INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

T.30

Amendment 1

(07/97)

SERIES T: TERMINALS FOR TELEMATIC SERVICES

Procedures for document facsimile transmission in the general switched telephone network

Amendment 1

ITU-T Recommendation T.30 – Amendment 1

(Previously CCITT Recommendation)

ITU-T T-SERIES RECOMMENDATIONS

TERMINALS FOR TELEMATIC SERVICES

For further details, please refer to ITU-T List of Recommendations.

ITU-T RECOMMENDATION T.30

PROCEDURES FOR DOCUMENT FACSIMILE TRANSMISSION IN THE GENERAL SWITCHED TELEPHONE NETWORK

AMENDMENT 1

Summary

Recommendation T.30 defines the protocols for Group 3 facsimile terminals.

Amendment 1 defines proposed changes to the main body of Recommendation T.30 and the introduction of new Annexes G, H and I.

The changes to the main body cover the introduction of new signals End of Selection (EOS and PPS-EOS), Field Not Valid (FNV), Polled SubAddress (PSA), renaming of the Password for Transmission to Sender ID (SID) and amendments to cover the introduction of the new annexes.

Annex G describes the use of the HKM key management system, the HFX40 cipher system, and the HFX40-I hashing system (all described in Recommendation T.36).

Annex H describes the use of the RSA algorithm.

The procedures proposed in Annexes G and H are based on those defined in the main body as well as Annexes A and C of Recommendation T.30.

Annex I contains the amendments to cover the use of colour and gray-scale image communication using the lossless coding scheme defined in Recommendation T.43.

Source

Amendment 1 to ITU-T Recommendation T.30, was prepared by ITU-T Study Group 8 (1997-2000) and was approved under the WTSC Resolution No. 1 procedure on the 2nd of July 1997.

FOREWORD

ITU (International Telecommunication Union) is the United Nations Specialized Agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the ITU. The ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

The approval of Recommendations by the Members of the ITU-T is covered by the procedure laid down in WTSC Resolution No. 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

INTELLECTUAL PROPERTY RIGHTS

The ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. The ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, the ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

PROCEDURES FOR DOCUMENT FACSIMILE TRANSMISSION IN THE GENERAL SWITCHED TELEPHONE NETWORK

AMENDMENT 1

(Geneva, 1997)

1 Section 1 Introduction of new signals and amendments to existing signals

1.1) Amend 5.3.6.1.2 5) to read as follows:

5) *Selective Polling (SEP)* – This optional signal indicates that the following FIF information is:

a) a subaddress for the polling mode; or

b) a specific document number.

(See 5.3.6.2.9/T.30 SEP coding format.) SEP is only sent if bit 47 in DIS is set.

Format: 1000 0101

NOTE – When PSA and SEP are used together in the polling mode, option b) is applied.

1.2) Add new item 6) to 5.3.6.1.2 as follows:

6) *Polled Subaddress (PSA)* – This optional signal indicates that the following FIF information is a subaddress for polling (see 5.3.6.2.13/T.30 PSA coding format). PSA is only sent if bit 35 in the DIS is set.

Format: 1000 0110

1.3) Amend 5.3.6.1.3 5) to read as follows:

"5) *Sender Identification (SID)* – This optional signal indicates that the following FIF information is the sender identity (see 5.3.6.2.11/T.30 SID coding format). SID is only sent if bit 50 in DIS is set.

Format: X100 0101"

1.4) In 5.3.6.1.6, add a new post-message command (item 7) to read as follows:

"Format: X111 1000

7) *End Of Selection (EOS)* – This optional command from the multiple-SEP-capable polling transmitter to the SEP-capable polling receiver shall be used to indicate that the end (last page or last block) of the currently selected document has been reached and that a return to phase B is expected for the purpose of eliciting any new SEP-selected document request. EOS may only be transmitted if bit 34 was set in the receiver's DTC".

1.5) Renumber existing items 5.3.6.1.6 7) to 5.3.6.1.6 9) as 5.3.6.1.6 8) to 5.3.6.1.6 10) respectively.

*1.6)	Add a new item 3) to 5.3.6.1.8 as follows:*

"3) Field Not Valid (FNV) – This optional signal indicates that the last received PWD, SEP, SUB, SID, TSI, PSA or secure fax signal (or any combination of these) is invalid or not accepted. FNV is only sent if bit 33 in DIS/DTC and DCS is set.

NOTE – FNV shall be sent in place of CFR/FTT when the FIF of one or more optional signals associated with DCS is invalid or not accepted. FNV shall also be sent in response to the DTC when one or more of the related optional signals is invalid or not accepted. FNV may also be sent in response to the DEC, DES, DTR or DER signals (as defined in Annex H/T.30).

Format:	X101 0011"

*1.7)	Add a new subclause 5.3.6.2.11 to read as follows:*

"**5.3.6.2.11 SID coding format**

The facsimile information field of the SID signal shall consist of 20 numeric digits coded as shown in Table 3 but excluding the "+" character. The least significant bit of the least significant digit shall be the first bit transmitted. The unused octets in the information field shall be filled with the "space" character and the information should be right justified."

*1.8)	Add a new subclause 5.3.6.2.12 as follows:*

"**5.3.6.2.12 FNV coding format**

The structure of the FIF for the FNV signal is as follows:

Reason Octets	Frame Number Octet	Diagnostic Information Octets

At least one reason octet is required in the FIF of the FNV signal. The other octets are optional, but a frame number octet is required if any of the optional diagnostic information octets are presented. Use of the optional octets is application-dependent. Terminals which implement the FNV signal must be able to receive these octets but are not required to process or respond to them.

Format for reason octets

The first octet is known as a reason octet and is used to identify cases where the contents of the Facsimile Information Field (FIF) for the specified signals is not valid. The values which apply for this octet are shown in the table below. A bit setting of "0" indicates "OK" and a bit setting of "1" indicates "invalid". Bit 8 is an extend bit, which shall be set to "1" if there are additional reason octets in the FIF. If the extend bit is set to "0", there are no additional reason octets.

Bit No.	Meaning
1	Incorrect password (PWD)
2	Selective polling reference (SEP) not known
3	Subaddress (SUB) not known
4	Sender identity (SID) not known
5	Secure fax error
6	Transmitting Subscriber Identification (TSI) not accepted
7	Polled SubAddress (PSA) not known
8	Extend Bit – default "0"
NOTE – As additional reason octets are defined, they shall have a bit structure which is consistent with the first reason octet. The first seven bits shall identify reasons (or be reserved) and the eighth bit is an extend bit for reason octets.	

Format for frame number of FNV

This is an eight bit binary number. The frame number 0-255 (maximum number is 255) is used to identify the sequence number of an FNV frame. The frame 0 is the first frame to be transmitted in a series of FNV frames. The least significant bit is transmitted first.

Format for diagnostic information octets of FNV

The diagnostic information for one or more signals may optionally be presented. The diagnostic information for each signal is presented in a series of octets using a type, length, value encoding. The order of transmission for the diagnostic information octets shall be left to right as printed and the least significant bit (right-most) shall be the first one transmitted, except as noted (see rules for value octets below).

The format for the diagnostic information for each signal is as follows:

Type	Length	Value – Invalid FIF content or other diagnostic information (variable number of octets)

Type – Specified based on reversing the FCF (Facsimile Control Field) of the signal or another unique designation. One octet identifiers are normally used, but an extension method is available. The types are defined as follows:

Type	**Description**
1100 0001	Incorrect password (PWD)
1010 0001	Selective polling reference (SEP) not known
1100 001X	Subaddress (SUB) not known
1010 001X	Sender identify (SID) not known
0000 1000	Secure fax error
0100 001X	Transmitting subscriber identification (TSI) not accepted
0110 0001	Polled SubAddress not known
NOTE – X is as defined in 5.3.6.1/T.30.	

Length – Number of octets in the value to follow. One octet is normally used, but an extension method is available.

Value – Contains the portion of the FIF which was invalid for the signal type or other diagnostic information. For cases where all or a portion of an unaccepted FIF is being returned, the data shall be presented in the same bit and octet order as originally transmitted.

If diagnostic information is available for more than one signal, the "type" octet for the second signal will immediately follow the last "value" octet for the prior signal. In a similar manner, all of the diagnostic information for all signals shall be presented in the FIF of the FNV until all diagnostic information has been transmitted. In cases where the amount of diagnostic information to be transmitted exceeds the limits for a single T.30 frame, the remaining diagnostic information shall be placed in additional FNV frames and the frame number will be incremented by 1 for each new frame. For such additional frames, the contents of the reason octets shall be identical to the first FNV frame and the content of the diagnostic information octets shall continue from the previous frame.

Syntax of FNV facsimile information field

The detailed syntax of the FNV FIF is presented below in Backus-Naur (BNF) form. The symbols used in the BNF are defined in H.6.1.4.5/T.30.

```
<bit>                   ::=  <0> | <1>
<octet>                 ::=  <bit><bit><bit><bit><bit><bit><bit><bit>
<8_bit_tag>             ::=  <octet>
<extend_octet>          ::=  {<1><1><1><1><1><1><1><1>}
```

```
<FNV_type>                    ::=  <8_bit_tag>|<extend octet><8_bit_tag><8_bit_tag>
<parameter_value>             ::=  <octet>{<octet>}
<count_extend_octet>          ::=  <0><0><0><0><0><0><0><0>
<parameter_length>            ::=  <octet> |<count_extend_octet> <octet> <octet>
<Diagnostic_Information>      ::=  {<FNV_type><parameter_length><parameter_value>}
<frame_number>                ::=  <octet>
<FNV_Reason_Octets>           ::=  <octet>{<octet>}
<FIF_of_FNV>                  ::=  <FNV_Reason_Octets>[<frame_number>< Diagnostic_Information>]
```

Coding examples for FNV facsimile information fields

Case A)

Password is invalid and no diagnostic information is sent.

	Reason Octet 1
Printed order	10000000
	b_1 b_8
Transmit order	10000000
	b_1 b_8

Case B)

Password is invalid and diagnostic information is sent.

The example of the password is "123456789"

	Reason Octet 1	Frame number	Type	Length	Value (ex. Password)							
Printed order	10000000	00000000	11000001	00010100	20	20	...	31	32	...	38	39
		b_7 b_0										
Transmit order	10000000	00000000	11000001	00101000	39	38	...	31	20	...	20	20
	b_1 b_8	b_0 b_7						00000100 transmit bit order				

Case C)

New error bits are defined in the second reason octet.

An error occurs in bit 1 of the second reason octet and diagnostic information is not sent.

	Reason Octet 1	Reason Octet 2
Printed order	00000001	10000000
Transmit order	00000001	10000000
	b_1 b_8	b_9 b_{16}

Case D)

A new error bit is defined in the second reason octet.

An error occurs in bit 1 of the second reason octet and diagnostic information is sent for a case where the FIF of the invalid signal is being returned.

	Reason Octet 1	Reason Octet 2	Frame number		Type	Length	Value
Printed order	00000001	10000000	00000000		FCF (reverse order)	length	Return of FIF (reverse order)
			b_7 b_0				
Transmit order	00000001	10000000	00000000		FCF (normal order)	length	Return of FIF (normal order)
	b_1 b_8	b_9 b_{16}	b_0 b_7				

Case E)

New error bits are defined in the second reason octet. A portion of the Subaddress is invalid (see bit 3) and an error is indicated in bit 9 or the second reason octet. Diagnostic Information is included for both errors. The example of the subaddress is "SSSSSSSSSSS1002#2002" and only extension 1002 is being rejected. A portion of the value of the Diagnostic Information for the second error extends over the frame boundary, so a second frame is transmitted with the continuation of the value. The diagnostic information for the second error does not include the return of a previous FIF, so the general rule for transmission bit order (LSB or right-most bit first) applies.

First frame

	Reason Octet 1	Reason Octet 2	Frame number	Type 1 (SUB)	Length (4)	Value (Returned Portion of FIF)			
Printed order	00100001	10000000	00000000	11000011	00000100	31	30	30	32
			b_7 b_0		Length of 1st block				
Transmit order	00100001	10000000	00000000	11000011	00100000	32	30	30	31
	b_1 b_8	b_9 b_{16}	b_0 b_7						10001100 transmit bit order

First frame (continued)

	Type 2	Length (128)	value
Printed order	Type	10000000	value
Transmit order	Type (LSB order)	00000001	value (LSB order)

Second frame

	Reason Octet 1	Reason Octet 2	Frame number (2)	value (continuation)
Printed order	00100001	10000000	00000001	value (continued)
			b_7 b_0	
Transmit order	00100001	10000000	10000000	value (LSB first)
	b_1 b_8	b_9 b_{16}	b_0 b_7	

1.9) Add a new subclause 5.3.6.2.13 as follows:

"**5.3.6.2.13 PSA coding format**

The facsimile information field of the PSA signal shall consist of 20 numeric digits coded as shown in Table 3/T.30 but excluding the "+" character. The least significant bit of the least significant digit shall be the first bit transmitted. The unused octets in the information field shall be filled with the "space" character and the information should be right justified."

1.10) Replace existing Table 2/T.30 with the following:

Table 2/T.30

Bit No.	DIS/DTC	Note	DCS	Note
1	Reserved	1	Reserved	1
2	Reserved	1	Reserved	1
3	Reserved	1	Reserved	1
4	Reserved	1	Reserved	1
5	Reserved	1	Reserved	1
6	V.8 capabilities	23	Invalid	24
7	"0" = 256 octets preferred "1" = 64 octets preferred	23, 42	Invalid	24
8	Reserved	1	Reserved	1
9	Ready to transmit a facsimile document (polling)	18	Set to "0"	
10	Receiver fax operation	19	Receiver fax operation	20
11, 12, 13, 14	Data signalling rate	3	Data signalling rate	33
0, 0, 0, 0	V.27 *ter* fall-back mode		2400 bit/s, Rec. V.27 *ter*	
0, 1, 0, 0	Rec. V.27 *ter*		4800 bit/s, Rec. V.27 *ter*	
1, 0, 0, 0	Rec. V.29		9600 bit/s, Rec. V.29	
1, 1, 0, 0	Recs. V.27 *ter* and V.29		7200 bit/s, Rec. V.29	
0, 0, 1, 0	Not used		Invalid	31
0, 1, 1, 0	Reserved		Invalid	31
1, 0, 1, 0	Not used		Reserved	
1, 1, 1, 0	Invalid	32	Reserved	
0, 0, 0, 1	Not used		14 400 bit/s, Rec. V.17	
0, 1, 0, 1	Reserved		12 000 bit/s, Rec. V.17	
1, 0, 0, 1	Not used		9600 bit/s, Rec. V.17	
1, 1, 0, 1	Recs. V.27 *ter*, V.29, and V.17		7200 bit/s, Rec. V.17	
0, 0, 1, 1	Not used		Reserved	
0, 1, 1, 1	Reserved		Reserved	
1, 0, 1, 1	Not used		Reserved	
1, 1, 1, 1	Reserved		Reserved	

Table 2/T.30 *(continued)*

Bit No.	DIS/DTC	Note	DCS	Note
15	R8 × 7.7 lines/mm and/or 200 × 200 pels/25.4 mm	10, 11, 13, 25	R8 × 7.7 lines/mm or 200 × 200 pels/25.4 mm	10, 11, 13
16	Two-dimensional coding capability		Two dimensional coding	
17, 18	Recording width capabilities	27	Recording width	27
(0,0)	Scan line length 215 mm ± 1%		Scan line length 215 mm ± 1%	
(0,1)	Scan line length 215 mm ± 1% and scan line length 255 mm ± 1% and scan line length 303 mm ± 1%		Scan line length 303 mm ± 1%	
(1,0)	Scan line length 215 mm ± 1% and scan line length 255 mm ± 1%		Scan line length 255 mm ± 1%	
(1,1)	Invalid	6	Invalid	
19, 20	Recording length capability	2	Recording length	2
(0,0)	A4 (297 mm)		A4 (297 mm)	
(0,1)	Unlimited		Unlimited	
(1,0)	A4 (297 mm) and B4 (364 mm)		B4 (364 mm)	
(1,1)	Invalid		Invalid	
21, 22, 23	Minimum scan line time capability at the receiver	4, 8, 23	Minimum scan line time	8, 24
(0,0,0)	20 ms at 3.85 l/mm: $T_{7.7} = T_{3.85}$		20 ms	
(0,0,1)	40 ms at 3.85 l/mm: $T_{7.7} = T_{3.85}$		40 ms	
(0,1,0)	10 ms at 3.85 l/mm: $T_{7.7} = T_{3.85}$		10 ms	
(1,0,0)	5 ms at 3.85 l/mm: $T_{7.7} = T_{3.85}$		5 ms	
(0,1,1)	10 ms at 3.85 l/mm: $T_{7.7} = 1/2\ T_{3.85}$			
(1,1,0)	20 ms at 3.85 l/mm: $T_{7.7} = 1/2\ T_{3.85}$			
(1,0,1)	40 ms at 3.85 l/mm: $T_{7.7} = 1/2\ T_{3.85}$			
(1,1,1)	0 ms at 3.85 l/mm: $T_{7.7} = T_{3.85}$		0 ms	
24	Extend field	5	Extend field	5
25	Reserved	1, 41	Reserved	1, 41
26	Uncompressed mode		Uncompressed mode	
27	Error correction mode	9, 17, 23, 25	Error correction mode	9, 17, 24, 34
28	Set to "0"		Frame size 0 = 256 octets Frame size 1 = 64 octets	7, 24
29	Reserved	1	Reserved	1
30	Reserved	1	Reserved	1
31	T.6 coding capability	9, 17	T.6 coding enabled	9, 17
32	Extend field	5	Extend field	5
33	Field not valid capability		Field not valid capability	
34	Multiple selective polling capability		Set to "0"	
35	Polled SubAddress	26, 44, 45	Set to "0"	
36	T.43 coding	17, 25, 34, 35, 37, 39, 40	T.43 coding	17, 25, 34, 35, 37, 39, 40
37	Plane interleave	25, 46	Plane interleave	25, 46
38	Reserved	1	Reserved	1
39	Reserved	1	Reserved	1
40	Extend field	5	Extend field	5

Table 2/T.30 *(continued)*

Bit No.	DIS/DTC	Note	DCS	Note
41	R8 × 15.4 lines/mm	10	R8 × 15.4 lines/mm	10, 34
42	300 × 300 pels/25.4 mm	34	300 × 300 pels/25.4 mm	34
43	R16 × 15.4 lines/mm and/or 400 × 400 pels/25.4 mm	10, 12, 13	R16 × 15.4 lines/mm and/or 400 × 400 pels/25.4 mm	10, 12, 13, 34
44	Inch based resolution preferred	13, 14	Resolution type selection "0": metric based resolution "1": inch based resolution	13, 14
45	Metric based resolution preferred	13, 14	Don't care	
46	Minimum scan line time capability for higher resolutions "0": $T_{15.4} = T_{7.7}$ "1": $T_{15.4} = 1/2\ T_{7.7}$	15	Don't care	
47	Selective polling	26, 44	Set to "0"	
48	Extend field	5	Extend field	5
49	Subaddressing capability		Subaddressing transmission	26
50	Password	26	Sender Identification transmission	26
51	Ready to transmit a data file (polling)	17, 21	Set to "0"	
52	Reserved	1	Reserved	1
53	Binary File Transfer (BFT)	16, 17, 21	Binary File Transfer (BFT)	16, 17,
54	Document Transfer Mode (DTM)	17, 21	Document Transfer Mode (DTM)	17
55	Electronic Data Interchange (EDI)	17	Electronic Data Interchange (EDI)	17
56	Extend field	5	Extend field	5
57	Basic Transfer Mode (BTM)	17, 21	Basic Transfer Mode (BTM)	17
58	Reserved	1	Reserved	1
59	Ready to transmit a character or mixed mode document (polling)	17, 22	Set to "0"	
60	Character mode	17, 22	Character mode	17, 22
61	Reserved	1	Reserved	1
62	Mixed mode (Annex D/T.4)	17, 22	Mixed mode (Annex D/T.4)	17, 22
63	Reserved	1	Reserved	1
64	Extend field	5	Extend field	5
65	Processable mode 26 (Rec. T.505)	17, 22	Processable mode 26 (Rec. T.505)	17, 22
66	Digital network capability	43	Digital network capability	43
67 (0) (1)	Duplex and half duplex capabilities Half duplex operation only Duplex and half duplex operation		Duplex and half duplex capabilities Half duplex operation only Duplex operation	
68	JPEG coding	25, 34, 35, 39, 40	JPEG coding	25, 34, 35, 39, 40
69	Full colour mode	25, 35	Full colour mode	25, 35
70	Set to "0"	36	Preferred Huffman tables	25, 36

Table 2/T.30 *(continued)*

Bit No.	DIS/DTC	Note	DCS	Note
71	12 bits/pel component	25, 37	12 bits/pel component	25, 37
72	Extend field	5	Extend field	5
73	No subsampling (1:1:1)	25, 38	No subsampling (1:1:1)	25, 38
74	Custom illuminant	25, 39	Custom illuminant	25, 39
75	Custom gamut range	25, 40	Custom gamut range	25, 40
76	North American Letter (215.9 × 279.4 mm) capability	28	North American Letter (215.9 × 279.4 mm)	
77	North American Legal (215.9 × 355.6 mm) capability	28	North American Legal (215.9 × 355.6 mm)	
78	Single-progression sequential coding (Rec. T.85) basic capability	17, 29, 30	Single-progression sequential coding (Rec. T.85) basic	17, 29
79	Single-progression sequential coding (Rec. T.85) optional L0 capability	17, 29, 30	Single-progression sequential coding (Rec. T.85) optional L0	17, 29
80	Extend field	5	Extend field	5
81	HKM key management capability		HKM key management selected	
82	RSA key management capability		RSA key management selected	47
83	Override mode capability		Override mode selected	
84	HFX40 cipher capability		HFX40 cipher selected	
85	Alternative cipher number 2 capability		Alternative cipher number 2 selected	
86	Alternative cipher number 3 capability		Alternative cipher number 3 selected	
87	HFX40-I hashing capability		HFX40-I hashing selected	
88	Extend field	5	Extend field	5
89	Alternative hashing system number 2 capability		Alternative hashing system number 2 selected	
90	Alternative hashing system number 3 capability		Alternative hashing system number 3 selected	
91	Reserved for future security features	1	Reserved for future security features	1
92	Reserved	1	Reserved	1
93	Reserved	1	Reserved	1
94	Reserved	1	Reserved	1
95	Reserved	1	Reserved	1
96	Extend field	5	Extend field	5

NOTE 1 – Bits that are indicated as "Reserved" shall be set to "0".

NOTE 2 – Standard facsimile terminals conforming to Recommendation T.4 must have the following capability: Paper length = 297 mm.

NOTE 3 – Where the DIS or DTC frame defines V.27 *ter* capabilities, the terminal may be assumed to be operable at either 4800 or 2400 bit/s.

Where the DIS or DTC frame defines V.29 capabilities, the terminal may be assumed to be operable at either 9600 or 7200 bit/s per Recommendation V.29; where it defines Recommendation V.17, the terminal may be assumed to be operable at 14 400 bit/s, 12 000 bit/s, 9600 bit/s or 7200 bit/s per Recommendation V.17.

Table 2/T.30 *(continued)*

NOTE 4 – $T_{7.7}$ and $T_{3.85}$ refer to the scan line times to be utilized when the vertical resolution is 7.7 lines/mm (or 200 lines/25.4 mm or 300 lines/25.4 mm) or 3.85 lines/mm, respectively (see bit 15 above). $T_{7.7}$ =1/2 $T_{3.85}$ indicates that when the vertical resolution is 7.7 lines/mm or 200 lines/25.4 mm or 300 lines/25.4 mm, the scan line time can be decreased by half.

NOTE 5 – The standard FIF field for the DIS, DTC and DCS signals is 24 bits long. If the "extend field" bit(s) is a "1", the FIF field shall be extended by an additional eight bits.

NOTE 6 – Existing terminals may send the invalid (1.1) condition for bits 17 and 18 of their DIS signal. If such a signal is received, it should be interpreted as (0,1).

NOTE 7 – The values of bit 28 in the DCS command is valid only when the indication of the Recommendation T.4 error correction mode is invoked by bit 27.

NOTE 8 – The optional T.4 error correction mode of operation requires 0 ms of the minimum scan line time capability. Bits 21-23 in DIS/DTC signals indicate the minimum scan line time of a receiver regardless of the availability of the error correction mode.

In case of error correction mode, the sender sends DCS signal with bits 21-23 set to "1, 1, 1" indicating 0 ms capability.

In case of normal transmission, the sender sends DCS signal with bits 21-23 set to the appropriateness according to the capabilities of the two terminals.

NOTE 9 – T.6 coding scheme capability specified by bit 31 is valid only when bit 27 (error correction mode) is set as a "1".

NOTE 10 – Resolutions of R8 and R16 are defined as follows:

R8 = 1728 pels/(215 mm ± 1%) for ISO A4, North American Letter and Legal.

R8 = 2048 pels/(255 mm ± 1%) for ISO B4.

R8 = 2432 pels/(303 mm ± 1%) for ISO A3.

R16 = 3456 pels/(215 mm ± 1%) for ISO A4, North American Letter and Legal.

R16 = 4096 pels/(255 mm ± 1%) for ISO B4.

R16 = 4864 pels/(303 mm ± 1%) for ISO A3.

NOTE 11 – Bit 15, when set to "1", is interpreted according to bits 44 and 45 as follows:

bit 44	bit 45	Interpretation
0	0	(invalid)
1	0	200 × 200 pels/25.4 mm
0	1	R8 × 7.7 lines/mm
1	1	R8 × 7.7 lines/mm and 200 × 200 pels/25.4 mm

"1" in bit 15 without bits 41, 42, 43, 44, 45 and 46 indicates R8 × 7.7 lines/mm.

NOTE 12 – Bit 43, when set to "1", is interpreted according to bits 44 and 45 as follows:

bit 44	bit 45	Interpretation
0	0	(invalid)
1	0	400 × 400 pels/25.4 mm
0	1	R16 × 15.4 lines/mm
1	1	R16 × 15.4 lines/mm and 400 × 400 pels/25.4 mm

NOTE 13 – Bits 44 and 45 are used only in conjunction with bits 15 and 43. Bit 44 in DCS, when used, shall correctly indicate the resolution of the transmitted document, which means that bit 44 in DCS may not always match the indication of bits 44 and 45 in DIS/DTC. Cross selection will cause the distortion and reduction of reproducible area.

If a receiver indicates in DIS that it prefers to receive metric based information but the transmitter has only the equivalent inch-based information (or vice versa), then communication shall still take place.

NOTE 14 – Bits 44 and 45 do not require the provision of any additional features on the terminal to indicate to the sending or receiving user whether the information was transmitted or received on a metric-metric, inch-inch, metric-inch, inch-metric basis.

NOTE 15 – $T_{15.4}$ refers to the scan line times to be utilized when the vertical resolution is 15.4 lines/mm or 400 lines/mm.

$T_{15.4}$ = 1/2 $T_{7.7}$ indicates that when $T_{7.7}$ is 10, 20 or 40 ms the scan line time can be decreased by half in higher resolution mode.

Table 2/T.30 *(continued)*

When $T_{7.7}$ is 5 ms [i.e. (bit 21, bit 22, bit 23) = (1, 0, 0), (0, 1, 1)] or 0 ms [i.e. (1, 1, 1)], bit 46 in DIS/DTC should be set to "0" ($T_{15.4} = T_{7.7}$).
NOTE 16 – The binary file transfer protocol is described in Recommendation T.434.
NOTE 17 – When either bit of 31, 36, 51, 53, 54, 55, 57, 59, 60, 62, 65, 78 and 79 is set to "1", bit 27 shall also be set to "1".
NOTE 18 – Bit 9 indicates that there is a facsimile document ready to be polled from the answering terminal. It is not an indication of a capability.
NOTE 19 – Bit 10 indicates that the answering terminal has receiving capabilities.
NOTE 20 – Bit 10 in DCS is a command to the receiving terminal to set itself in the receive mode.
NOTE 21 – Bit 51 indicates that there is a data file ready to be polled from the answering terminal. It is not an indication of a capability. This bit is used in conjunction with bits 53, 54 and 57.
NOTE 22 – Bit 59 indicates that there is a character coded or mixed mode document ready to be polled from the answering terminal. It is not an indication of a capability. This bit is used in conjunction with bits 60, 62 and 65.
NOTE 23 – When the optional procedure defined in Annex C/T.30 is used, in DIS/DTC bits 6 and 7 shall be set to "0" and bits 21 to 23 and 27 shall be set to "1".
NOTE 24 – When the optional procedure defined in Annex C/T.30 is used, in DCS bits 6, 7 and 28 shall be set to "0" and bits 21 to 23 and 27 shall be set to "1".
NOTE 25 – The optional continuous-tone colour mode and gray-scale mode (JPEG mode) protocols and the optional lossless encoded colour and gray-scale mode (T.43 mode) are described in Annexes E/T.30 and I/T.30 respectively. If bit 68 in the DIS/DTC frame is set to "1", this indicates JPEG mode capability. If bits 36 and 68 are set to "1", this indicates that the T.43 capability is also available. Bit 36 in the DIS/DTC frame shall only be set to "1" when bit 68 is also set to "1". Additionally, then bits 15 and 27 in the DIS/DTC frame shall also be set to "1", if bit 68 or bits 36 and 68 are set to "1". Bit 15 indicates 200 × 200 pels/25.4 mm resolution capability, which is basic for colour facsimile. Bit 27 indicates error correction mode capability, which is mandatory for colour facsimile. Bits 69 to 71 and 73 to 75 are relevant only if bit 68 is set to "1". Bit 73 is relevant only for JPEG mode. Bits 69, 71, 74 and 75 are relevant for JPEG mode and/or T.43 mode. Bit 37 is relevant only when bit 36 is set to "1" – see also Notes 39 and 40.
NOTE 26 – To provide an error recovery mechanism, when PWD/SEP/SUB/SID/PSA frames are sent with DCS or DTC, bits 49 and 50 in DCS or bits 47 and 50 and 35 in DTC shall be set to "1". For bit 47, setting "1" for DTC means selective polling transmission and for DIS means selective polling capability. For bit 50, setting "1" for DTC means password transmission and for DIS means password or Sender ID capability. For bit 35, setting "1" for DTC means Polled SubAddress transmission and for DIS means Polled SubAddress capability. Terminals conforming to the 1993 versions of this Recommendation may set the above bits to "0" even though PWD/SEP/SUB frames are transmitted.
NOTE 27 – The corresponding scan line lengths for inch-based resolutions can be found in 2.2/T.4.
NOTE 28 – While using bits 76 and 77 in DIS/DTC, the terminal is required to be able to receive ISO A4 documents in every combination of bits 76 and 77. A4, B4 and A3 transmitters may ignore the settings of bits 76 and 77.
NOTE 29 – The coding scheme indicated by the bits 78 and 79 is defined in Recommendation T.85.
NOTE 30 – When bit 79 in DIS is set to "1", bit 78 shall also be set to "1".
NOTE 31 – Some terminals which conform to the 1994 and earlier versions of this Recommendation may have used this bit to indicate use of the V.33 modulation system.
NOTE 32 – Some terminals which conform to the 1994 and earlier versions of this Recommendation may have used this bit sequence to indicate V.27 *ter*, V.29 and V.33 capabilities. In order to maintain compatibility with such terminals, a terminal which has the capability to receive using the modulation system defined in Recommendation V.17 must also be capable of receiving using the modulation system defined in Recommendation V.33. Further, a terminal which has the capability to receive using the modulation system defined in Recommendation V.33 must also be capable of receiving using the modulation system defined in Recommendation V.29.
NOTE 33 – When the modulation system defined in Recommendation V.34 is used, bits 11-14 in DCS are invalid and should be set to "0".
NOTE 34 – Setting bit 68 to "0" indicates that the called terminal's JPEG mode and T.43 mode are not available and it cannot decode JPEG or T.43 encoded data. In a DCS frame, setting bit 68 to "1" indicates that the calling terminal's JPEG mode is used and JPEG encoded image data are sent. Setting bit 68 to "0" and bit 36 to "1" indicates that the calling terminal's T.43 mode is used and T.43 encoded image data is sent. If bit 68 or 36 in the DCS is set to "1" then bits 41 or 42 or 43, and 27 in the DCS frame shall also be set to "1". Bits 42 and 43 indicate 300 × 300 and 400 × 400 pels/25.4 mm resolution respectively. Setting bit 68 and 36 to "0" indicates neither the JPEG mode nor the T.43 mode is used, image is not encoded using JPEG nor Recommendation T.43.

