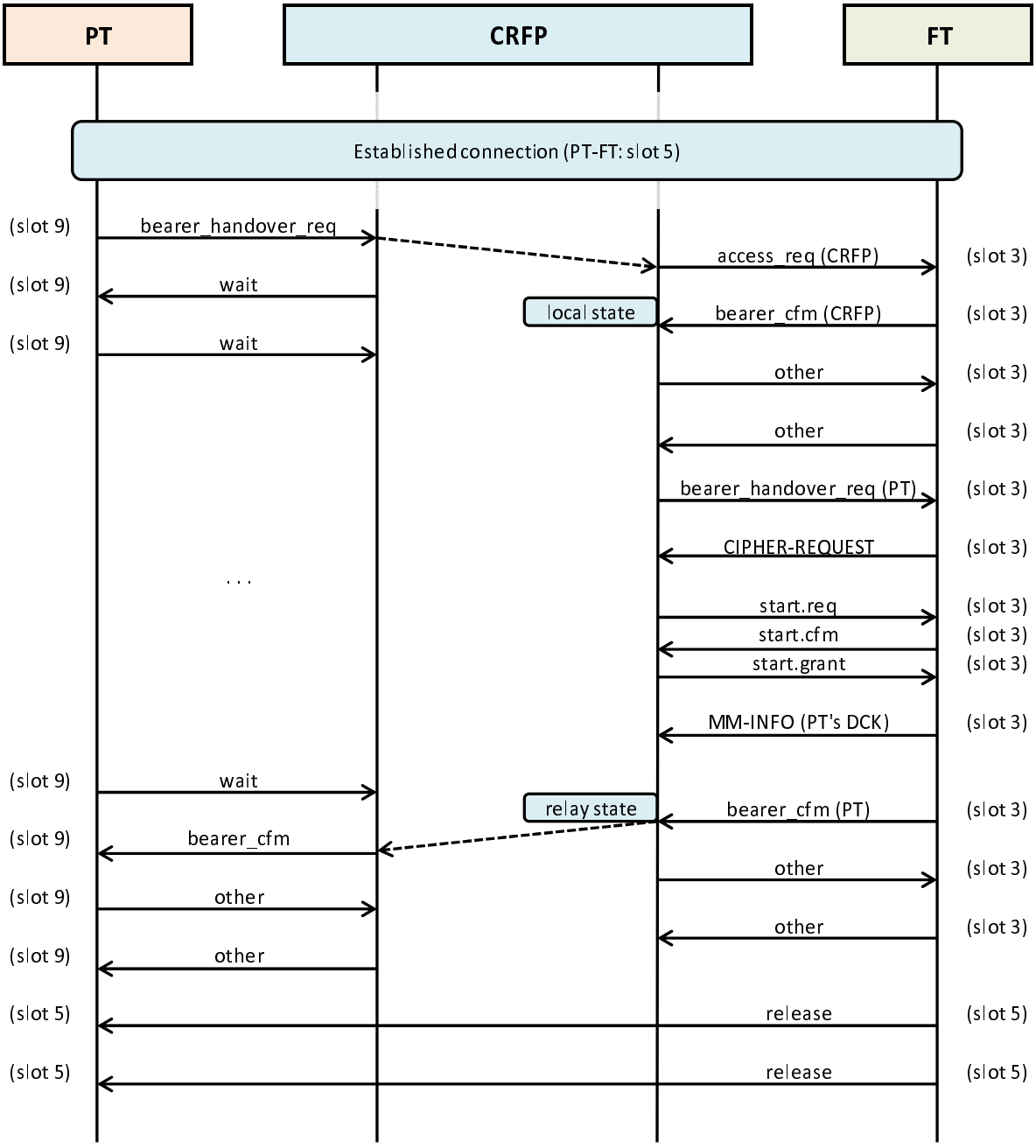

Figure 15: Bearer handover from RFP to CRFP (dual C/O bearer setup, basic connection)

NOTE 3: The sequence depicted in Figure 15 includes the encryption of the upper segment, and transfer of the cipher key for the lower segment. These procedures are described in detail in clause 7.7.

7.4.13 Relay of higher layer data

All PT network and higher layer information is relayed through the CRFP. As an example, Figure 16 shows a typical outgoing encrypted call setup with MAC and NWK layer messages via the CRFP. For clarity, the establishment of the MAC connection is not shown, which would normally be achieved by one of the other procedures (e.g. clauses 7.4.10.3, 7.4.10.4, 7.4.10.5 or 7.4.10.6).

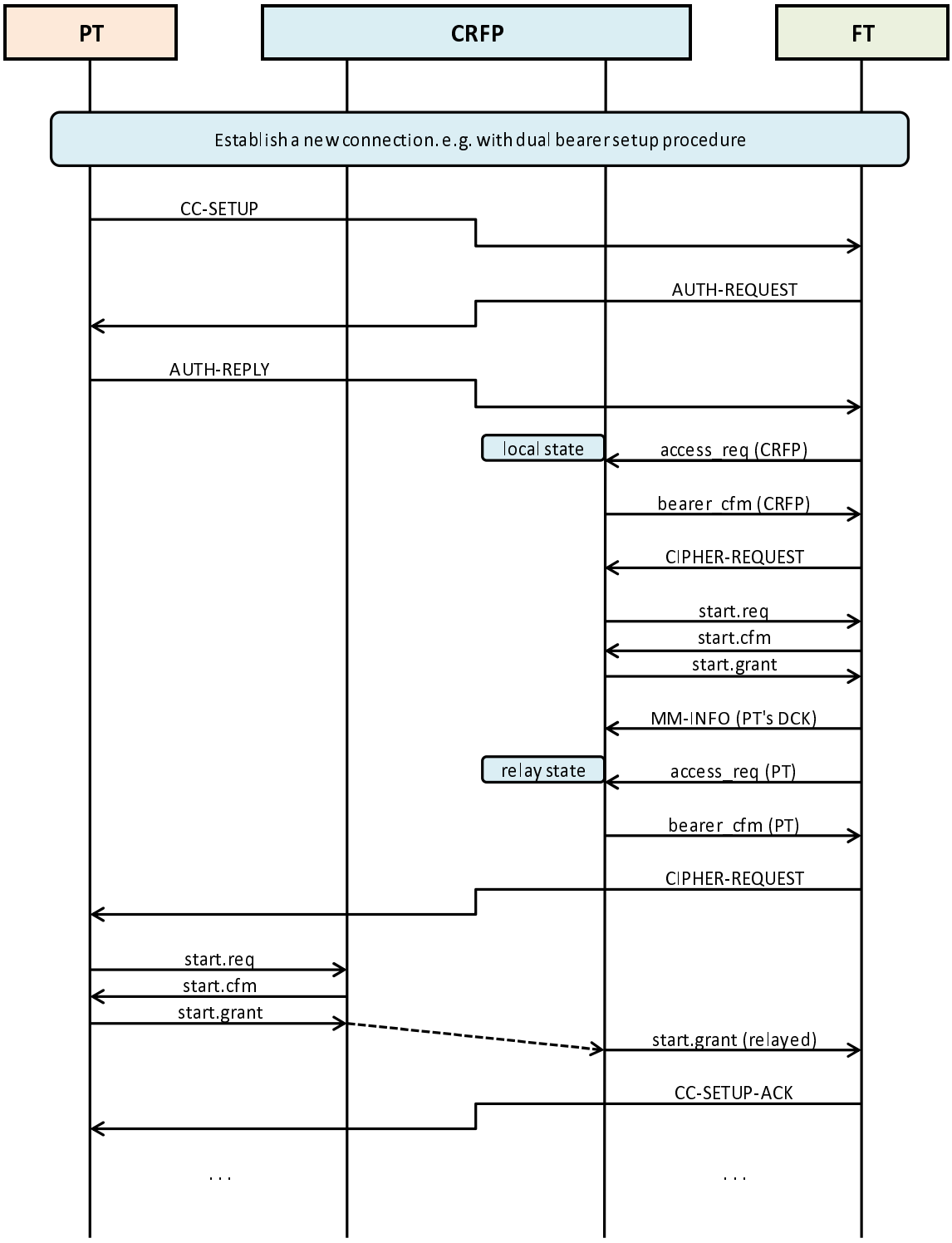

Figure 16: Typical call setup message diagram (with encryption)

7.4.14 "No emission" mode

"No emission" mode is not compliable with a system comprising of one or more repeaters. Therefore, the WRS shall not support "No emission" mode. This shall be indicated to the FP when the WRS registers itself.

The WRS shall always use bit a_{23} = 0 and bit a_{35} = 0 for the "Extended Fixed Part Capabilities (Part 2)" message (see ETSI EN 300 175-3 [3], clause 7.2.3.11.2 and ETSI EN 300 175-5 [5], Annex F) on its own downlink broadcast.

The WRS shall always use bit 7 = 0 for the "Profile/Application Indicator 6" of the << TERMINAL-CAPABILITY>> Information Element (see ETSI EN 300 175-5 [5], clause 7.7.41), where applicable, e.g. during access rights and location registration procedures.

7.4.15 ULE related procedures

7.4.15.1 Relay of I_P_error_correct service

The WRS shall support the relay of the MAC service I_P_error_correct as defined in ETSI EN 300 175-3 [3], clause 10.8.2.

The integrity of each packet shall be individually checked for each transmission segment and the MOD2 retransmission mechanism shall be used according to ETSI EN 300 175-3 [3], clause 10.8.2 for each individual segment. Only correctly received packets shall be relayed to the following node.

When there is no new packet for relay (e.g. due to bad reception or any other reason), either an "unnecessary I_P retransmission" or a "no-B-field" frame may be used in the next hop (assuming that the next node is requesting a new packet by means of the BCK bit setting).

The WRS sending side shall obey the meaning of the BCK bit received from the following node, which may also cause the insertion of mandatory unnecessary retransmissions.

The setting of BCK bit towards previous nodes described in clause 7.4.15.3 shall be used, which in practice acts as a flow control mechanism preventing any buffer overflow at the WRS.

7.4.15.2 Setting the Q2 bit

In ULE relayed connections, the Q2 bit shall be set in each DECT segment according exclusively to local quality in this segment.

Q2 shall be set as given in ETSI EN 300 175-3 [3], clause 10.8.2.4.1 "Q2 and BCK bit setting for I_P_error_correction services". Q2 set to "0" indicates bad quality (with criteria of ETSI EN 300 175-3 [3], clause 10.8.2.4.1) in the same segment and is independent of the bit setting in other segment of the repeater chain.

When a B-field carries control multiplexer data (i.e. in E-mux or E+U-mux mode) the setting shall be given in ETSI EN 300 175-3 [3], clause 10.8.1.3.5.

When a B-field carries "no B-field" the setting shall be given in ETSI EN 300 175-3 [3], clause 10.8.1.3.6.

7.4.15.3 Use of BCK bit for flow control and end-to-end integrity

7.4.15.3.1 General

The ULE "packet mode" data transfer service uses MOD-2 error correction. The feature ULE1-M.11 defines the packet lifetime used by the error correction service, at two levels (see ETSI TS 102 939-1 [12], clause 10.12.2). There is a packet lifetime at the TBC level and at one at overall MAC level. The default values are 3 and 7 frames respectively, although different values can also be negotiated.

A repeater shall use the "BCK" mechanism for flow control (see ETSI EN 300 175-3 [3], clause 10.8.2.4). For example, in order to provide additional time to establish the connection to the FP, or to allow it to deliver the packet to the FP before sending MAC acknowledgement to the PP.

The setting of BCK bit shall be as given in ETSI EN 300 175-3 [3], clause 10.8.2.4.1 "Q2 and BCK bit setting for I_P_error_correction services". According to ETSI EN 300 175-3 [3], clause 10.8.2.4.1, the BCK sending side (receiver of the packet) has the choice to either advance the value of BCK (causing the transmission of a new I_P packet) or repeating it (causing a retransmission). This choice shall be used to ensure end-to-end integrity of the transmission by implementing the following rule:

- A WRS shall only advance the value of BCK when it has confirmation of the correct reception of the packet by the terminal end-node (FP or PP).

To implement this rule the WRS will implement the following mechanics:

1) When a WRS receives a packet (in any direction) it shall report back (to the sending node) the proper Q2 bit (according to the CRC check) and a BCK bit identical to the received packet number (which would request a retransmission) unless the rule for advance described in step 3 happens.

2) The rule described in step 1 will be followed by in any subsequent repeater in the chain, until the packet reaches a terminal node (a FP or PP). When this happens, the FP or PP will follow the normal rules given in ETSI EN 300 175-3 [3], clause 10.8.2, and will (in most cases, see note 1) "advance" the BCK value requesting the transmission of a new packet.

3) When the WRS closest to the destination node received the "advanced" BCK, it shall also advance the BCK reported back to the previous node.

4) Regarding transmission, as this WRS does not have (yet) the requested packet, it shall send either "no-B-field" or an unnecessary retransmission of previous packet (implementation choice).

5) When the "advanced" BCK reaches the originating node, this node shall normally (see note 2) "advance" the packet by sending a new packet (whose I_P number is the one requested by the BCK).

6) The process shall be repeated with the new packet starting at step 1 until termination of the packet burst.

NOTE 1: The terminal node should normally advance the BCK. However, it will not do that if there was an error in the reception the packet (in such a case it should request a retransmission). Even in the normal case of correct reception, ETSI EN 300 175-3 [3] allows not advancing the BCK (causing an unnecessary retransmission). However, this is assumed to happen in only a few exceptional cases since it goes against the system efficiency.

NOTE 2: In theory, ETSI EN 300 175-3 [3] allows the node to not advance the packet and retransmitting the old one. This is the "unnecessary retransmission" case described in table.10.10 (case c) of ETSI EN 300 175-3 [3], clause 10.8.2.5.2, and therefore will be detected properly by the next node. However, it is assumed that this exceptional behaviour will happen only in only a few exceptional cases since it goes against the system efficiency.

NOTE 3: Refer to clause 7.4.15.8 for examples.

7.4.15.3.2 Lifetime counters

This use of the "BCK" mechanism as described (no advance of BCK) shall not cause the TBC packet lifetime to be decremented (see ETSI EN 300 175-3 [3], clause 10.8.2.2.1.4). Lifetime shall only be decremented when there is an advance of BCK. The overall MAC layer counter still applies, even in the case of the BCK mechanism.

7.4.15.3.3 Setting of BCK/Q2 bits in "no-B-field" frames

When "no-B-field" frames are inserted in a ULE connection, the setting of bits a_3 and a_7 shall always be done according to the format of the frame they acknowledge (see ETSI EN 300 175-3 [3], clause 10.8.1.3). If the frame they acknowledge (i.e. the frame sent in the opposite direction a half-frame before) contained an I_P packet, then bit a_3 shall be coded as a BCK bit. If the acknowledged frame was also a "no-B-field" frame, or it was not possible to decode it, then bit a_3 shall contain a Q1 bit.

The same principle applies when an I_P frame carries a_3 and a_7 bits acknowledging a "no-B-field" frame. In such a case bit a_3 contains a Q1 bit (see ETSI EN 300 175-3 [3], clause 10.8.1.3).

The Q1 or BCK bit shall only be evaluated if bit Q2 indicates correct reception (bit Q2 set to "1").

7.4.15.4 Repeater upper segment channel selection

The WRS shall behave as a ULE PP "fast actuator" type for the upper segment channel selection.

The WRS shall use the option of continuous analysis of the channel selection information received in the dummy bearer M_U channel, and it shall continuously pre-select at least one access channel for the upper segment in each frame, using the ULE channel selection algorithm M1 (see ETSI EN 300 175-3 [3], clause 11.12.5). These access channel(s) will be used in the event of incoming traffic coming from the lower segment (from a PP or other repeater).

7.4.15.5 Relay of MAC expedited messages

MAC expedited messages shall always be relayed, however this relay is not completely transparent. The messages have a local meaning in the segment in which they are exchanged which follows the general rules for ULE. In addition to that, they trigger a continuation action (setup or release) towards the final node.

The following addresses shall be used in all M_T control (setup and release) messages related to ULE connections (in those messages where an address have to be inserted):

- the PMID of the PP terminal node;
- the FMID of the upper node in the segment where the message is exchanged (it may be the FP or a WRS).

7.4.15.6 Conversion of single-burst access to multi-burst setup

Single-burst setups need to be transformed when there are repeaters in the connection. When a repeater receives an access request for a single burst access (Mt "expedited access request ready for release"), it shall convert this access to a multi-bearer setup by returning "bearer confirm".

The repeater may also try a single-burst access to the next node (towards the FP). See detailed flowcharts in clause 7.4.15.8.

7.4.15.7 Use of "Wait" message

A repeater may use a "Wait" message in response to a PP's "expedited access request" or "expedited access request ready for release" message. The use of the "Wait" allows the repeater additional time to establish the connection to the FP, whilst also informing the PP that it should not expect an immediate response from the FP.

There is no explicit "Wait" message in the Advanced connection control part 2 set of messages (see ETSI EN 300 175-3 [3], clause 7.2.5.12). Instead, the repeater shall use a "bearer confirm" (M_T Advanced Control message command "0100"B) with BA bits indicating "no B-field" (code "111"B). No data is transferred in the B-field of this "wait" message, and a short slot shall **not** be used.

The "wait" message may be used in conjunction with the "BCK" mechanism as described in clause 10.4.15.3, in which case the PP will re-transmit the same packet as requested.

The PP shall handle the "wait" message just like a normal "bearer confirm" message, which means the connection is treated as a "multi-burst" connection (see ETSI EN 300 175-3 [3], clauses 10.5.1.8.2.3 and 10.5.1.8.3) even if the FP has no data or only a single packet of data to send.

7.4.15.8 C/O scenarios mandatory sequences

7.4.15.8.1 General

All WRS shall at least support the scenario and response sequences given in clauses 7.4.15.8.2 to 7.4.15.8.9. These diagrams are similar in nature, and the following common description applies where appropriate:

- "(ULE dummy bearer)" represents a periodic transmission of the ULE dummy bearer.
- "(lms)" represents the "last minute scan", i.e. making an RSSI measurement to ensure the suitability of the intended channel.

- "Access-req-rel" represents the "Expedited Access Request ready for release" message (see ETSI TS 102 939-1 [12], clause 10.10.2).
- "Confirm" represents the "Bearer confirm" message (see ETSI TS 102 939-1 [12], clause 10.10.2).
- "Release" represents the "Bearer release" message (or the "Expedited Release with G_{FA} transmission" message if a G_{FA} value is specified). See ETSI TS 102 939-1 [12], clause 10.10.2.
- "Ready for release" represents the "Expedited Access Request ready for release" message (or the "Ready for release with G_{FA} transmission" message if a G_{FA} value is specified). See ETSI TS 102 939-1 [12], clause 10.10.2.
- The identifier "IP1" or "IP0" represents which IP packet is being transmitted.
- The identifier "BCK = N" represents the value of the BCK bit in the transmitted message.
- The identifier "no B" represents no B-field content in the transmitted message.
- The identifier "G_{FA} = N" represents the use of the G_{FA} channel, usually to acknowledge a DLC packet.