Table 2/T.30 *(continued)*

NOTE 35 – In DIS/DTC frame, setting bit 69 to "1" indicates that the called terminal has full colour capability. It can accept full colour image data in CIELAB space. If bit 36 is also set to "1", it can also accept colour image data defined in Recommendation T.43. Setting bit 69 to "0" and bit 68 or bits 68 and 36 to "1" indicates that the called terminal has gray-scale mode only, it accepts only the lightness component (the L* component) in the CIELAB representation for JPEG mode and for T.43 mode respectively. In a DCS frame, setting bits 68 and 69 to "1" indicates that the calling terminal sends image in full colour representation in the CIELAB space in JPEG mode. In a DCS frame, setting bits 36 and 69 to "1" indicates that the calling terminal sends colour image in T.43 mode. Setting bit 68 or 36 to "1" and bit 69 to "0" indicates that the calling terminal sends only the lightness component (the L* component) in the CIELAB representation for JPEG or T.43 mode respectively. Note that colour image will be transmitted only when bits 68 and 69 or 36 and 69 are both set to "1".

NOTE 36 – Bit 70 is called "Indication of default Huffman tables". A means is provided to indicate to the called terminal that the Huffman tables are the default tables. Default tables are specified only for the default image intensity resolution (8 bits/pel/component). The default Huffman tables are to be determined (for example, Tables K.3/T.81-K.6/T.81). In a DIS/DTC frame, bit 70 is not used and is set to "0". In a DCS frame, setting bit 70 to "0" indicates that the calling terminal does not identify the Huffman tables that it uses to encode the image data as the default tables. Setting bit 70 to "1" indicates that the calling terminal identifies the Huffman tables that it uses to encode the image data as the default tables.

NOTE 37 – In a DIS/DTC frame, setting bit 71 to "0" indicates that the called terminal can only accept image data which has been digitised to 8 bits/pel/component for JPEG mode. This is also true for T.43 mode if bit 36 is also set to "1". Setting bit 71 to "1" indicates that the called terminal can also accept image data that are digitised to 12 bits/pel/component for JPEG mode. This is also true for T.43 mode if bit 36 is also set to "1". In a DCS frame, setting bit 71 to "0" indicates that the calling terminal's image data are digitised to 8 bits/pel/component for JPEG mode. This is also true for T.43 mode if bit 36 is also set to "1". Setting bit 71 to "1" indicates that the calling terminal transmits image data which has been digitised to 12 bits/pel/component for JPEG mode. This is also true for T.43 mode if bit 36 is also set to "1".

NOTE 38 – In a DIS/DTC frame, setting bit 73 to "0" indicates that the called terminal expects a 4:1:1 subsampling ratio of the chrominance components in the image data, the a* and b* components in the CIELAB colour space representation are subsampled four times to one against the L* (Lightness) component. The details are described in Annex E/T.4. Setting bit 73 to "1" indicates that the called terminal, as an option, accepts no subsampling in the chrominance components in the image data. In a DCS frame, setting bit 73 to "0" indicates that the called terminal uses a 4:1:1 subsampling ratio of the a* and b* components in the image data. Setting bit 73 to "1" indicates that the called terminal does no subsampling.

NOTE 39 – In a DIS/DTC frame, setting bit 74 to "0" indicates that the called terminal expects that the CIE Standard Illuminant D50 is used in the colour image data as specified in Recommendation T.42. Setting bit 74 to "1" indicates that the called terminal can also accept other illuminant types besides the D50 illuminant. Setting bit 68 to "1" indicates that the terminal has the JPEG coding capability as described in Annex E/T.4. Setting bit 36 to "1" indicates that the terminal has the colour coding capability as described in Recommendation T.43. In a DCS frame, setting bit 74 to "0" and bit 68 or bit 36 to "1", indicates the calling terminal uses the D50 illuminant in the colour image data representation a specified in Recommendation T.42. Setting bit 74 to "1" indicates that another type of illuminant is used. When bits 68 and 74 are set to "1" the specification is embedded into the JPEG syntax as described in Annex E/T.4. When bits 36 and 74 are set to "1" the specification is embedded into the T.43 syntax as described in Recommendation T.43.

NOTE 40 – In a DIS/DTC frame, setting bit 75 to "0" indicates that the called terminal expects that the colour image data are represented using the default gamut range as specified in Recommendation T.42. Setting bit 75 to "1" indicates that the called terminal can also accept other gamut ranges. Setting bit 68 to "1" indicates that the terminal has the JPEG coding capability, as described in Annex E/T.4. Setting bit 36 to "1" indicates that the terminal has the colour coding capability, as described in Recommendation T.43 . In a DCS frame, setting bit 75 to "0" and bit 68 or bit 36 to "1", indicates that the calling terminal uses the default gamut range as specified in Recommendation T.42. Setting bit 75 to "1" indicates that the calling terminal uses a different gamut range. When bits 68 and 75 are set to "1", the specification is embedded into the JPEG syntax as described in Annex E/T.4. When bits 36 and 75 are set to "1", the specification is embedded into the T.43 syntax as described in Recommendation T.43.

NOTE 41 – Some terminals which conform to the pre-1996 versions of this Recommendation may set this bit to "1". Such terminals will give an answering sequence as shown in Figure III.2/T.30.

NOTE 42 – It is understood that for backwards compatibility, a transmitting terminal may ignore the request for the 64 octet frame and therefore the receiving terminal must be prepared to handle 256 octet frames by some means.

NOTE 43 – See C.7.2/T.30.

NOTE 44 – Clarification on the use of selective polling based on the settings of bit 47 and bit 35 is given in 5.3.6.1.2 5)/T.30.

NOTE 45 – Clarification on the use of subaddress for polling based on the setting of bit 35 is given in 5.3.6.1.2 6)/T.30.

Table 2/T.30 *(end)*

NOTE 46 – In a DIS/DTC frame, setting bit 37 to "0" indicates that the called terminal can only accept image data that are interleaved by stripe interleave (128 line/stripe or less). Setting bit 37 to "1" indicates that the called terminal can also accept plane interleaved image data. In a DCS frame, setting bit 37 to "0" indicates that the calling terminal's image data are interleaved through stripe interleave. Setting bit 37 to "1" indicates that the calling terminal's image data are interleaved through plane interleave. The detail of both interleaving methods are described in Recommendation T.43. NOTE 47 – The DCS is not emitted in the context of Annex H/T.30; FIF of DCS is included within the new signal "DEC' (see H.6.1/T.30) where the corresponding bit 82 must be set to "1".

1.11) In Figure A.1/T.30 revise the FCF2 description to read:

FCF2 Facsimile control field 2: Post message command (NULL, MPS, EOM, EOP, EOS, and PRI-Q)

1.12) Definition of PPS-EOS signal

In A.4.3, Figure A.1/T.30, revise Note 1 to read as follows:

FCF2	Meaning
0000 0000	NULL code which indicates the partial page boundary
1111 0000	EOM in optional T.4 error correction mode
1111 0010	MPS in optional T.4 error correction mode
1111 0100	EOP in optional T.4 error correction mode
1111 1000	EOS in optional T.4 error correction mode
1111 1001	PRI-EOM in optional T.4 error correction mode
1111 1010	PRI-MPS in optional T.4 error correction mode
1111 1100	PRI-EOP in optional T.4 error correction mode

2 Section 2

Add a new Annex G as follows:

Annex G

Procedures for secure Group 3 document facsimile transmission using the HKM and HFX system

G.1 Introduction

G.1.1 This Annex describes the protocol used by Group 3 document facsimile terminals to provide secure communications using the HKM and HFX systems. The procedures used are based upon those defined in the main body as well as Annexes A/T.30 and C/T.30.

G.1.2 Use of this Annex is optional.

G.1.3 The error correction defined in Annex A/T.30 or C/T.30 (as appropriate) is mandatory.

G.2 Outline of the secure facsimile document procedure

G.2.1 The HKM and HFX systems provide the following capabilities for secure document communications between entities (terminals or terminal operators):

- mutual entity authentication;
- secret session key establishment;
- document confidentiality;
- confirmation of receipt;
- confirmation or denial of document integrity.

G.2.2 Functions

Key management is provided using the HKM system defined in Annex B/T.36. Two procedures are defined: the first being registration and the second being the secure transmission of a secret key. Registration establishes mutual secrets and enables all subsequent transmissions to be provided securely. In subsequent transmissions, the HKM system provides mutual authentication, a secret session key for document confidentiality and integrity, confirmation of receipt and a confirmation or denial of document integrity.

Document confidentiality is provided using the carrier cipher defined in Annex D/T.36. The carrier cipher uses a 12-decimal digit key which is approximately equivalent to 40 bits.

Document integrity is provided using the system defined in Annex E/T.36. Recommendation T.36 defines the hashing algorithm including the associated calculations and information exchange.

G.2.3 Method

In the registration mode, the two terminals exchange information which enables entities to uniquely identify each other. This is based upon the agreement between the users of a secret one-time key. Each entity stores a 16-digit number which is uniquely associated with the entity with which it has carried out registration.

When it is required to send a document securely, the transmitting terminal transmits the 16-digit secret number associated with the receiving entity together with a random number and an encrypted session key as a challenge to the receiving entity. The receiving terminal responds by transmitting the 16-digit key associated with the transmitting entity along with a random number and a re-encrypted version of the challenge from the transmitting entity. At the same time it transmits a random number and an encrypted session key as a challenge to the transmitting entity. The transmitting terminal responds with a random number and a re-encrypted version of the challenge from the receiving entity. This procedure enables the two entities to mutually authenticate each other. At the same time the transmitting terminal transmits a random number and the encrypted session key to be used for encrypting and hashing.

After transmission of the document, the transmitting terminal transmits a random number and an encrypted session key as a challenge to the receiving entity. At the same time it sends a random number and encrypted hash value which enables the receiving entity to ensure the integrity of the received document. The receiving terminal transmits a random number and the re-encrypted version of the challenge from the transmitting entity. At the same time it sends a random number and encrypted Integrity Document to act as confirmation or denial of the integrity of the received document.

The hashing algorithm used for document integrity is carried out on the whole document.

An override mode is provided that does not involve the exchange of any security signals between the two terminals. The users agree a one-time secret session key to be entered manually. This is used by the transmitting terminal to encrypt the document and by the receiving terminal to decrypt the document.

G.3 References

The following ITU-T Recommendations, and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendation and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

- ITU-T Recommendation T.4 (1996), *Standardization of Group 3 facsimile terminals for document transmission.*

- ITU-T Recommendation T.36 (1997), *Security capabilities for use with Group 3 facsimile terminals.*

G.4 Definitions

G.4.1 Operation on the PSTN using the V.27 *ter*, V.29, V.17 and V.34 (half-duplex mode) modulation systems

The signals and definitions used with the secure facsimile document procedures are as defined in the main body and Annex A/T.30 together with those detailed in G.6.1/T.30.

G.4.2 Operation on the PSTN using the V.34 (full-duplex mode) modulation system and on the ISDN

The signals and definitions used with the secure facsimile document procedures are as defined in Annex C/T.30 together with those in G.6.1/T.30.

G.5 Abbreviations

G.5.1 The abbreviations used for secure facsimile transmission are as defined in the main body of this Recommendation and Annexes A/T.30 and C/T.30 together with those specified below.

ESHx	Encrypted Scrambled Hash Value from the transmitter
ESIMy	Encrypted Scrambled Integrity Message from the receiver
ESSC1x	Encrypted Scrambled Secret Challenge key from the transmitter
ESSC1y	Encrypted Scrambled Secret Challenge key from the receiver
ESSC2x	Encrypted Scrambled Secret Challenge key from the transmitter
ESSR1x	Encrypted Scrambled Secret Response key from the transmitter
ESSR1y	Encrypted Scrambled Secret Response key from the receiver
ESSR2y	Encrypted Scrambled Secret Response key from the receiver
ESSS1x	Encrypted Scrambled Secret session key from the transmitter
RCNx	Registered Crypt Number (16 decimal digits in 16 octets) associated with the transmitter
RCNy	Registered Crypt Number (16 decimal digits in 16 octets) associated with the receiver
RK	Receiver Keys – see G.6.1/T.30
RNC1x	Random number associated with a secret challenge from the transmitter
RNC1y	Random number associated with a secret challenge from the receiver

RNC2x	Random number associated with a secret challenge from the transmitter
RNIMy	Random number associated with an integrity message from the receiver
RNSR1x	Random number associated with a secret response from the transmitter
RNSR1y	Random number associated with a secret response from the receiver
RNSR2y	Random number associated with a secret response from the receiver
RNSS1x	Random number associated with a secret session key from the transmitter
RTC	Return to control – as defined in Recommendation T.4
TK	Transmitter Keys – see G.6.1/T.30
TKx	Transfer Key provided by the transmitter
TKy	Transfer Key provided by the receiver
TNR	Transmitter Not Ready – see G.6.1/T.30
TR	Transmitter Ready – see G.6.1/T.30

NOTE 1 – All Random Number values are 4 decimal digits in 4 octets.

NOTE 2 – All Encrypted Scrambled values are 12 decimal digits in 12 octets.

G.6 Facsimile procedures

G.6.1 Facsimile control field

The HKM Key Management system uses the T.30 Transmitter Keys (TK) and Receiver Keys (RK) frames. The FIF contents of these signals vary according to use and are listed G.6.2/T.30. Each TK and RK signal is suffixed by a digit for cross reference to the flow diagrams and signal sequence diagrams in this Annex.

Each key transferred (other than during Registration) is in Encrypted Scrambled (ES) format and is accompanied by an associated Random Number (RN).

1) *Transmitter Not Ready (TNR)* – This signal is used to indicate that the transmitter is not yet ready to transmit.

   Format:
   X101 0111

2) *Transmitter Ready (TR)* – This signal is used to ask the status of the transmitter.

   Format:
   X101 0110

3) *Transmitter Keys (TK)* – This signal is used to carry security keys, etc. from the document transmitter to the document receiver. The FIF contents of this signal are defined later in this Annex and will vary according to the circumstances under which they are used.

   Format:
   1101 0010

4) *Receiver Keys (RK)* – This signal is used to carry security keys, etc. from the document receiver to the document transmitter. The FIF contents of this signal are defined later in this Annex and will vary according to the circumstances under which they are used.

   Format:
   0101 0010

G.6.2 Facsimile information fields

The coding of the keys shall be as shown in Table 3/T.30 and the least significant bit of the least significant digit shall be the first bit transmitted.

G.6.2.1 Mutual Registration and authentication

See Table G.1/T.30

Table G.1/T.30

Signal	FIF octets	FIF contents
TK0	1	0000 0000
	2 length	0010 0000
	3-18	TKx
	19-22	RNC0x
	23-34	ESSC0x
RK1	1	0000 0001
	2 length	0100 0000
	3-18	RCNy
	19-34	TKy
	35-38	RNSR0y
	39-50	ESSR0y
	51-54	RNC0y
	55-66	ESSC0y
TK2	1	0000 0010
	2 length	0010 0000
	3-18	RCNx
	19-22	RNSR0x
	23-34	ESSR0x

G.6.2.2 Pre-message signals: mutual authentication and exchange of secret session key

See Table G.2/T.30

Table G.2/T.30

Signal	FIF octets	FIF contents
TK8	1	0000 1100
	2 length	0010 0000
	3-18	RCNy
	19-22	RNC1x
	23-34	ESSC1x
RK9	1	0000 1001
	2 length	0011 0000
	3-18	RCNx
	19-22	RNSR1y
	23-34	ESSR1y
	35-38	RNC1y
	39-50	ESSC1y
TK10	1	0000 1010
	2 length	0010 0000
	3-6	RNSR1x
	7-18	ESSR1x
	19-21	RNSS1x
	23-34	ESSS1x
NOTE – If the document is not encrypted, RNC1x and ESSS1x are set to all zeroes.		

G.6.2.3 In-message procedure

From the transmitter to the receiver. The in-message procedure formats and specific signals shall be as defined in Annex A/T.4.

G.6.2.4 Post message signals: document confirmation and integrity (normal transmission)

See Table G.3/T.30

Table G.3/T.30

Signal	FIF octets	FIF contents
TK16	1 2 length 3-6 7-18 19-42	0001 0000 0010 1000 RNC2x ESSC2x ESHx
RK17	1 2 length 3-6 7-18 19-22 23-34	0001 0001 0010 0000 RNSR2y ESSR2y RNIMy ESIMy
NOTE 1 – If the document does not have an integrity check, ESHx, RNIMy and ESIMy are set to all zeroes. NOTE 2 – Frame TK16 is not provided if DCS indicates no hashing. NOTE 3 – Frame RK17 is not provided if TK16 is not provided.		

G.6.2.5 General notes

1) During registration, challenges and responses are mandatory. The challenge/response mechanism is defined in Recommendation T.36.

2) During normal calls, all valid challenges and responses must have a non-zero random number. Random numbers set to zero in challenges or responses indicate that mutual authentication is not supported.

3) TK16/RK17 are normally sent with/after PPS-EOP except in the case of turnaround polling when they may be sent with/after PPS-EOM.

4) Hashing/encryption are determined by the first DIS/DCS exchange and apply to every document transmitted in that session.

G.7 Flow diagrams

G.7.1 Operation on the PSTN using the V.27 *ter*, V.29, V.17 and V.34 (half-duplex mode) modulation systems

The flow diagrams in Figure G.7-1/T.30 show the phase B, pre-message procedures, phase C, message procedure, phase D, post-message procedure and phase E, call release, for both the transmitting and receiving terminals.

Reference should also be made to the procedures defined in Recommendation T.36.

G.7.2 Flow diagram rules

The flow diagrams follow two simple rules:

1) All lines have an arrow at the destination only.

2) No lines cross.

G.7.3 Timers used in flow diagrams

T1	35 s ± 5 s
T2	6 s ± 1 s
T3	10 s ± 5 s
T4	4.5 s ± 15% for manual units
T4	3.0 s ± 15% for automatic units
T5	60 s ± 5 s

G.7.4 Abbreviations and descriptions used in the flow diagrams

Unless defined otherwise below, the definition of the flow chart terms is as given in the main body and/or Annex A/T.30.

Authen reqd? Check to see if mutual authentication is required at the beginning of the transmission.

NOTE 1 – Once mutual authentication has been completed, then within the same session the "No" exit should always be followed.

Reg mode? Check to see if security registration is required.

First page? Check to see if mutual authentication is required at the beginning of the transmission.

NOTE 2 – Once mutual authentication has been completed, then within the same session the "No" exit should always be followed.

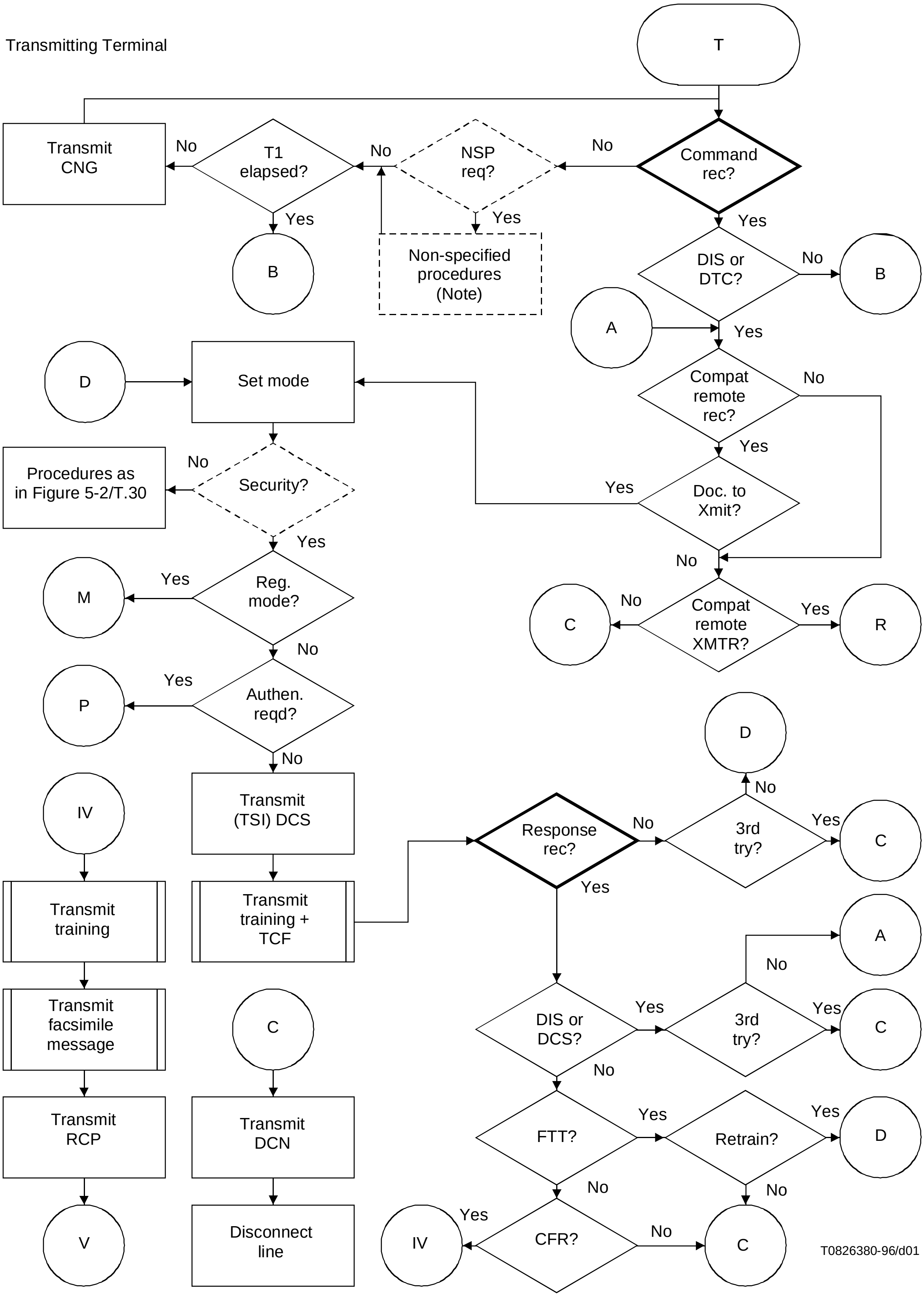
G.8 Flow diagrams

G.8.1 Operation on the PSTN using the V.34 (full-duplex mode) modulation system and on the ISDN

The operation of secure document facsimile on the PSTN using the V.34 (full-duplex) modulation system and on the ISDN is exactly as defined in Annex C/T.30 with the exceptions shown on the flow diagrams below.

The flow diagrams in Figure G.8/T.30 show the phase B, pre-message procedures, phase D, post-message procedure and phase E, call release, for both the transmitting and receiving terminals.

Reference should also be made to the procedures defined in Recommendation T.36.



NOTE – The non-specified procedure, NSP, refers to a procedure which takes 6 seconds or less to complete. It may not necessarily be a definable signal sequence.

Figure G.7-1/T.30 (sheet 1 of 20)

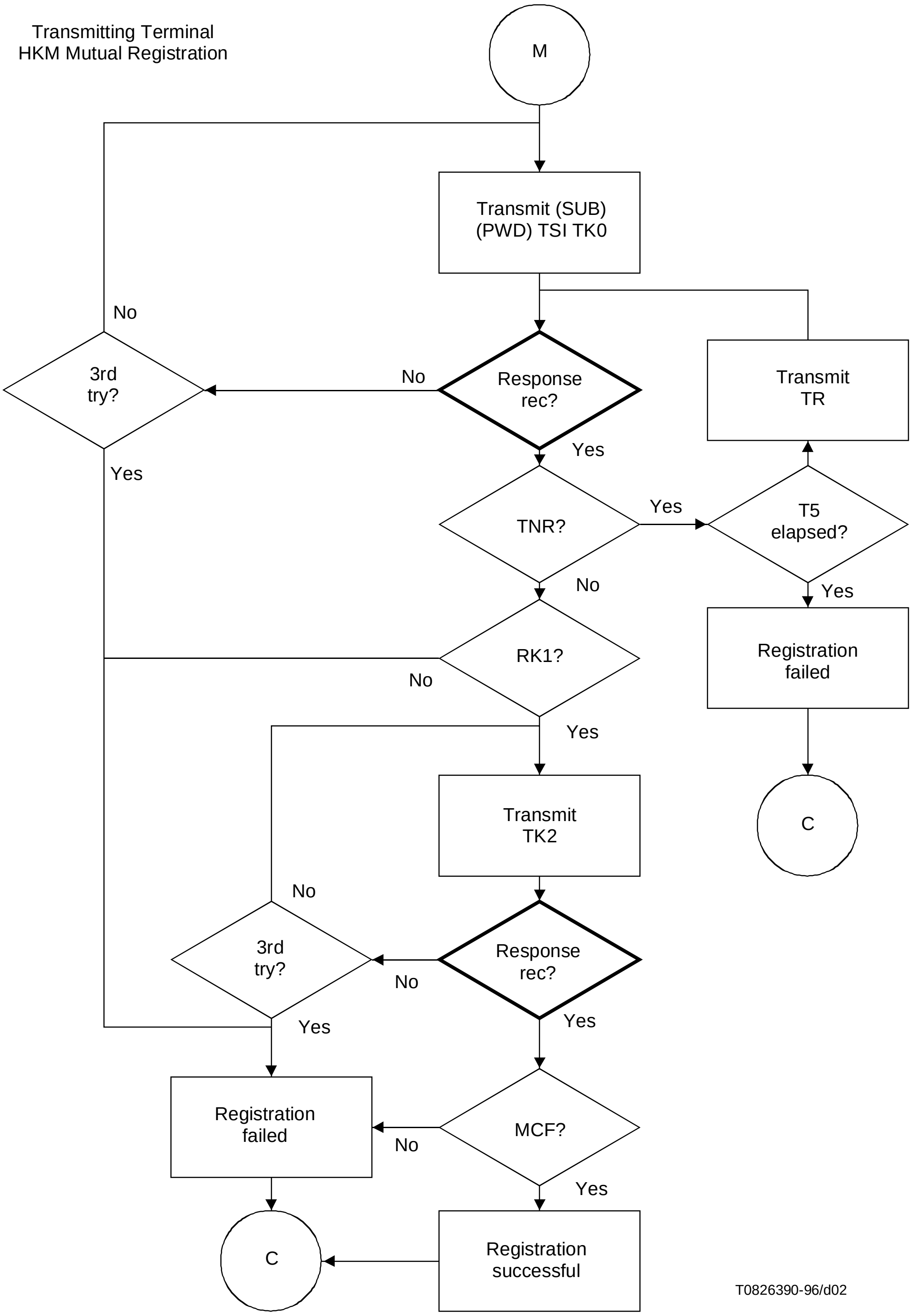


Figure G.7-1/T.30 (sheet 2 of 20)

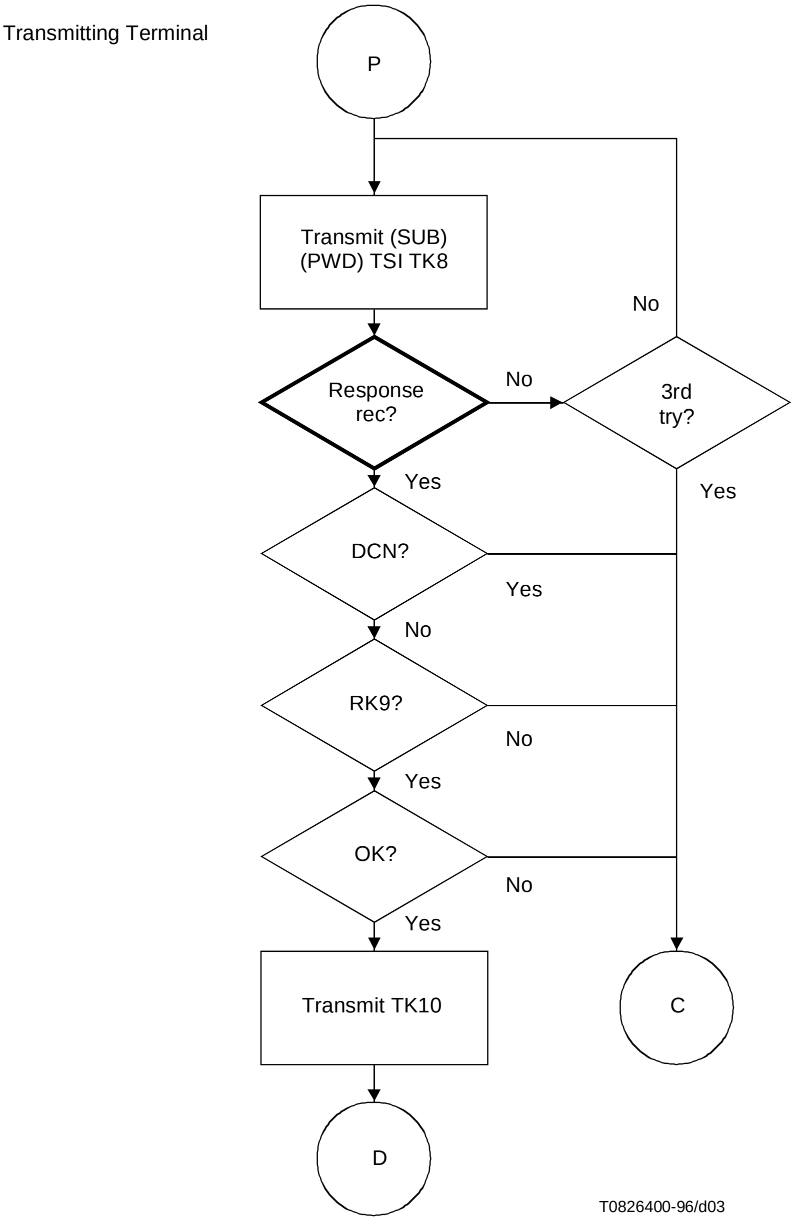


Figure G.7-1/T.30 (sheet 3 of 20)

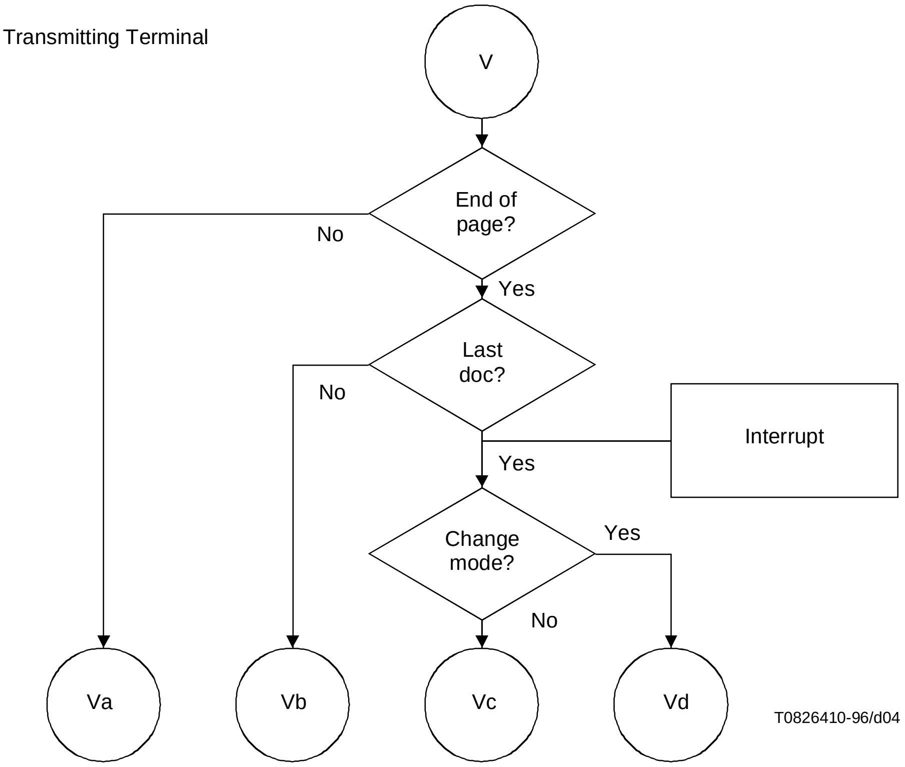


Figure G.7-1/T.30 (sheet 4 of 20)

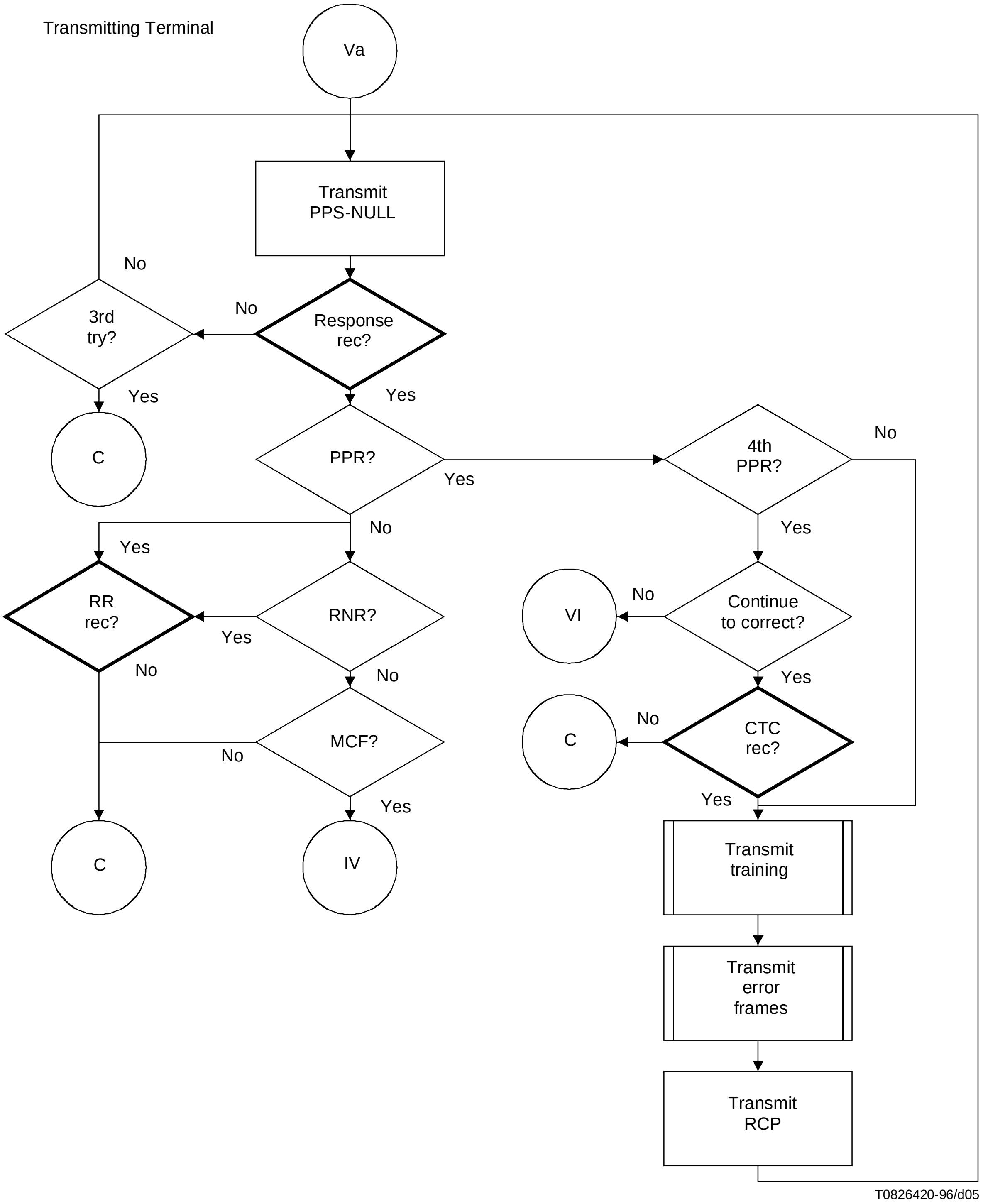


Figure G.7-1/T.30 (sheet 5 of 20)

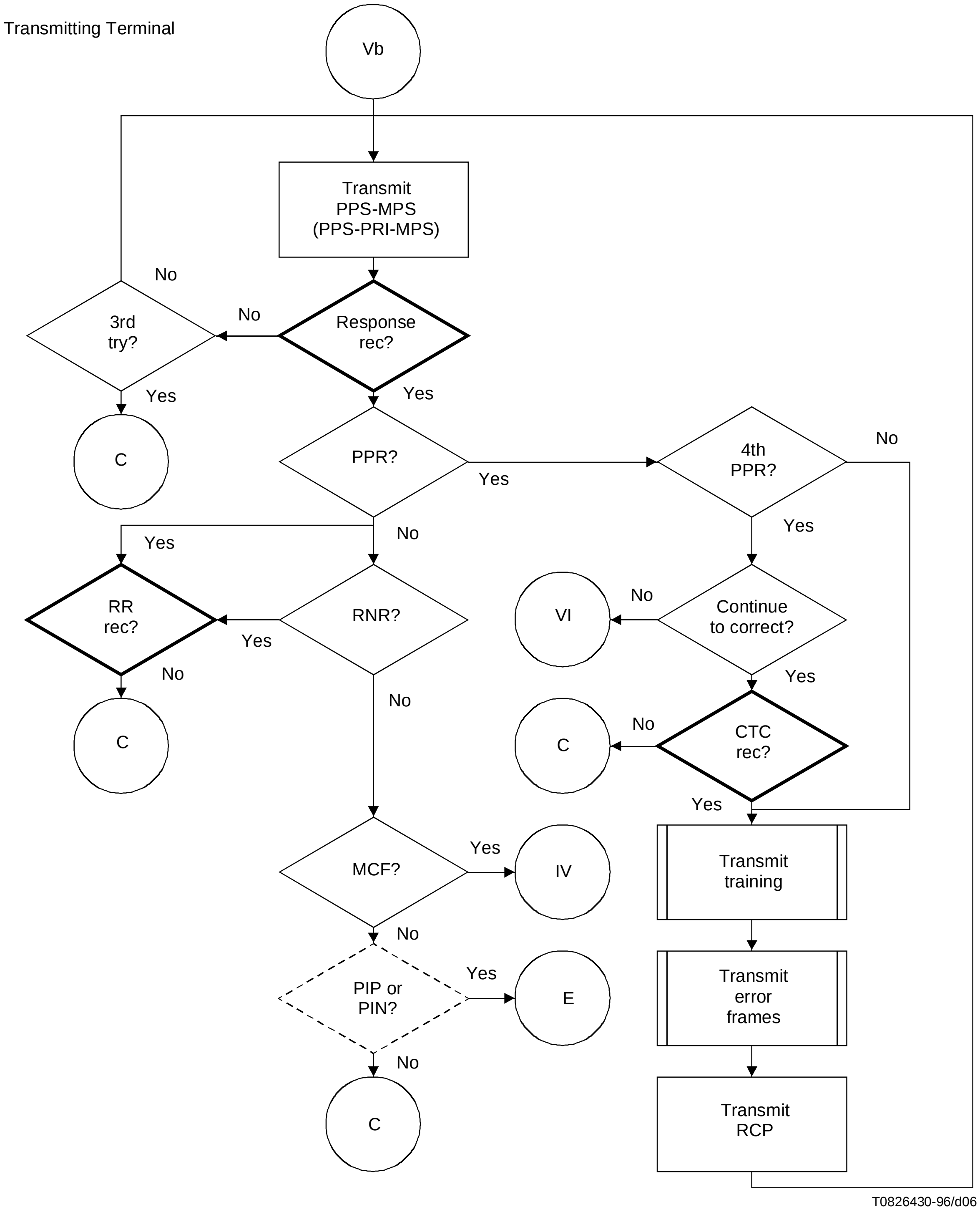


Figure G.7-1/T.30 (sheet 6 of 20)

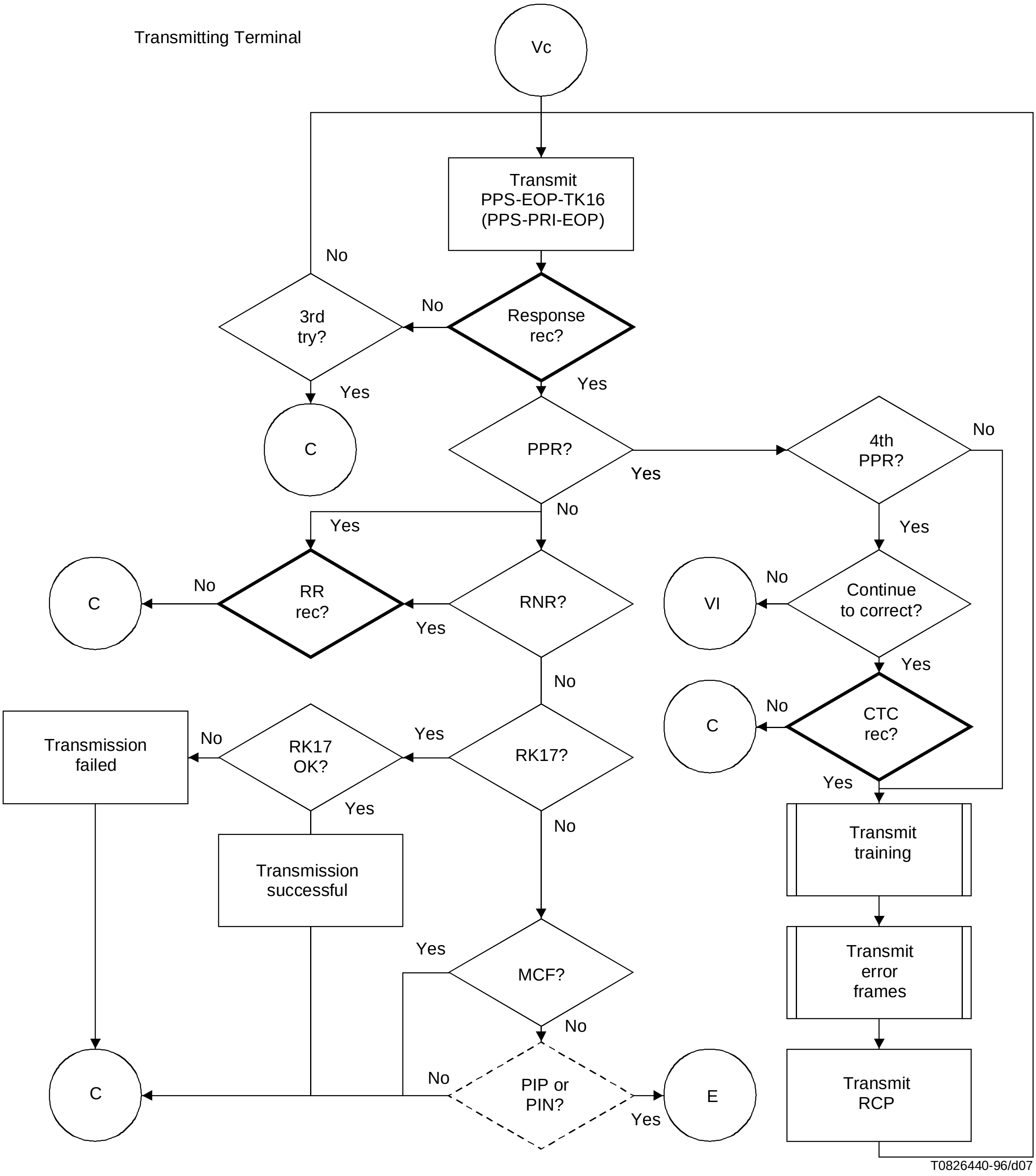


Figure G.7-1/T.30 (sheet 7 of 20)

Transmitting Terminal

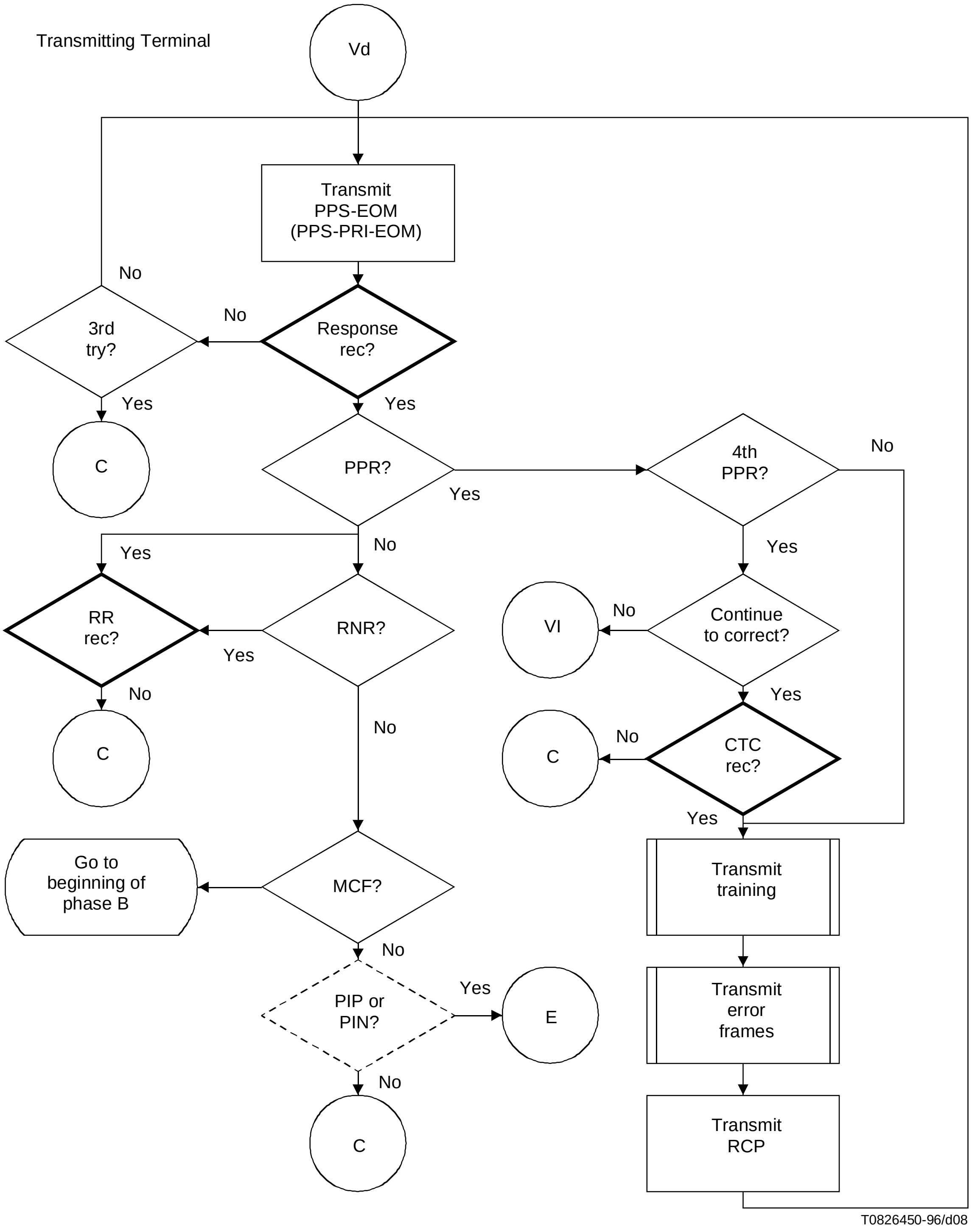


Figure G.7-1/T.30 (sheet 8 of 20)

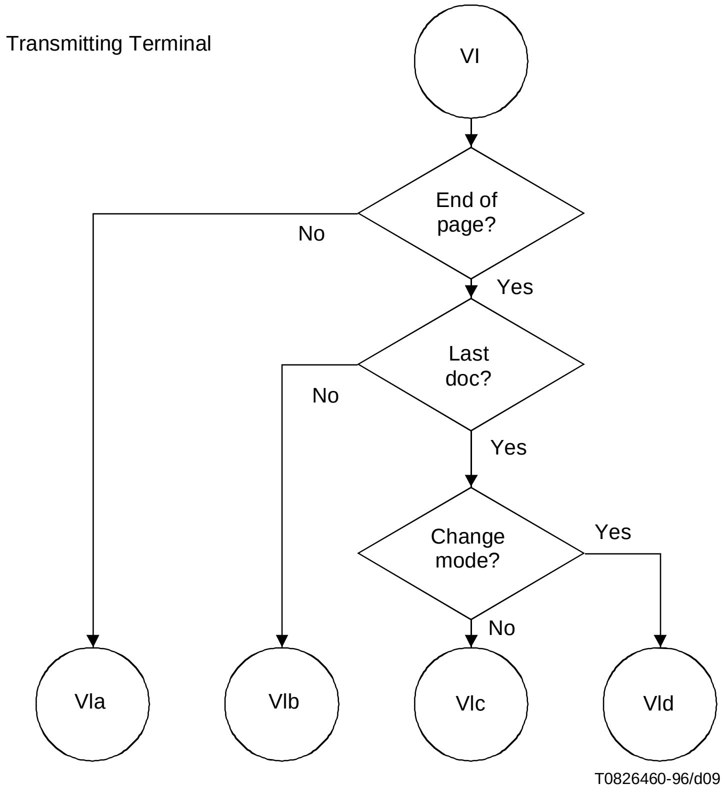


Figure G.7-1/T.30 (sheet 9 of 20)

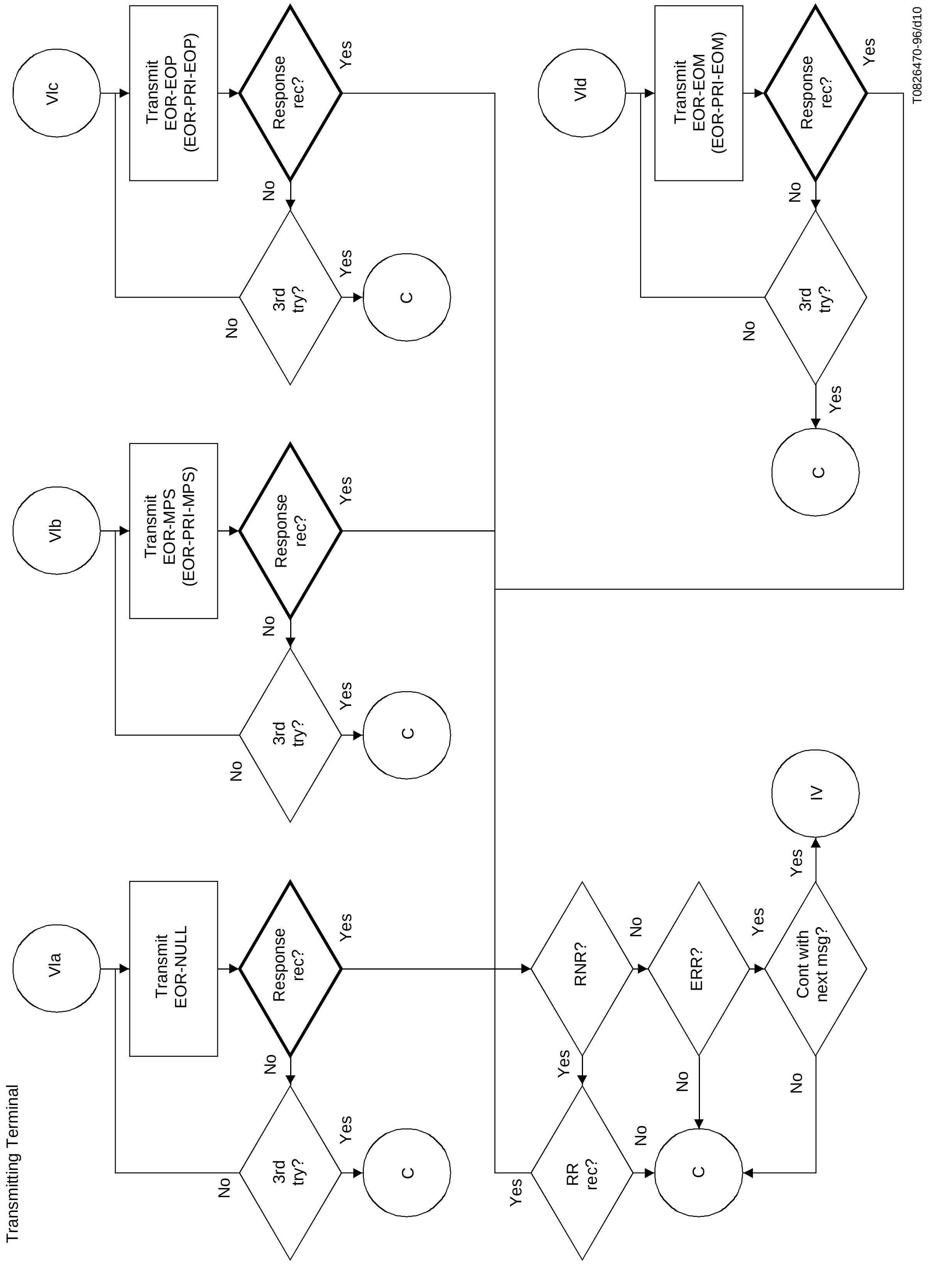


Figure G.7-1/T.30 (sheet 10 of 20)

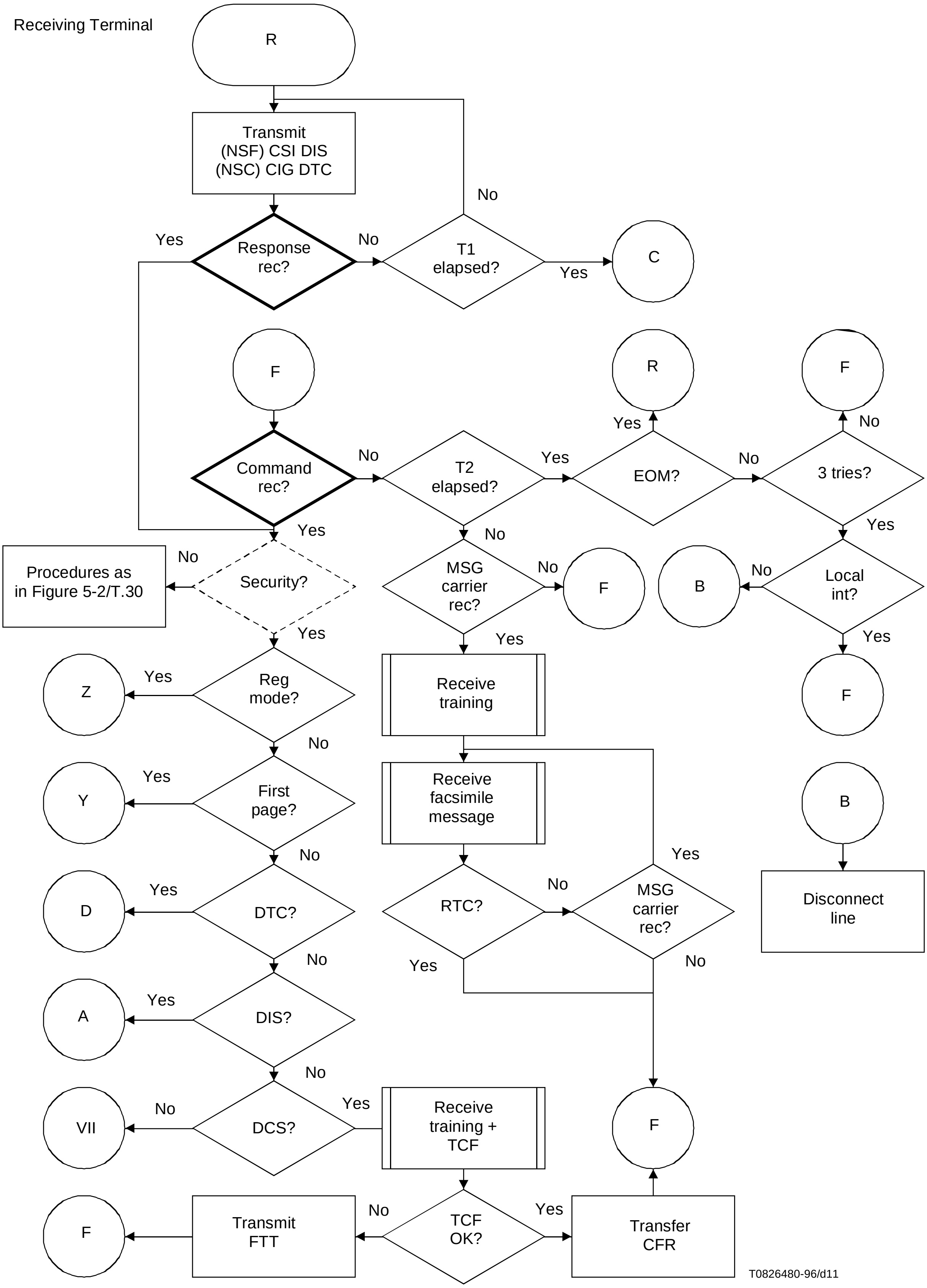


Figure G.7-1/T.30 (sheet 11 of 20)