7.4.15.8.2 Single burst uplink, PT initiated (1)

The WRS shall support relay of single packets of data from PP to FP. Figure 17 shows an example of such a scenario.

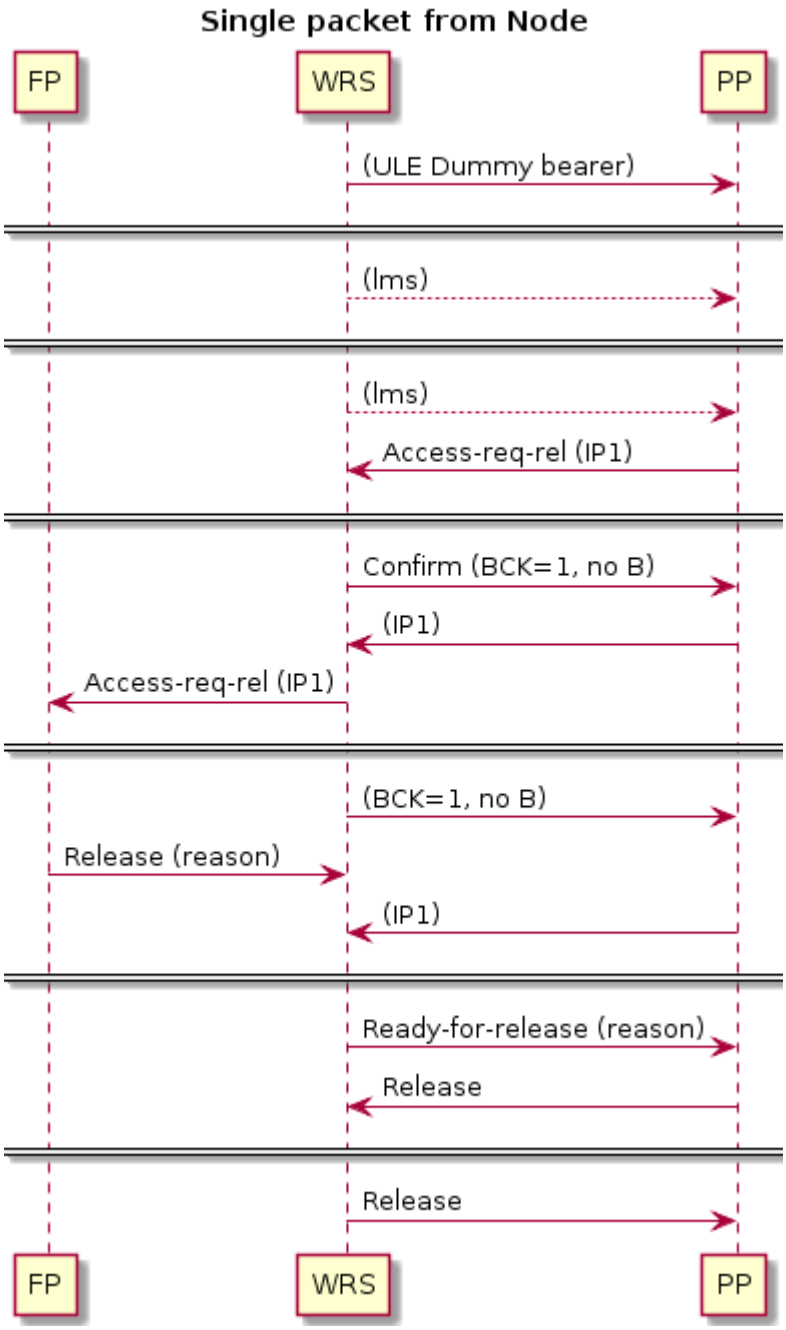

Figure 17: Single burst uplink, PT initiated

7.4.15.8.3 Single burst uplink, PT initiated (2)

The WRS shall support relay of single packets of data from PP to FP. Figure 18 shows an example of such a scenario.

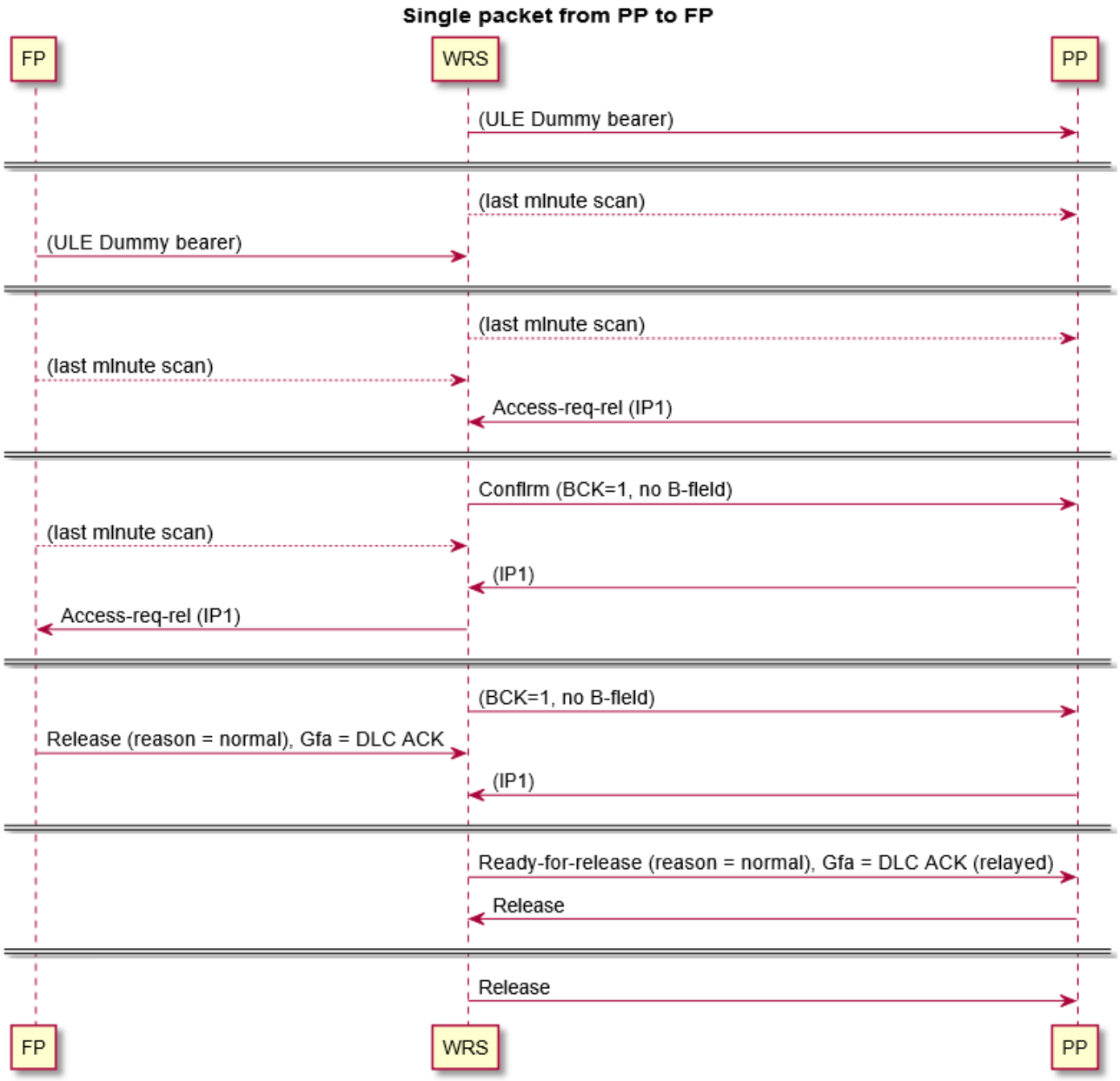

Figure 18: Single burst uplink, PT initiated

7.4.15.8.4 Single burst uplink, PT initiated - optimal slot positions

The WRS shall support relay of single packets of data from PP to FP. Figure 19 shows an example of such a scenario.

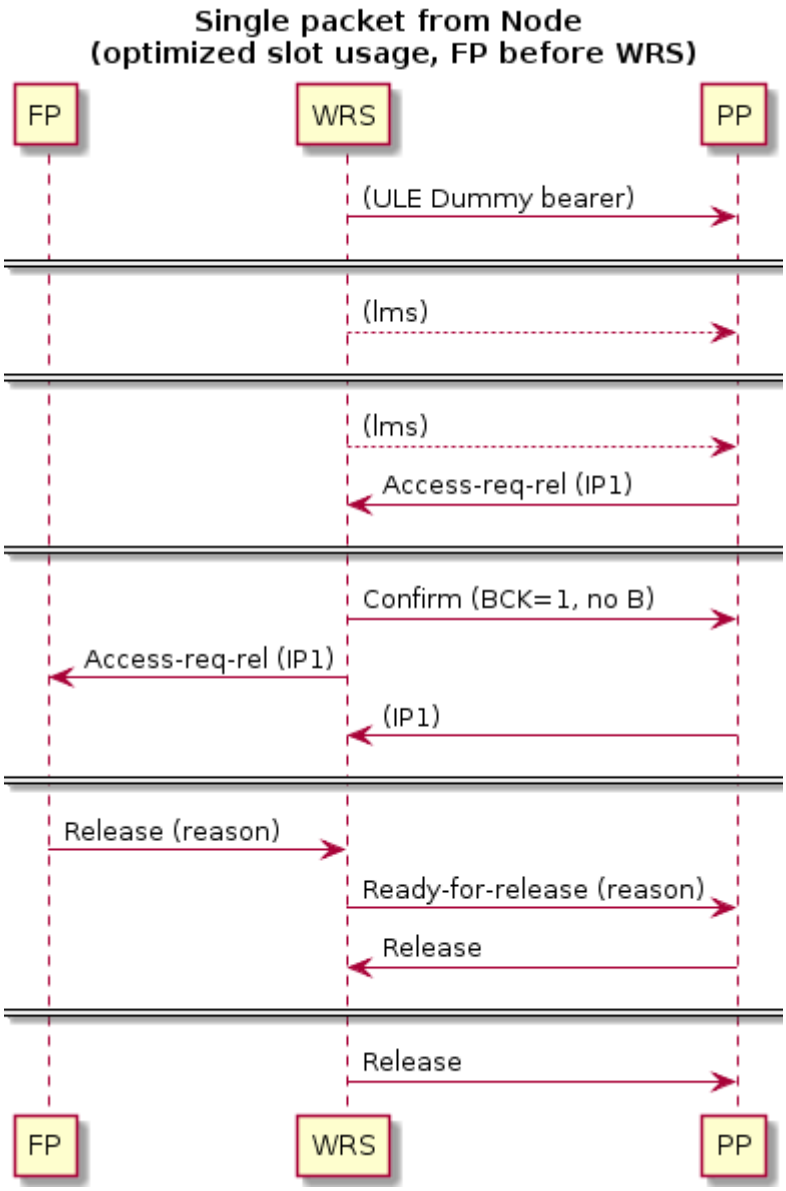

Figure 19: Single burst uplink, PT initiated - optimal slot positions

7.4.15.8.5 Single burst downlink PT initiated

The WRS shall support relay of single packets of data from FP to PP. Figure 20 shows an example of such a scenario.

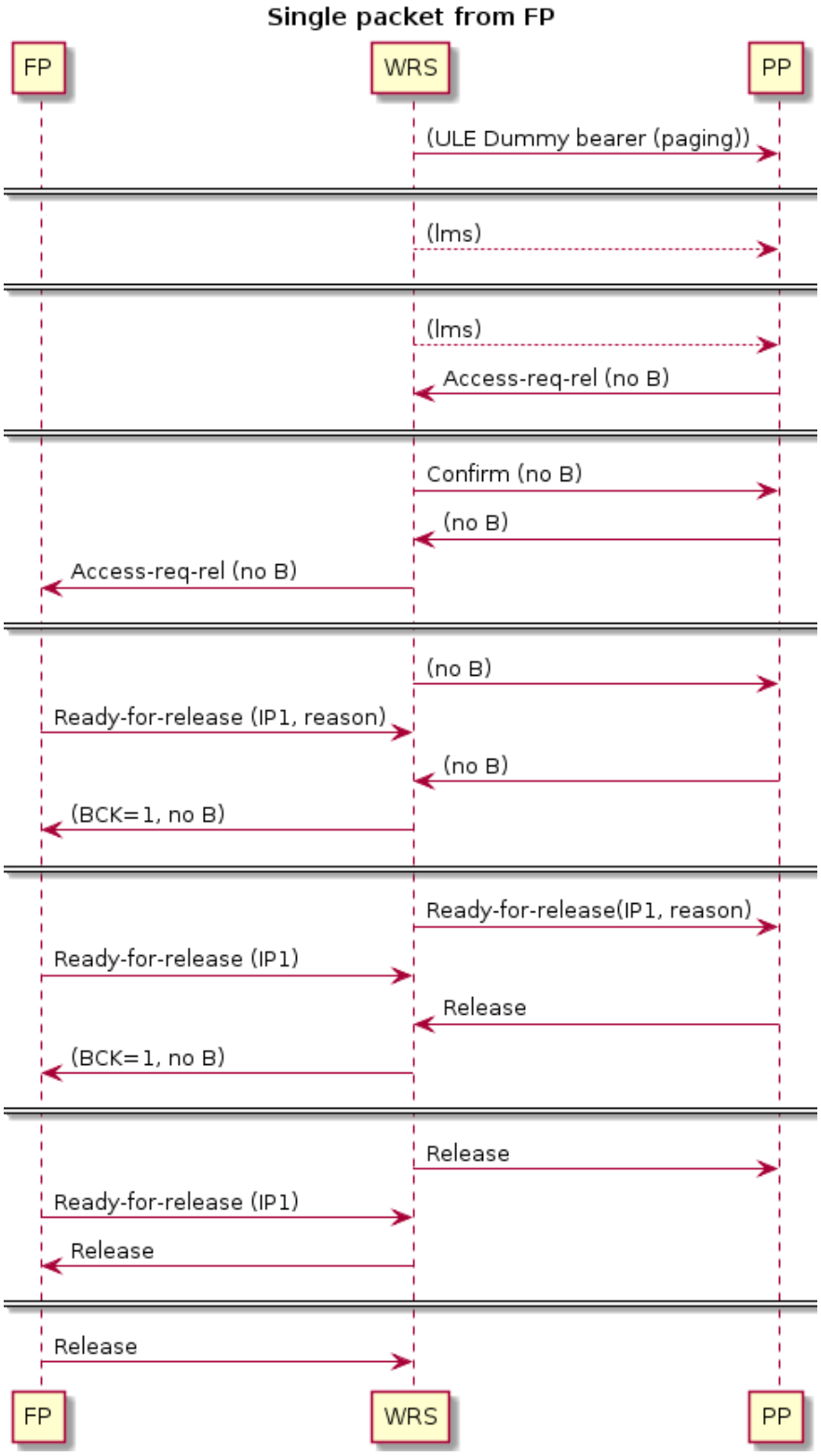

Figure 20: Single burst downlink PT initiated

7.4.15.8.6 Single burst downlink PT initiated - optimal slot positions

The WRS shall support relay of single packets of data from FP to PP. Figure 21 shows an example of such a scenario.

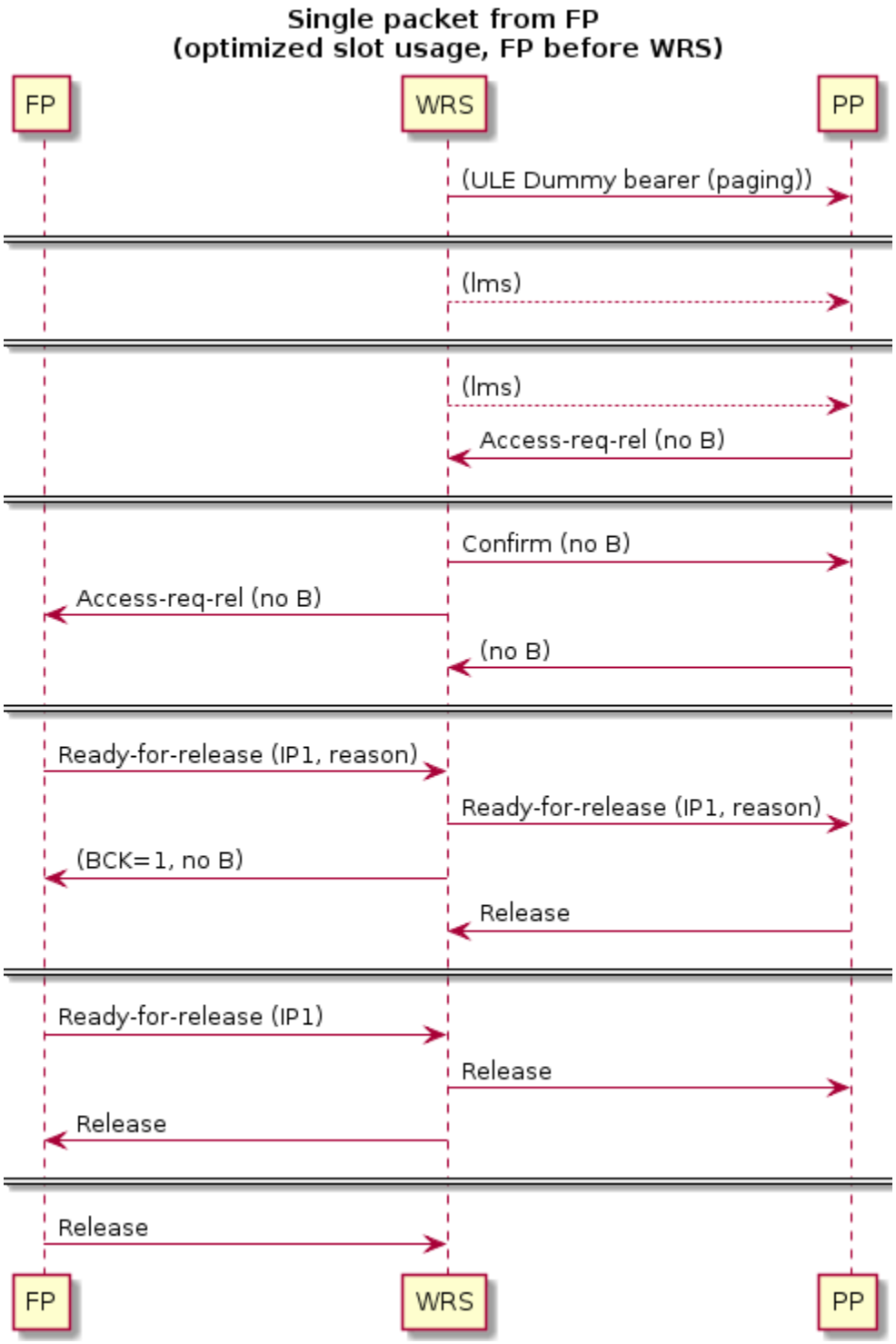

Figure 21: Single burst downlink PT initiated - optimal slot positions

7.4.15.8.7 Bidirectional - Single bursts in both directions - PT initiated

The WRS shall support relay of bi-directional packets of data between the FP and PP. Figure 22 and Figure 23 show two examples of such a scenario.

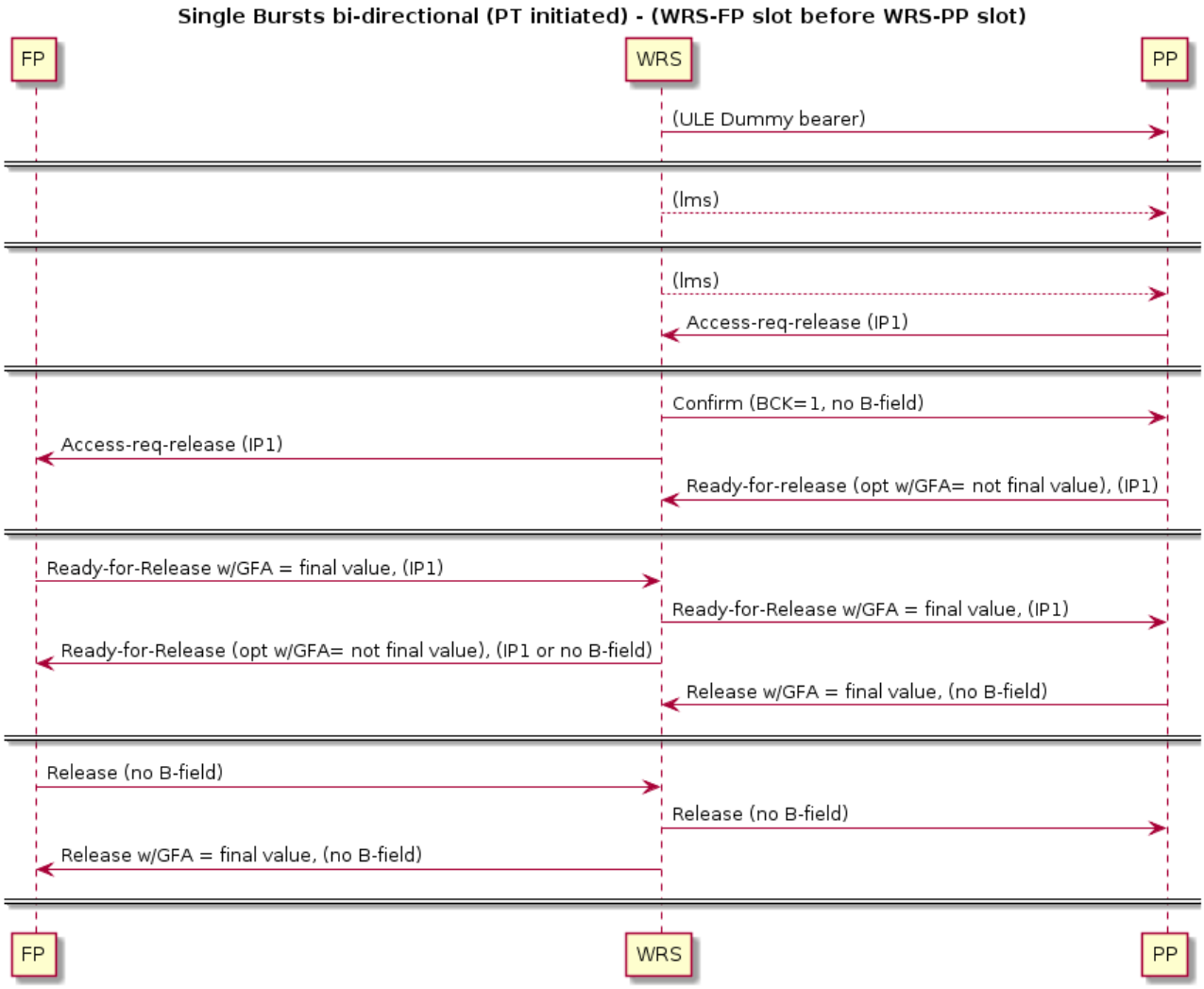

Figure 22: Bidirectional - Single bursts in both directions - PT initiated (slot for FP-WRS segment before slot for PP-WRS segment)

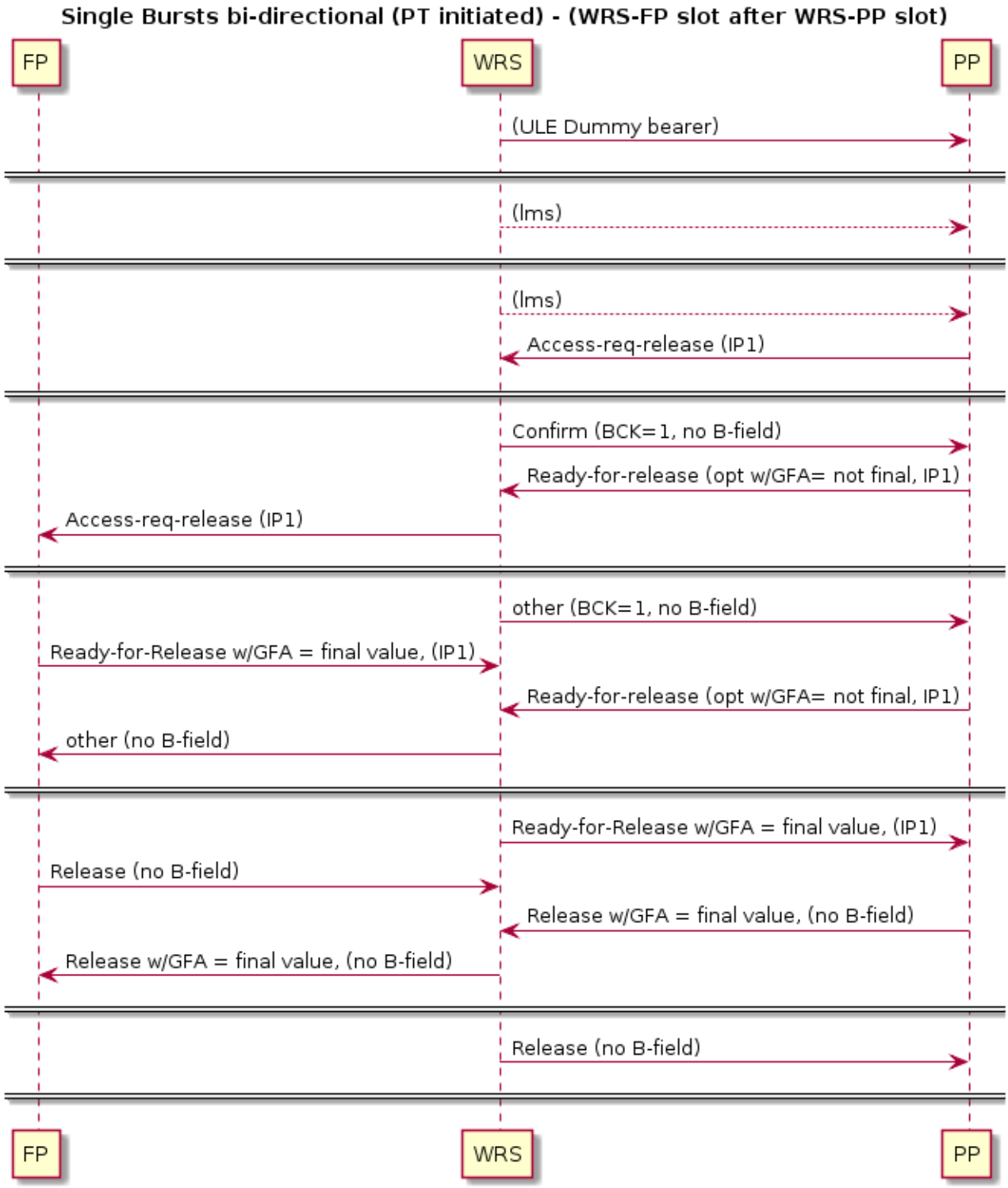

Figure 23: Bidirectional - Single bursts in both directions - PT initiated (slot for FP-WRS segment after slot for PP-WRS segment)

7.4.15.8.8 Bidirectional - Multi-bursts (two packets) in both directions - PT initiated

The WRS shall support relay of bi-directional packets of data between the FP and PP. Figure 24 shows an example of such a scenario.

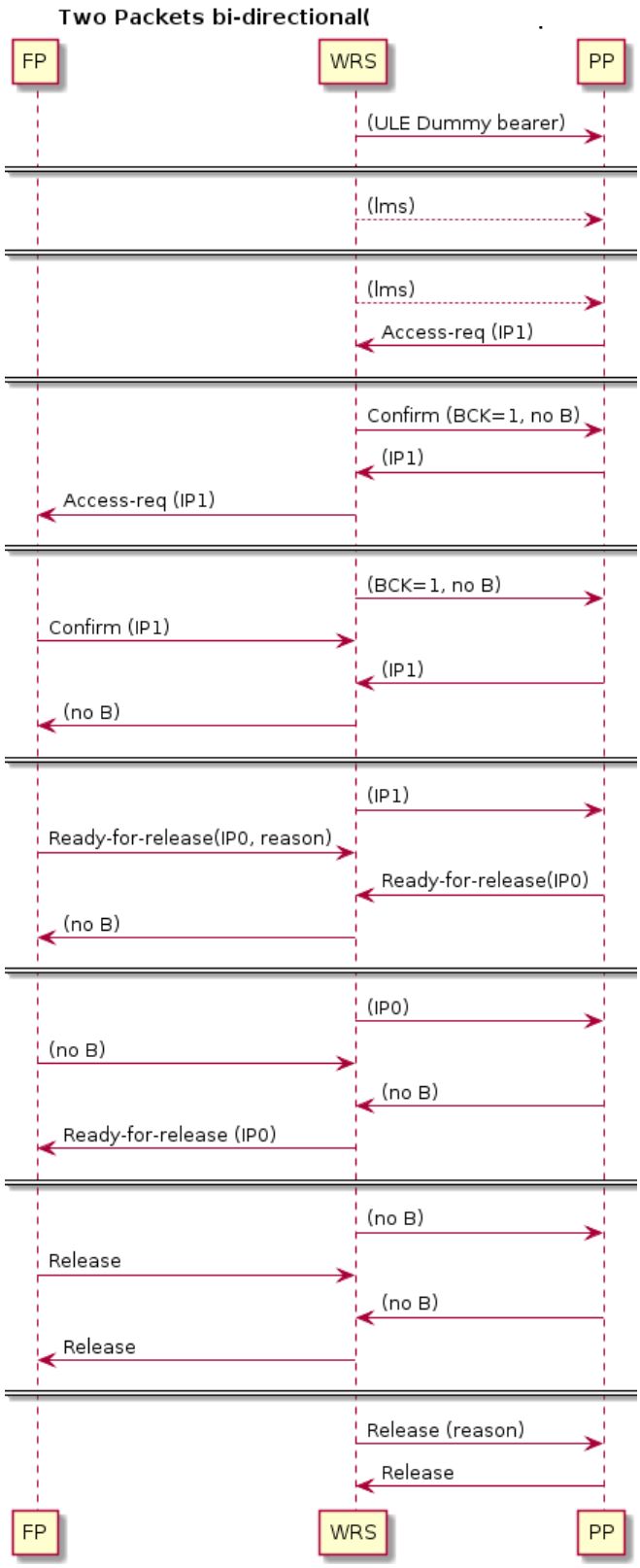

Figure 24: Bidirectional - Multi-bursts (two packets) in both directions - PT initiated

7.4.15.8.9 Bidirectional - Multi-bursts (two packets) in both directions - PT initiated - optimal slot positions

The WRS shall support relay of bi-directional packets of data between the FP and PP. Figure 25 shows an example of such a scenario.

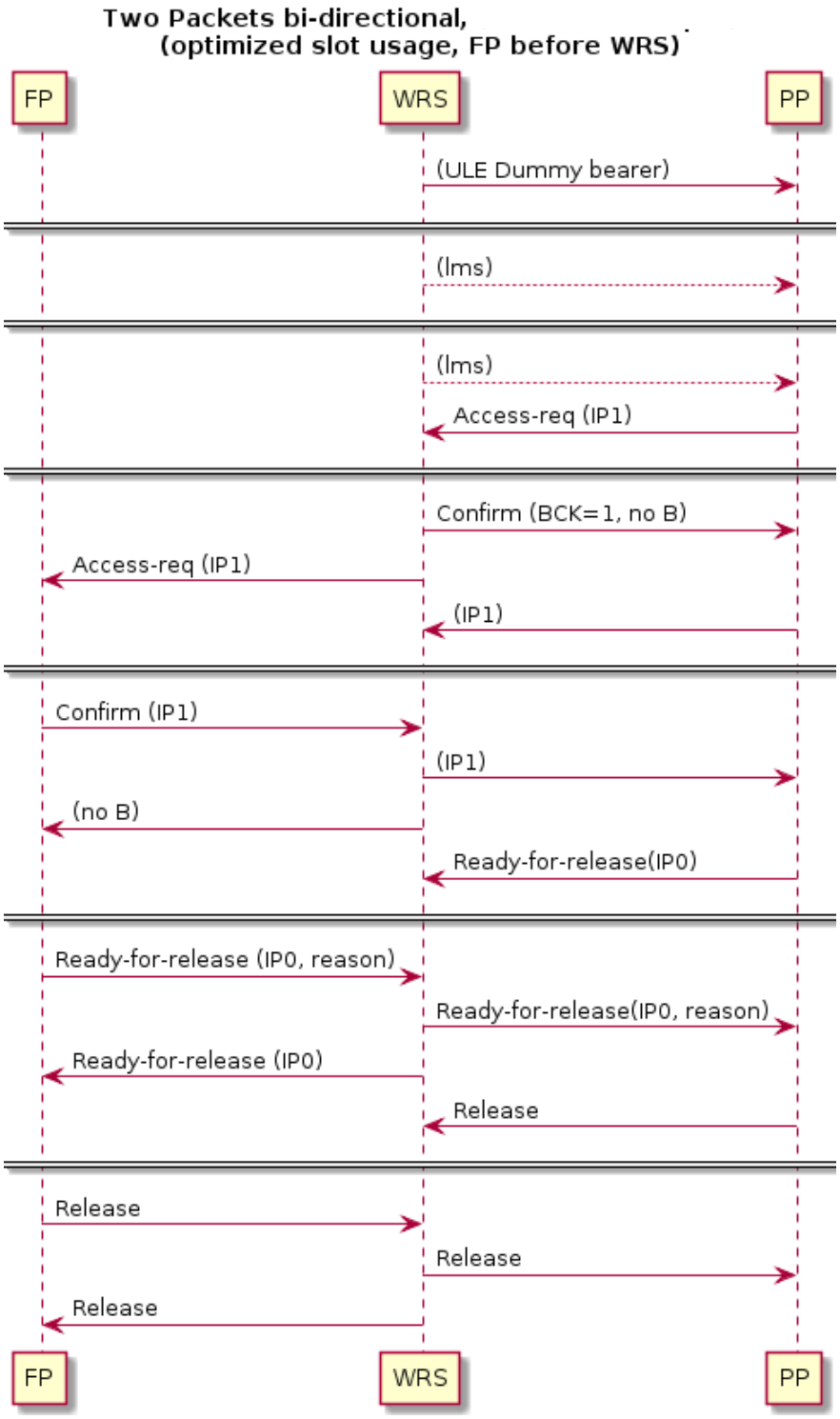

Figure 25: Bidirectional - Multi-bursts (two packets) in both directions - PT initiated - optimal slot positions

7.4.15.9 G_{FA} channel relay

The WRS shall be able to relay the G_{FA} channel.

The relay shall be transparent with regard to the content of the channel. The WRS does not need to open or understand the payload of the channel (DLC frame FU10d).

However the relay shall not be transparent with regard to the message carrying the channel. A G_{FA} transported by an "expedited release" message over one segment may continue in the next segment transported by a "ready for release" message or vice versa. The rule shall be that the MAC layer of the WRS shall relay the content of the channel in the first opportunity. First opportunity shall be understood as the first MAC message able to carry the G_{FA} channel content. In most cases the message shall not be the same carrying the content over the previous "leg".

EXAMPLE: See the sequence given in clause 7.4.15.8.3, Figure 18.

7.4.15.10 Handling of ULE bearer replacement (inter-cell)

A ULE PP is able to perform inter-cell bearer replacement, by setting up new TBCs within the same logical connection. The following rules apply:

- The bearer replacement shall be always implemented by dropping the existing bearer before establishing the new one.
- There should not be more than one ULE bearer over the air per segment at any time.
- Inter-cell bearer replacement shall only be performed at SDU boundaries.
- This procedure only applies to ULE packet mode connections.

A WRS shall be able to perform the same procedure towards the next node in the direction of the FP (the FP itself or another WRS). This procedure shall be used when the WRS detects quality issues in this segment.

The WRS shall handle separately the bearer replacements in both segments. Completion of a bearer replacement in one of the sides does not cause the procedure in the other.

7.4.16 Procedures for the relay of I_P_error_detect service

7.4.16.1 Transparent relay of I_P_error_detect service

The WRS shall support the transparent relay of the MAC service I_P_error_detect (as defined in ETSI EN 300 175-3 [3], clause 10.8.3.3).

7.4.16.2 Detection and setting of the I_P_error_detect service

The WRS shall detect and setup the service of a connection for I_P_error_detect when the following situation happens:

- an advanced connection has been established between the FT and a PT; and
- there has been an exchange of the M_T ATTRIBUTES (Req/Cfm) messages between both sides (FT and a PT) setting the MAC service to I_P_error_detect

NOTE: This clause is concerned with the establishment of a connection using the I_P_error_detect service.

7.4.16.3 Service change to/from I_P_error_detect service

When FT and PT execute a MAC service change to/from the I_P_error_detect service from/to any other MAC service (e.g. I_N), the WRS shall detect the change by means of the observation of the exchanged M_T ATTRIBUTES messages and shall change the service accordingly. The service shall be changed only upon the observation of the confirmation message.

NOTE: This clause is concerned with the service change of a connection to/from the I_P_error_detect service.

7.4.16.4 BA codes supported

7.4.16.4.1 General

The WRS shall support the following BA codes, as defined in ETSI EN 300 175-3 [3], clause 7.1.4, when relaying an I_P_error_detect service connection:

- BA = 001: "U-type, I_P_error_detect".
- BA = 000: "no valid I_P_error_detect channel data".
- BA = 111: "no B-field".

The WRS shall always relay the BA coding and the B-field content except in the error handling case described in clause 7.4.16.5.

7.4.16.4.2 Handling of "no-B field" case

The "no-B-field" coding when in MAC service "I_P_error_detect" shall always be understood as transmitting content (energy) in the B-field.

The WRS shall relay the received B-field, except when it is not possible to decode it correctly; in that case an appropriate filling pattern shall be used.

NOTE: For security considerations, in certain cases, a random filling pattern should be used to fill in the B-field, or the B-field should not be encrypted. This rule, when needed, will be prescribed by the security procedure.

7.4.16.5 Handling of error cases in I_P_error_detect service

7.4.16.5.1 Setting the bits Q1 and Q2

Bits Q1 and Q2 shall always be set according to the evaluation of CRC, detected quality and normal rules for each individual segment between adjacent nodes. The received Q1/Q2 setting received from other segments shall not interfere with this setting except in the exceptional case described in clause 7.4.16.5.3.