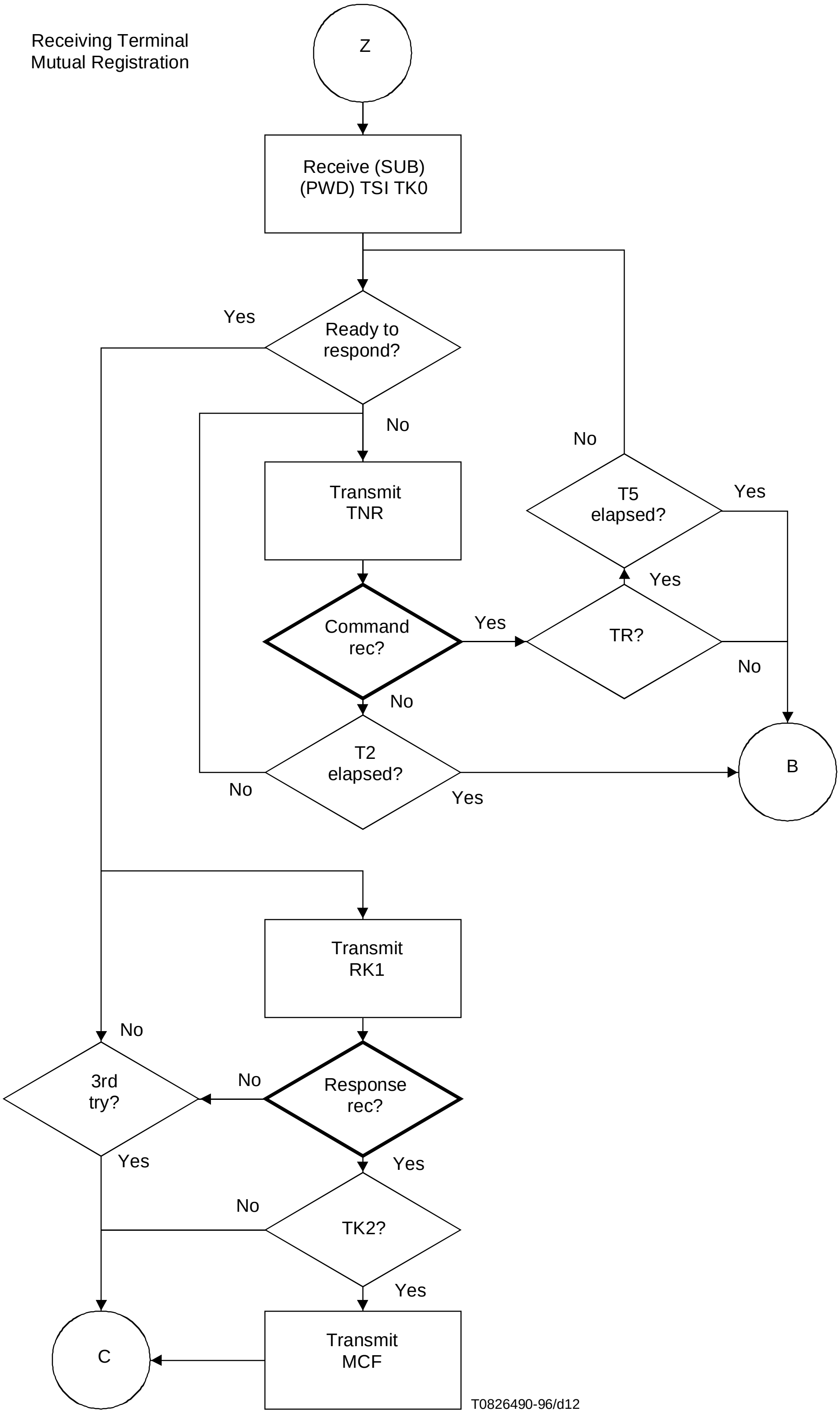


Figure G.7-1/T.30 (sheet 12 of 20)

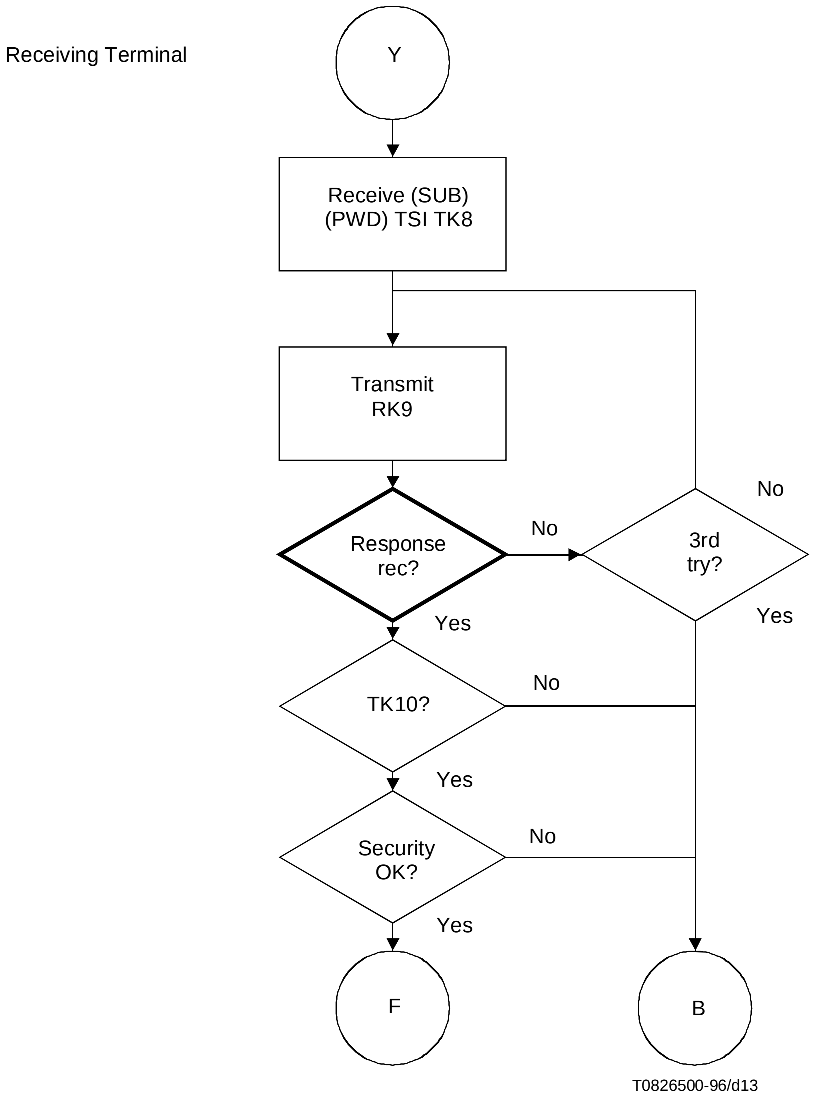


Figure G.7-1/T.30 (sheet 13 of 20)

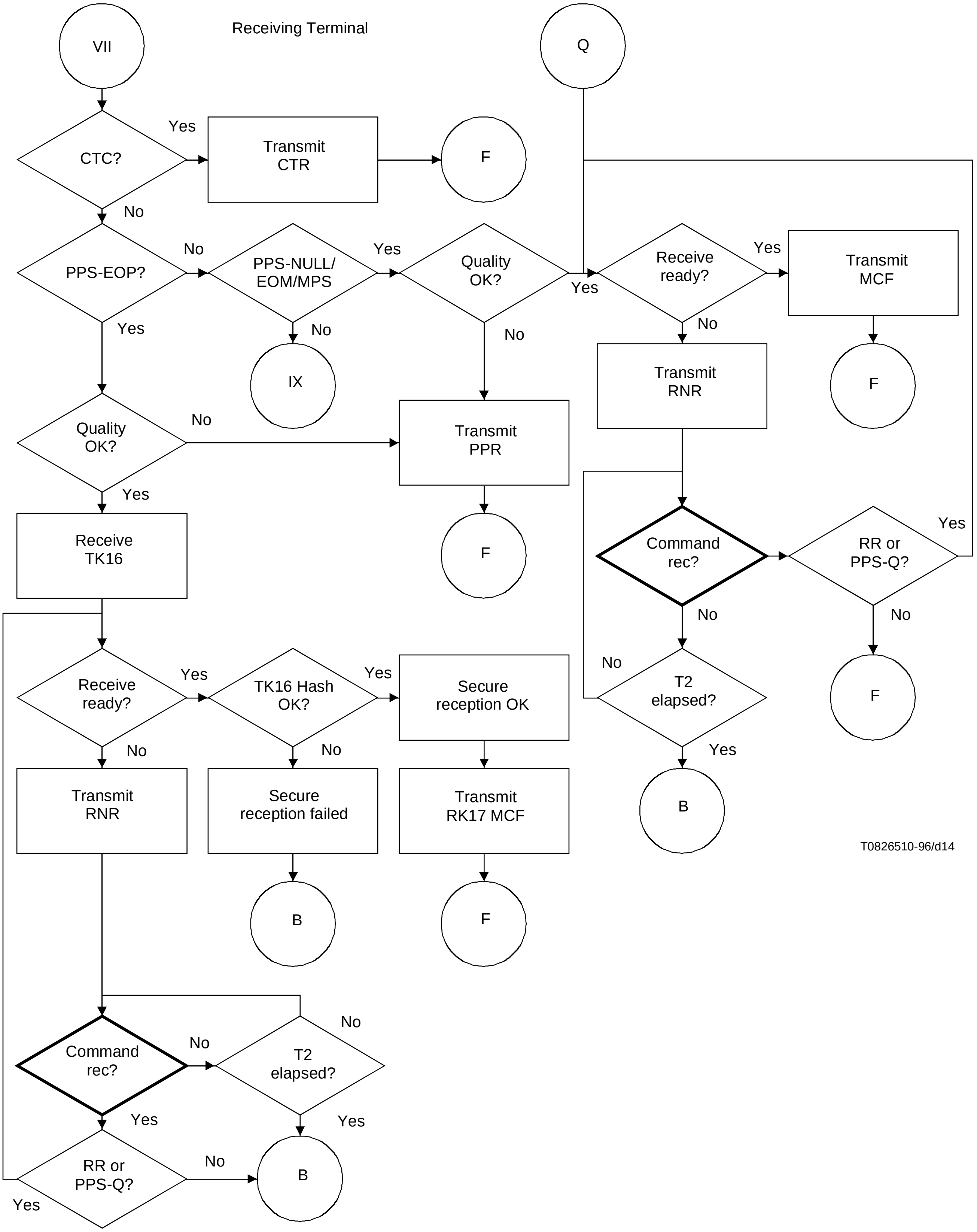


Figure G.7-1/T.30 (sheet 14 of 20)

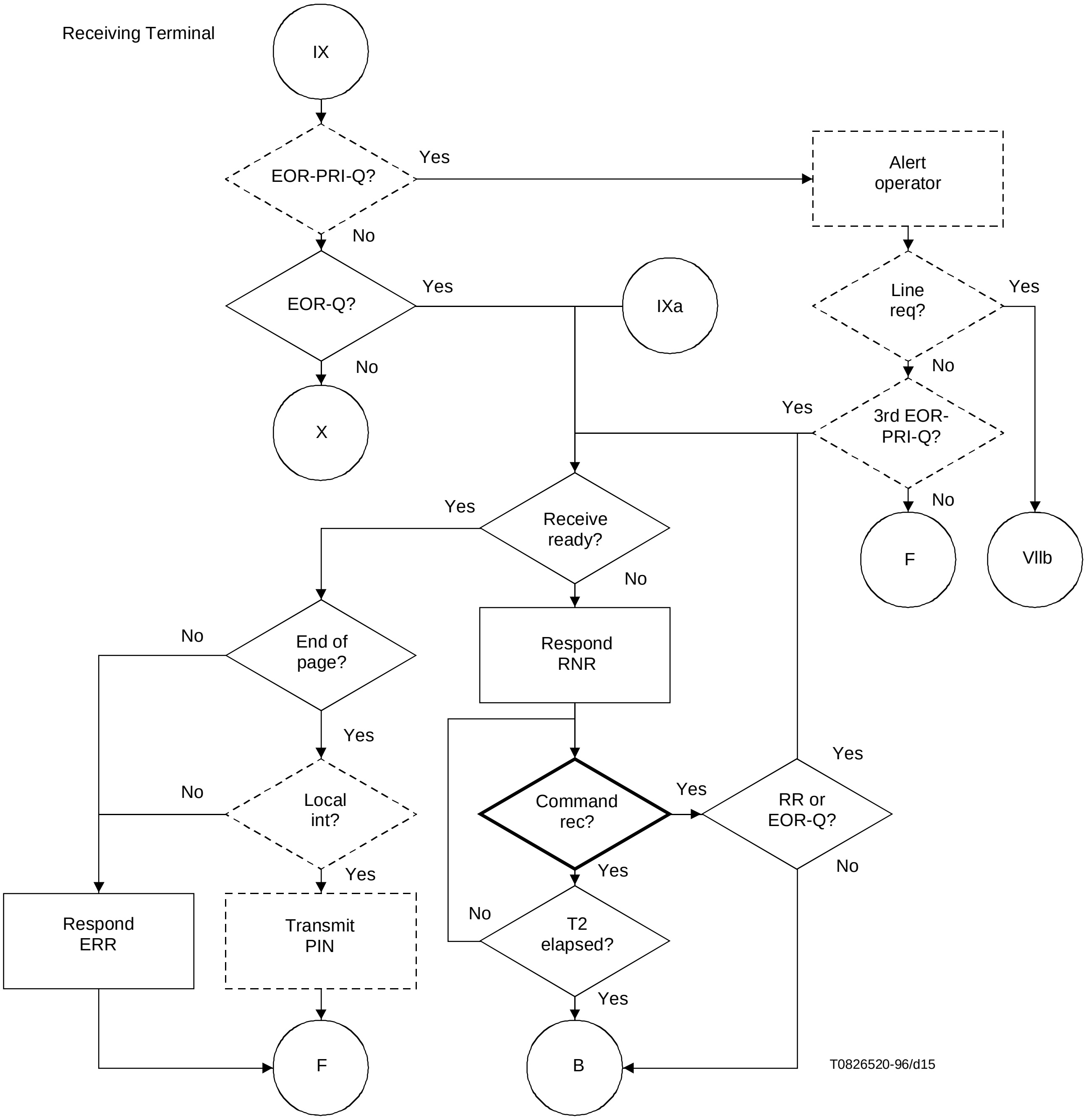


Figure G.7-1/T.30 (sheet 15 of 20)

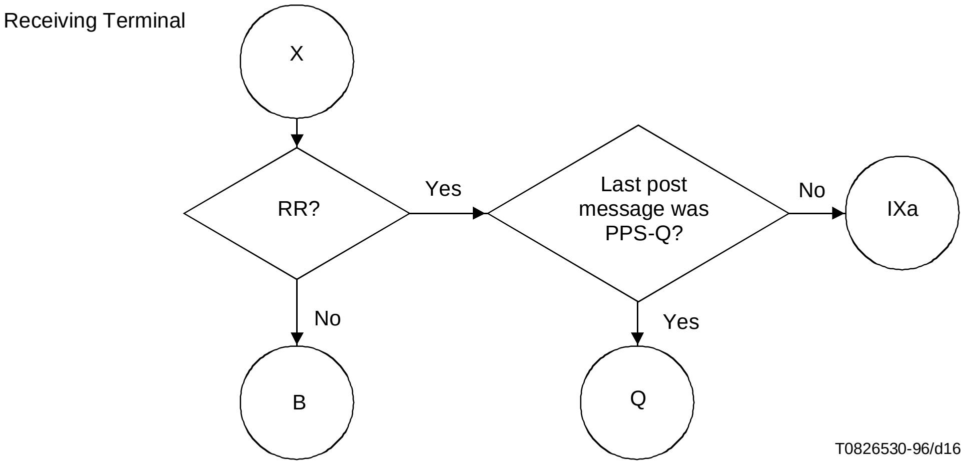


Figure G.7-1/T.30 (sheet 16 of 20)

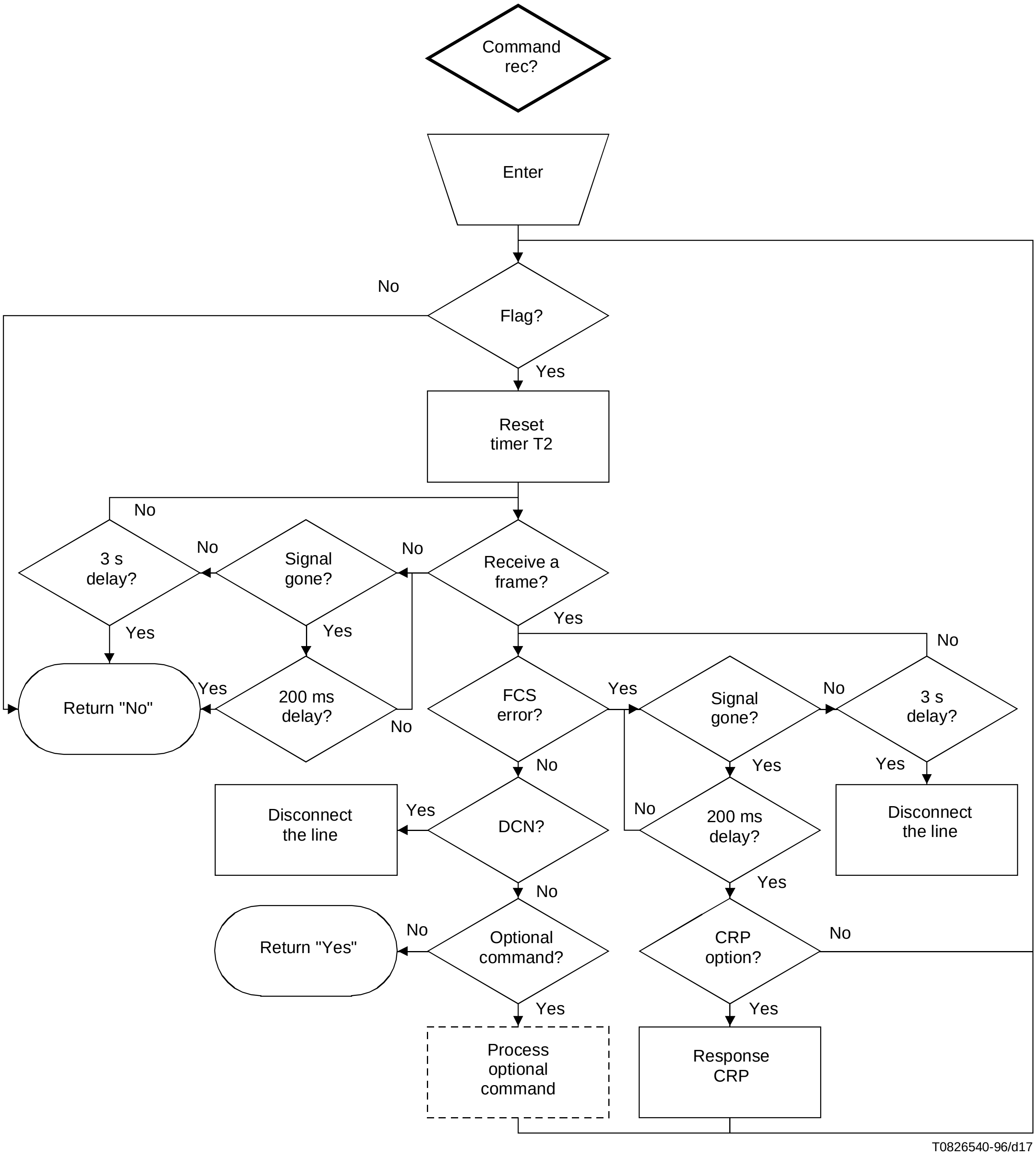


Figure G.7-1/T.30 (sheet 17 of 20)

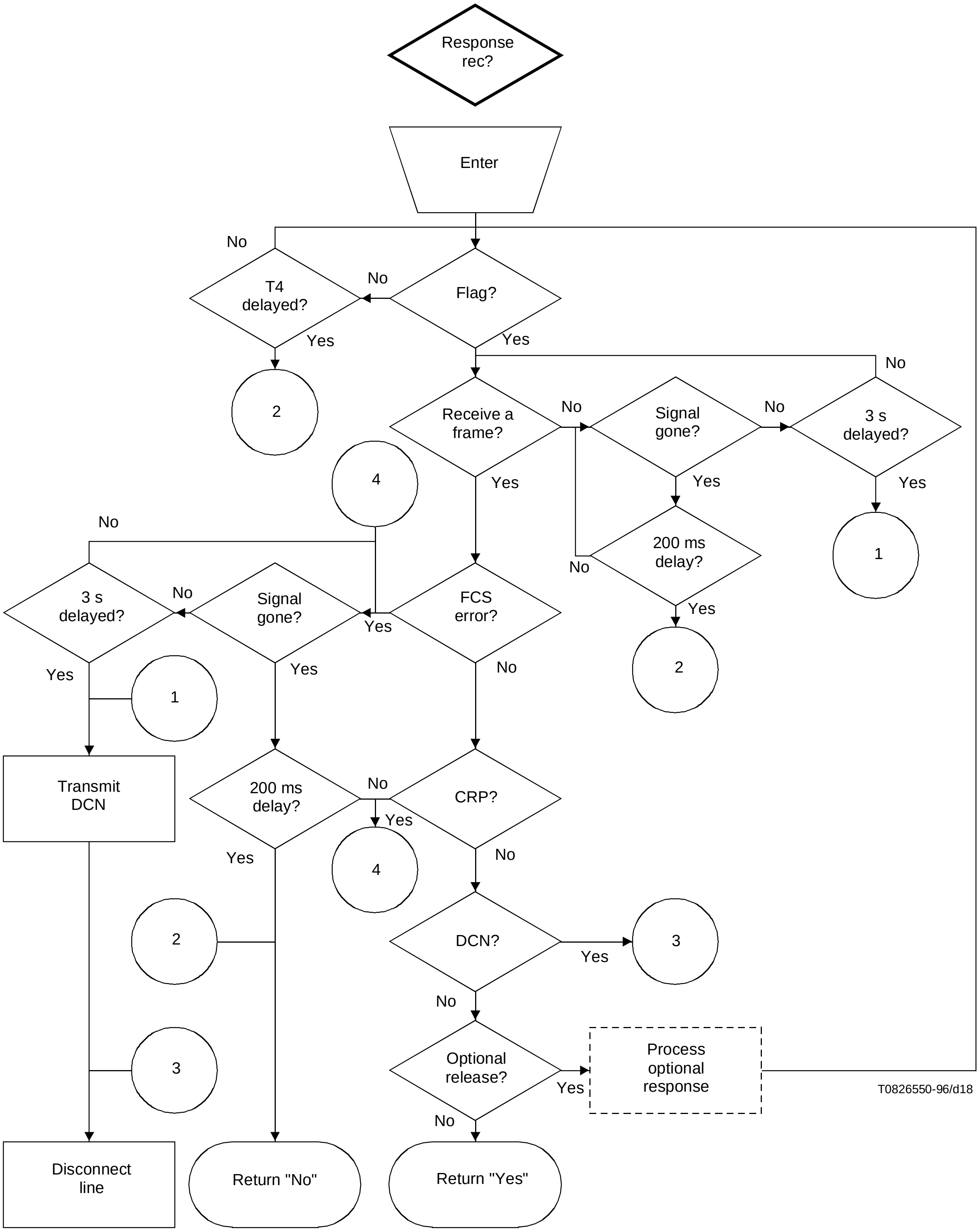


Figure G.7-1/T.30 (sheet 18 of 20)

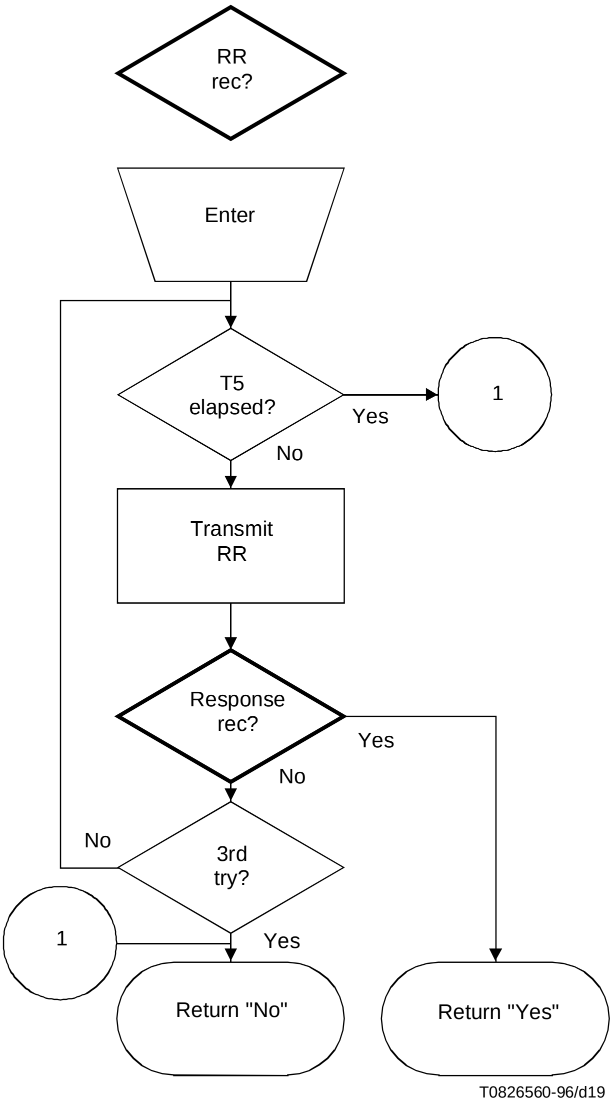


Figure G.7-1/T.30 (sheet 19 of 20)

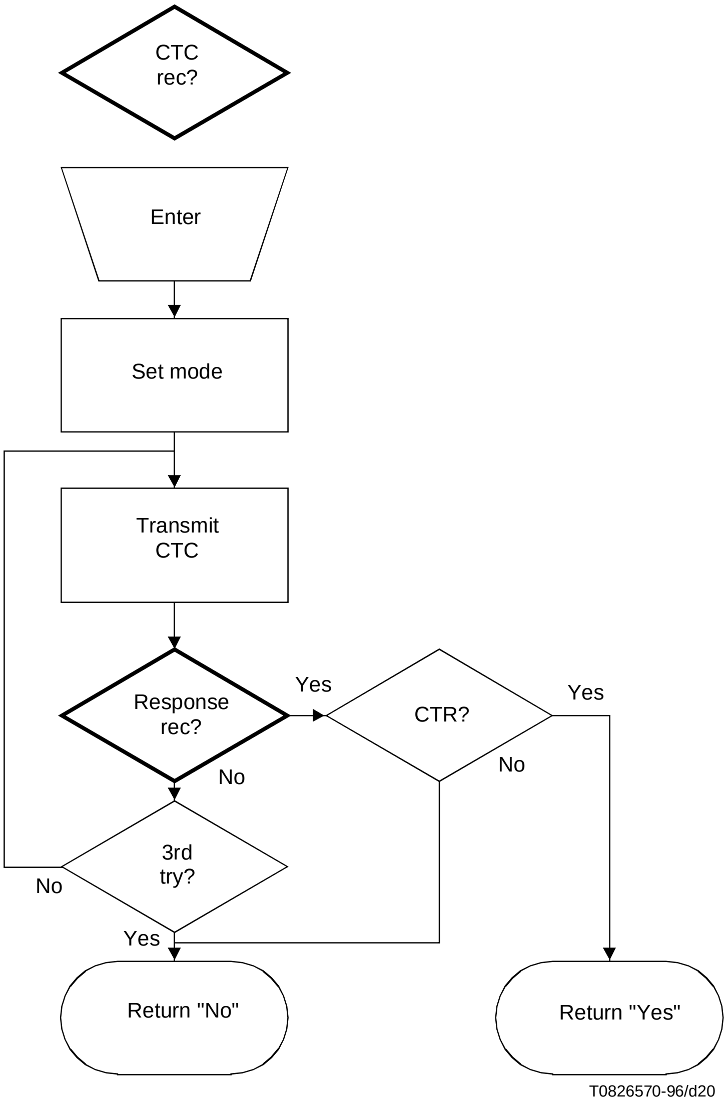


Figure G.7-1/T.30 (sheet 20 of 20)