The rules given in ETSI EN 300 175-3 [3], clause 10.8.1.3 shall be used for setting the bits in each individual segment. For instance, antenna switching and sliding collision may be requested/reported using this mechanism.

EXAMPLE 1: In a system with two chained repeaters (FP-WRS1-WRS2-PP), the transmission of a I_P_error_detect packet between a PP and a WRS2 is successful (good A-field and B-field CRCs), fails in the transmission between the WRS2 and WRS1 (bad B-field CRC), but is successful in the transmission between WRS1 and the FP. Furthermore, this situation is repeated for several successive frames. No antenna switching is requested: Q1/Q2 bits always shall be set to 0/1 in the PP-WRS2 and WRS1-FP segments and to 1/0 in the WRS1-WRS2 segment.

The antenna switching request, when used, shall always be understood as local and not relayed.

EXAMPLE 2: PP sends to a WRS an "antenna switch" request (code Q1=1/Q2=1). The WRS is the node that should execute the antenna switch (if available), and it should not relay the request to the FP.

7.4.16.5.2 Setting the BA bits and B-field content

When a WRS receives an error frame (either A-field or B-field failed), in addition to reporting the error by means of the Q1/Q2 bits, it shall relay to the following node the content in BA bits and B-field as defined below:

- BA bits shall be set to code 000 ("no valid I_P_error_detect channel data") and B-field shall be filled with the received Ip content (received with bad B-CRC) when at least A-field CRC has succeeded, or with a filling pattern when A-field CRC has not succeeded and/or B-field decoding has been impossible.

7.4.16.5.3 Flow control with C_S or C_F traffics

When a WRS is relaying C_S or C_F traffic, and receives a bad CRC report from the next node (e.g. Q-bits indicating that the other node did not correctly receive the last packet), then it shall retransmit the C_S or C_F content according to normal MAC rules. If the WRS continues receiving C_S or C_F traffic, it shall store it in a buffer delaying its transmission until after the retransmissions of previous packets. The size of this buffer is implementation choice.

When the buffer limit is approaching, the WRS is allowed to send a "fake" Q1/Q2 report to the previous node in order to control the flow of C_S or C_F channels. In general, the code Q1=0/Q2=0 shall be used in order to force a retransmission of the C_S channel and the code Q1=1/Q2=0 shall be used in order to force a retransmission of the C_F channel.

7.4.17 Procedures for the local/relayed mode switching

7.4.17.1 General and managing rules

7.4.17.1.1 General

The WRS local mode is a special mode of the WRS that allows the exchange of signalling between the FP and the WRS itself, instead of relaying it to the following nodes (and eventually to the PP).

There is no possibility to exchange higher layer signalling directly between the PP and a WRS or between two WRSs in a chain. For the exchange of MAC signalling (which is possible in some cases) refer to clause 7.4.17.7.4.

7.4.17.1.2 Terminology

From the point of view of a WRS, it may be in one of two modes: relayed or local.

Relayed mode is the normal situation.

From the point of view of the system (which is also the view of the FP) the system may be in "normal" (full relayed) mode (i.e. all WRS in relayed mode), in "local to the WRS" mode (if there is only one WRS) or in one of several "local modes" in case of chains of repeaters.

The terminology "local to WRSx" (where x = 1, 2, 3, etc.) will be used to avoid ambiguities, which means that the mode is configured to exchange signalling between the FP and WRSx. This means setting WRSx to local mode and all other WRS in between the FP and WRSx (if any) to relayed mode.

NOTE: There may be other temporary *local states* such as the one created at the initial stages of bearer setup. These *local states* are different from the *local mode* described in the present clause.

7.4.17.1.3 Management

The local mode is managed by the FP, which knows the local/relayed state of all WRS in the system and the intended destination for the signalling.

The FP shall be in charge of ensuring that any local mode is activated for the minimum time necessary to perform the intended signalling operation and it shall de-activate the mode - switching all nodes back to the "full-relayed" normal mode - at the earliest opportunity.

7.4.17.2 Switching to local mode

The switching to local mode is implemented by exchanging an Access Request/Bearer Confirm pair of messages with the following addressing:

- FMID = the FMID of the FP.
- PMID = the PMID of the WRS intended to be set in local mode.

This operation may be initiated by either the FP or the WRS.

Any repeater located between the FP and the addressed WRS shall continue to be in relayed mode. Only the addressed WRS shall switch to local mode. Messages shall not be relayed further downstream past the addressed WRS.

NOTE: Therefore the PP (or any WRS located downstream) is not aware of this switching to local mode.

7.4.17.3 Switching to full-relayed mode

The switching to full-relayed mode is implemented by exchanging an Access Request/Bearer Confirm pair of messages with the following addressing:

- FMID = the FMID of the FP.
- PMID = the PMID of the PP.

This procedure shall only be initiated by the FP.

In case of chains of repeaters, the messages shall be relayed downstream (towards the PP) until the last WRS in the chain, which should not further relay it to the PP.

When a WRS receives an Access Request/Bearer Confirm pair of messages with any PMID different from its own PMID, it shall switch to relayed mode.

7.4.17.4 Switching between local modes

In systems with chains of repeaters, the switching between several local modes in the direction towards the PP is allowed. This is implemented by exchanging an Access Request/Bearer Confirm pair of messages with the following addressing:

- FMID = the FMID of the FP.
- PMID = the PMID of the WRS intended to be set in local mode.

The switching between local modes is not allowed in the direction towards the FP. If this change were needed, the FP shall set the connections to full relayed mode and then shall switch to the desired local mode. For example, in a system with 2 WRS (FP-WRS1-WRS2-PP), if the FP is in local mode with WRS2, it is not possible to switch the local mode directly to WRS1.

When a WRS receives an Access Request/Bearer Confirm pair of messages with any PMID different from its own PMID, it shall switch to relayed mode.

7.4.17.5 Switching point and error handling

The transition point shall be the same half-frame that carries the Bearer Confirm message. Therefore, this half frame is already in the target mode. However in order to avoid any error due to different synchronization, the initiating node (often the FP) shall do the following:

1) The initiating node shall repeat the procedure until reception of a valid Bearer Confirm. To do that, the node shall take into account the time needed for getting the response (depending on the repeater chaining).

2) The initiating node shall not transmit any higher layer signalling (C_S or C_F) before the successful completion of the procedure (due to possible ambiguity in the destination).

3) The switching procedure shall not be executed if there are pending transmissions (or retransmissions) of C_S or C_F packets.

4) C_S or C_F packets received after initiating the procedure and before receiving the bearer confirm shall be ignored, since there is ambiguity of their origin.

7.4.17.6 Higher layer signalling handling

From the point of view of higher layer signalling (channels C_S and C_F) the WRS shall have a "local" instance of C-plane DLC that shall be connected to channels C_S and C_F when in local mode. Only one instance for both is enough (see clause 7.4.18 on C-channel operation). The FP shall have independent C-plane DLC instances for each PP and for each of the WRS users (virtual entities).

7.4.17.7 Effects of the local mode

7.4.17.7.1 U-plane

The U-plane is not affected by the local mode and is always relayed. U-plane packets (e.g. I_N voice data, or I_P data) may be normally exchanged during the local mode and during the switching procedures without any change.

7.4.17.7.2 Channel C_S

The channel C_S is affected by the local mode. When in local mode, the C_S channel is routed towards its own local WRS C-plane DLC instance or peer instance at the FP.

7.4.17.7.3 Channel C_F

The channel C_F is affected by the local mode. When in local mode, the C_F channel is routed towards its own local WRS C-plane DLC instance or peer instance at the FP.

7.4.17.7.4 A-field M_T channel signalling

7.4.17.7.4.1 General

Operation of the A-field M_T channel signalling can be impacted by the local mode. However the effect depends on the message, as described in the following clauses.

7.4.17.7.4.2 Messages containing FMID/PMID addresses, including bearer request/confirm messages

Messages containing FMID/PMID addresses, including bearer request messages should be routed to the given addresses, and perform an appropriate action as given by the addresses. Additional actions may result for intermediate nodes (see clauses 7.4.17.2, 7.4.17.3 and 7.4.17.4).

7.4.17.7.4.3 Encryption control messages

Encryption control messages are always local to the segment where they are exchanged. These messages are an exception to the general rule because they are allowed to be exchanged in any segment (including PP to WRS).

NOTE: The message "start encryption with cipher key-index" does not contain FMID/PMID addresses. This message should always be understood as local.

In addition to having a local meaning, the START.GRANT message can also be relayed (see clause 7.7.7). When relayed towards the FP it shall always be relayed irrespective of the state of any intermediate node (WRS).

7.4.17.7.4.4 Quality control messages

See ETSI EN 300 175-3 [3], clause 7.2.5.5. These messages are always local. They can be used to exchange commands between adjacent nodes. They are allowed to be exchanged in any segment (including PP to WRS).

7.4.17.7.4.5 ATTRIBUTES_T_{Req;Cfm}

These messages are affected by the local/relayed mode; however the effect depends on the type of message.

When in any local mode, the Attributes messages shall be exchanged between the FP and the node in local mode. All intermediate nodes shall merely observe and relay the message. The message shall not be further relayed downstream by the target node of local mode.

- Slot type, Service type and max lifetime, impacts to all nodes in the chain (between FP and the local node). Intermediate WRSs (that "observe" the message) shall apply the parameter (without any negotiation capability). The FP shall be in charge of ensuring that any accepted Attributes setting is compatible with the repeaters.
- C_F flag impacts to all nodes in the chain (between FP and the local node). However it shall be understood by the intermediate nodes as C_F "relay only" capability. To set C_F termination capability in an intermediate node, a separate Attributes exchange (in local mode to such node) should be performed.
- ECN impacts the whole chain. Therefore all segments use the same ECN.
- LBN impacts the whole chain. If the LBN is different from the existing one, it changes the LBN to the given value for all nodes in the chain and for the connection that carries the message).
- Parameters for High Level modulation are for further study.

7.4.17.7.4.6 Release

The Release message shall not normally be used in local mode, except in the following circumstances:

- Release message in the Bearer handover procedure executed between the WRS and the FP (or another intermediate WRS), when the WRS is in local mode.
- Exceptional case when transition to full-relayed mode is impossible.

7.4.17.7.4.7 Expedited messages

Expedited messages (e.g. for ULE) are not to be used in local mode.

The possible use of Expedited messages in local mode is for further study.

7.4.17.7.4.8 Escape

Escape message is impacted by the local/relayed mode. It may be used to exchange commands between FP and PP (when in relayed mode) or in between FP and any WRS (when in local mode).

7.4.17.7.4.9 All others

All other M_T messages are for further study.

7.4.17.7.5 B-field MAC control signalling

Operation of B-field MAC control signalling is for further study.

The G_F channel is considered B-field MAC control for this discussion.

7.4.18 C channel operation

7.4.18.1 C_S channel

7.4.18.1.1 General

The WRS and FP shall support C_S channel data transmission and reception as defined in ETSI EN 300 175-3 [3], clauses 10.8.1 and 10.8.1.1.

7.4.18.1.2 C_S channel transparent relay

The WRS shall support the transparent relay of the C_S channel.

7.4.18.1.3 C_S channel end-system operation

The WRS and FP shall support the termination of the C_S channel allowing exchanging of higher layer signalling between the FP and the WRS itself. This operation shall be enabled when the WRS is set in "local mode" as defined in clause 7.4.17.

7.4.18.1.4 C_S channel retransmission and flow control

When relaying C_S channel the WRS shall support channel protection (error detection and automatic retransmission) performing the roles described in ETSI EN 300 175-3 [3] for the transmitting and receiving side in the two relayed segments.

In case of error in the reception (bad A-field CRC), the WRS shall request the retransmission as given in ETSI EN 300 175-3 [3].

In case of error in the transmission of any of the segments (bad Q1/Q2 report), in addition to perform the retransmission, the WRS shall store in a buffer the subsequent received segments. The size of this buffer is implementation choice. If, due to multiple retransmissions, the buffer is approaching its limit, the WRS is allowed to reply to the sending side with a fake Q1/Q2 report in order to control the flow. The code Q1=0/Q2=1 shall be used in order to force an unnecessary retransmission of the incoming C_S channel.

7.4.18.2 C_F channel

7.4.18.2.1 General

The WRS and FP shall support C_F channel data transmission and reception as defined in ETSI EN 300 175-3 [3], clauses 10.8.1 and 10.8.1.2.

For the FP, it is only mandatory to support C_F on links between the FP and a WRS (when in local state with that WRS). An FP may support C_F between the FP and a PP, according to other supported profiles.

7.4.18.2.2 B-field control Multiplexer (E/U-MUX), C_F modes

The WRS and FP shall support E-type mode multiplexer as defined in ETSI EN 300 175-3 [3], clauses 6.2.2.2 and 6.2.2.3, including the modes "E-type all C_F", and "E-type not all C_F" over traffic C/O bearers.

The WRS and FP shall support all E-type modes as defined in ETSI EN 300 175-3 [3], clause 6.2.2.3 (tables 6.24 to 6.33) for the supported D-field mappings and modulation types.

The following modes shall be supported:

- BA = "010"B: E-type, all C_F, packet number 0;
- BA = "011"B: E-type, all C_F, packet number 1;
- BA = "100"B: E-type, not all C_F, packet number 0;
- BA = "101"B: E-type, not all C_F, packet number 1;
- BA = "110" E-type all MAC signalling.

NOTE: The transmission of C_F over the dummy bearer is not allowed.

7.4.18.2.3 C_F channel transparent relay

The WRS shall support the transparent relay of the C_F channel.

7.4.18.2.4 C_F channel end-system operation

The WRS and FP shall support the termination of the C_F channel allowing exchanging of higher layer signalling between the FP and the WRS itself. This operation shall be enabled when the WRS is set in "local mode" as defined in clause 7.4.17.

7.4.18.2.5 C_F channel relay activation

The C_F channel relay function shall be activated upon observation by the WRS of an Mt Attributes exchange between end peers setting the C_F channel attribute bit. The WRS does not participate in the negotiation. There is no need for setting a local mode towards the WRS for setting the rely function.

Once the relay function is active, the end peers may insert C-MUX packets containing the C_F channel at any time (by means of the proper BA bit coding) and the WRS shall be ready to relay the E-MUX mode frames containing C_F packets.

7.4.18.2.6 C_F channel retransmission and flow control

When relaying C_F channel the WRS shall support channel protection (error detection and automatic retransmission) performing the roles described in ETSI EN 300 175-3 [3] for the transmitting and receiving side in the two relayed segments.

In case of error in the reception of any of the segments (bad CRC), in addition to request the retransmission, the WRS shall insert a NULL frame in the relayed segment, until a valid C_F frame is received. The NULL frame shall be built as B-field = "E-type all MAC signalling" and repetition of the MAC B-field command "NULL" (ETSI EN 300 175-3 [3], clause 7.3.3) in all subfields.

In case of error in the transmission of any of the segments (bad Q1/Q2 report), in addition to perform the retransmission, the WRS shall store in a buffer the subsequent received segments. The size of this buffer is implementation choice. If, due to multiple retransmissions, the buffer is approaching its limit, the WRS is allowed to reply to the sending side with a fake Q1/Q2 report in order to control the flow. The code Q1=1/Q2=0 shall be used in order to force an unnecessary retransmission of the incoming C_F channel.

7.4.18.2.7 C_F channel end-system specific WRS procedures: activation

The WRS and FP shall support the termination of the C_F channel (end-system). This mode shall operate only when the WRS is in local mode.

The activation of the end-system mode requires a previous setting of the service by the FP. This shall be done by exchanging a pair of M_T ATTRIBUTES messages when in local mode to the target WRS and with the C_F flag activated. Once this has been done, the C_F channel towards a WRS may be sent simply setting MAC local mode towards such WRS.

Refer to clause 7.4.17 for the setting and operation of the local mode towards the WRS.

7.4.18.2.8 C_F channel end-system specific WRS procedures: single LAPC instance and coordination with C_S channel

The WRS is assumed to have only one DLC C-plane instance to be used in local mode. An equivalent instance (the "peer" instance) is assumed to exist at the FP. The FP shall support one instance of the DLC C-plane per CRFP user. Both channels C_S and C_F shall share these DLC C-plane instances.

Channel C_S shall remain open when the C_F channel is activated. In order to ensure correct operation, channels C_S and C_F shall not be used at the same time and both peers (FP and WRS) shall wait until complete transmission of a message in any of the channels before attempting to use the other.

If, by errors or abnormal operation, the LAPC receives a first segment in one of the channels, while a partial received message over the other channel is still in buffer, then the partial received message should be discarded and should start the processing of the new one.

Unless specifically stated in the present document, the WRS shall use for replying to any NWK layer operation initiated by the FP, the same channel chosen by the FP to transport it.

7.4.19 ULE C/L procedures

7.4.19.1 ULE Dummy bearer operation: general

The WRS shall behave as a ULE PP for the purpose of receiving the ULE dummy bearer transmitted from the upper node (FP or another WRS) and shall behave as a FP for the purpose of generating a new ULE dummy bearer content to be broadcasted downstream (to PP or further WRS).

The generation of the different ULE dummy bearer channels to be broadcasted by the WRS is described in clauses 7.4.19.2 to 7.4.19.4.

For moving dummy bearer position (to a new slot and carrier), the WRS shall behave as a FP.

The WRS shall only behave as an ULE FP and shall only broadcast the ULE dummy bearer when it is attached to a ULE FP. Otherwise, it shall not broadcast the ULE dummy bearer channels.

7.4.19.2 ULE Dummy bearer generation: subfield B0 fields and N_C channel

All fields in subfield B0 shall be freshly generated by the WRS as if it were a FP. The N_C channel (split into subfields B0 and B1) shall contain the RFPI of the WRS.

7.4.19.3 ULE Dummy bearer generation; paging channel P_U and paging related fields: HN, CA, SFa, SFb

The paging channel P_U that is transmitted on subfield B1 (part) and on subfield B3 (complete) shall be transparently related by the WRS. However, it shall be delayed by one frame in all cases and irrespective of dummy bearer slot positions.

SFa, SFb and CA fields (subfield B1) shall be transparently relayed by the WRS, however delayed by one frame in all cases and irrespective of dummy bearer slot positions.

EXAMPLE: If received dummy is on slot 1 and WRS generated dummy is on slot 3, even if it were possible to transparently relay the content between dummies in the same frame, the WRS should relay the content received in frame n (slot 1) to frame n+1 (slot 3).

If subfield B1 is in index format, the WRS shall observe the bit 143 and, if set to "1", shall also observe the bit 142 and the index X4 sent on bits 133 to 141. All these bits shall be handled as described in clause 7.4.19.8 "C/L multicast procedures: multicast channel over additional C/L bearers".

If bit 143 is set to "0", the WRS does not need any special handling of these bits and they shall be transparently relayed as the rest of the paging channel.

If the WRS does not support the procedure "C/L multicast procedures: multicast channel over additional C/L bearers" (clause 7.4.19.8), and bit 143 has been received as set to "1", then the WRS shall set this bit (143) and bit 142 to "0" and bits 133 to 141 to "1".

If subfield B3 is in index format, the WRS shall observe the bit 303 and, if set to "1", shall also observe the bit 302 and the index X10 sent on bits 293 to 301. All these bits shall be handled as described in clause 7.4.19.8 "C/L multicast procedures: multicast channel over additional C/L bearers".

If bit 303 is set to "0", the WRS does not need any special handling of these bits and they shall be transparently relayed as the rest of the paging channel.

If the WRS does not support the procedure "C/L multicast procedures: multicast channel over additional C/L bearers" (clause 7.4.19.8), and bit 303 has been received as set to "1", then the WRS shall set this bit (303) and bit 302 to "0" and bits 293 to 301 to "1".

Field HN (Hop number, subfield B1) shall be newly generated by adding 1 to the value received by the WRS from the node to which it is attached (FP or other WRS). The equation shall be as follows:

transmitted HN = received HN + 1.

NOTE: A true FP always broadcast HN = 0

7.4.19.4 ULE Dummy bearer generation: subfield B2 fields: channels Q_U and M_U

All subfield B2 fields shall be freshly generated by the WRS. Channel Q_U (slot number, PSCN, frame counter, multi-frame counter) shall be generated by the WRS based on the position of the downlink dummy bearer slot. Frame and multi-frame counters are aligned with the FP.

RF control bits (RF1 and RF2) fields shall be set and coded as follows:

- RFC1 bit shall be set by the WRS (as if it were a FP) as described in ETSI TS 102 939-2 [13], clause 10.1.1 "Quiet Channel Indication"
- RFC2 bit is intended for systems for operation in Japan. If this is the case, it shall be set as described in ETSI TS 102 939-2 [13], clause 10.1.2 "PHS Detection Indication". Otherwise it shall be set to "0".

Channel M_U (channel selection data) shall be freshly generated by the WRS based on its own observation of available slots and measured RSSI. The WRS shall behave as an RFP for this generation. It shall not relay the received channel M_U info.

7.4.19.5 B-field paging addressed to a WRS

WRSs does not need to support B-field paging (ULE paging) detection other than the handing of indices X4 and X10 as described in clause 7.4.19.3. There is no ULE paging addressed to WRSs (see note).

NOTE: Unless the WRS implements at the same time a ULE terminal (PP) device.

7.4.19.6 C/L multicast procedures: general

The WRS shall support the transparent relay of downlink multicast transmissions. These transmissions may happen over the dummy bearer or over additional dummy bearers.

7.4.19.7 C/L multicast procedures: multicast channel over the dummy bearer

For multicast transmissions over the dummy bearer, the WRS shall support:

- Transparent relay of the paging channel P_U as described in clause 7.4.19.3. This also relays any "announcement of multicast". No special provision is needed.
- Relay of the C/L downlink U-plane frames sent over the dummy. These frames are identified by the BA bits in A-field coded indicating "SIP" (see ETSI EN 300 175-3 [3], clause 9.1.4.1). The WRS shall transparently relay such frames delayed always by 1 frame (irrespective of slot positions) and with "SIP" coding in the BA bits.
- Since WRS and FP are aligned in frame and multi-frame counters, the multiplexing cycle described in ETSI TS 102 939-2 [13], clause 10.5.2.1 is always delayed by one frame by each WRS in the chain. This means that a WRS relay station directly attached to a FP will broadcast the C/L U-plane frames in frames 2, 6, 10 and 14. A second WRS will do that in frames 3, 7, 11 and 15, and so on. The PP (and any other WRS located at downside) may know the delay by means of the observation of the bits HN (hop number) in subfield B1.

7.4.19.8 C/L multicast procedures: multicast channel over additional C/L bearers

7.4.19.8.1 General

For multicast transmissions over the dummy bearer, the WRS shall support:

- Transparent relay of the paging channel P_U as described in clause 7.4.19.3. This also relays any "announcement of multicast". No special provision is needed.
- Handling of bits 133 to 143 (B1) and 293 to 303 (B3) as follows:
  - The WRS shall understand that there will be a C/L transmission over additional bearers (on next frame) when either subfield B1 is in index format and bit 143 is set to "1" and/or subfield B3 is in index format and bit 303 is set to "1",

- If this happens, the WRS shall decode the position of the C/L bearer by means of index X4 and bit 142 or index X10 and bit 302 (see ETSI TS 102 939-2 [13], clause 10.6.2.5.4 "Coding of additional C/L bearer position").

- Only one C/L transmission over an additional bearer on the same frame needs to be supported. Therefore if bits 143 and 303 are both coded to "1", the position information sent on X4 and X10 should be the same.

- After detection of a C/L downlink transmission the WRS shall be ready to transmit a new C/L bearer on frame N+2. To do that, it shall initiate the channel selection procedures described in ETSI TS 102 939-2 [13], clause 10.5.3.1 "Channel selection and transmission start"). The WRS should be ready to send the C/L frame containing the U-plane packet on frame N+2.

- As described in ETSI TS 102 939-2 [13], clause 10.5.3.1, the WRS has the choice to start the C/L transmission on frame N+1, but the packet containing the useful U-plane data has to be sent on frame N+2.

- In any case, the decision on channel selection should be ready before broadcasting the dummy bearer in frame N+1.

- In frame N+1, the WRS has to relay the received P_U channel. The indices X4 and/or X10 (and associated bits 142 and 302) shall be recoded indicating the selected slot/carrier intended for the C/L transmission.

- The WRS shall receive the C/L transmission on frame N+1, over the slot/carrier received from previous node) and shall transparent relay such transmission on frame N+2 using the newly selected slot/carrier.

- Delay shall always be 1 frame irrespective or slot positions.

- The content of the transmitted frame shall be identical to the received one, including BA bit coding ("SI_P") and B-field content. A-field tail content shall be as given in ETSI TS 102 939-2 [13], clauses 10.5.3.2 and 10.5.3.3 "MAC signalling in the additional C/L downlink bearer".

- Continuation of the C/L downlink over several frames may happen and shall be supported (see ETSI TS 102 939-2 [13], clause 10.5.3.3).

7.4.19.8.2 Error handling

If the WRS is unable to receive correctly the C/L transmission, it shall send nothing (no transmission energy) downstream.

7.4.20 Downlink broadcast

7.4.20.1 N_T message

The CRFP shall be able to receive, process and transmit the N_T message as defined in table 16.

Table 16: Nt message

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	-

7.4.20.2 Q_T - static system information (Q_H = 0)

The CRFP shall be able to receive, process and transmit the Q_T message as defined in table 17.

Table 17: Qt static system information message

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
<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

7.4.20.3 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 table 18.

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 18: Qt extended RF carrier information message

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

7.4.20.4 Q_T - FP capabilities (Q_H = 3), extended FP capabilities (Q_H = 4) and extended FP capabilities part 2(Q_H = 12)

The requirements are defined in clause 7.4.4.

Higher layer broadcast contents are defined in clause 7.6.7.

7.4.20.5 Q_T - SARI support (Q_H = 5)

The CRFP shall be able to receive, process and transmit the Q_T message as defined in table 19.

The CRFP shall transmit the Q_t -SARI support only if the FP sends it.

Table 19: Qt SARI support message

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 cannot be guaranteed by GAP CRFP
<Black yes/no>	All	Copy from RFP	-
<ARI or black-ARI>	All	Copy from RFP	-

7.4.20.6 Q_T - Multiframe number (Q_H = 6)

The CRFP shall be able to receive, process and transmit the Q_T message as defined in table 20.

The CRFP shall transmit the Q_t-multiframe number only if the FP sends it.

Table 20: Qt multi-frame number message

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	-

7.4.21 A-field paging broadcast

7.4.21.1 Short page, normal/extended paging

The CRFP shall be able to receive, process and transmit the Pt message as defined in table 21.

The B_S data shall also be delivered to the DLC layer as a MAC_PAGE-ind primitive via the MA-SAP.

NOTE: Page messages directed towards the WRS itself are handled by the higher layers, and can result in the establishment of a link (by indirect link establishment procedures). This may be required for various WRS maintenance procedures.

Table 21: Pt short page message

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 CRFP shall send out its local blind slot information (as defined in clause 10.3.3 of ETSI EN 300 444 [9]) 2: other bearer and 5: dummy or C/L bearer position CRFP shall send out corresponding local bearer positions 9: bearer handover information CRFP shall copy the "info type" received from the RFP

7.4.21.2 Zero-length page, normal/extended paging

The CRFP shall be able to receive, process and transmit the Pt message as defined in table 22.

Table 22: Pt zero-length page message

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 CRFP shall send out its local blind slot information (as defined in clause 10.3.3 of ETSI EN 300 444 [9]) 2: other bearer and 5: dummy or C/L bearer position CRFP shall send out corresponding local bearer positions 9: bearer handover information CRFP shall copy the "info type" received from the RFP

7.5 DLC procedures

7.5.1 General

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

7.5.2 DLC variables

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

7.5.3 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 ETSI 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).

6) This handover is a combination of 2) and 3).

7.5.4 Lc frame delimiting and sequencing service

7.5.4.1 General

7.5.4.2 C_S channel fragmentation and recombination

The procedure shall be performed as defined in ETSI EN 300 175-4 [4], clauses 6.1.2, 6.1.3, 6.1.4 and 6.1.4.2. The complete frame shall be fragmented into 5 octet fragments.

7.5.4.3 C_F channel fragmentation and recombination

The C_F channel shall be operated according to the procedures defined in ETSI EN 300 175-4 [4], clauses 6.1.2, 6.1.3, 6.1.4 and 6.1.4.1. The complete frame shall be fragmented into 8 octet fragments.

7.5.4.4 Selection of logical channels (C_S and C_F)

The selection of the C_F instead of the CS channel for Lc operation, shall be done according to the conditions defined in ETSI EN 300 175-4 [4], clause 10.2.5.

7.5.5 Class A link establishment

The procedure shall be performed as defined in ETSI EN 300 444 [9], clause 9.1, with the following additions/modifications.

Class A link establishment consists of an exchange of messages to initialize the link. The initiating side sends an I-frame with the New Link Flag (NLF) set and the peer responds with an RR response frame.

For the special cases of a dual C/O bearer establishment (see clauses 7.4.10.5 and 7.4.10.6) and CRFP connection suspend and resume (see clause 7.4.11), this initial exchange of messages shall be omitted in order to reduce the time taken to establish the link. In these cases (and only in these cases) the following procedure for link establishment applies:

- The initiating side shall not send the initial I-frame with NLF set.
- The peer will not send the RR response frame - since there was no initial message to respond to.
- The initiating side shall initialize the LAPC associated with this MAC connection as follows:
  - The class A sequence variables V(S), V(R) and V(A) shall be set to "0".
  - The entity shall clear all existing exception conditions and reset the retransmission counter.
  - The timer <DL.07> shall not be started.
  - The entity shall enter the class A established state. This is reported to the higher layers (by a DL_ESTABLISH-cfm primitive).
- The peer side shall initialize the LAPC associated with this MAC connection as follows:
  - The class A sequence variables V(S) and V(A) to "0", the class A sequence variable V(R) to "1"
  - The entity shall clear all existing exception conditions and reset the retransmission counter.
  - The timer <DL.07> shall not be started.

- The entity shall enter the class A established state. This is reported to the higher layers (by a DL_ESTABLISH-ind primitive).

NOTE: The procedure outlined above only applies for the link establishment in these special cases. Once the link has been established, the operation continues according to the normal rules and procedures.

7.6 NWK procedures

7.6.1 General

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

7.6.2 Over-the-air maintenance

7.6.2.1 General

For various maintenance tasks, the WRS may use the Operation, Administration and Maintenance (OA&M) information transfer service. This service uses the <<IWU-TO-IWU>> information element (see ETSI EN 300 175-5 [5], clause 7.7.23) with specific content in NWK layer messages. This information 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.

7.6.2.2 Retrieval of WRS RPN

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clause 13.7, parameter retrieval initiated by PT, with the additions/modifications as defined in this clause (including Figure 26 and tables 23 and 24).

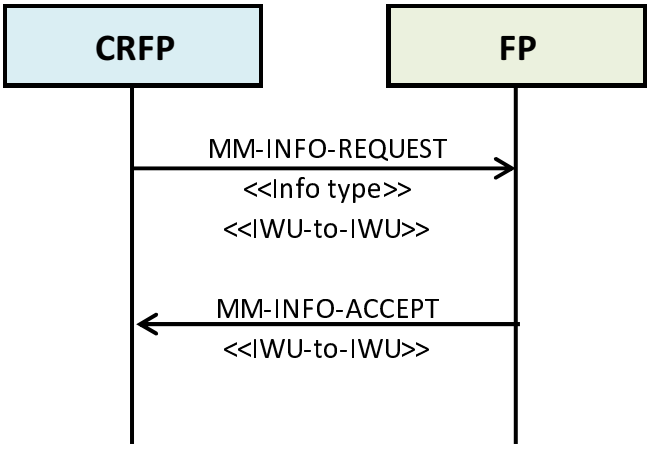

Figure 26: Retrieval of WRS RPN

Table 23: 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 24: 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

7.6.2.3 Indication/modification of WRS RPN

The procedure shall be performed as defined in ETSI EN 300 175-5 [5], clause 13.7, parameter retrieval initiated by FT, with the additions/modifications as defined in this clause (including Figure 27 and table 25).

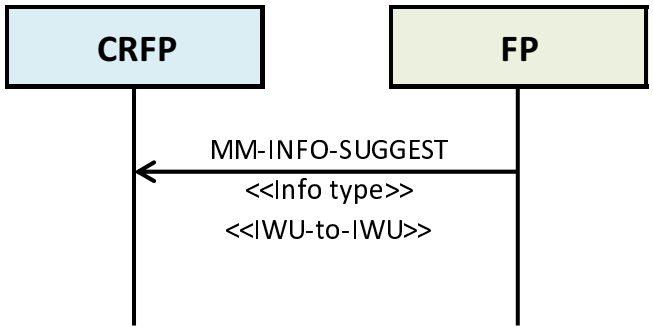

Figure 27: Indication/modification of WRS RPN

Table 25: 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

7.6.3 Identities and addressing

A WRS shall comply with the general FT identities requirements for RFPs. 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 shall have additional specific PT identities when PT DLC and NWK layer functionality is included.

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 ETSI 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 shall define one IPUI of the available ones, which shall be used for over-the-air maintenance procedures. The FT may use other IPUIs of the CRFP to derive Derived Cipher Key (DCK) from a User Authentication Key (UAK).

7.6.4 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 26 into the CRFP during the subscription process. 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 26: 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)	M	All	See note.
UAK/AC (1..n)	M	All	See note.
NOTE: The number "n" is the number of CRFP users, which is the maximum supported number of simultaneous connections from the CRFP that require higher layer control in the CRFP.			

7.6.5 Obtaining access rights for WRS

The procedure as defined in clause 8.30 of ETSI EN 300 444 [9] applies with the additions/modifications as defined in this clause (including Figure 28 and table 27).

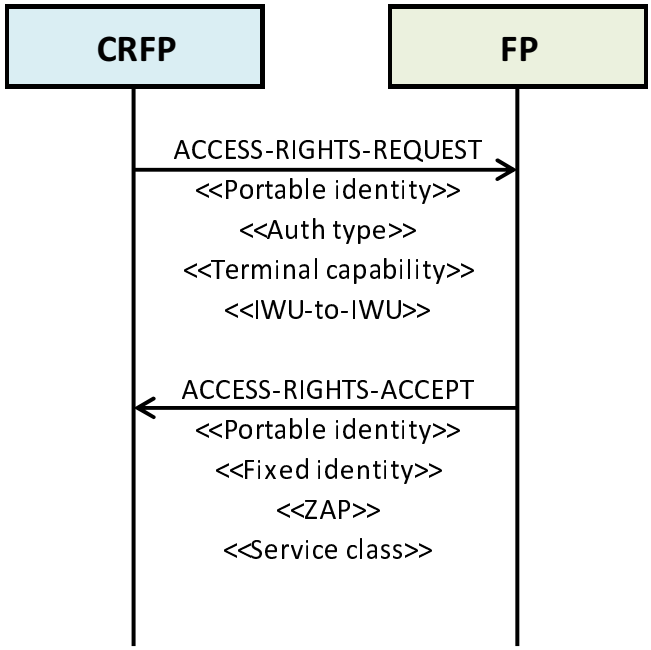

Figure 28: Obtaining access rights for WRSTable 27: Additions/modification to the {ACCESS-RIGHTS-REQUEST} message

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>	'xxxxx0x'	Bit 2 set to 1 indicates that device is a "V1 WRS". A WRS supporting the present document shall have this bet set to 0. See note.
	<Profile_Indicator_4>	All	
	<Profile_Indicator_5>	All	
	<Profile_Indicator_6>	All	
	<Profile_Indicator_7>	All	
	<Profile_Indicator_8>	All	
	<Profile_Indicator_9>	All	
	<Profile_Indicator_10>	'xxX1xxx'	Bit 4 set to 1 indicates that this device is a "V2 WRS". See note. Bit 5 set to 1 indicates that the WRS supports relay of ULE C/L Downlink on additional bearers (see ETSI TS 102 939-2 [13])
	<Control codes>	All	
<<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 reattempt the procedure with the same subscription number
NOTE: The present document underwent a major overhaul for revision 2.1.1, including the definition and modification of several features. In order to address compatibility and interoperability issues and to distinguish between support of "V1" repeaters (i.e. before revision 2.1.1) and "V2" repeaters (i.e. revision 2.1.1 or later), a capability bit was introduced into the <<Terminal Capabilities>> Information Element.			

7.6.6 Location registration for WRS

The procedure as defined in clause 8.28 of ETSI EN 300 444 [9] applies with the additions/modifications as defined in this clause (including Figure 29 and table 28).

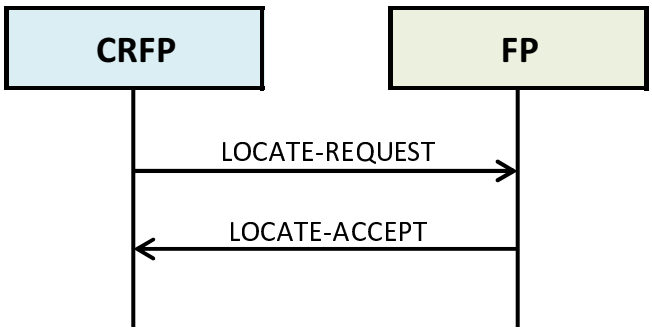

Figure 29: Location registration for WRS

Table 28: Additions/modification to the {LOCATE-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>	'xxxxx0x'	Bit 2 set to 1 indicates that device is a "V1 WRS". A WRS supporting the present document shall have this bet set to 0. See note.
	<Profile_Indicator_4>	All	
	<Profile_Indicator_5>	All	
	<Profile_Indicator_6>	All	
	<Profile_Indicator_7>	All	
	<Profile_Indicator_8>	All	
	<Profile_Indicator_9>	All	
	<Profile_Indicator_10>	'xxX1xxx'	Bit 4 set to 1 indicates that this device is a "V2 WRS". See note. Bit 5 set to 1 indicates that the WRS supports relay of ULE C/L Downlink on additional bearers (see ETSI TS 102 939-2 [13])
	<Control codes>	All	
NOTE: The present document underwent a major overhaul for revision 2.1.1, including the definition and modification of several features. In order to address compatibility and interoperability issues and to distinguish between support of "V1" repeaters (i.e. before revision 2.1.1) and "V2" repeaters (i.e. revision 2.1.1 or later), a capability bit was introduced into the <<Terminal Capabilities>> Information Element.			