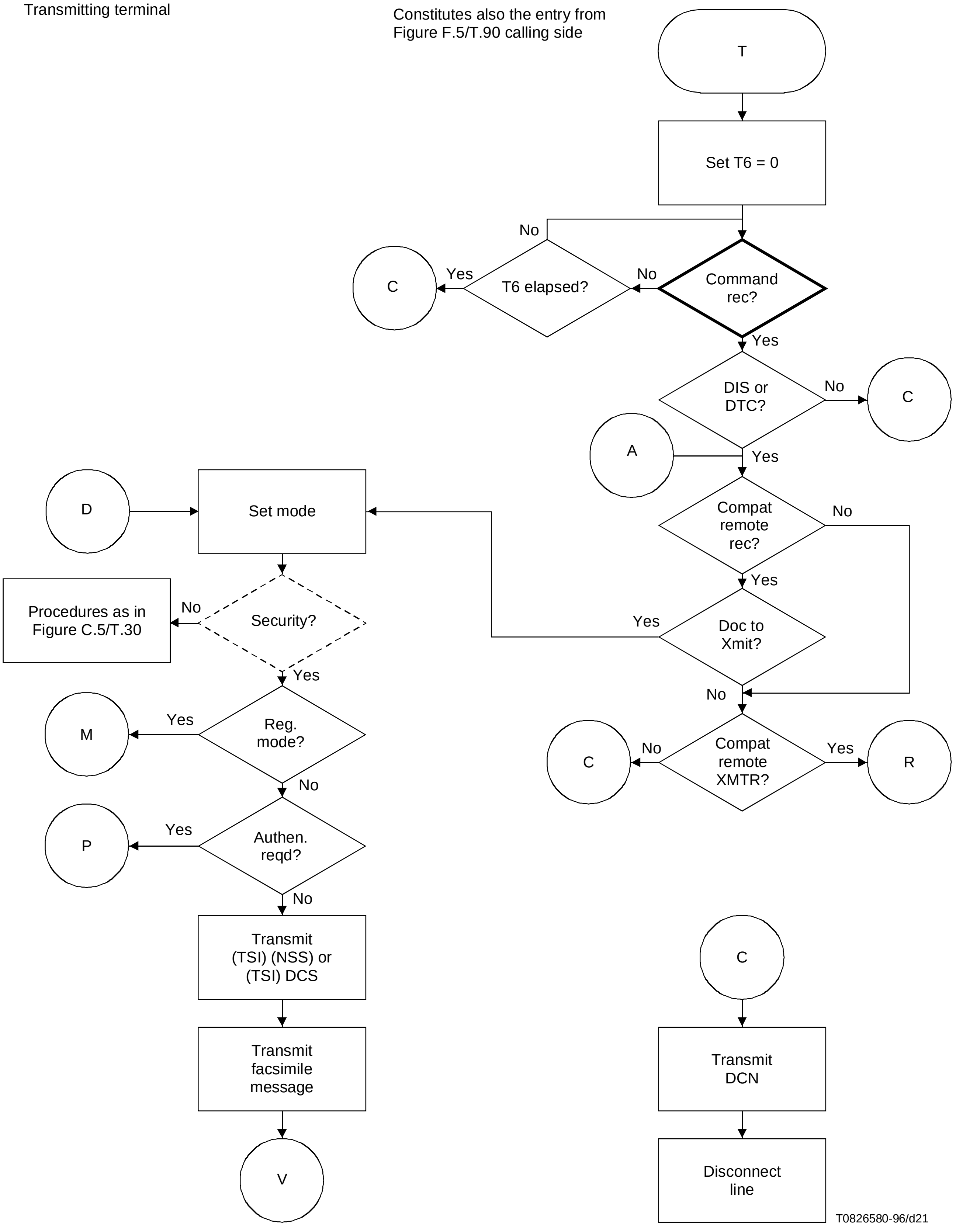


Figure G.8-1/T.30 (sheet 1 of 3) (Used instead of Figure C.5/T.30) Duplex

Transmitting terminal
HKM mutual registration

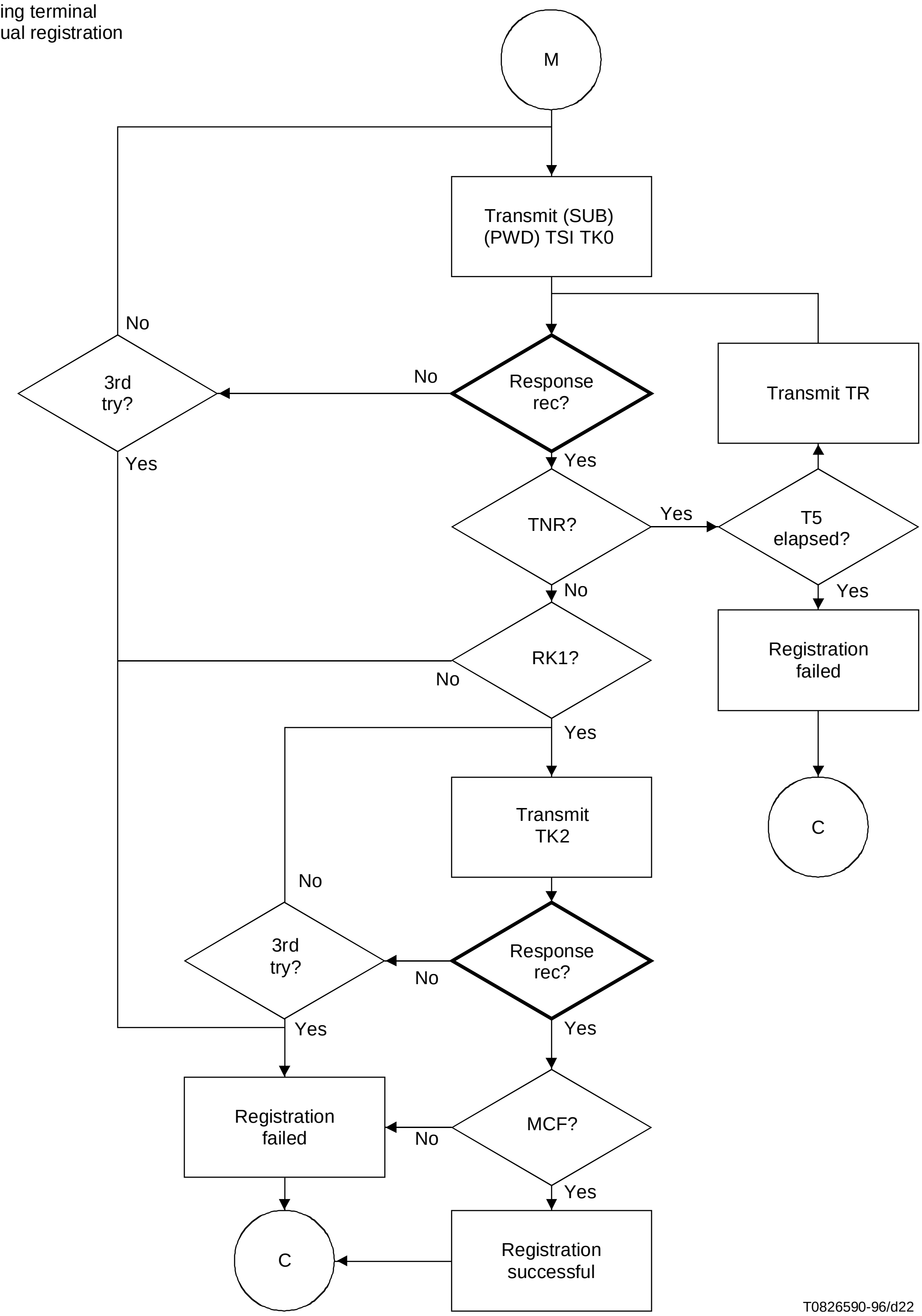


Figure G.8-1/T.30 (sheet 2 of 3) (Used instead of figure C.5/T.30) Duplex

Transmitting terminal

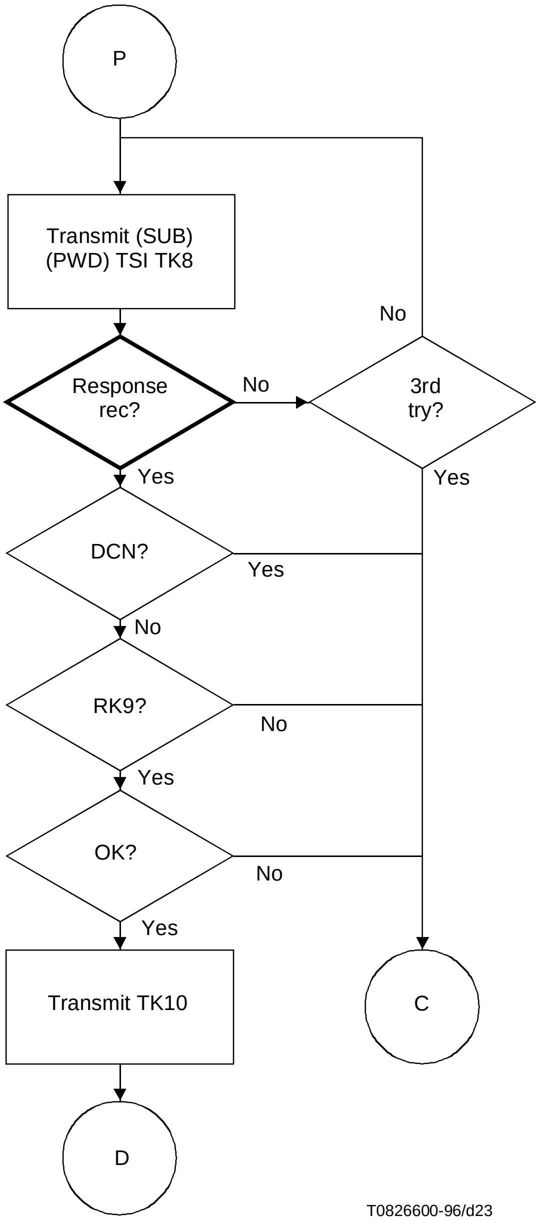


Figure G.8-1/T.30 (sheet 3 of 3) (Used instead of figure C.5/T.30) Duplex

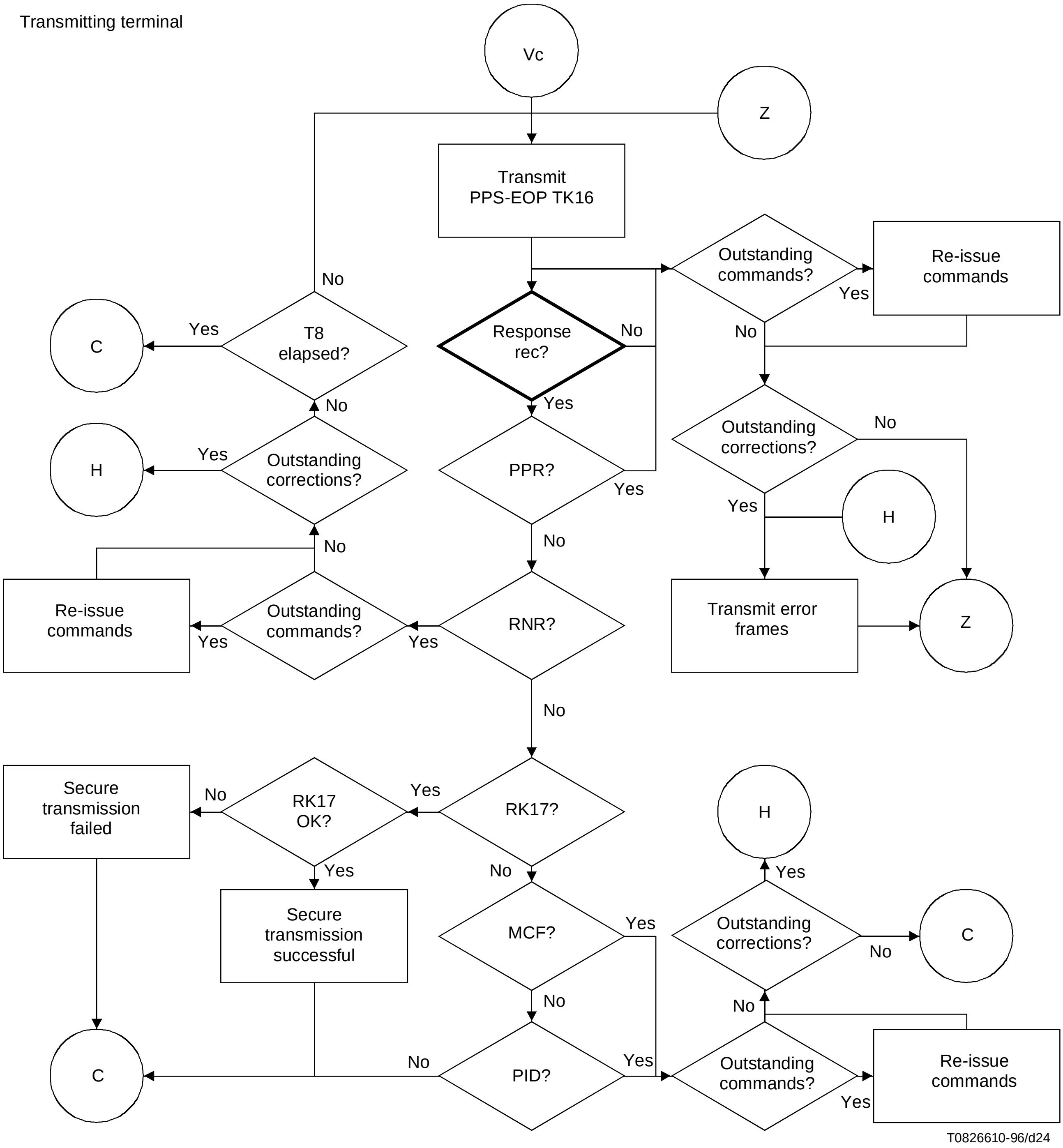


Figure G.8-2/T.30 (Used instead of figure C.9/T.30) Duplex

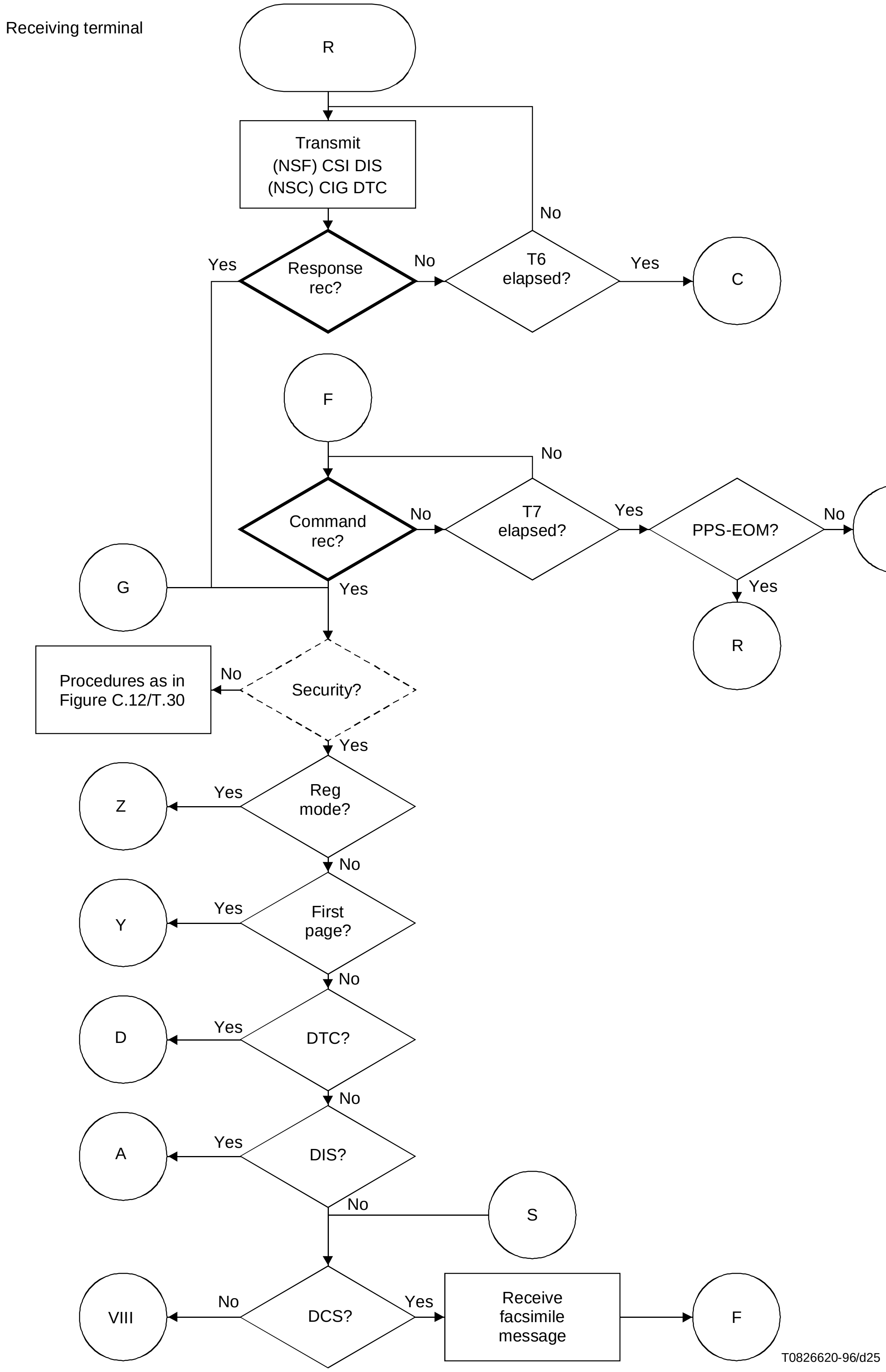


Figure G.8-3/T.30 (sheet 1 of 3) (Used instead of figure C.12/T.30) Duplex

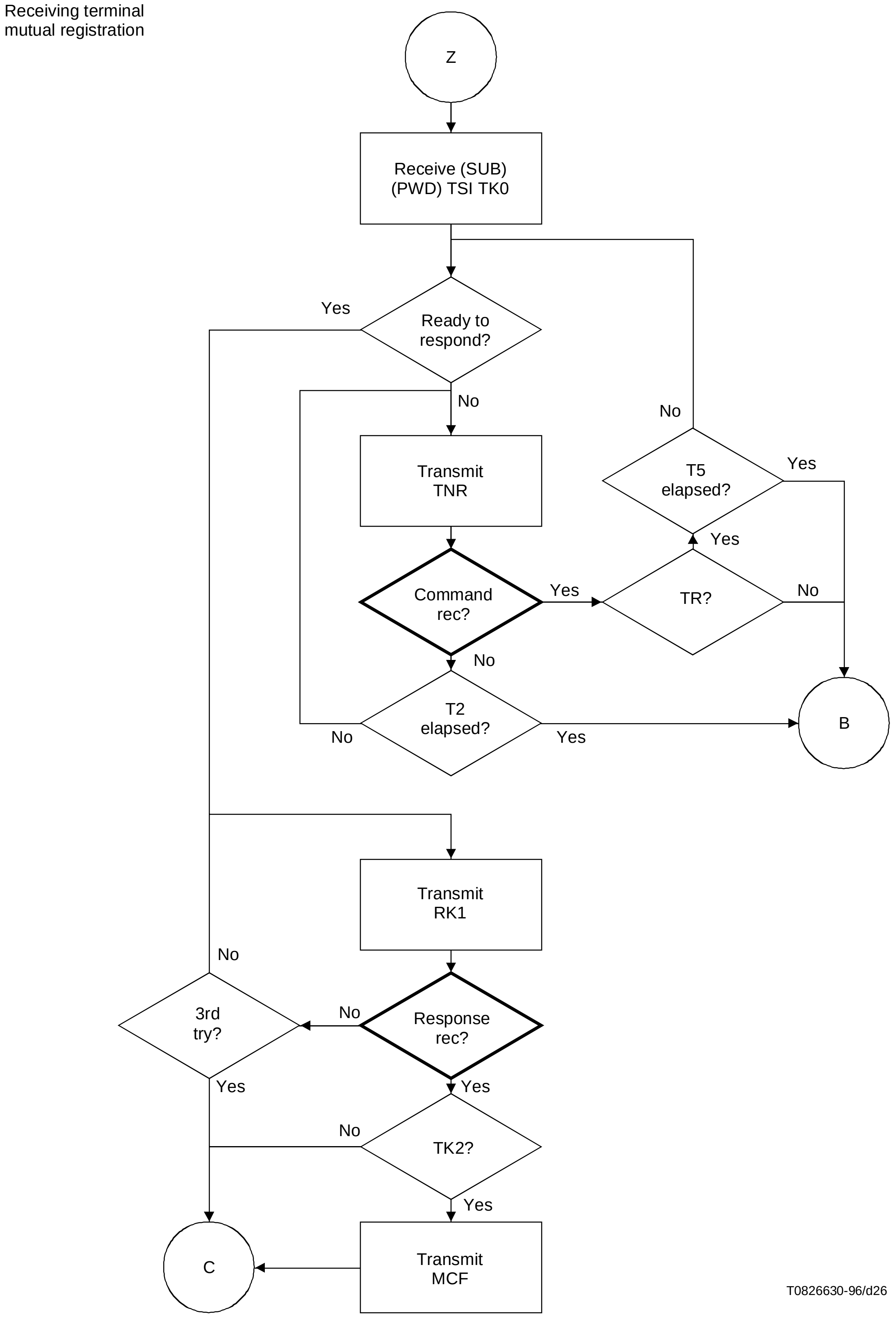


Figure G.8-3/T.30 (sheet 2 of 3) (Used instead of figure C.12/T.30) Duplex

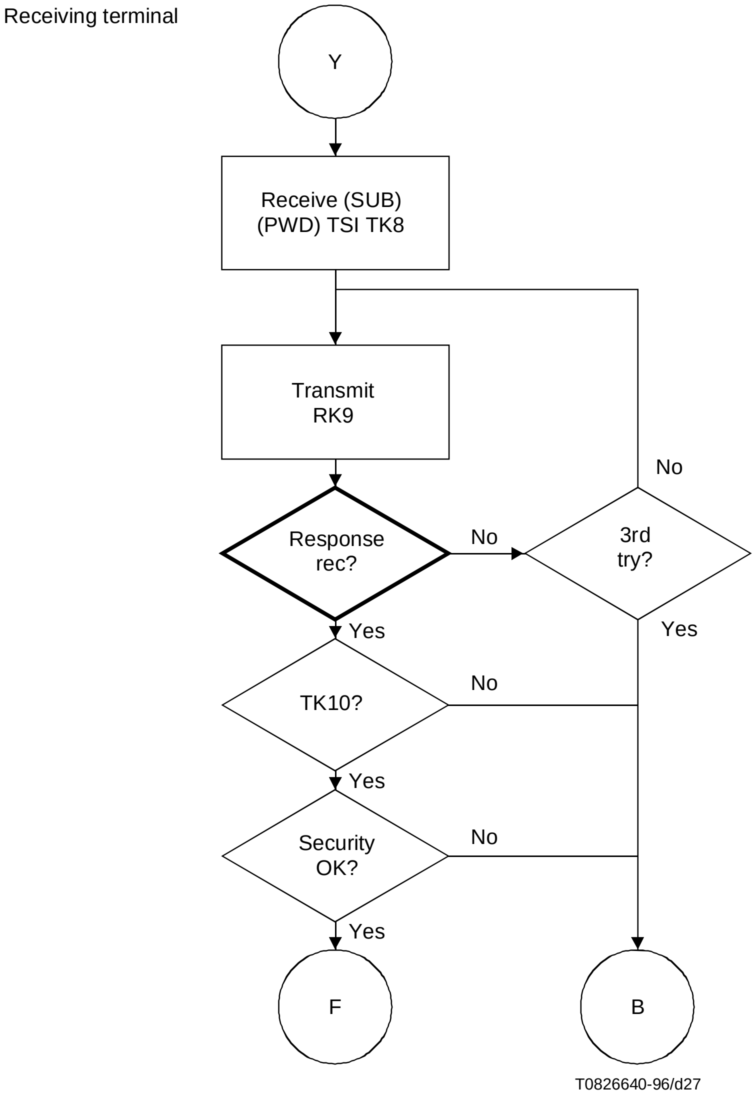


Figure G.8-3/T.30 (sheet 3 of 3) (Used instead of figure C.12/T.30) Full Duplex

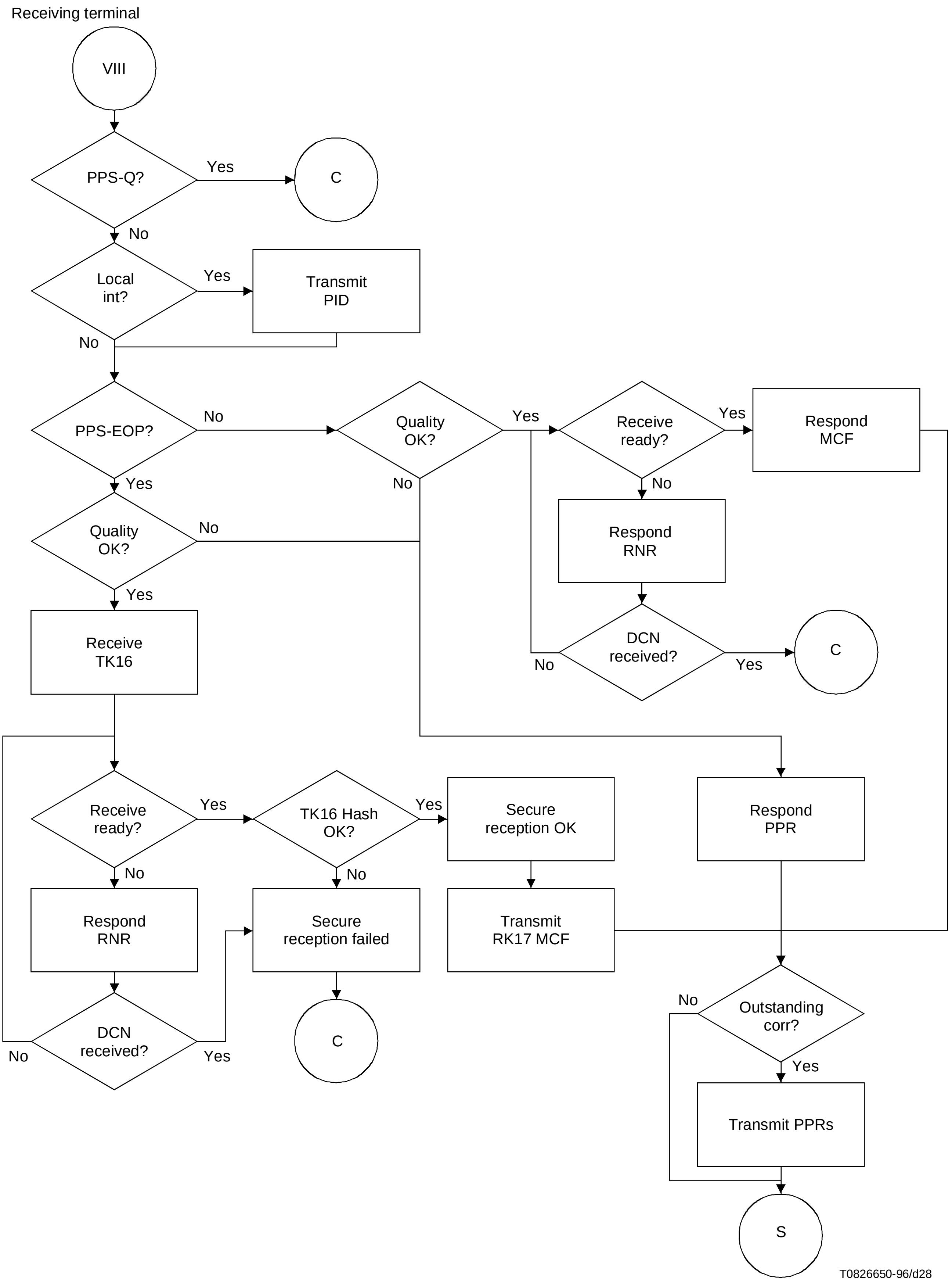


Figure G.8-4/T.30 (Used instead of figure C.13/T.30) Duplex

Transmitting terminal

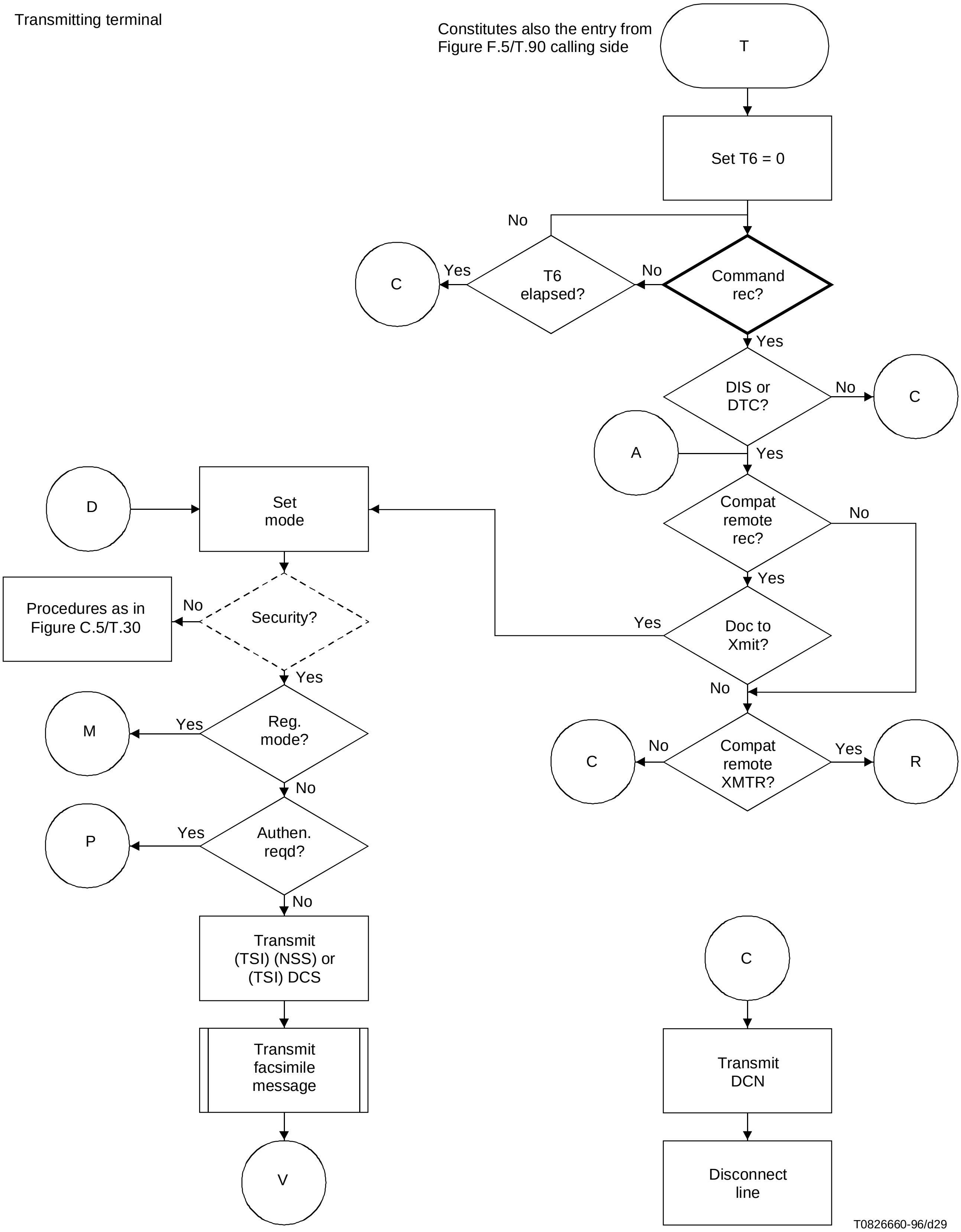


Figure G.8-5/T.30 (sheet 1 of 3) (Used instead of figure C.14/T.30) Duplex

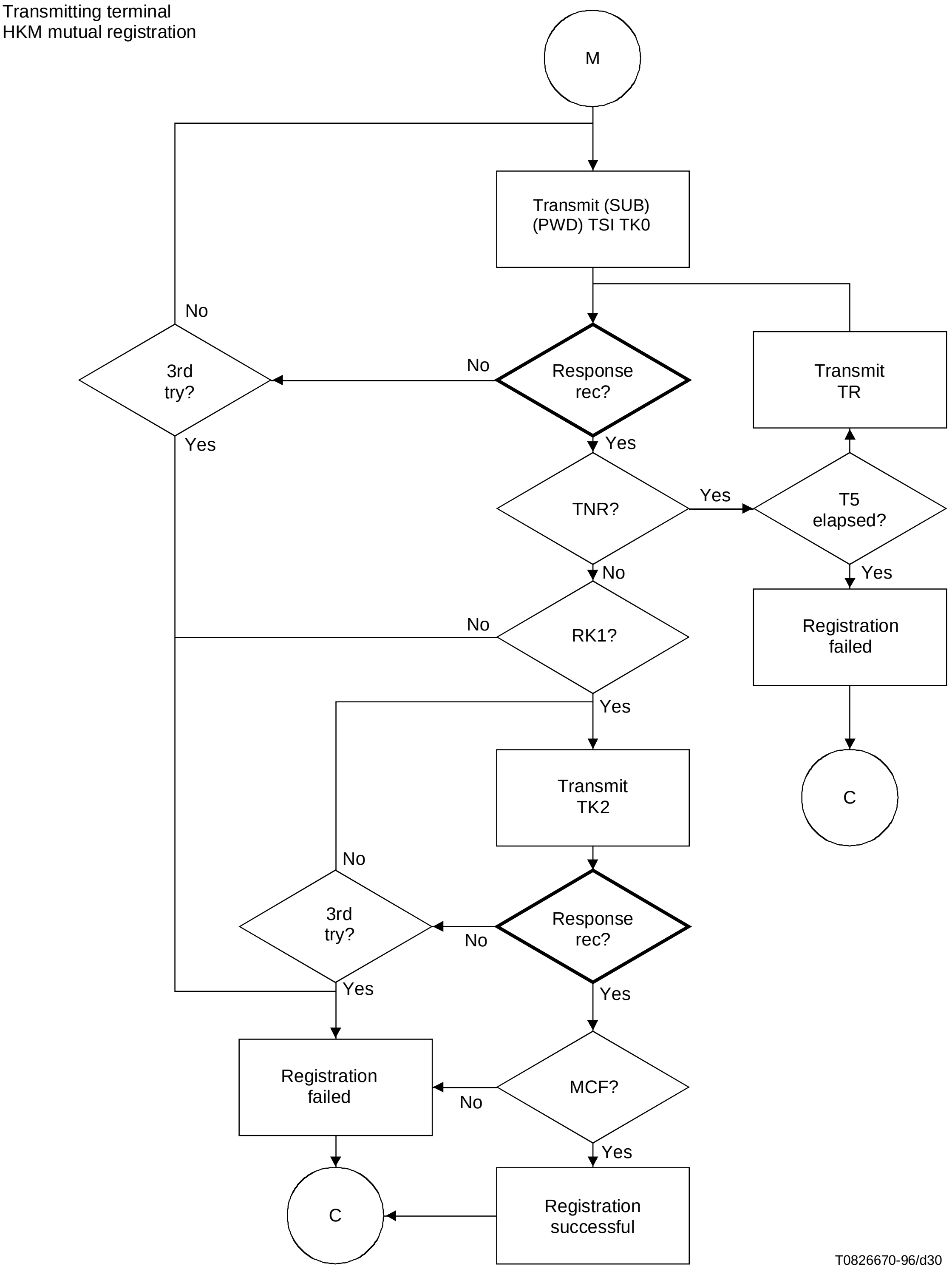


Figure G.8-5/T.30 (sheet 2 of 3) (Used instead of figure C.14/T.30) Duplex

Transmitting terminal

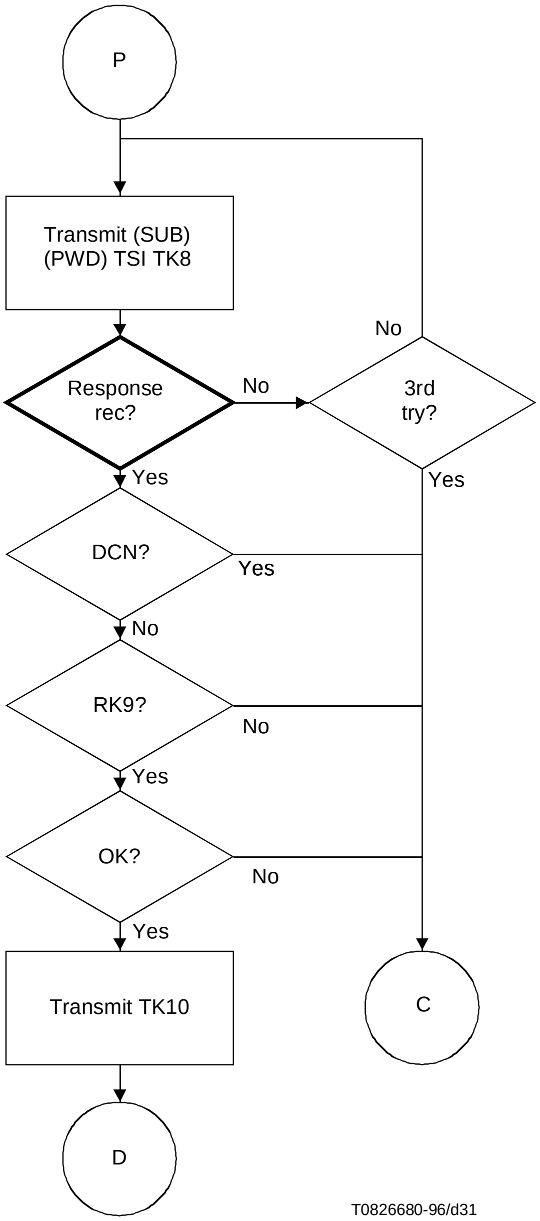


Figure G.8-5/T.30 (sheet 3 of 3) (Used instead of figure C.14/T.30) Duplex

Transmitting terminal

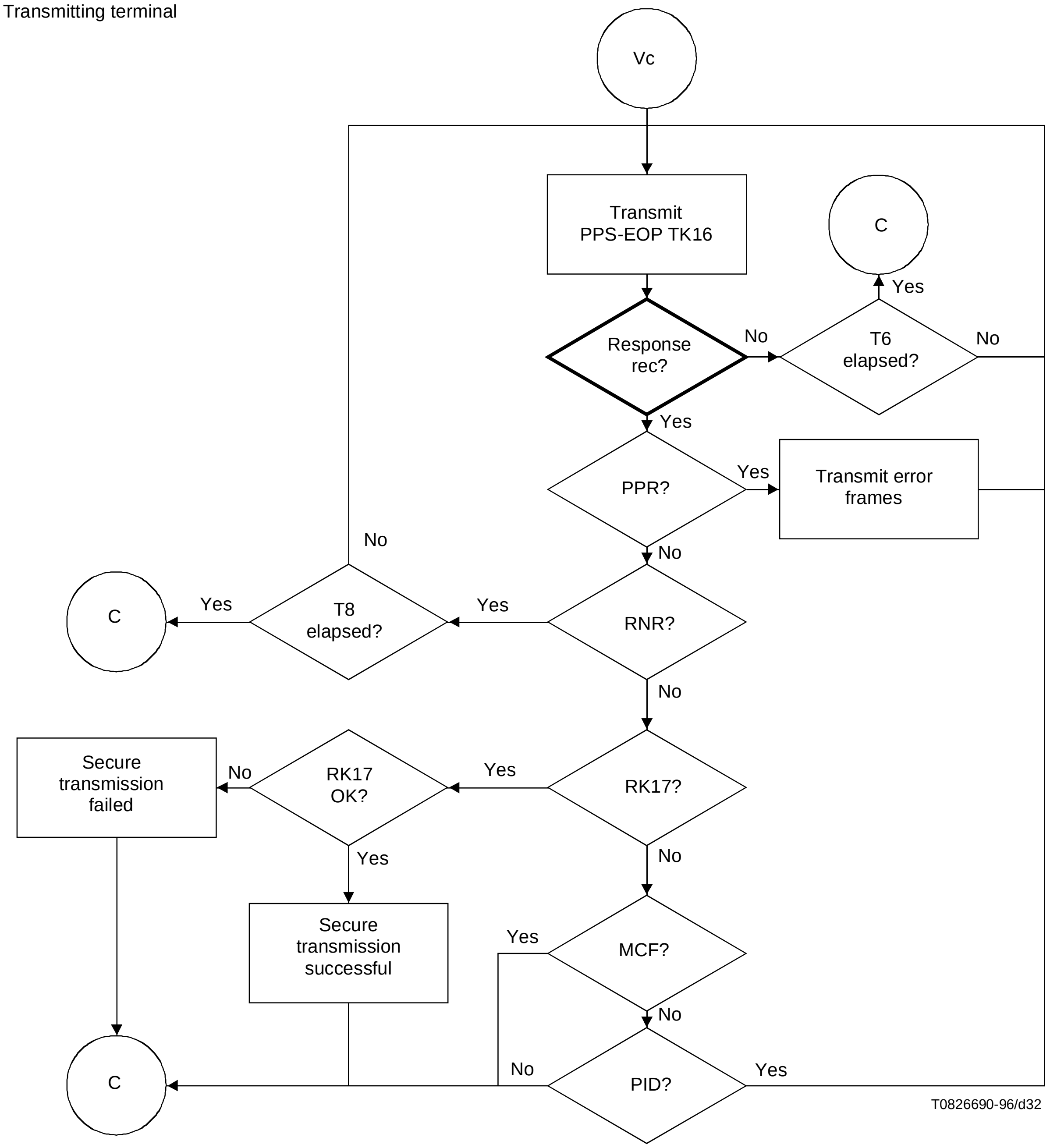


Figure G.8-6/T.30 (Used instead of figure C.18/T.30) Duplex

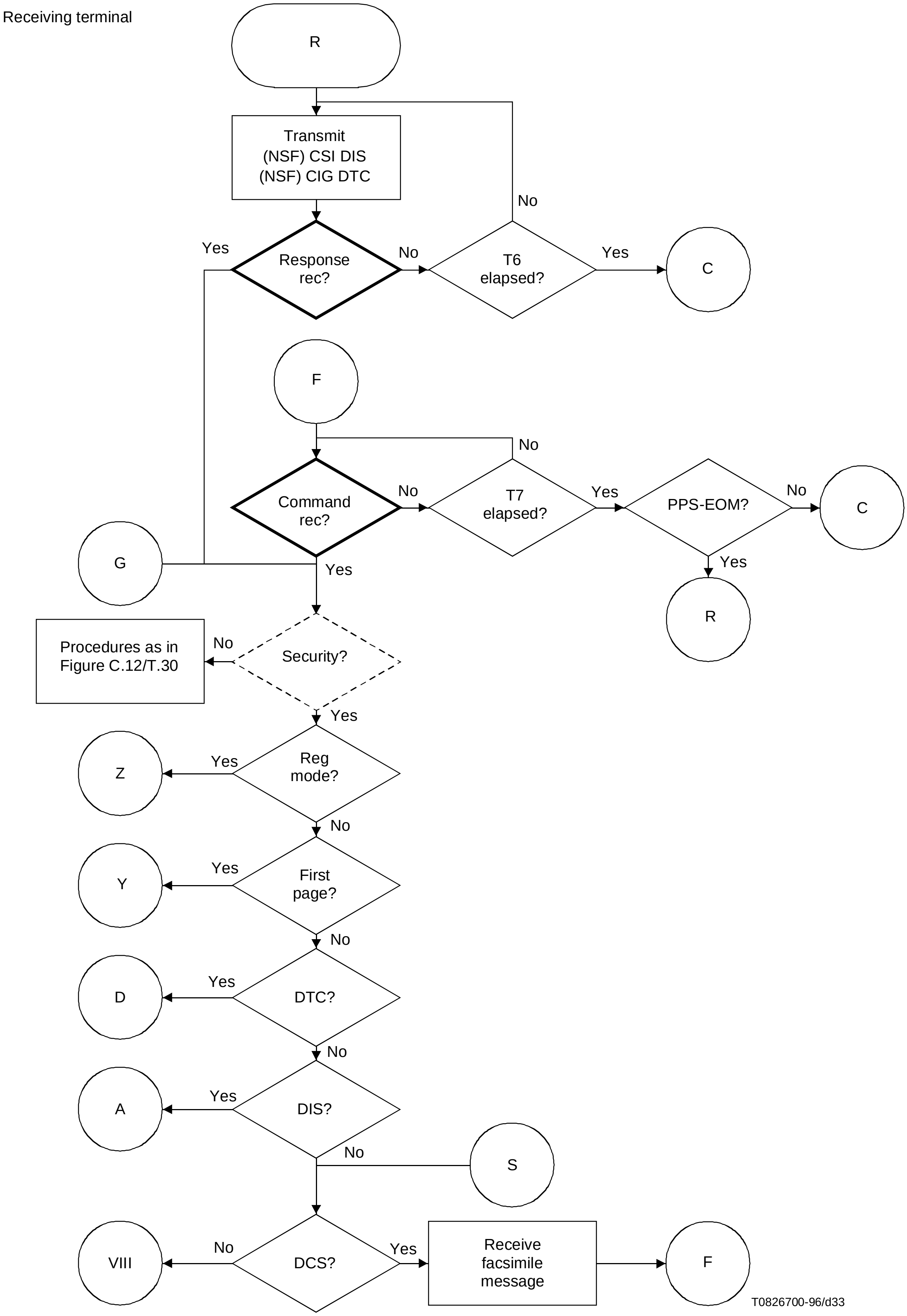


Figure G.8-7/T.30 (Used instead of figure C.21/T.30) Duplex

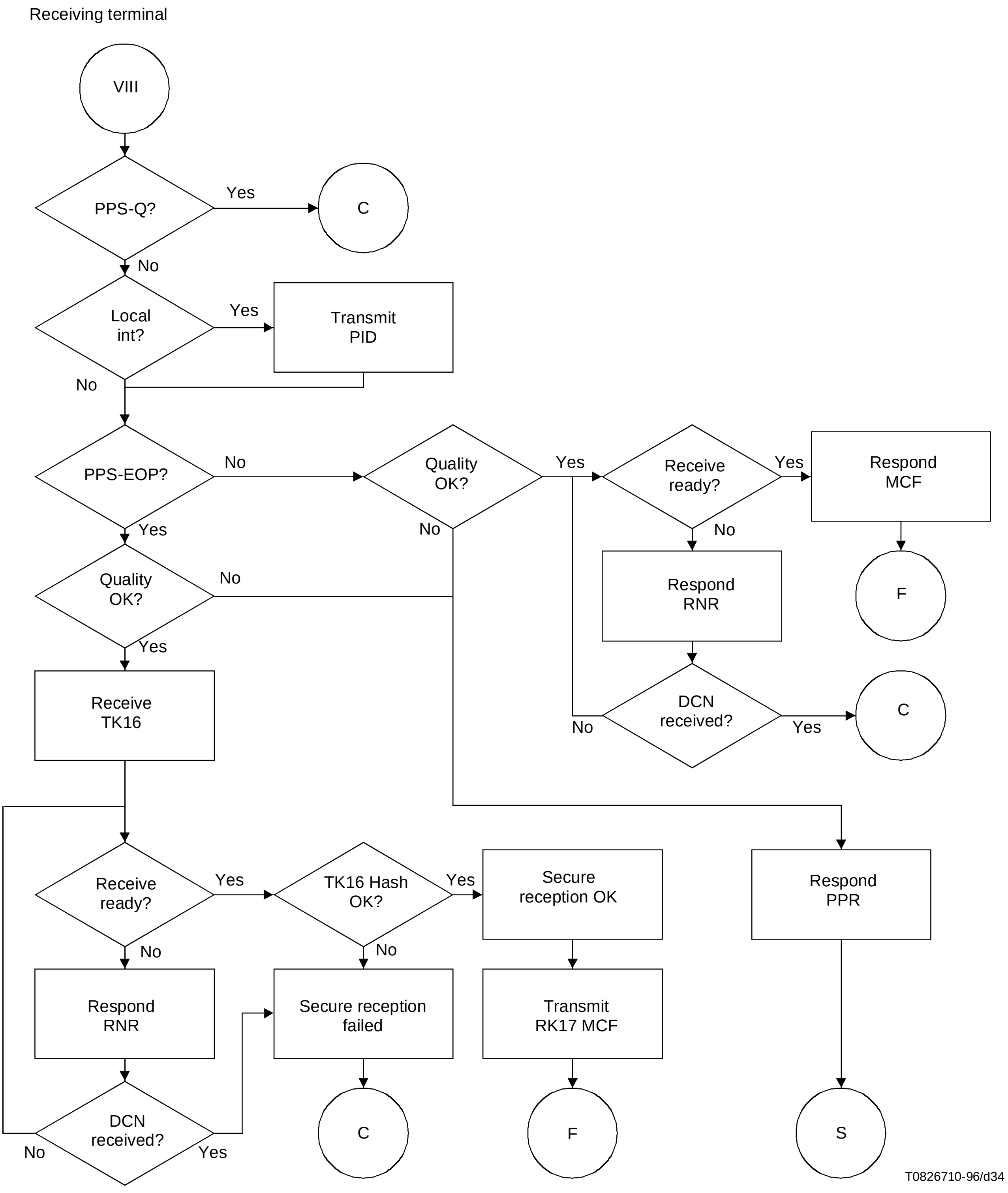


Figure G.8-8/T.30 (Used instead of figure C.22/T.30) Duplex

G.8.2 Flow diagram rules

The flow diagrams follow two simple rules:

1) All lines have an arrow at the destination only.

2) No lines cross.

G.8.3 Timers used in flow diagrams

T1	35 s ± 5 s
T2	6 s ± 1 s
T3	10 s ± 5 s
T4	4.5 s ± 15% for manual units
T4	3.0 s ± 15% for automatic units
T5	60 s ± 5 s
T6	5 s ± 0.5 s
T7	6 s ± 1 s
T8	10 s ± 1 s
T9	Duration of 256 flags

G.8.4 Abbreviations and descriptions used in the flow diagrams

Unless defined otherwise below, the definition of the flow chart terms is as given in the main body and/or Annex A/T.30.

Authen reqd? Check to see if mutual authentication is required at the beginning of the transmission.

NOTE 1 – Once mutual authentication has been completed, then within the same session the "No" exit should always be followed.

Reg mode? Check to see if security registration is required.

First page? Check to see if mutual authentication is required at the beginning of the transmission.

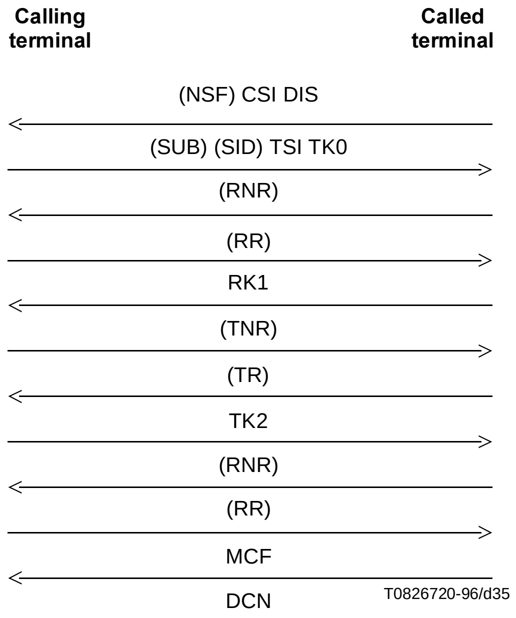
NOTE 2 – Once mutual authentication has been completed, then within the same session the "No" exit should always be followed.

G.9 Signal sequence examples in case of secure facsimile procedure

The examples in Figures G.9-1/T.30-G.9-2/T.30 are based on the flow diagrams and are for illustrative and instructional purposes only. They should not be interpreted as establishing or limiting the protocol. The exchanges of the various signals and responses are limited only by the rules specified in this Recommendation.

NOTE – The hold-off signals, RNR/RR and TNR/TR, may be used at any time during phase B and phase D to enable the receiver or transmitter time to carry out any processing involving in calculating security values or to obtain keys from storage or, in the case of registration, from the operator.

G.9.1 HKM mutual registration



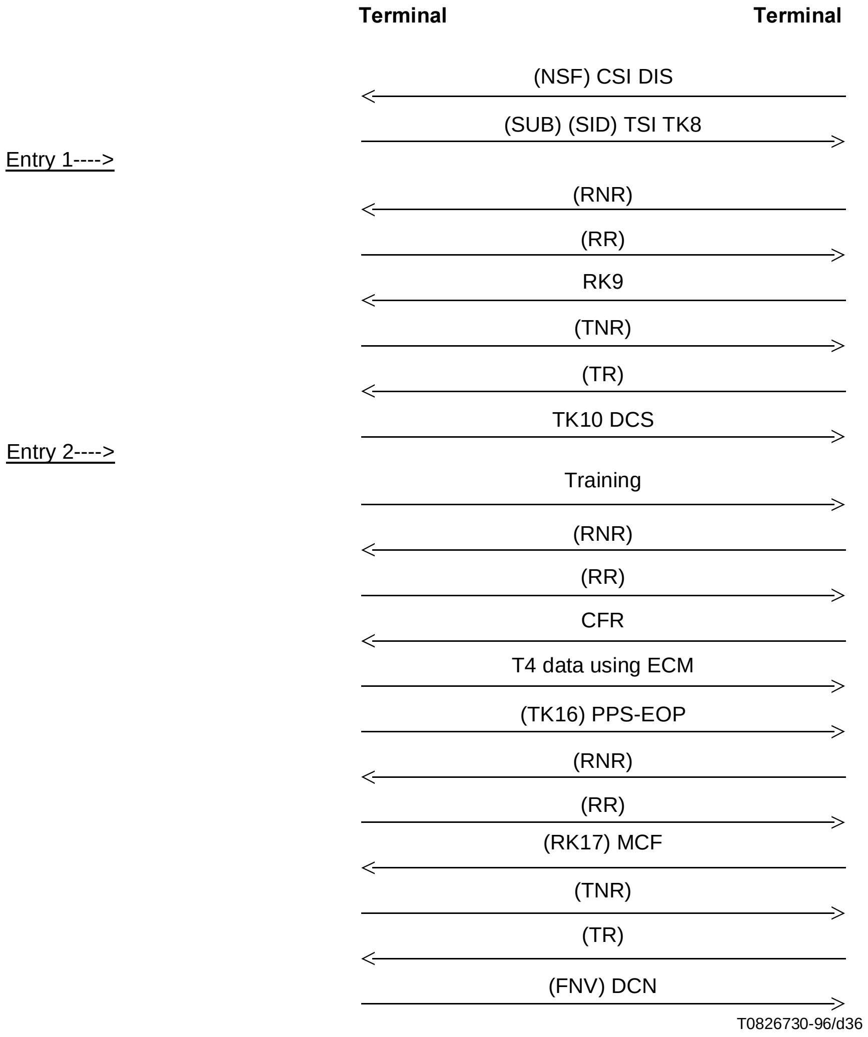
NOTE 1 – The operator of the called terminal may require time to enter the One Time key. If this is being entered manually in real time, RNR/RR is used to hold off the calling terminal. RNR/RR provides a delay of up to 65 seconds.

NOTE 2 – The SUB signal may be used to identify an individual within the domain of the called terminal with whom registration is requested.

NOTE 3 – The SID, Sender IDentification, signal may be used to identify an individual within the domain of the calling terminal who is requesting the registration.

Figure G.9-1/T.30

G.9.2 HKM secure transmission with optional encryption and hashing



NOTE 1 – The SUB signal may be used to identify an individual within the domain of the called terminal to receive the secure facsimile document.

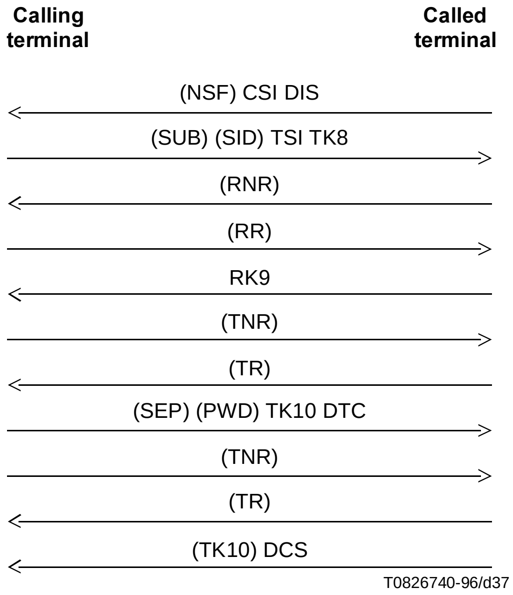
NOTE 2 – The SID, Sender IDentification, signal may be used to identify an individual within the domain of the calling terminal who is sending the secure facsimile document.

NOTE 3 – Data to be transmitted should be in exactly the same format as it would be if encryption was not being used, i.e. complete with any padding, etc. Encryption takes place immediately before these data are actually transmitted. When the receiving terminal decrypts the data, it should do so immediately before normal processing.

Figure G.9-2/T.30

G.9.3 HKM secure polling with optional encryption and hashing

See Figure G.9-3/T.30.



Rejoin transmission at Entry 2 or send document without security

NOTE 1 – The SUB signal may be used to identify an individual within the domain of the called terminal to receive the secure facsimile document.

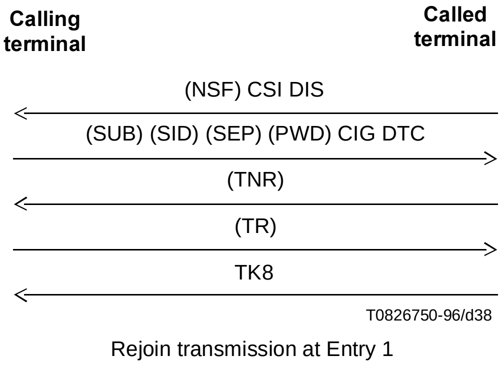
NOTE 2 – The SID, Sender IDentification, signal may be used to identify an individual within the domain of the calling terminal who is sending the secure facsimile document.

NOTE 3 – Data to be transmitted should be in exactly the same format as it would be if encryption was not being used, i.e. complete with any padding, etc. Encryption takes place immediately before these data are actually transmitted. When the receiving terminal decrypts the data, it should do so immediately before normal processing.

Figure G.9-3/T.30

G.9.4 HKM secure polling (initiated by polled system) with optional encryption and hashing

See Figure G.9-4/T.30.



NOTE 1 – The SUB signal may be used to identify an individual within the domain of the called terminal to provide the secure facsimile document.

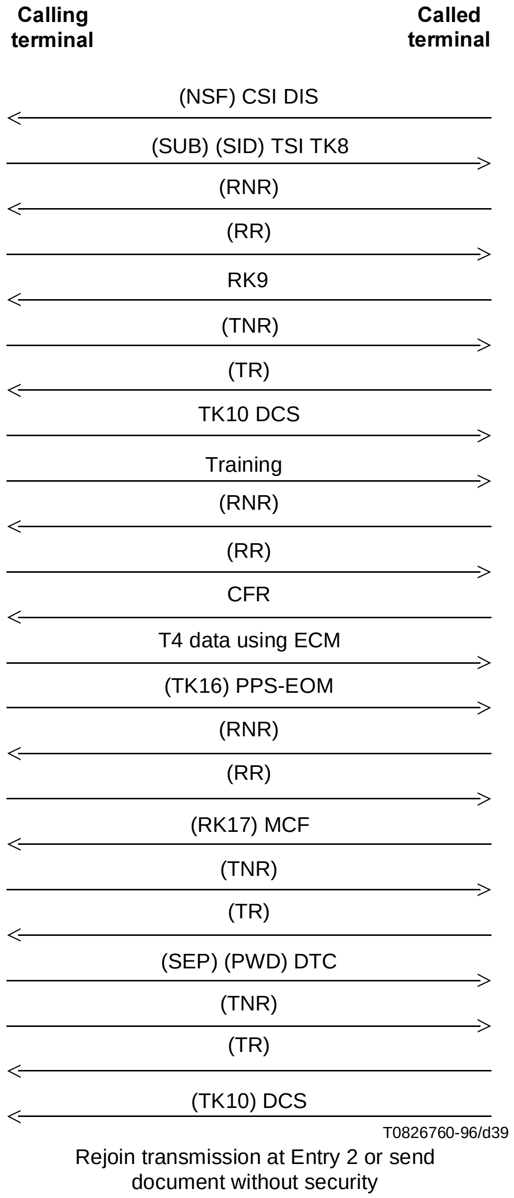
NOTE 2 – The SID, Sender IDentification, signal may be used to identify an individual within the domain of the calling terminal who is polling the secure facsimile document.

NOTE 3 – Data to be transmitted should be in exactly the same format as it would be if encryption was not being used, i.e. complete with any padding, etc. Encryption takes place immediately before these data are actually transmitted. When the receiving terminal decrypts the data, it should do so immediately before normal processing.

Figure G.9-4/T.30

G.9.5 HKM secure turnaround poll with optional encryption and hashing

See Figure G.9-5/T.30.



NOTE 1 – The SUB signal may be used to identify an individual within the domain of the called terminal to receive the secure facsimile document.

NOTE 2 – The SID, Sender IDentification, signal may be used to identify an individual within the domain of the calling terminal who is sending the secure facsimile document.

NOTE 3 – Data to be transmitted should be in exactly the same format as it would be if encryption was not being used, i.e. complete with any padding, etc. Encryption takes place immediately before these data are actually transmitted. When the receiving terminal decrypts the data, it should do so immediately before normal processing.

NOTE 4 – TK10 is optional and, if present, will contain a new session key with the response values set to zero.

Figure G.9-5/T.30

3 Section 3

Add a new Annex H as follows:

Annex H

Security in facsimile G3 based on the RSA algorithm

H.1 Preamble

(The preamble is left blank on purpose)

H.2 Introduction

This Annex specifies the mechanisms to offer security features based on the RSA cryptographic mechanism. The coding scheme of the document transmitted with security features may be of any kind defined in Recommendations T.4 and T.30 (Modified Huffmann, MR, MMR, Character mode as defined in Annex D/T.4, BFT, other file transfer mode defined in Annex C/T.4).

H.3 References

- ISO/IEC 9796:1991, *Information technology – Security techniques – Digital signature scheme giving message recovery*.

  Annex A: RSA: R.L. Rivest, A. Shamir, L. Adleman: A method for obtaining digital signatures and public-key cryptosystems, *CACM (Communications of the ACM)*, Vol. 21, No. 2, pp. 120-126, 1978.

- ISO/IEC 10118-3[1], *Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions*.

  Ref Number: ISO/IEC JTC 1/SC27 N1108:

  SHA-1 (Secure Hash Algorithm), described in *Secure Hash Standard*, FIPS (Federal Information Processing Standard) PUB 180-1, April 1995, an algorithm which comes from the NIST (National Institute of Standardization) in USA.