At the CRFP:

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

At the FP:

FPs that support CRFP defined by the present document shall also support Location Registration for WRS and shall always use this procedure with the CRFP initiated location registration.

7.6.7 Higher layer information FP broadcast

The Higher Layer Information component of these messages shall be coded as follows:

Any bit shall be coded as the logical product (AND) of the received value and the capability of the WRS to support the feature.

NOTE 1: For bits corresponding to features mandatory to support by the present document, this is equivalent to relying the bit.

NOTE 2: Bit a35 in extended higher layer information (part 2) for "no-emission mode" is always set to '0'.

NOTE 3: Bit a44 in extended higher layer information (part 2) for "DSC2" is coded following the general rule. This means that DSC2 can only be used if both, the repeater and the FP support it. Additionally, in the case of chains of repeaters, all preceding nodes should support it.

7.7 Security procedures

7.7.1 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 ETSI 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 30 shows the protocol diagram for the CRFP supporting encryption on these relayed connections.

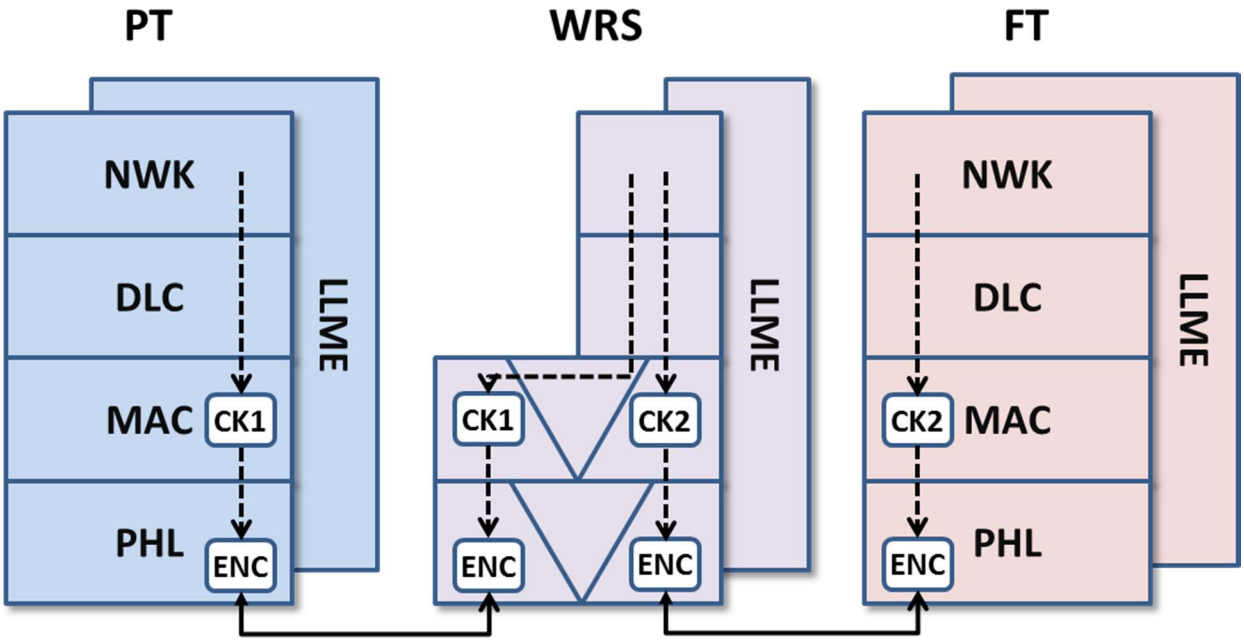

Figure 30: Protocol stack for encryption

Figure 30 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 clause 7.7.4 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.

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.

Figure 16 and Figure 31 show typical examples of the procedure for basic connections.

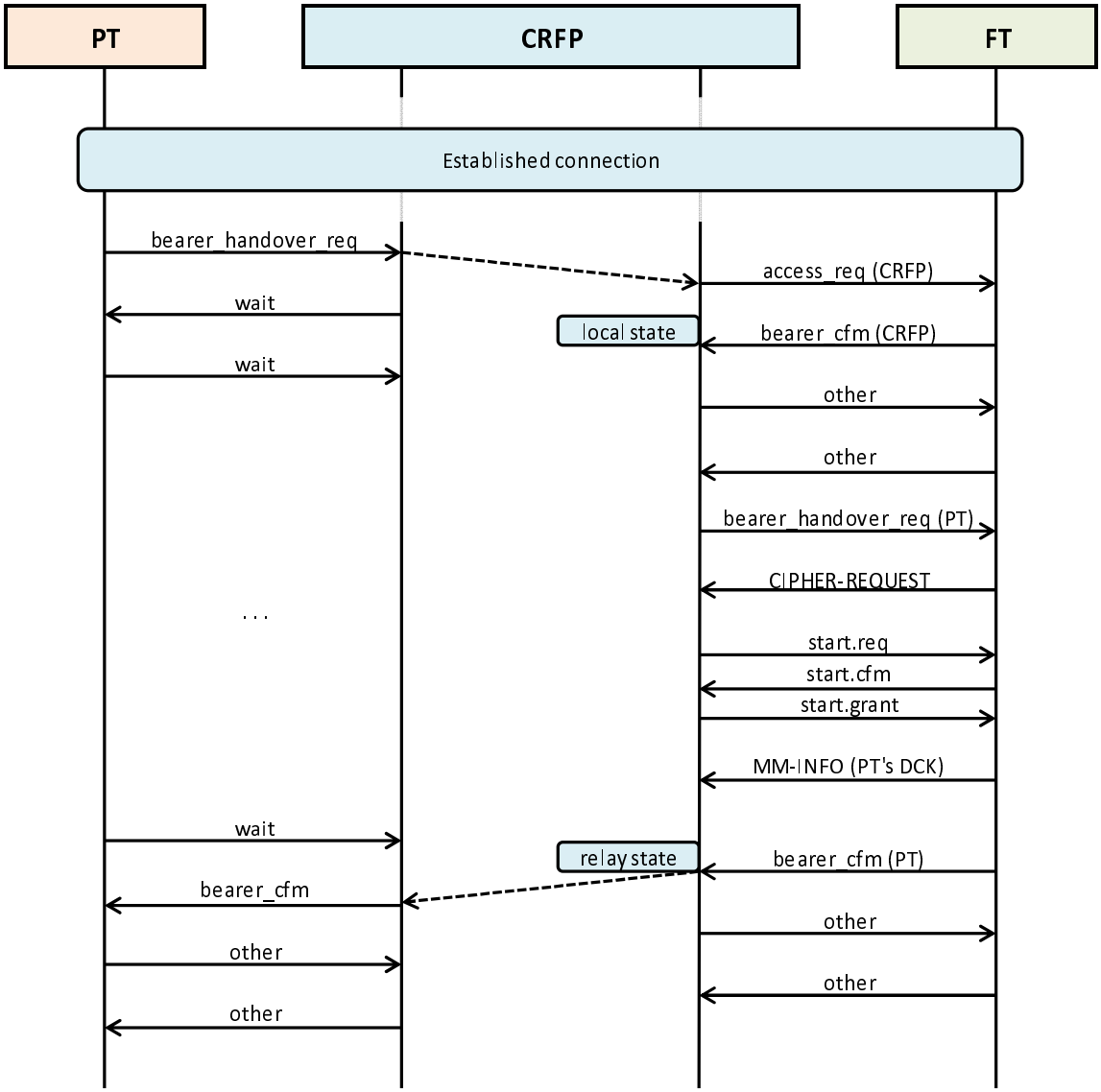

Figure 31: Bearer handover from a RFP to CRFP (dual setup with encryption)

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.

The procedure for advanced connections is very similar to the basic connection, except for the use of the equivalent advanced connection control set of messages, and the requirement to exchange the ATTRIBUTES_T request/confirm messages in accordance with ETSI EN 300 175-3 [3], clause 10.5.1.2.

7.7.2 CRFP initialization of PT cipher key

The FT shall initiate ciphering between FT and the CRFP that requires a PT CK using {CIPHER-REQUEST} message with the CRFP's CK.

The CRFP is often allocated its DCK during the access rights (7.6.5) and/or location registration (see clause 7.6.6) procedures. However, a fresh DCK may also be generated by an authentication procedure (see ETSI EN 300 444 [9], clause 8.27) prior to sending the {CIPHER-REQUEST}.

When the connection between the FT and the destination CRFP is completely ciphered (as indicated by the reception of START.GRANT message), the FT sends the PT CK to the CRFP_PT using the {MM-INFO-SUGGEST} message (see clause 7.7.4).

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 might be the CRFP_PT of a relayed CRFP setup or handover.

7.7.3 Management for encryption of relayed connections

In order to support encryption of relayed connections, the CRFP shall obtain access rights with the FP. It shall do this according to the procedures described in clause 7.8.1.

7.7.4 Indication of cipher key

The Indication of cipher key 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 ETSI EN 300 175-5 [5], clause 13.7, with the additions/modifications as defined in this clause (including Figure 32 and table 29).

Prior to the cipher key transfer, the FP shall ensure that the link to the CRFP is switched to local mode. Upon completion of the cipher key transfer procedure, and assuming there are no other NWK layer procedures to be conducted in local mode, the FP shall switch the link back to relayed mode. See clauses 7.4.11 and 7.4.17.

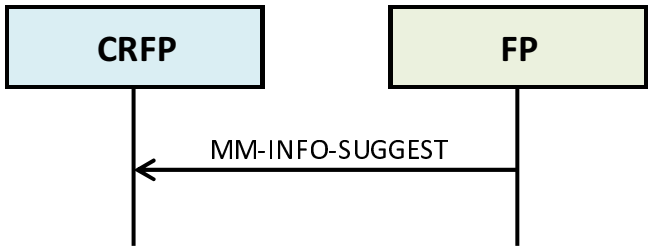

Figure 32: Indication of WRS cipher key

Table 29: Values used within the {MM-INFO-SUGGEST} message

Information element	Field within the information element	Standard values within the field/IE	Normative action/comment
<<Info-type>>			
	<ext>	0	
	<Parameter type>	0100010'B	CK transfer
<<KEY>>			
	<Key type>	10010000 10010001 10010010 10010011	DCK for DSC DCK for DSC2 Default Cipher Key for DSC Default Cipher Key for DSC2
	<Key>	Any	In the case of Default Cipher Key (<Key type> 10010010'B or 10010011'B) the <Key> data field also includes the associated Default Cipher Key Index. See ETSI EN 300 175-5 [5], clause 7.7.24.

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

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

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

7.7.5 Enhanced security procedures

7.7.5.1 Re-keying

7.7.5.1.1 General

Re-keying provides a mechanism to change the cipher key during an ongoing call. This involves a combination of MAC and NWK procedures.

Re-keying shall be used to periodically re-key an already encrypted connection, as well as to re-cipher a connection that was started using Early Encryption, in order to provide improved security.

NOTE: The underlying aim of re-keying is to minimize the exposure and use of a cipher key, in order to mitigate the threat of brute-force attacks for recovering the cipher key. Each key can be considered to have an "age" which starts aging as soon as the key is first exposed/used. "Fresh" keys are those that have a very low age, i.e. not exposed/used for very long at all.

7.7.5.1.2 MAC Re-keying

The MAC procedure for re-keying shall be performed as specified in ETSI EN 300 175-7 [7], clause 6.4.6.5.

This procedure is used for both the upper segment (i.e. between FT and WRS) and the lower segment (i.e. between WRS and PT). In the case of chained repeaters, the FT or PT could include the FT or PT component of another WRS.

NOTE: The associated NWK procedures ensure that the appropriate cipher key is available prior to activation of the MAC procedure.

7.7.5.1.3 NWK Re-keying

The NWK procedure for re-keying shall be performed as specified in ETSI EN 300 444 [9], clause 8.45.2, with the following additions and modifications.

At the FP:

The FP is responsible for initiating the re-keying procedure for the connections of all components (PPs and WRSs) within its system at an appropriate frequency, fulfilling the requirement given in ETSI EN 300 444 [9], clause 8.45.2.

NOTE: ETSI EN 300 444 [9], clause 8.45.2 specifies that the time between successive {AUTHENTICATION-REQUEST} messages should be less than the timer <MM_re-keying.1> (the value of which is defined in ETSI EN 300 175-5 [5], clause A.5).

The FP shall take into consideration the possible delays caused by any repeater, or chain of repeaters, when scheduling the frequency of re-keying operations, as well as the additional requirements in this clause, in order to meet aforementioned <MM_re-keying.1> requirement.

Prior to issuing the {CIPHER-REQUEST} message to a PT as part of the re-keying procedure, the FP shall provide that PT's new cipher key to the WRS, by using the Indication of cipher key procedure (clause 7.7.4). In the case of chained repeaters, the PT could also be the PT component of another WRS.

In order to provide the best possible security, the Indication of cipher key procedure (clause 7.7.4) shall be performed on a freshly ciphered connection, at least fulfilling the criteria given by ETSI EN 300 444 [9], clause 8.45.2 (and if possible better). It is therefore recommended to re-key the WRS before re-keying the PP. In the case of chained repeaters, it is recommended to re-key the WRSs in order of their closeness to the FP, i.e. closest WRS is re-keyed first, then the next closest WRS, and so on, and finally the PP.

For the purposes of the timer <MM_re-keying.1>, the following additional rule shall apply:

- When a cipher key is transferred using the Indication of cipher key procedure (clause 7.7.4) it shall be considered that this key has an initial age equal to the age of the key that was used to cipher the link used by the procedure. The key shall continue aging immediately after this point.

EXAMPLE: If a PT's cipher key is transferred using the Indication of cipher key procedure on a ciphered link whose key is already 15 seconds old, then the transferred key has an initial age of 15 seconds, and will continue to age immediately.

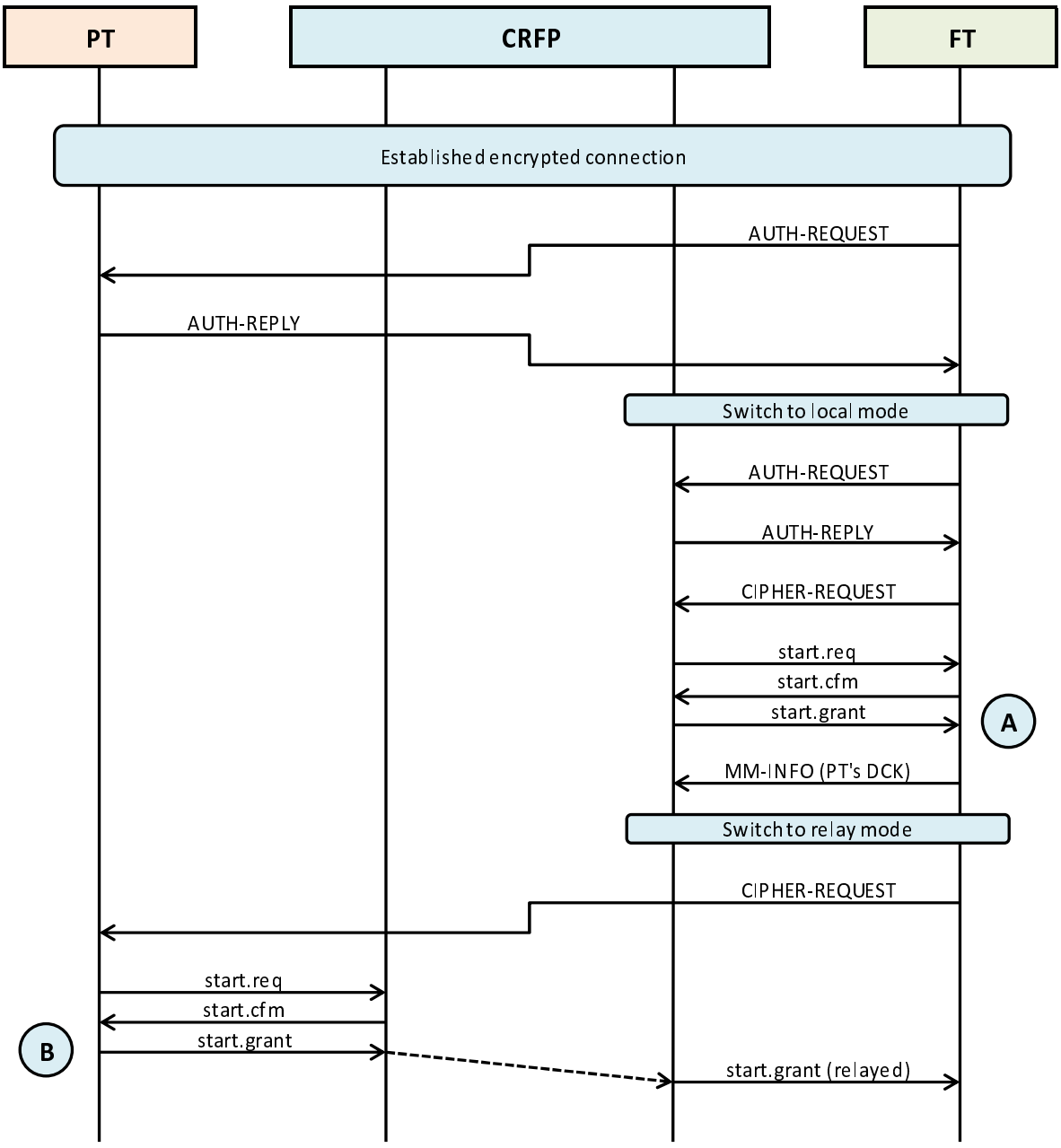

Figure 33: Re-keying scenario

The diagram in Figure 33 shows a typical re-keying scenario involving a single WRS and a PP. The point marked "A" shows the completion of the re-keying of the upper segment (FP-WRS link), and the point marked "B" shows the completion of the re-keying of the lower segment (WRS-PP link).

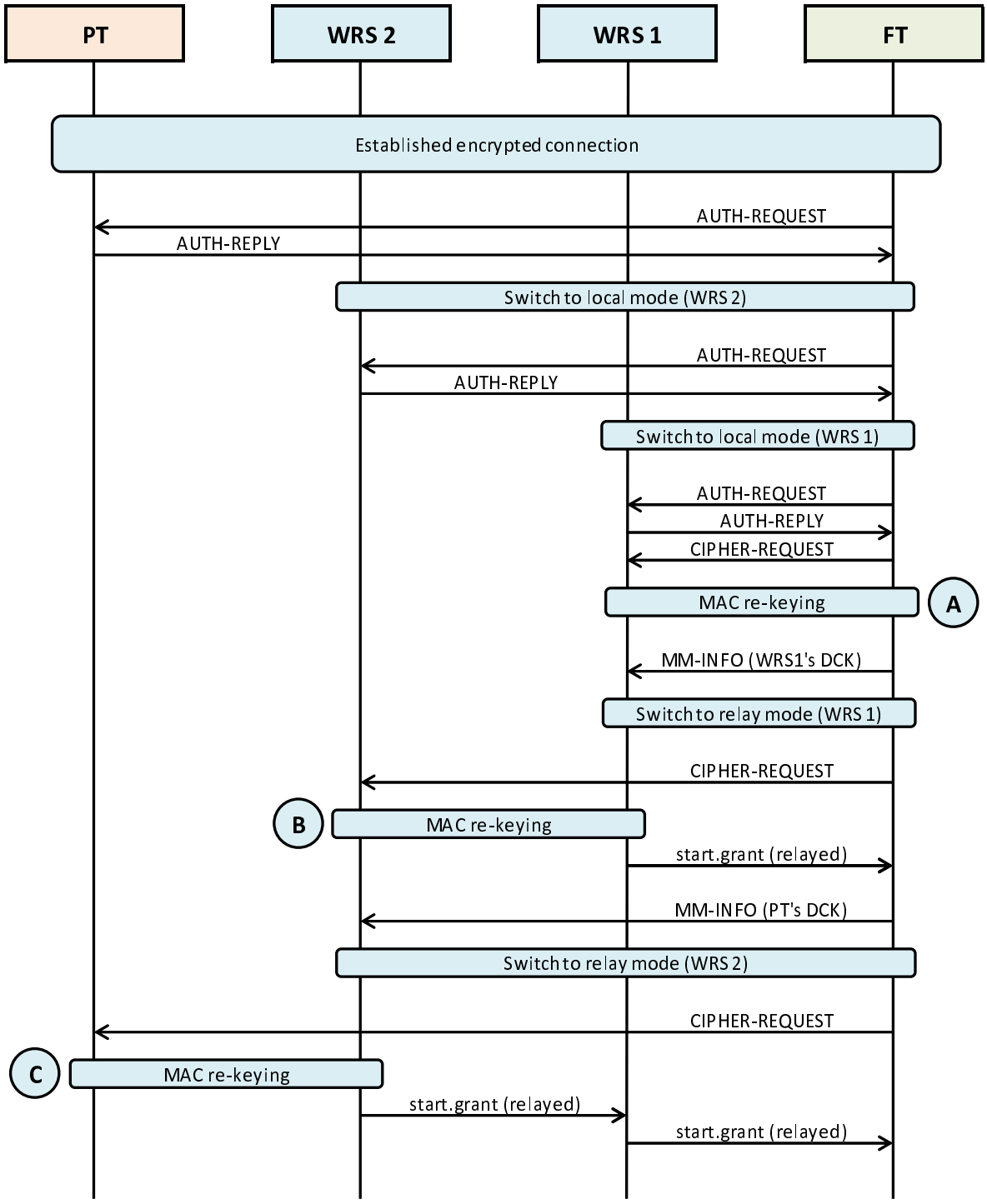

Figure 34: Re-keying of repeater chain

The diagram in Figure 34 shows a typical re-keying scenario involving two WRSs and a PP. The point marked "A" shows the completion of the re-keying of the upper segment (FP-WRS1 link), the point marked "B" shows the completion of the re-keying of the middle segment (WRS1-WRS2 link), and the point marked "C" shows the completion of the re-keying of the lower segment (WRS2-PP link).

7.7.5.2 Early Encryption

7.7.5.2.1 General

Early Encryption provides a mechanism to activate encryption immediately after connection establishment at MAC layer.

This involves a combination of MAC and NWK procedures.

The early encryption of the upper segment (i.e. between FT and WRS) and the lower segment (i.e. between WRS and PT) is handled independently, and the process of obtaining the keys for each segment is fundamentally different. In the following clauses the term "upper segment key" refers to the key used on the upper segment, and the term "lower segment key" refers to key used on the lower segment.

7.7.5.2.2 MAC Early Encryption

The MAC procedure for early encryption shall be performed as specified in ETSI EN 300 175-7 [7], clause 6.4.6, with the following additions and modifications.

This procedure is used for both the upper segment (i.e. between FT and WRS) and the lower segment (i.e. between WRS and PT). In the case of chained repeaters, the FT or PT could include the FT or PT component of another WRS.

NOTE: The associated NWK procedures ensure that the appropriate cipher key is available prior to activation of the MAC procedure.

Early encryption of upper segment (i.e. between WRS and FT):

The WRS shall only attempt to activate early encryption on the upper segment if it is supported by the FT (as indicated by the "Extended Fixed Part Capabilities (part 2)" message bit a42, see ETSI EN 300 175-5 [5], clause F.3), and if the WRS has one or more valid Default Cipher Keys assigned for the upper segment.

The WRS may use any one of its assigned upper segment keys, for early encryption.

If the FT rejects the WRS's attempt to activate early encryption on the upper segment, then the connection will continue in clear mode (see ETSI EN 300 175-7 [7], clause 6.4.6). The WRS may attempt to activate encryption at a later stage (after a suitable encryption key has been assigned).

Figure 35 shows an early encryption scenario for the upper segment.

Early encryption of lower segment (i.e. between WRS and PT):

If the PT attempts to activate early encryption on the lower segment with a Default Cipher Key index that is unknown to the WRS, then the WRS shall reject the encryption attempt by responding with a START.REJECT message (see ETSI EN 300 175-7 [7], clause 6.4.6). The connection shall continue in clear mode. The PT may attempt to activate encryption at a later stage (after a suitable encryption key has been assigned).

Figure 36 shows an early encryption scenario for the lower segment.

Figure 37 shows another early encryption attempt for the lower segment. In this example, the attempt has been rejected by the WRS (presumably because the requested DefCK was not available).

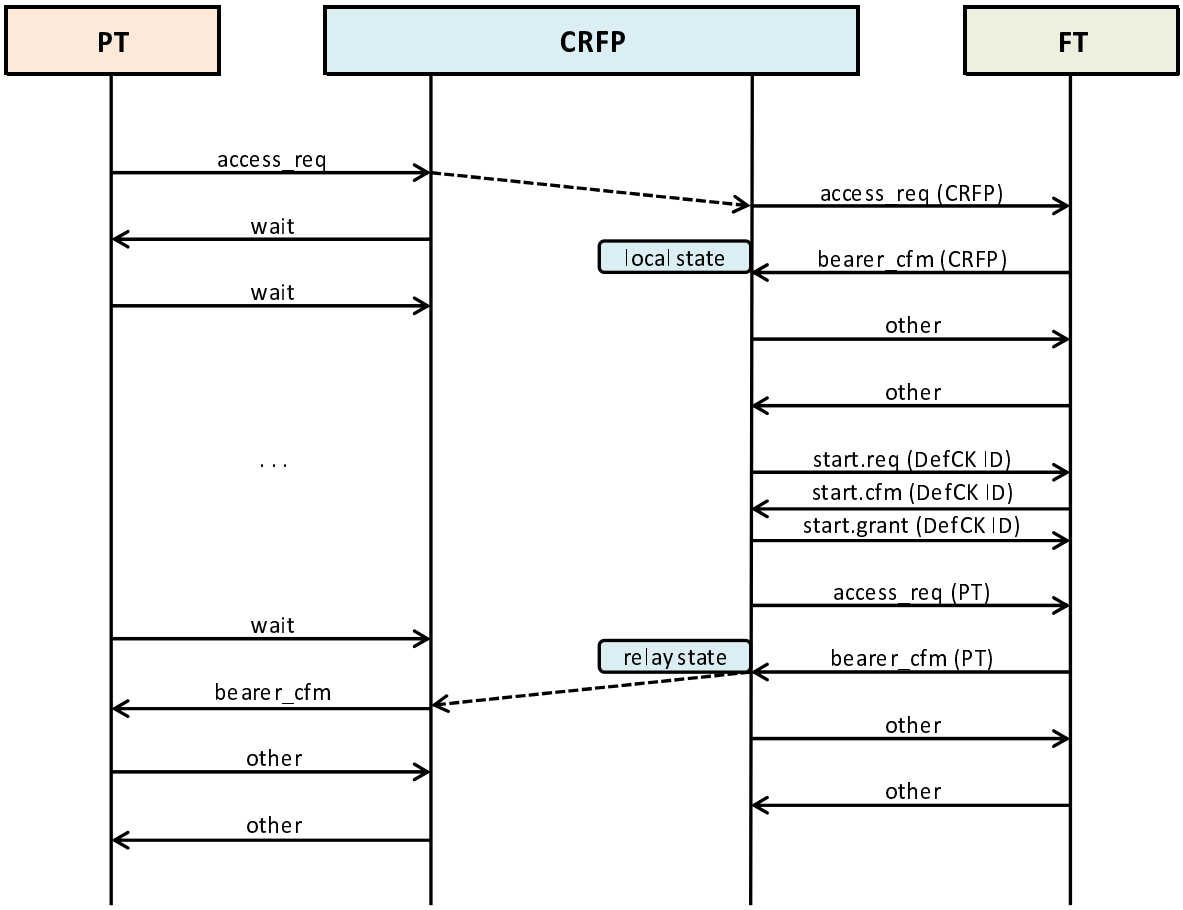

Figure 35: Early encryption on upper-segment

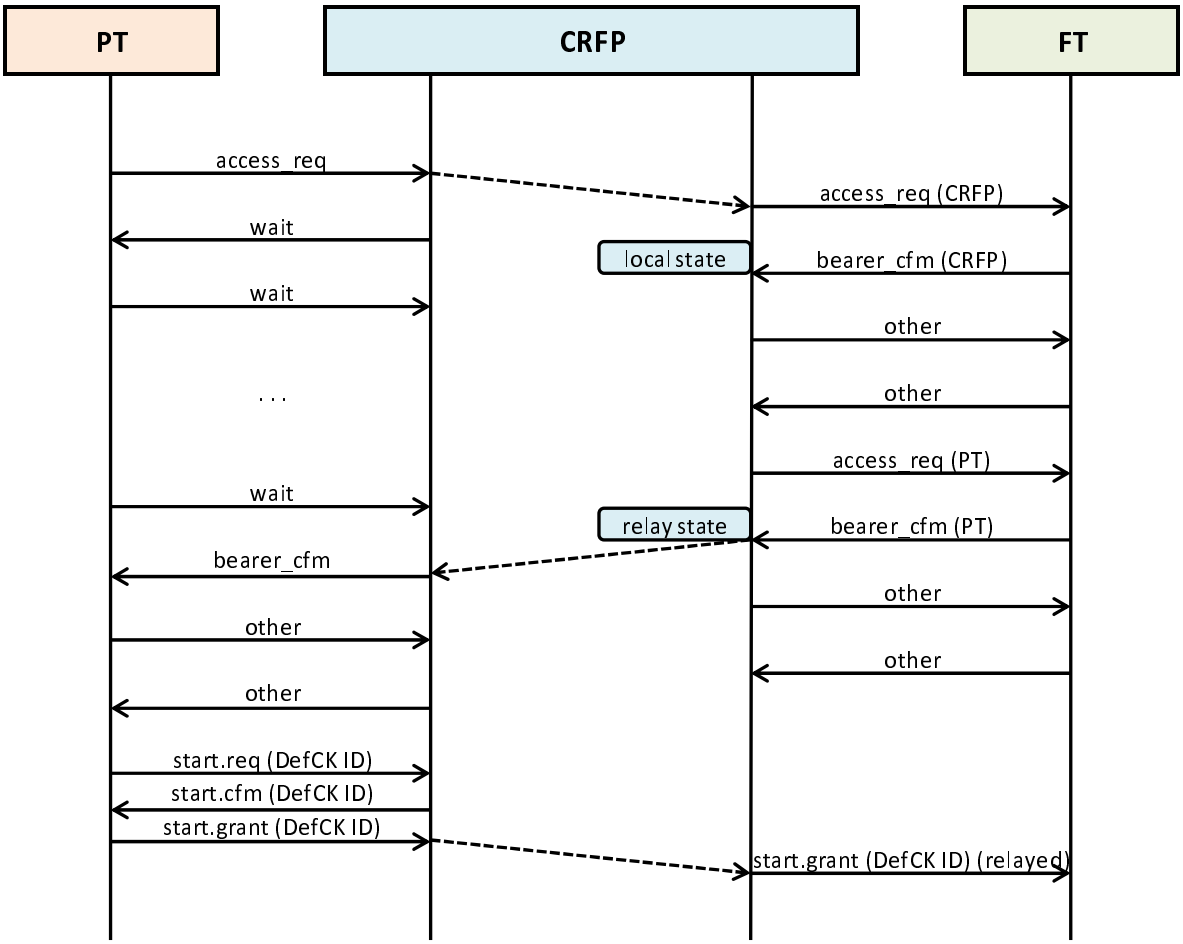

Figure 36: Early encryption on lower-segment

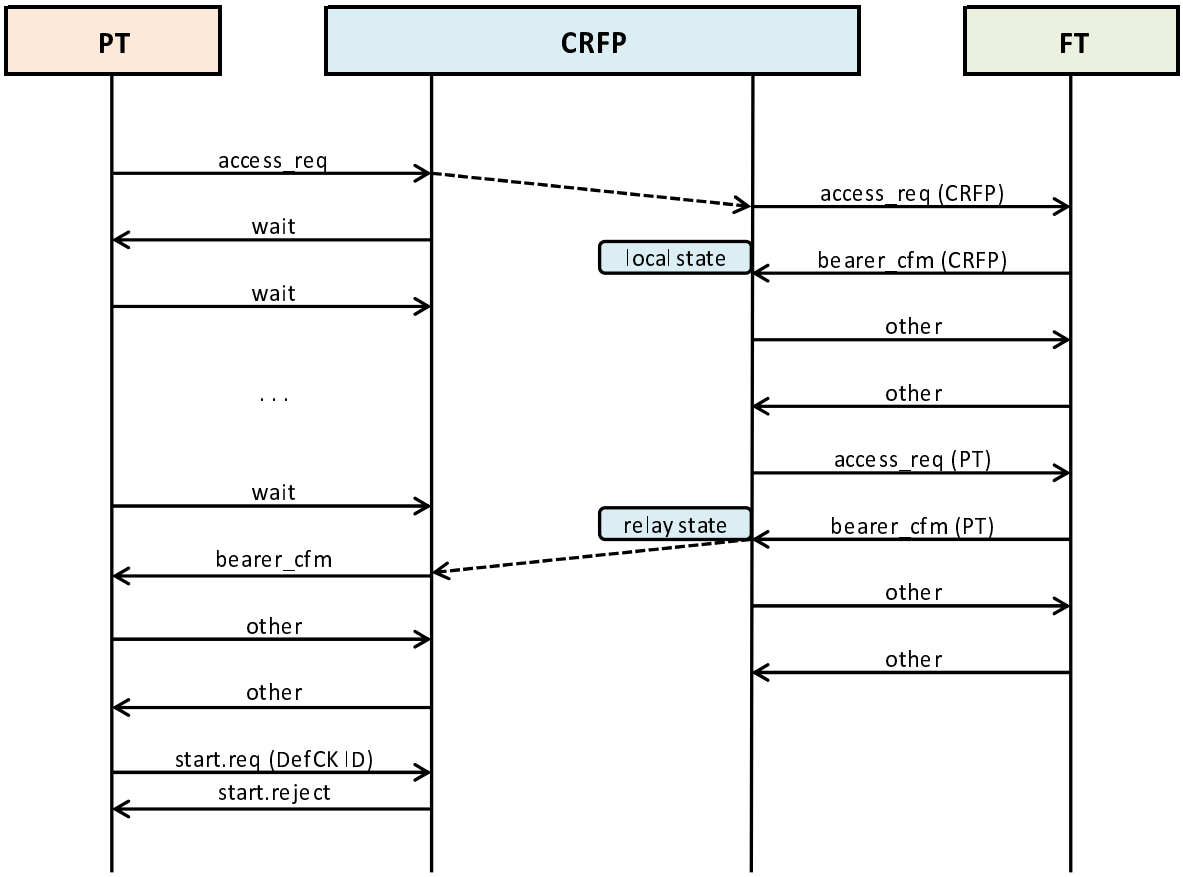

Figure 37: Early encryption on lower-segment, with rejection

7.7.5.2.3 NWK Early Encryption

The NWK procedure for early encryption shall be performed as specified in ETSI EN 300 444 [9], clause 8.45.3, with the following additions and modifications.

Early Encryption on upper segment (i.e. between WRS and FT):

In order to use early encryption on the upper segment, the FP has to assign at least one Default Cipher Key (DefCK) to the WRS. Default Cipher Keys are often assigned after a successful subscription procedure and at the latest within timer <MM_early_encryption.1> after the start of encryption of the first call. See ETSI EN 300 444 [9], clause 8.45.3.

The DefCKs assigned in this way, are upper segment keys and shall only be used for early encryption of the upper segment.

Early Encryption on lower segment (i.e. between WRS and PT):

In order to use early encryption on the lower segment, the FP has to provide the WRS with the PTs' Default Cipher Keys (DefCK) before a PT attempts to activate MAC encryption using the Default Cipher Key.

This can be achieved in one of two ways:

1) the keys can be provided to the WRS in advance of any call (see clause 7.7.5.2.4); or

2) the key can be provided to the WRS "just-in-time" (see clause 7.7.5.2.5).

The DefCKs obtained in either of these ways, are lower segment keys and shall only be used for early encryption of the lower segment.

7.7.5.2.4 Provision of lower DefCKs in advance

The FP may provide a WRS with a full or partial list of lower segment DefCKs in advance of their intended use.

This provision may be performed at various times, for example:

- After a successful subscription of a WRS with the FP (in order to provide the WRS with a list of existing lower segment DefCKs).
- After the FP assigns a new DefCK to a PP (in order to provide the WRS with the newly created lower segment DefCK).
- As part of regular house-keeping/maintenance activity (e.g. nightly update of all lower segment DefCKs).

The intention is to provide the WRS with a cache of lower segment DefCKs (and the associated indices) which will be available to the MAC layer procedure if/when a PT attempts to activate MAC encryption with a Default Cipher Key.

The FP provides the lower segment DefCKs to the WRS using the Indication of cipher key procedure (clause 7.7.4). The decision regarding when the DefCKs are transferred, and which DefCKs are transferred (if any) is left to the FP implementation.

The WRS shall be able to store at least 32 lower segment DefCKs. If more than 32 lower segment DefCKs are provided, then it is recommended that the WRS stores the most recently provided keys.

NOTE: The mechanisms described are only intended to transfer lower segment DefCKs. The upper segment DefCKs belonging to the WRS itself are assigned by the normal mechanism (i.e. a specific use of "Authentication of PP" procedure, see ETSI EN 300 444 [9], clause 8.45.3).

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

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

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

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

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

NOTE 2: Always supplying the DefCK in this way is redundant when it has already been provided in advance. However, doing it this way is simpler (since the FP does not have to remember which keys it has provided) and so the implementation is allowed to do it.

NOTE 3: Multiple DefCKs could be assigned to a PT. However, it is recommended that only one DefCK per PT is assigned in order to reduce overhead and complexity (see clause 7.7.5.2.3).