- MD-5 (RFC 1321): *Message digest algorithm*.
- ISO/IEC 9979:1991, *Data cryptographic techniques – Procedures for the registration of cryptographic algorithms*.

H.4 Security mechanisms

H.4.1 Digital signature mechanism and keys management

The basic algorithm used for the digital signature (authentication and integrity type services) is the **RSA**.

The couple of keys used for this purpose is "public key"/"secret key".

When the optional confidentiality service is offered, the token containing the session key "Ks", used for enciphering the document, is encrypted also by the means of RSA algorithm. The couple of keys used for this purpose called ("encipherment public key"/"encipherment secret key") is not the same one as that used for authentication and integrity types services. This is for decoupling the two kinds of use.

The implementation of RSA which is used in this Annex is described in ISO/IEC 9796 ("Digital signature scheme giving message recovery").

[1] Presently at the stage of draft.

For encipherment of the token containing the session key, the rules of redundancy when processing the algorithm RSA are the same ones as those specified in ISO/IEC 9796.

Note – Certain Administrations in addition to RSA, (which is the basic mechanism in the context of this Annex), may require that an optional mechanism be implemented: the DSA.

References

- ISO/IEC CD 14888-3:1995.

  Ref Number: ISO/IEC JTC 1/SC27 N1113.

- FIPS PUB 186-1: Digital Signature Standard, *U.S NIST*, 1 February 1993.

H.4.2 Length of the public keys, secret keys and digital signatures

As a basic feature, the length of the public keys, secret keys and digital signatures is **512 bits**. Longer lengths may be used as recognised options; they are negotiated through the protocol (see further).

H.4.3 Length of the public exponent of RSA

For digital signatures, the public exponent has a fixed value equal to 3.

For encipherment of the token which includes the session key "Ks", the public exponent has a fixed value equal to: $2^{16} + 1$. The session key is used in case of encipherment of the document, see further.

H.4.4 Certification authorities

By default, certification authorities are not used.

As an option, certification authorities may be used to certificate the validity of the public key of the sender of the facsimile message. In such a case, the public key may be certified as specified in the Recommendation X.509.

The means to transmit the certificate of the public key of the sender is described in this Annex, but the precise format of the certificate is left for further study (in further versions of this Annex).

The actual transmission of the certificate is negotiated in the protocol.

H.4.5 Registration mode

As a **mandatory** feature, a *registration mode* is provided. It permits the sender and the receiver to register and store the public keys of the other party in confident manner prior to any secure facsimile communication between the two parties.

Registration mode can avoid the user to enter manually in the terminal the public keys of its correspondents (the public keys are fairly long, 64 octets or more).

Because the registration mode permits to exchange the public keys and store them in the terminals, it is not necessary to transmit them during the facsimile communications.

The scheme of the registration mode is detailed further in this Annex.

H.4.6 Hash function

As described in this Annex, some signatures are applied on the result of a "hash function".

The hash function which is used is either SHA-1 (*Secured Hash Algorithm*, an algorithm which comes from the "NIST" in USA) or MD-5 (RFC 1321).

For SHA-1, the length of the result of the hashing process is on **160 bits**.

For MD-5, the length of the result of the hashing process is on **128 bits**.

A terminal may implement either SHA-1 or MD-5 or both.

The use of one algorithm or the other is negotiated in the protocol (see further).

In the future, other optional hash functions may be added in this Annex.

H.4.7 Encipherment

H.4.7.1 General

The encipherment of the data for provision of the confidentiality service is optional. Five optional encipherment schemes are registered in the scope of this Annex:

FEAL-32, SAFER K-64, RC5, IDEA and HFX40 (as described in Recommendation T.36). In some countries, their use may be subject to national regulation.

Other optional algorithms could be registered in the future.

Other optional algorithms may also be used. They are chosen conforming to the ISO/IEC 9979 ("Procedure for registering cryptographic algorithms").

The capability of the terminal to handle one of these algorithms and the actual use of a particular one during the communication is negotiated in the protocol.

A session key is used for encipherment. The session key is called "**Ks**".

The basic length of Ks is 40 bits.

– For algorithms which use a 40 bits session key (e.g. HFX40), the session key Ks is the key actually used in the encipherment algorithm.

– For algorithms which require keys longer than 40 bits (e.g. FEAL-32, IDEA, SAFER K-64 requiring respectively: 64 bits, 128 bits and 64 bits), a redundancy mechanism is performed to get the necessary length. The resultant key is called the "redundant session key". The "redundant session key" is the key which is actually used in the encipherment algorithm.

The redundancy mechanism is described in the next subclause.

The token "BE" which includes Ks (see further) is enciphered by the "encipherment public key" of the recipient and sent to it by the sender.

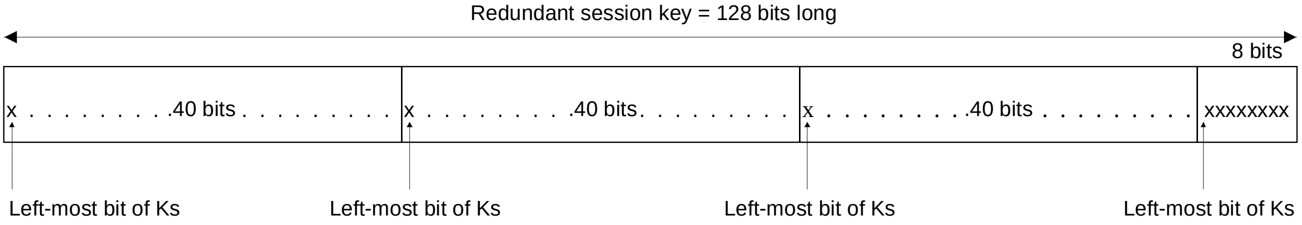
When a redundancy key is necessary, the receiving terminal regenerates it from the token "BE" received from the emitting terminal.

H.4.7.2 Redundancy mechanism to get the redundant session key when necessary

When a "redundant session key" is necessary (the encipherment algorithm needs a key longer than 40 bits), this entity is generated as follows:

The pattern of bits Ks is repeated as many times as necessary to get the necessary length required for the algorithm. If necessary, a portion of the pattern (beginning with the left-most bit) is appended at the end to fit the correct length.

This principle is illustrated on an example below where the algorithm requires 128 bits (e.g. IDEA).

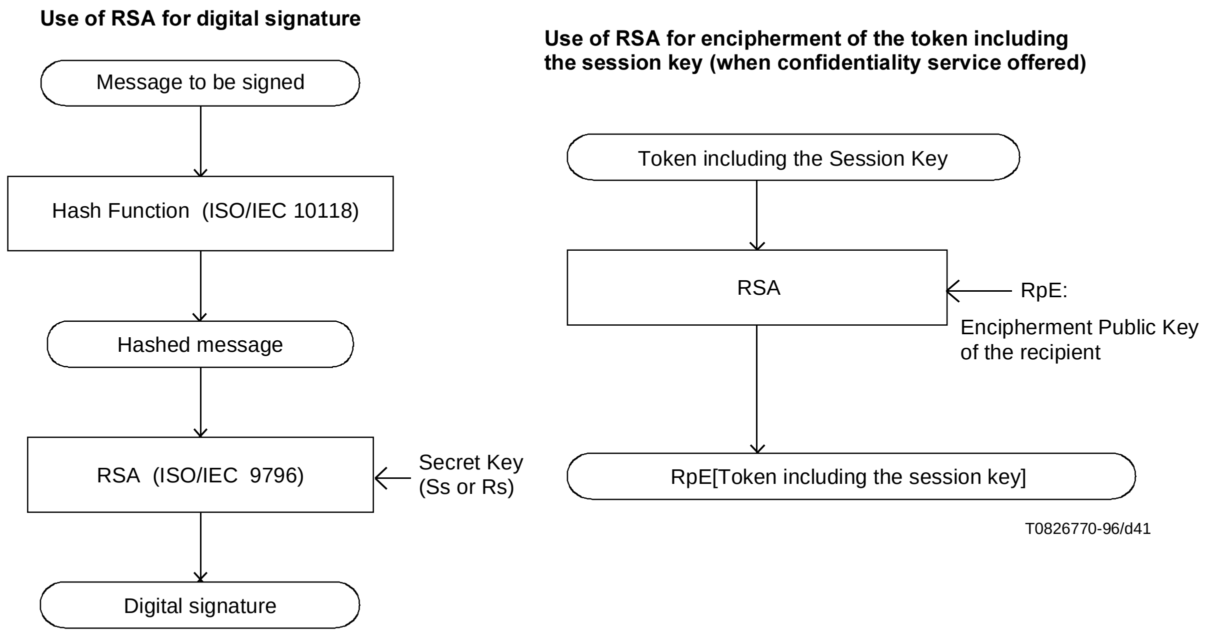

Redundant session key = 128 bits long
8 bits
x . . . . .40 bits . . . .
x . . . . .40 bits. . . . .
x . . . . .40 bits . . . .
xxxxxxxx
Left-most bit of Ks
Left-most bit of Ks
Left-most bit of Ks
Left-most bit of Ks

T0828020-98/d40

H.4.8 Use of hash function and RSA algorithm

H.4.8.1 General scheme

See Figure H.1/T.30


Use of RSA for digital signature
Message to be signed
Hash Function (ISO/IEC 10118)
Hashed message
RSA (ISO/IEC 9796)
Secret Key (Ss or Rs)
Digital signature
Use of RSA for encipherment of the token including the session key (when confidentiality service offered)
Token including the Session Key
RSA
RpE:
Encipherment Public Key of the recipient
RpE[Token including the session key]
T0826770-96/d41

NOTE – ISO/IEC 9796 has been designed to RSA-sign a short data, which may be either the message to be signed (if it is short), or the hash code of the message to be signed (if the message is too long), see ISO/IEC 9796.

Figure H.1/T.30

H.4.8.2 Bit order for transmission

Throughout this Annex:

1) All the sequence of octets are transmitted such as the left-most octet (as represented in this Annex) is the first octet transmitted.

   The rule for bit transmission order within each octet is defined below.

2) Except for the content of the **FIF** of the DES, DEC, DER and DTR signals which are defined below, for each octet represented in this annex, the order in which the bits are transmitted is from left to right as printed, this is the case, for example, for the FCF codes.

3) For the content of the **FIF** of the signals DES, DEC, DER and DTR:

   3a) There is a "General rule" which is the following:

   For each octet, the least significant bit is the first transmitted.

   When numbered in tables, the least significant bit is numbered "`bit No. 0`".

   For example: the octet "`1 0 1 1 0 0 1 1`"

   and numbered (if numbered):

```
bit No. 7 6 5 4 3 2 1 0
        1 0 1 1 0 0 1 1
```

   will be transmitted as follows:

   Transmission order ==>

   1 1 0 0 1 1 0 1

   3b) For the cases where the content of the FIF of the existing T.30 signals is encapsulated within a tag encoded structure (see H.6.1.4.7 "Encapsulted Frame Supergroup"), consistency is maintained with the transmission order of the octets and bits for the FIF as previously defined for these signals (see 5.3 and 5.3.6.2).

3c) Within the FIF of the DES, DEC, DER and DTR, an exception to the general rule is for parameters identified as "binary coded" within Table H.1/T.30. For these parameters, the following rule applies:

the first bit transmitted on the line is the left-most bit of the left-most octet:

```
left-most bit
|
|
↓         left-most octet        |    left-most octet but one    |  ...
0   1   2   3   4   5   6   7    0   1   2   3   4   5   6   7   0  ...
|
0   1   2   3   4   5   6   7    8   9  10  11  12  13  14  15  16  ..
Transmission order ==>
```

H.4.8.3 Bits order in the hash and RSA processes

The hash function standards (SHA-1 and MD-5) define a bit string upon which the hashing process is applied and a bit string which is the hash result.

The first bit of these bit strings is the left-most bit (as represented in the figures of these Standards).

In this Annex, various parameters are specified on which hash function is applied. Some hash results are transmitted on the line. The rules for bit order on the line and bit order for processing in the hash function are the same ones:

- the first bit passing through the hash function is the left-most bit of the left-most octet.

If the hash function is applied on several concatenated entities, for example h(a,b,c,...), the bit string to be hashed is the bit string [a] immediately followed by the bit string [b], etc.

For the RSA function, the same principle applies:

the first bit passing through RSA function is the left-most bit of the left-most octet.

The bit order through hash function and RSA is illustrated as follows (the bit strings represented are only for example).

```
|left-most bit in the entry of the hash function
|= first bit when transmitted on the line
|
↓
0010101010010101010100001000100..........
|
↓HASH  FUNCTION

result of the hash function: 160 bits (or 128 bits if MD-5):
0101111001001010 ......     00010101
↑
|left-most bit at the result of the hash function
|= left-most bit in the entry of the RSA function
|
↓RSA

result of the RSA: 64 octets (or more if negotiated as such, see further)
101001010000000101010.........101010
↑
|
|left-most bit at the result of the RSA function
|= first bit when transmitted on the line
```

This principle is valid also for the parameters passing directly into the RSA function without hashing (e.g. Token which includes the Session Key "Ks").

If RSA is applied on several concatenated entities, for example (a,b,c,...), the bit string to be processed by RSA is the bit string [a] immediately followed by the bit string [b], etc.

H.5 Security parameters

Table H.1/T.30 defines the various security parameters some of which are exchanged.

For all the security parameters, a basic length is defined. The support of this basic length is mandatory.

In addition, some parameters permit optional longer lengths which can be negotiated in the protocol.

Table H.1/T.30 indicates also the type of coding of the parameters (binary, ASCII, ...).

The means to transmit these parameters in the signals DES, DEC, DER and DTR is specified further in this Annex.

Table H.1/T.30 – Security parameters

Abbreviation	Description	Basic length	Optional longer lengths	Coding of the field
S	Sender's identity	20 octets	For further study	IA5 coded (Note 1)
Sp	Sender's public key	64 octets	Possible	Binary coded (Note 2)
Ss	Sender's secret key	64 octets	Same as Sp	Binary coded (Note 2)
SpE	Encipherment Sender's public key (for encryption of token containing the session key)	64 octets	Possible	Binary coded (Note 2)
SsE	Encipherment Sender's secret key (for decryption of encrypted token containing the session key)	64 octets	Same as SpE	Binary coded (Note 2)
Sra	Random number created by the sender for authentication of the recipient	8 octets	Possible	Binary coded (Note 2)
Srd	Random number created by the sender for the digital signature	8 octets	Possible	Binary coded (Note 2)
R	Recipient's identity	20 octets	For further study	IA5 coded (Note 1)
Rp	Recipient's public key	64 octets	Possible	Binary coded (Note 2)
Rs	Recipient's secret key	64 octets	Same as Rp	Binary coded (Note 2)
RpE	Encipherment Recipient's public key (for encryption of token containing the session key)	64 octets	Possible	Binary coded (Note 2)
RsE	Encipherment Recipient's secret key (for decryption of encrypted token containing the session key)	64 octets	Same as RpE	Binary coded (Note 2)
Rra	Random number created by the recipient for authentication of the sender	8 octets	Possible	Binary coded (Note 2)
Ks	Session key	40 bits	For further study	Binary coded (Note 2)
BE	BE = RpE[S, Ks] = Sender identity and session key concatenated and encrypted by RpE	64 octets	Same as RpE	Binary coded (Note 2)
UTCd	Date/time chosen by the sender (date/time of the generation/signature of the document)	8 octets	For further study	YY MM DD HH MM SS offset GMT BCD coded (Note 3)
UTCr	Date/time chosen by the recipient (date/time of the confirmation of message receipt)	8 octets	For further study	YY MM DD HH MM SS offset GMT BCD coded (Note 3)
Lm	Length of the document	4 octets	For further study	Corresponds to the number of octets of the whole document transmitted (data octets + pad bits, see H.6.5/T.30). BCD coded (Note 4)

Table H.1/T.30 – Security parameters *(end)*

Abbreviation	Description	Basic length	Optional longer lengths	Coding of the field
h(...)	Hashed result of the entity enclosed in brackets	160 bits or 128 bits depending on the hash-function	For further study	Binary coded (Note 2)
Rs[h(...)]	Hashed result of the entity enclosed in brackets signed by the recipient	64 octets	Same as Rp	Binary coded (Note 2)
Ss[h(...)]	Hashed result of the entity enclosed in brackets signed by the sender	64 octets	Same as Sp	Binary coded (Note 2)
Sia	Indicator in the token used for authentification of the sender	1 octet	No	Octet equal to: "00000000" (Note 5)
Ria	Indicator in the token used for authentification of the recipient	1 octet	No	Octet equal to: "00000001" (Note 5)
Sis	Indicator in the token used for digital signature	1 octet	No	Octet equal to: "00000010" (Note 5)
Ris	Indicator in the token used for confirmation of message receipt	1 octet	No	Octet equal to: "00000011" (Note 5)
document	The document sent during the secure facsimile transmission mode	Variable	Irrelevant	Irrelevant
enc. document	The encrypted document sent during the secure facsimile transmission mode when confidentiality service is invoked. The encryption of the document is made with session key Ks (or the redundant session key if the algorithm requires more bits than Ks to work).	Variable	Irrelevant	Irrelevant

NOTE 1 – The general rule for FIF of DES/DEC/DER/DTR applies: the least significant bit of each octet is the first one transmitted.

NOTE 2 – The rule for transmission of binary coded elements is defined in H.4.8.2/T.30.

NOTE 3 – Example: for the 24th March of 1995. 8H25 05s PM. Offset GMT: 3 H:

```
"1    9    9    5    0    3    2    4    2    0    2    5    0    5    0    3"
0001 1001  1001 0101  0000 0011  0010 0100  0010 0000  0010 0101  0000 0101  0000 0011
```

The general rule for FIF of DES/DEC/DER/DTR applies: the right-most bit of each octet is the first one transmitted.

NOTE 4 – Example: for a document lentgth of 123456 octets:

```
"0    0     1    2     3    4     5    6"
0000 0000   0001 0010   0011 0100   0101 0110
```

The general rule for FIF of DES/DEC/DER/DTR applies: the right-most bit of each octet is the first one transmitted.

NOTE 5 – The general rule for FIF of DES/DEC/DER/DTR applies: the right-most bit of each octet is the first one transmitted.

H.6 Exchanges of security parameters

The Error Correction Mode (ECM) described in Annex A/T.30 is required for offering the security services based on RSA.

Some specific security parameters must be transmitted during the facsimile communication at the protocol level (phases B and D of the T.30 protocol). As an option, see further "security page", some security parameters are transmitted at the message level (phase C of T.30 protocol).

H.6.1 Exchange of security parameters at the protocol level

The eight new signals which are used are the following:

– DER: Digital Extended Request

This command is sent by the sending terminal. It can set security parameters for the session and also requests further details on the security capabilities of the receiving machine.

– DES: Digital Extended Signal

Sent by the receiving device; contains security capabilities of the receiving machine.

– DEC: Digital Extended Command

Sent by the sending terminal in response to DES or DTR.

DEC contains all the settings for the current communication.

DEC replaces DCS which is not sent. The information which is normally contained in the FIF of the DCS is contained in the DEC. DEC contains also the various security parameters sent from the emitting terminal to the receiving terminal.

– DTR: Digital Turnaround Request

May be sent by the calling terminal in response to DIS or DES; used when polling or turnaround desired.

DTR replaces DTC which is not sent. The information which is normally contained in the FIF of the DTC is contained in the DTR. DTR contains also the various security parameters sent from the receiving terminal to the emitting terminal.

– DNK: Digital Not Acknowledge

DER, DES, DEC or DTR are structured in HDLC frames.

DNK indicates that the previous command (DER, DES, DEC or DTR) has not been satisfactorily received and that the frames specified in the FIF of DNK are required to be retransmitted. DNK may be issued either by the emitting terminal or by the receiving terminal (contrary to PPR in Annex A/T.30 which can only be sent by the receiving terminal).

DNK is also used to reject TCF.

– TNR: Transmitter Not Ready

This signal is used to indicate that the transmitter is not yet ready to transmit.

Format:

FCF: X101 0111 (X is the bit defined in 5.3.6.1/T.30).

– TR: Transmitter Ready?

This signal is used to ask the status of the transmitter.

Format:

FCF: X101 0110 (X is the bit defined in 5.3.6.1/T.30).

– PPS-PSS: Partial Page Signal – Present Signature Signal

This signal is used to indicate the end of the document and that a digital signature signal follows.

Format:

FCF1: X111 1101 (X is the bit defined in 5.3.6.1/T.30)

FCF2: 1111 1000.

The particular coding of DER, DES, DEC, DTR and DNK is detailed further in this Annex.

H.6.1.1 Structure of DER, DES, DEC and DTR

H.6.1.1.1 General

DER, DES, DEC and DTR signals are structured in HDLC frames.

The structure of the sequence of frames follows the same rules as that of the multi-frames commands already specified in Recommendation T.30 (e.g. NSF-CSI-DIS). These rules are described in 5.3.1, 5.3.3, 5.3.4 and 5.3.5 of Recommendation T.30.

H.6.1.1.2 FCF (Facsimile Control Field)

The FCF of the frames is the following:

– DES frames:	0000 0101
– DEC frames:	1100 1001
– DER frames:	1100 1010
– DTR frames:	1000 1000

H.6.1.1.3 FIF (Facsimile Information Field)

The specifications for the FIF of DES, DEC, DER and DTR in the scope of Annex H are the following:

The maximum length of a the FIF of a frame is 65 octets. If a frame is an intermediate frame (not the last one), its FIF must be 65 octets long, **except when the content of the frame is "FIF of DCS"** (see further). In this latter case, the frame is as long as necessary to contain the FIF octets of the DCS but no more (no pad octet is allowed).

If it is the last frame, the length of the FIF may be less than 65 octets depending on the number of data octets to carry. No pad octet is allowed.

The first octet of the FIF of each frame contains the frame number, then follows the data field. The frame number is an eight bits binary number. The general rules for FIF of DES/DEC/DER/DTR applies: the least significant bit of the frame number (right-most bit) is transmitted the first.

The frame numbered "0" is transmitted first.

Figure H.2/T.30 illustrates these principles.

NOTE – The use of frames with FIF longer than 65 octets is for further study.

Preamble	HDLC Address	Control field	Facsimile Control Field	FIF		FCS	Flag(s)	HDLC address	Control field	Facsimile Control Field	FIF		FCS	Flag(s)
Flags	1111 1111	1100 X000 X = 0 (non final frame)	DEC = 1100 1001	Frame number 0000 0000	Data field 64 octets	FCS	At least one flag	1111 1111	1100 X000 X = 1 (final frame)	DEC = 1100 1001	Frame number 0000 0001	Data field ≤ 64 octets	FCS	At least one flag

NOTE 1 – The FCF is transmitted with the left-most bit (as printed in the figure) being the first one transmitted.

NOTE 2 – The Frame number is transmitted with the right-most bit (as printed in the figure) being the first one transmitted.

In the example, for the frame number of the second frame:

1000 0000

transmission order ===>

NOTE 3 – **The data field of frame "0" may be less than 64 octets if containing the "FIF of DCS".**

Figure H.2/T.30 – Example for a DEC consisting in 2 frames

H.6.1.2 Use and structure of DNK

H.6.1.2.1 Structure of the DNK

Definition

In the rest of this Annex, the terms "signal X" or "X" designate either the signal DER, DES, DEC or DTR.

When some frames of "signal X" are faultily received, DNK permits to request the retransmission of those specific frames.

DNK is also used to reject TCF, see further.

NOTE – When all the frames of an X signal have been received correctly, the normal answer (as specified in this Annex) is used as an implicit acknowledgement, except if TCF is to be rejected (DNK is used for this rejection).

DNK consists in one HDLC frame whose structure follows the same rules as for the other T.30 signals (rules described in 5.3.1, 5.3.3, 5.3.4, 5.3.5 of Recommendation T.30).

H.6.1.2.2 FCF of the DNK

The FCF is the following: X101 1001

The definition of the X bit is in 5.3.6.1/T.30.

H.6.1.2.3 FIF of the DNK

H.6.1.2.3.1 General

The FIF consists in an integer number of octets.

For each octet of the FIF of DNK, the left-most bit (as printed) is the first one transmitted. It is numbered bit "0".

The transmission order corresponding to the bit numbering is the following:

```
Bit No.   01234567 01234567 01234567 …

          transmission order ========>
```

The first octet of DNK is used to reject TCF when needed (TCF received corrupted).

The further octets are used to request frames received in error.

H.6.1.2.3.2 Request of frames received in error

Beginning with the second octet of the FIF, each bit corresponds to a frame in the previously sent command or response, i.e. the first transmitted bit to the first frame, etc. For frames which are received correctly, the corresponding bit shall be set to "0; those that are received incorrectly shall have their bit set to "1". Pad bits of value "1" shall be added as required to align on the last octet boundary.

Likewise in ECM mode described in Annex A/T.30 (but here at the protocol modulation speed), if more than one DNK is transmitted (consecutive to several faulty attempts of transmission of X frames), the bit corresponding to an X frame which has been already correctly received must always be set to "0".

NOTE 1 – It may happen that DNK is resent with a FIF of a different size.

For example: the X signal is received quite faultily and is found to be only 7 frames long whereas it is in fact 9 frames long. In such case, the FIF of the DNK will contain only two octets (the first one which is used for the TCF rejection – see further – and the second one which is sufficient to indicate the frames detected in error). Once the frames of the X signal are re-emitted, the receiving machine finds that the X signal is 9 frames length. If it happens again that some frames are corrupted, a new DNK is sent with 3 octets in its FIF. This example is illustrated below.

NOTE 2 – It must be noticed that the terminal receiving the X signal can locate the last frame with the bit "x" of the HDLC control field (set to "1").

Example with a DEC received faultily (the same principles apply for a corrupted DES, DER or DTR signal)

-------------------->

DEC

9 frames <--------------------

DNK with FIF 2 octets long:

```
Bit No.  0123   4567   01234567
         xxxx   xxx0   10101111
```

first octet for TCF rejection (see explanation further)
frames 0, 2, 4, 5 and 6 faultily received
frames 7 and 8 not received
(the last bit "1" is only for octet alignment)

-------------------->

DEC

frames 0, 2, 4, 5, 7 and 8 <--------------------

DNK with FIF 3 octets long:

```
Bit No.  0123   4567   01234567  01234567
         xxxx   xxx0   10000000  01111111
```

only frame 0 faultily received

-------------------->

DEC

frame 0 <--------------------

frame correctly received
normal response = implicit acknowledgment
(depends on the context)

H.6.1.2.3.3 Maximum time for retransmissions of signal X upon DNK occurrences

Concerning the retransmission of the signal X upon DNK occurrences, the "fail-safe" timer called Tx is defined.

– The fail-safe timer Tx is defined as follows:

  Tx = 60 s ± 5 s.

– At the transmitter of the signal X, the timer Tx is started at the time of the first DNK recognition and is stopped at the time of the normal response recognition or FNV.

– If the timer Tx has expired, the transmitter of the signal X sends a DCN command for call release.

H.6.1.2.3.4 Specific rejection by DNK

The left-most bit of the first octet of the FIF of DNK (numbered "No. 0" in Table H.2/T.30) is used for rejection of TCF (TCF corrupted); this is the equivalent role of FTT in normal T.30.

The TCF rejection defined in Table H.2./T.30 cannot be combined with the indication of frames X received in error as defined in H.6.1.2.3.2/T.30.

The process of rejection is sequential as follows:

1) First all the corrupted frames of the DEC (or DES, or DER or DTR) are requested by the DNK. The bit No. 7 and bit No. 0 of the first DNK octet are set to "0" (bit No. 0 meaningless at this stage).

2) Once all the frames have been corrected, the content of the DEC (or DES, or DER or DTR) may be rejected by FNV if necessary (see further);

   or if the content of DEC is correct and in case of the TCF following the DEC is corrupted, the TCF is rejected by the first octet of DNK.

Table H.2/T.30 – "Specific rejection by first octet of FIF of DNK"

Specific rejection	Coding of the first octet of FIF of DNK
TCF corrupted (equivalent of FTT in normal mode)	Bit No. 0 1 2 3 4 5 6 7 1 x x x x x x x
Bits 1 to 6 are reserved for future use	Bit No. 0 1 2 3 4 5 6 7 x x x x x x x x
The bit No. 7 must be set to "1" if all the frames have been correctly received and DNK is sent only for TCF rejection. If bit No. 7 is set to 1, the octets after the first one are not sent.	Bit No. 0 1 2 3 4 5 6 7 x x x x x x x 1

Precisions:

– As precised in this Annex, the bits of the FIF of DCS are placed in the first HDLC frame of the DEC.

– As for the other frames, frame No. 0 of a DEC containing the FIF of DCS is re-emitted only when requested by the DNK (if this frame has been faultily received). There is an exception to this rule when TCF is rejected: in such a case, frame No. 0 must always be sent along with the TCF, see example further.

Example with a DEC followed by TCF

-------------------->

DEC 3 frames

——————>

TCF

<--------------------

DNK with FIF 2 octets long:

Bit No. 01234567 01234567

00000000 01011111

frame 1 faultily received,
frames 0 and 2 correctly received

-------------------->

DEC 1 frame:
frame 1

——————>

TCF

<--------------------

DNK with FIF 1 octet long:

Bit No. 01234567

10000001

frame 1 correctly received,
TCF rejection

-------------------->

DEC 1 frame:

frame 0 (contains FIF of DCS)

——————>

TCF

<--------------------

frame 0 correctly received and TCF correct
normal response = implicit acknowledgment
(depends on the context)

H.6.1.3 Precisions for the use of FNV in Annex H

FNV defined in 5.3.6.2.12/T.30 is used only after the following condition is satisfied:

– There is no pending frame of a signal X to be corrected.

Example

```
------------------->

DEC 3 frames

————————————>

TCF                                         <-------------------

                                            DNK with FIF 2 octets long:

                                  Bit No.   01234567   01234567

                                            00000000   01011111

                                            frame 1 faultily received,
                                            frames 0 and 2 correctly received

------------------->

DEC 1 frame:
frame 1

————————————>

TCF                                         <-------------------

                                            frame 1 correctly received,
                                            FNV (because error in the parameter content)
```

H.6.1.4 Data encoding within the FIFs of the DER, DES, DEC and DTR

H.6.1.4.1 Supergroups and Groups

The sequence of the Facsimile Information Fields of DER, DES, DEC and DTR signals is structured in Groups and Supergroups.