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

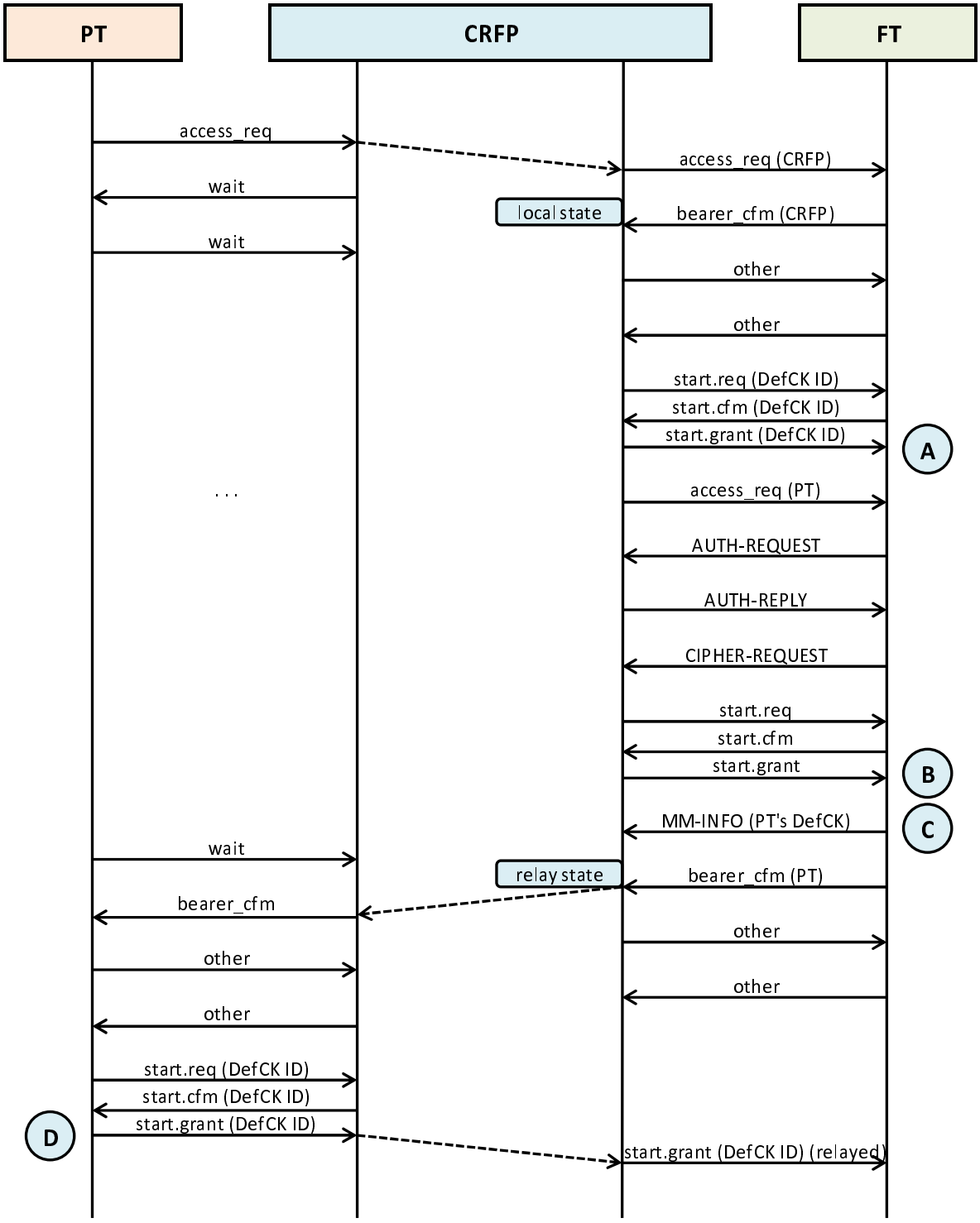

Figure 38: Early encryption of upper and lower segments with, just-in-time key provision

At the FP:

In order to use the "just-in-time" provision of lower DefCKs, the FP shall maintain an association between assigned PMID and the Default Cipher Key index. This association allows a lower Default Cipher Key index to be determined from the PT's PMID.

It is recommended that the FP does not assign a large number of DefCKs per PT. In fact, it is recommended, unless absolutely necessary, that a maximum of one DefCK per PT is assigned. Also, if it is required to renew a PT's DefCK, then it is recommended that the new DefCK is assigned using the same index (thus replacing the old key).

7.7.6 DSC2 operation

There are some considerations if DCS2 is used in a system employing repeaters.

The ciphering algorithm (DSC or DSC2) is selected by the FP and is specified in the <<Cipher Info>> Information Element of the {CIPHER-REQUEST} message, and therefore this could change on a call by call basis.

Of course, the FP should never specify DSC2 if it is not supported by the PT (as indicated by the PT's <<Terminal Capability>> Information Element).

NOTE: For highest security, DSC2 should be used whenever possible. However the FP might have resource limitations and is not able to provide DSC2 on all active connections. This is particularly true if DSC2 is implemented in software.

Non-relayed connections:

The FT and PT shall use the ciphering algorithm specified in the {CIPHER-REQUEST} message.

Relayed connections:

The FT provides the CRFP with the PT's DCK (for the lower segment) before sending the {CIPHER-REQUEST} message to the PT. This lower segment DCK is provided using the Indication of cipher key procedure (clause 7.7.4). The procedure also specifies the ciphering algorithm in the <<KEY>> Information Element of the {MM-INFO-SUGGEST} message.

The FT shall specify the same ciphering algorithm for the PT's {CIPHER-REQUEST} message as it specified in the CRFP's {MM-INFO-SUGGEST} message.

For the lower segment, the CRFP shall use the ciphering algorithm that was indicated in the {MM-INFO-SUGGEST} message, and the PT shall use the same ciphering algorithm which was indicated in the {CIPHER-REQUEST} message.

Mixed DSC and DSC2:

There exists the possibility to have different ciphering algorithms used for different (upper/lower) segments of a relayed connection. For example, the upper segment could be using DSC2 and the lower segment could be using DSC. This is allowed, and achievable given the above requirements.

However, problems could arise if the FP and PP support DSC2, and the WRS does not. For example, suppose the PP has a direct link with the FP, encrypted using DSC2. If that PP performs a bearer handover to the WRS, then it would continue to use DSC2, but the WRS is unable to support it.

To mitigate this problem the following is recommended:

- If an FP has one or more subscribed WRSs that don't support DSC2, then the FP should not use DSC2. This could be achieved by a) the FP could not specify DSC2 in the {CIPHER-REQUEST} message to the PP, and/or b) the FP could indicate no support of DSC2 in the "Extended Fixed Part Capabilities (part 2)" message bit a42, see ETSI EN 300 175-5 [5], clause F.3).
- A PP with an active call encrypted with DSC2 should not handover to a WRS that does not support DSC2.

7.7.7 Relay of the "START.GRANT" message

A CRFP shall relay any received START.GRANT message upwards towards the FP.

The relayed START.GRANT message shall be coded with the following addresses:

- with the same PMID received in the START.GRANT message from the lower node;
- with the FMID of the next node upstream (the FP or another CRFP).

For robustness, the relayed START.GRANT message may be sent twice by the WRS.

At the FT side the receipt of the relayed START.GRANT message(s) 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 MAC_ENC_EKS and DL_ENCRYPT primitives may be used, as defined in ETSI EN 300 175 Parts 3 [3] and 4 [4] respectively. For the behaviour of the FT in case of successful completion of ciphering procedure the requirements in ETSI 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.

In case of default cipher keys (early encryption procedure, see clause 7.7.5.2.2) the START.GRANT (DefCK) message shall, be relayed with the same DefCK index (see Figure 36 in clause 7.7.5.2.2 and Figure 38 in clause 7.7.5.2.5).

7.8 Management Entity procedures

7.8.1 Initialization of CRFP

At the CRFP:

The CRFP shall have installed at least as many IPEIs as supported CRFP users, see clause 7.6.3.

For the use of OA&M procedures an additional specific IPEI may also be installed.

To attach a CRFP to an existing DECT system, on user request, the CRFP shall perform the following actions:

- If the CRFP has a specific IPEI for OA&M use installed, then it shall obtain access rights with the FP using this IPEI (see clause 7.6.5). The received PARK and IPUI shall be used for establishment of connection for OA&M purposes.
- Additionally, for every other installed IPEI (for CRFP users), the CRFP shall obtain access rights with the FP using this IPEI (see clause 7.6.5). The received PARKs and IPUIs shall be used for the respective CRFP users, e.g. when performing location registration, authentication, ciphering.
- If no specific IPEI for OA&M use was installed, then the CRFP may use any of the other assigned PARK and IPUIs for establishment of connection for OA&M purposes.
- If the FP does not support ciphering the CRFP shall not initiate this procedure.

For location registration, see clause 7.6.6.

At the FP:

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 clause 7.6.2.3.

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.

For each CRFP user a DCK shall be established (see ETSI EN 300 444 [9], clause 8.27).

Additionally, if the FP supports Early Encryption, then for each CRFP user a Default Cipher Key (DefCK) shall also be established (see ETSI EN 300 444 [9], clause 8.45.3).

For Cipher Key derivation the FP shall perform in advance a Key allocation procedure to establish a UAK, as defined in ETSI EN 300 444 [9].

For location registration, see clause 7.6.6.

7.8.2 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 ETSI EN 300 175-3 [3]);
- Dual MAC mode (defined in this clause).

To support encryption the CRFP shall be able to 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, or when it indicates that it supports "V2" WRSs (see clause 7.4.4.3 of the present document and ETSI EN 300 175-3 [3], clause 7.2.3.5).

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

7.8.3 CRFP states and state transitions

The CRFP combines states of both PT and RFP as defined in ETSI 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 shall 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.

Annex A (normative): WRS interworking for Fixed Parts

A.1 Introduction

In addition to the requirements mandated by whatever profile(s) the FP supports (e.g. GAP, NG-DECT, ULE), there are also some additional requirements when support for a WRS is required. This annex defines those additional requirements.

A.2 Fixed Part requirements

A.2.1 MAC layer

An FP supporting a WRS shall also support the MAC features/procedures in table A.1.

Table A.1: MAC support

Item	Service	Procedure	Reference	Status
1	Downlink broadcast			M
		Q_T - Fixed part capabilities	A.3.1	M
		Q_T - Extended fixed part capabilities	A.3.2	M
2	Intra-cell bearer handover			M
		Intra-cell bearer handover	A.3.3	M
3	Dual bearer C/O procedures			M
		General	[3], 10.9.0	M
		Dual C/O bearer setup	[3], 10.9.1	M
		C/O connection release of connection with CRFP	[3], 10.9.2	M
		C/O connection suspend and resume	[3], 10.9.3	M
4	C_F higher layer signalling			M
		General	7.4.18.2.1	M
		B-field control Multiplexer (E/U-MUX), C_F modes	7.4.18.2.2	M
		C_F channel end-system operation	7.4.18.2.4	M
		C_F channel end-system specific WRS procedures: activation	7.4.18.2.7	M
		C_F channel end-system specific WRS procedures: single LAPC instance and coordination with C_S channel	7.4.18.2.8	M
		CS and CF management in links between FP and any WRS	A.3.6	M
NOTE:	The reference column refers to the relevant clause in the present document unless a specific reference document is noted.			

A.2.2 DLC layer

An FP supporting a WRS shall also support the features/procedures in table A.2.

Table A.2: DLC support

Item	Service	Procedure	Reference	Status
This table is intentionally left blank in order to facilitate future modification.				
NOTE:	The reference column refers to the relevant clause in the present document unless a specific reference document is noted.			

A.2.3 NWK layer

An FP supporting a WRS shall also support the features/procedures in table A.3.

Table A.3: NWK support

Item	Service	Procedure	Reference	Status
1	WRS subscription on air			M
		Obtaining access rights for WRS	7.6.5	M
2	Location registration for WRS			M
		Location registration for WRS	7.6.6	M
3	Assignment of WRS RPN			M
		Retrieval of WRS RPN	7.6.2.2	O
		Indication/Modification of WRS RPN	7.6.2.3	M
4	Management			M
		Initialization of CRFP	7.8.1	M
		Bearer handover bit mask management	A.3.4	M
		Indication/Modification of WRS RPN	A.3.5	M
5	Encryption of relayed connections			M
		General	7.7.1	M
		CRFP initialization of PT cipher key	7.7.2	M
		Management for encryption of relayed connections	7.7.3	M
		Indication of cipher key	7.7.4	M
		DSC2 operation	7.7.6	C3201
		Relay of START.GRANT message	7.7.7	M
		Dual cipher switching	A.3.7	M
6	Enhanced security			M
		Encryption of all calls	8.45.1, [9]	M
		Re-keying during a call	7.7.5.1	M
		Early encryption	7.7.5.2	M
		Subscription requirements	8.45.4, [9]	M
		Behaviour against legacy devices	8.45.5, [9]	M
C3201:	IF GAP.M.17 then M else N/A			
NOTE:	The reference column refers to the relevant clause in the present document unless a specific reference document is noted.			

A.3 Fixed Part procedures

A.3.1 Q_T - Fixed part capabilities

An FT capable of supporting a WRS shall be capable of sending Q_t Extended Fixed Part Capabilities message (as defined in ETSI EN 300 175-3 [3], clause 7.2.3.4), with the following additions.

Bit a26 of the Fixed Part Capabilities message indicates support for the C_F service.

An FT capable of supporting a WRS, as defined in the present document, shall support the use of the C_F service between the FT and the WRS. However, this does necessitate that the FT also supports the C_F service with PTs, and there is no need to set bit a26 to "1" for this reason. The FT shall only be required to set bit a26 to "1" if it generally supports C_F services with PTs, e.g. according to some other profile.

A.3.2 Q_T - Extended fixed part capabilities

An FT capable of supporting a WRS shall be capable of sending Q_t Extended Fixed Part Capabilities message (as defined in ETSI EN 300 175-3 [3], clause 7.2.3.5) with the following contents (table A.4).

Table A.4: 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 '01'B '10'B	1 CRFP is allowed 2 cascaded CRFPs are allowed 3 cascaded CRFPs are allowed
	<a14>	0, 1	0: "V1" CRFP encryption not supported 1: "V1" CRFP encryption supported (see note)
	<a15, a16, a17>	'001'B	"V2" WRS supported (see note)
NOTE: If bit a14 is set to 1, this means that "V1" CRFP encryption is supported by the FP. This bit need not be set if the FP only supports "V2" WRS, since encryption is mandatory for all "V2" WRS.			

A.3.3 Intra-cell Bearer Handover

An FT capable of supporting a WRS shall support the GAP-feature GAP.M.9 Bearer Handover intra-cell (see ETSI EN 300 444 [9]).

A.3.4 Bearer handover bit mask management

This clause is relates to FPs, which use the bit mask inside the MAC layer information "bearer handover info" (see clause 7.2.4.3.8 of ETSI 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 A.3.5) 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.

A.3.5 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 ETSI EN 300 175-6 [6].

A.3.6 C_S and C_F management in links between FP and any WRS

This procedure is for FP use only.

The ME of the FP may dynamically select the use of either C_S or C_F channels for any signalling operation between the FP and a WRS.

The rules given in clause 7.4.18.2.8 for C_S and C_F channel coordination shall be fulfilled.

EXAMPLE: For MM operations (e.g. authentication), the FP may select the channel to be used in order to provide the minimum disturbance to the user and depending on the traffic and processing loads, security timers, etc.

A.3.7 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 ETSI EN 300 444 [9].

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 ETSI EN 300 444 [9], 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 ETSI EN 300 444 [9].

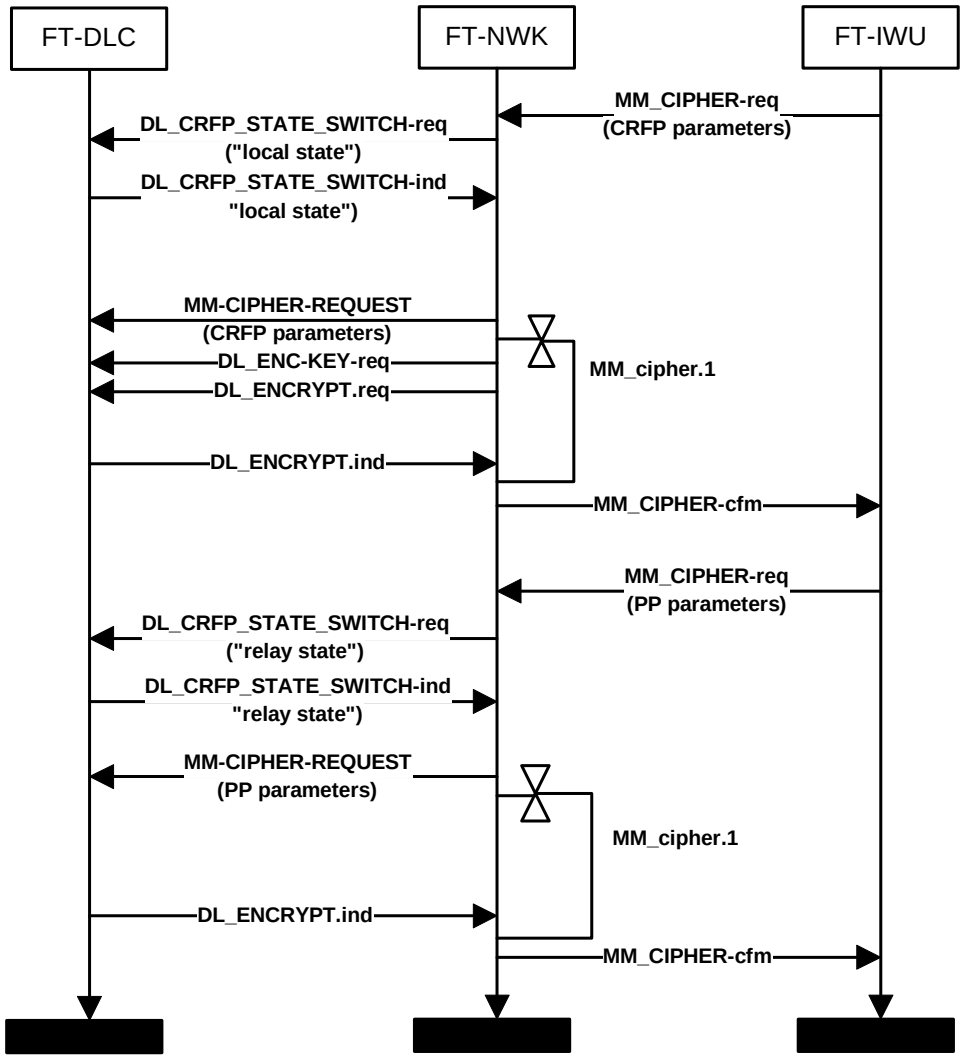

Figure A.1: Dual cipher switching initiated by FT procedure NWK layer prospective

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.

History

Document history		
Edition 1	March 1997	Publication as ETSI ETS 300 700
V1.2.1	September 2000	Publication
V2.0.21	August 2016	EN Approval Procedure AP 20161106: 2016-08-08 to 2016-11-07