Groups are collections of similar or related terminal or session attributes that will often need to be negotiated at the same time.

Supergroups provide an additional hierarchy so that Groups of related attributes may be kept together.

The general sequence of Supergroups and Groups which can be presented in the sequence of Facsimile Information Fields of DER, DES, DEC and DTR signals is as follows:

SG1[G1..G2...G3...]SG2[G1..G2..G3...]...SGn[G1..G2..G3...]

where SG indicates Supergroups and G indicates Groups.

Supergroups are identified by Supergroup Tags, called also in this Annex "super-tags".

Supergoups contain Groups identified by Group Tags, called also in this Annex simply as "tags".

A super-tag is followed by the length of the Supergroup it identifies and then by the sequence of the Groups of the Supergroup.

For each Group, the tag which identifies the Group is followed by the length of the Group and then by the content of the Group.

Notations

– Within this Annex, the content of the Group is called "parameter".

– The length of the Group is called "length of the parameter value".

– The content of the Group is called "value of the parameter".

H.6.1.4.2 Tag Assignment

1) The super-tags are eight bits long.

   An initial tag value of Hex FF indicates an extension of 8 additional bits (may be used in future versions of this Annex).

2) The tags are eight bits long. The extension principle applied is the same as used for super-tags.

H.6.1.4.3 Length of Supergroups – Length of Groups

The count is in units of octets. The first octet after the super-tag or tag contains the number of octets that follow. If the initial count octet is 0, then the two octets following the count octet indicate the number of octets to follow.

Examples: for a 20 octets long parameter value, the length octet will be: "00010100".

Examples: for a 257 octets long parameter value, the length octets will be:
"0000 0000   0000 0001   0000 0001".

The general rule for FIF of DES/DEC/DER/DTR applies: the right-most bit of each octet as printed (least significant bit) is the first one transmitted.

H.6.1.4.4 Encoding rules

A formal description of the encoding rules for encoding the Facsimile Information Fields of DER, DES, DEC and DTR signals follows in Backus-Naur Form (BNF):

ENCODING RULES FOR FACSIMILE TAG ENCODING SYNTAX

```
<bit>                  ::=   <0> | <1>
<octet>                ::=   <bit><bit><bit><bit><bit><bit><bit><bit>
<8_bit_tag>            ::=   <octet>
<extend_octet>         ::=   {< 1><1><1><1><1><1><1><1>}
<tag>                  ::=   <8_bit_tag> | <extend_octet> | <8_bit_tag><8_bit_tag>
<parameter_value>      ::=   <octet>{<octet>}
<count_extend_octet>   ::=   <0><0><0><0><0><0><0><0>
<parameter_length>     ::=   <octet> | <count_extend_octet> <octet> <octet>
<Group>                ::=   <tag><parameter_length><parameter_value>
<frame_number>         ::=   <octet>
<Supergroup_tag>       ::=   <tag>
<Supergroup_length>    ::=   <parameter_length>
<Supergroup>           ::=   <Supergroup_tag> <Supergroup_length><Group>{<Group>}
<Tag_Encoded_Data>     ::=   <Supergroup>{<Supergroup>}
<FIF>                  ::=   <frame_number>< Tag_Encoded_Data>
```

NOTE – The Tag_Encoded_Data may extend over multiple frames, see H.6.1.4.6/T.30.

H.6.1.4.5 Description of Backus-Naur Form

The following provides a description of the Backus-Naur style syntax which is used in the chapter above.

Symbol	**Description of use**
literal	A token (or component) is noted by a literal.
::=	This is the production assignment operator.
|	This symbol is used to separate alternative tokens or groups of tokens.
< >	A non-terminal token is noted by a literal enclosed by the "<" and ">" characters.
[ ]	An optional token or group of tokens is enclosed by the "[" and "]" characters.
{ }	A group of tokens enclosed in "{" and "}" may be repeated 0, 1 or more times.

H.6.1.4.6 Relationship between FIFs encoding and the structure in HDLC frames

The formatting in super-tags, tags and parameters as described above is independent of the structure in HDLC frames described in H.6.1.1/T.30. The series of octets which constitutes the sequence of super-tags, tags and corresponding parameters is orderly inserted in the FIF of the HDLC frames: filling firstly the FIF of the first frame (frame "0"), then filling the FIF of the second frame "1", etc.

H.6.1.4.7 Encapsulated Frame Supergroup

A Supergroup is created which gathers all the Groups which contain the FIF of the following usual T.30 frames: DCS, TSI, SUB, SID, DTC, CIG, SEP, PWD, PSA.

This Supergroup is called "Encapsulated Frame Supergroup".

The super-tag which identifies this Supergroup is: 0000 0001

H.6.1.4.8 The two Supergroups for security

Two Supergroups are created for security:

– one for the registration mode;

– another for the secure transmission mode.

H.6.1.4.9 List of the super-tags

See Table H.3/T.30

Table H.3/T.30 – List of the super-tags

Code of the super-tag	Name of the super-tag	Description
0000 0001	Encapsulated Frame (Abbreviation "E-F")	This super-tag is that of the Encapsulated Frame Supergroup which gathers all the Groups which contain the FIF of usual T.30 frames.
0000 0010	Registration mode	This super-tag is that of the Supergroup which gathers all the Groups transmitted in the registration mode.
0000 0011	Secure transmission mode	This super-tag is that of the Supergroup which gathers all the Groups transmitted in the secure facsimile communication.

H.6.1.4.10 List of the tags within the Encapsulated Frame Supergroup

See Table H.4/T.30

H.6.1.4.11 List of tags for security features

The following tags can be introduced by:

- the security super-tags "Registration mode"; or
- "Secure transmission mode".

Some of the parameters are only used at the message level ("security page", see further); they are marked by a star character "*" in Table H.5/T.30.

H.6.1.4.12 Order of super-tags and tags

In the sequence of super-tags, tags and parameters values, the order is the following:

– encapsulated Frame Supergroup is transmitted before the security Supergroups;

– within each Supergroup, the order of tags is unfixed, except that:

  - within the Encapsulated Frame Supergroup, the Tag "**FIF of DCS**" **must be the first transmitted** (if present); that is for easiness in case of re-emission after TCF rejected [the data field of the first DEC frame which contains (and only contains) "FIF of DCS" **is shorter than 64 octets**];

– within each sequence of tags (and parameters values) introduced by security super-tags, the order of tags is unfixed.

Table H.4/T.30 – List of the tags within the Encapsulated Frame Supergroup

Code of the tag	Name of the tag	Description
1000 0011	FIF of DCS	This tag delimitates the zone where are placed the bits corresponding to the FIF of the DCS (bits of Table 2/T.30).
0100 0011	FIF of TSI	This tag delimitates the zone where are placed the bits corresponding to the FIF of the TSI (when used).
1100 0011	FIF of SUB	This tag delimitates the zone where are placed the bits corresponding to the FIF of the SUB (when used).
1010 0011	FIF of SID	This tag delimitates the zone where are placed the bits corresponding to the FIF of the SID (when used).
1000 0001	FIF of DTC	This tag delimitates the zone where are placed the bits corresponding to the FIF of the DTC (when used).
0100 0001	FIF of CIG	This tag delimitates the zone where are placed the bits corresponding to the FIF of the CIG (when used).
1100 0001	FIF of PWD	This tag delimitates the zone where are placed the bits corresponding to the FIF of the PWD (when used).
1010 0001	FIF of SEP	This tag delimitates the zone where are placed the bits corresponding to the FIF of the SEP (when used).
0110 0001	FIF of PSA	This tag delimitates the zone where are placed the bits corresponding to the FIF of the PSA (when used).

H.6.1.4.13 Coding of the "Security services" parameter

Table H.6/T.30 gives the coding of the parameter value which follows the tag "Security services" and the relevant length octet.

The length octet is "0000 0001" (the parameter is only one octet long). In the next versions of this Annex, the parameter may be longer.

Table H.5/T.30 – List of tags for security features

Code of tag		Name of the tag	Description
0001 0001		S	Sender's identity
0001 0010		Sp	Sender's public key
0001 0011		Ss	Sender's secret key
0001 0100		SpE	Encipherment Sender's public key
0001 0101		SsE	Encipherment Sender's secret key
0001 0110		R	Recipient's identity
0001 0111		Rp	Recipient's public key
0001 1000		Rs	Recipient's secret key
0001 1001		RpE	Encipherment Recipient's public key
0001 1010		RsE	Encipherment Recipient's secret key
0001 1011		Srd/Rra	Random number created respectively by the sender for the digital signature and by the recipient for authentication of the sender
0001 1100		BE = RpE[S, Ks]	Sender identity and Session key encrypted by RpE
0001 1101		UTCd	Date/time chosen by the sender (date/time of the generation/signature of the document)
0001 1110		UTCr	Date/time chosen by the recipient (date/time of the confirmation of message receipt)
0001 1111		Lm	Length of the document
0010 0000		Token 2 = Ss[h(Sra, Rra, R), Sia]	Token used for authentication of the sender when the [Message confidentiality + Session Key establishment] service has not been invoked
0010 0001		Token 2-enc. = Ss[h(Sra, Rra, R, BE), Sia]	Token used for authentication of the sender when the [Message confidentiality + Session Key establishment] service has been invoked
0010 0010		Token 3 = Rs[h(Rra, Sra, S), Ria]	Token used for authentication of the recipient
0010 0011		Token 4 = Ss[h(Srd, UTCd, Lm, R, h(document)), Sis]	Token used for providing the message integrity when the [Message confidentiality + Session Key establishment] has not been invoked
0010 0100		Token 4-enc. = Ss[h(Srd, UTCd, Lm, R, BE, h(enc.document)), Sis]	Token used for providing the message integrity when the [Message confidentiality + Session Key establishment] has been invoked
0010 0101		Token 5 = Rs[h(Srd, UTCr, Lm, S, h(document)), Ris]	Token used for confirmation of message receipt when the [Message confidentiality + Session Key establishment] service has not been invoked
0010 0110		Token 5-enc. = Rs[h(Srd, UTCr, Lm, S, BE, h(enc.document)), Ris]	Token used for confirmation of message receipt when the [Message confidentiality + Session Key establishment] service has been invoked
0010 0111		Security services	Security services
0010 1000		Security mechanisms	Key management mechanisms, hash functions, encipherment algorithms
0010 1001		Optional lengths capability	Optional lengths capability
0010 1010		Request of security capabilities	By use of this tag (and the relevant parameter), the terminal requests the remote terminal for the indication of its security capabilities
0010 1011		Acknowledgment	Acknowledgment used in registration mode
0010 1100	*	Security-page-indicator	Indicates the page where the security page is
0010 1101	*	Security-Page-Type-Identification	Indicates the version number of the security page. In the next versions of this Annex, other types of security pages may be allowed, there will be given other version numbers
0010 1110	*	Certification path	Certification path
0010 1111		Unstandardized features	Unstandardized features

NOTE – The optional tag "Unstandardized features" may be used on the basis of recognition of identification codes in the NSF. The information contained in the initial octets of the "Unstandardized features" parameter value shall be consistent with the identification rules defined in 5.3.6.2.7/T.30 (Non-standard capabilities NSF, NSC, NSS).

Table H.6/T.30 – "Security services" parameter

Security services	Status	Coding of the field
Mutual authentication	Mandatory	Bit No. 7 6 5 4 3 2 1 0 x x x x x x x x No necessity of bit assignment because mandatory
Security service which includes: • Mutual authentication • Message integrity • Confirmation of message receipt	Optional	Bit No. 7 6 5 4 3 2 1 0 x x x x x x x 1
Security service which includes: • Mutual authentication • Message confidentiality (encryption) • Session Key establishment	Optional	Bit No. 7 6 5 4 3 2 1 0 x x x x x x 1 x
Security service which includes: • Mutual authentication • Message integrity • Confirmation of message receipt • Message confidentiality (encryption) • Session Key establishment	Optional	Bit No. 7 6 5 4 3 2 1 0 x x x x x x 1 1
NOTE 1 – Registration service does not need bit allocation because it is mandatory. NOTE 2 – If no optional service, the bit allocation is "0000 0000". NOTE 3 – If the security service "Mutual authentication" is only selected by the sender (for Secure facsimile transmission mode), the "Security services" parameter is not sent (because "Mutual authentication" is the basic service).		

The four sets of services as described in Table H.6/T.30 can be depicted in Table H.7/T.30 where 4 profiles of services can been identified:

Table H.7/T.30 – Security profiles in Annex H

Security services	Service profiles			
	1	2	3	4
Mutual authentication	X	X	X	X
• Message integrity • Confirmation of message receipt		X		X
• Message confidentiality (encryption) • Session Key establishment			X	X

H.6.1.4.14 Coding of the "Security mechanisms" parameter

Table H.8/T.30 gives the coding of the parameter value which follows the tag "Security mechanisms" and the relevant length octet.

The length octet depends on the number of optional encipherment algorithms which are indicated (see Table H.8/T.30).

For the negotiation:

– if requested by the emitting terminal, the receiving terminal indicates the security mechanisms it supports in sending the "Security mechanisms" parameter;

– the emitting terminal selects the security mechanisms for the session: one hash function, one (or none) encipherment algorithm.

In the "security page" (see further), the "Security mechanisms" parameter indicates also the security mechanisms which have been selected for the session.

Table H.8/T.30 – "Security mechanisms" parameter

Mechanisms	Status	Coding of the field

Version of the security system	Mandatory	`Bit No. 7 6 5 4 3 2 1 0`
		`        x x x x x x 0 0`
		(Note)

SHA-1
(hash function)
	Optional	`Bit No. 7 6 5 4 3 2 1 0`
		`        x x x x x 1 x x`

MD-5
(hash function)
	Optional	`Bit No. 7 6 5 4 3 2 1 0`
		`        x x x x 1 x x x`

Security page	Optional	`Bit No. 7 6 5 4 3 2 1 0`
		`        x x x 1 x x x x`

SAFER K-64
(encipherment algorithm)
	Optional	`Bit No. 7 6 5 4 3 2 1 0`
		`        x x 1 x x x x x`

FEAL-32
(encipherment algorithm)
	Optional	`Bit No. 7 6 5 4 3 2 1 0`
		`        x 1 x x x x x x`

RC5
(encipherment algorithm)
	Optional	`Bit No. 7 6 5 4 3 2 1 0`
		`        1 x x x x x x x`

Second octet	Optional	

IDEA
(encipherment algorithm)
	Optional	`Bit No. 7 6 5 4 3 2 1 0`
		`        x x x x x x x 1`

HFX40	Optional	`Bit No. 7 6 5 4 3 2 1 0`
		`        x x x x x x 1 x`

DSA
(key management)
	Optional	`Bit No. 7 6 5 4 3 2 1 0`
		`        x x x x x 1 x x`

Bits 3 to 7 reserved for future use (set to "0")		`Bit No. 7 6 5 4 3 2 1 0`
		`        x x x x x x x x`

....	Optional	`Bit No. 7 6 5 4 3 2 1 0`
		`        x x x x x x x x`

Last octet	Optional	`Bit No. 7 6 5 4 3 2 1 0`
		`        x x x x x x x x`

NOTE – As new versions of the Annex H/T.30 security system are introduced, backward compatibility should be maintained.

The second octet is optional.

The octets from the third one to the last one are also optional octets. They may be absent.

Each of these octets codes an optional encipherment algorithm available in the receiving terminal. The octet is the number of one encipherment algorithm registered in the entry index of Attachment 2 of ISO/IEC 9979 ("Procedure for registering cryptographic algorithms"); this number is binary coded (e.g. "0000 0000" for the entry No. 00).

When the emitting terminal selects the mechanisms, the "Security mechanisms" parameter is usually only one or two octets long. The third octet is only necessary in case of selection of an encipherment algorithm registered in ISO/IEC 9979 and which is not SAFER K-64, nor FEAL-32, nor RC5, nor IDEA, nor HFX40 (the third octet indicates the algorithm selected).

H.6.1.4.15 Coding of the "Optional lengths capability" parameter

H.6.1.4.15.1 Principle

For indication of the optional lengths capabilities, the "Optional lengths capability" tag, length octet and corresponding parameter value are sent.

H.6.1.4.15.2 Coding of the parameter "Optional lengths capability"

For coding the parameter, the following principles are defined:

– Offsets permit to indicate the maximal lengths which can be processed by the terminal.

  These offsets are binary coded on 4 bits or 8 bits depending on the parameter which is concerned.

– These offsets are used on a specific order:

Octet No. 0								
Bit No.	7	6	5	4	3	2	1	0
			offset a	offset b				
Octet No. 1								
Bit No.	7	6	5	4	3	2	1	0
			offset c	reserved				

First, the octet No. 0 which contains:

– firstly the offset "a" (4 bits) for indication of the maximum length of Public and Secret keys accepted;

– then the offset "b" (4 bits) for indication of the length of the Random numbers accepted (Sra, Srd, Rra).

Then, the octet No. 1 (optional) which contains:

– the offset "c" (4 bits) for indication of the maximum length of Encipherment Public and Encipherment Secret keys accepted.

Therefore, the length octet of the "Optional lengths capability" parameter is either "0000 0001" (one octet long if the [Message confidentiality + Session Key establishment] service is not offered) or "0000 0010" (two octets if the [Message confidentiality + Session Key establishment] service is offered). In the next versions of this Annex, the parameter may be longer.

H.6.1.4.15.3 Rules for using the offsets

Maximum length (in octets) of the Public and Secret keys =

64 (basic length) + ([offset a] × 16) octets

with $0 \leq$ offset a ≤ 4 octets

The terminal must be capable to handle all the lengths between the basic length and the maximum length, by 16 octets increments.

Maximum length (in octets) of Random numbers =

8 (basic length) + [offset b] octets

with $0 \leq$ offset b ≤ 8 octets

The terminal must be capable to handle all the lengths between the basic length and the maximum length.

Maximum length (in octets) of the Encipherment Public and Encipherment Secret keys =

64 (basic length) + ([offset c] × 16) octets

with $0 \leq$ offset c ≤ 4 octets

The terminal must be capable to handle all the lengths between the basic length and the maximum length, by 16 octets increments.

H.6.1.4.15.4 Examples

Example 1

Octet No. 0								
Bit No.	7	6	5	4	3	2	1	0
	0	0	0	1	0	0	0	0
Octet No. 1								
Bit No.	7	6	5	4	3	2	1	0
	0	0	0	1	0	0	0	0

In this example:

- – Maximum length of Public and Secret key = $64 + 16 \times 1$ = 80 octets
- – Maximum length of Random numbers = $8 + 0$ = 8 octets (no optional lengths supported)
- – Maximum length of Encipherment Public and Encipherment Secret key = $64 + 16 \times 1$ = 80 octets

Example 2

Octet No. 0								
Bit No.	7	6	5	4	3	2	1	0
	0	0	0	0	0	0	0	0

In this example, the terminal indicates the only basic capabilities.

H.6.1.4.16 Coding of the "Request of security capabilities" parameter

By use of this tag (and the relevant parameter), the terminal requests the remote terminal for the indication of its security capabilities. See Table H.9/T.30.

The length octet is "0000 0001" (the parameter is only one octet long). In the next versions of this Annex, the parameter may be longer.

Table H.9/T.30 – "Request of security capabilities" parameter

Capabilities indication requested	Status	Coding of the field
Request of the "Security services"	Optional	Bit No. 7 6 5 4 3 2 1 0 x x x x x x x 1
Request of the "Security mechanisms"	Optional	Bit No. 7 6 5 4 3 2 1 0 x x x x x x 1 x
Request of "Optional lengths capability"	Optional	Bit No. 7 6 5 4 3 2 1 0 x x x x x 1 x x
Request of "Unstandardized features"	Optional	Bit No. 7 6 5 4 3 2 1 0 x x x x 1 x x x
NOTE – If the "Request of security capabilities" parameter is used, at least one bit must be set to "1" (otherwise, there is no purpose of using this parameter for the session).		

H.6.2 Registration mode

H.6.2.1 Scheme

The scheme is described in Figure H.3/T.30. It comprises of two steps:

– *Step one:*

  [The identity of the sender and its public key are hashed by the sending terminal.

  The identity of the recipient and its public key are hashed by the receiving terminal].

  OR/AND

  [(The identity of the sender and its encipherment public key are hashed by the sending terminal).

  OR/AND

  (The identity of the recipient and its encipherment public key is hashed by the receiving terminal)].

  These hash results are exchanged out-of-band (direct hand-to-hand, by mail, by phone, etc.) and stored in the terminals.

– *Step two:*

  Exchange, by T.30 protocol means, of the identities and the public keys between the two parties. Storage in the terminals.

The order of the two steps is not fixed.

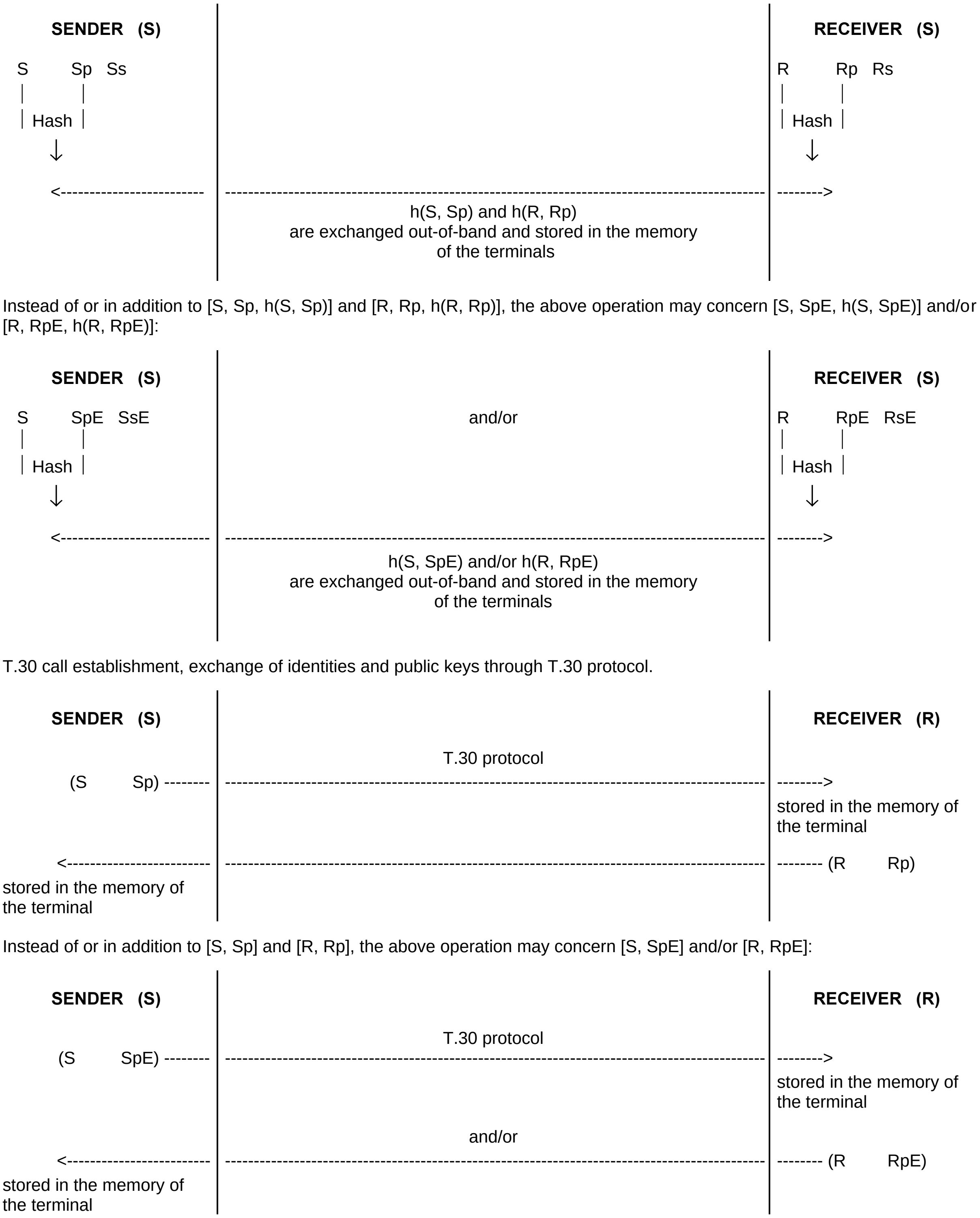
The validity of the identity and the public key(s) of the other party is assessed in comparing the hash result exchanged out-of-band with the hash result of the identity and public key(s) received through the protocol.

Once validated, these values [identity and public key(s) of the remote party] are stored in the terminals and are used for the further secure facsimile communications with this party.

The registration of either the public keys or the encipherment public keys or both is fixed by agreement between the users of the two terminals. For the encipherment public keys, the registration may concern only one user or both.

Settings of the terminals for the relevant registrations is a local matter.

Exchange of the hash results out-of-band and storage in the terminals.



SENDER (S)
RECEIVER (S)
S Sp Ss
Hash
R Rp Rs
Hash
h(S, Sp) and h(R, Rp)
are exchanged out-of-band and stored in the memory
of the terminals

Instead of or in addition to [S, Sp, h(S, Sp)] and [R, Rp, h(R, Rp)], the above operation may concern [S, SpE, h(S, SpE)] and/or [R, RpE, h(R, RpE)]:

SENDER (S)
RECEIVER (S)
S SpE SsE
and/or
R RpE RsE
Hash
Hash
h(S, SpE) and/or h(R, RpE)
are exchanged out-of-band and stored in the memory
of the terminals

T.30 call establishment, exchange of identities and public keys through T.30 protocol.

SENDER (S)
RECEIVER (R)
T.30 protocol
(S Sp)
stored in the memory of the terminal
(R Rp)
stored in the memory of the terminal

Instead of or in addition to [S, Sp] and [R, Rp], the above operation may concern [S, SpE] and/or [R, RpE]:

SENDER (S)
RECEIVER (R)
T.30 protocol
(S SpE)
stored in the memory of the terminal
and/or
(R RpE)
stored in the memory of the terminal

Figure H.3/T.30 – Scheme of registration mode

H.6.2.2 Use of DER, DES and DEC for registration mode

In the second step of the registration mode, the signals DER, DES, DEC are used as in Figure H.4/T.30.

```
Calling side                                                    Called side


                    ---------------------------CNG------------------------->            | (Note)
                    <-------------------------CED----------------------------            |


                    <------------------(NSF)-(CSI)-DIS--------------------
                    -------------------DER-----(phase 0)----------------->            | Optional


                    <-----------------DES-----(phase 1)-------------------            |
                    --------DER contains [S and Sp] (phase 2)------->
                    <------DES contains [R and Rp] (phase 3)--------
                    --------DEC (acknowledgement) (phase 4)------->
                    <-------DES (acknowledgement) (phase 5)--------


                    --------------------------DCN----------------------------->
```

NOTE – The call establishment CNG/CED which is depicted in the figure is given for example.

The other operating methods defined in 3.1 may take place as well.

Instead of or in addition to respectively Sp and Rp, the above operation may concern SpE and/or RpE.

The timers used for the signals exchange above are the same ones as those for the standard T.30 protocol (T1, T2, T4,...). Upon no response after timer T4, the command from the emitting side (DER, DEC or DNK) is resent (for DER and DEC, only the frames not yet acknowledged).

Figure H.4/T.30 – Signals exchange for registration mode

H.6.2.3 Bits allocation in the DIS

The bits allocation in the FIF of the DIS to indicate the security capabilities based on the RSA algorithm is given in Table 2/T.30. Bit No. 82 is used.

H.6.2.4 Format of the Facsimile Information Fields of DER, DES and DEC for registration mode

Convention

In the figures of this Annex, when the tag (and the relevant length octet and parameter value) is represented in grey boxes, its use is optional.

When represented in white boxes, its use is mandatory.

H.6.2.4.1 Phase 0 OPTIONAL

If the calling side does not wish to use optional capabilities, phase 0 is optional; registration mode is carried on with the basic features (Sp, Rp are 64 octets long, no exchange of Encipherment public keys).

The sequence contained in the FIF(s) of the DER is:

Super-tag "E-F"	Length of Supergroup	Tag "FIF of SUB"	Length + Content of "FIF of SUB"	Tag "FIF of SID"	Length + Content of "FIF of SID"	Tag "FIF of TSI"	Length + Content of "FIF of TSI"

Super-tag "Registration mode"	Length of Supergroup	Tag "Request of security capabilities"	Length + Content of "Request of security capabilities"

Tag "Unstandardized features"	Length + Content of" Unstandardized features"

Conventions

For simplicity, the representations of sequences [super-tags, tags, length octets and parameters values] do not describe the internal HDLC structure of the signal (preamble, flags, address, control, ..., FCS, flags).

A sequence may be represented by boxes on several rows. This is only for commodity; the sequence is continuous.

These remarks apply for the rest of this Annex where such representations are given.

H.6.2.4.2 Phase 1 OPTIONAL

Phase 1 takes place only if phase 0 exists.

The sequence contained in the FIF(s) of the DES is:

Super-tag "Registration mode"	Length of Supergroup	Tag "Security services"	Length + Content of "Security services"

Tag "Security mechanisms"	Length + Content of "Security mechanisms"	Tag "Optional lengths capability"	Length + Content of "Optional lengths capability"	Tag "Unstandardized features"	Length + Content of "Unstandardized features"

The optional [tag, length octet and parameter value] groups are present depending on the requests in phase 0 (bits in the "Request of security capabilities" parameter).

H.6.2.4.3 Phase 2

The sequence contained in the FIF(s) of the DER is:

Super-tag "E-F"	Length of Supergroup	Tag "FIF of SUB"	Length + Content of "FIF of SUB"	Tag "FIF of SID"	Length + Content of "FIF of SID"	Tag "FIF of TSI"	Length + Content of "FIF of TSI"

Super-tag "Registration mode"	Length of Supergroup	Tag "S"	Length + Content of "S"	Tag "Sp"	Length + Content of "Sp"

Tag "SpE"	Length octet + Content of "SpE"	Tag "Security mechanisms"	Length octet + Content of "Security mechanisms"	Tag "Unstandardized features"	Length + Content of "Unstandardized features"

Above is an example of registration of Sp and SpE at the same time.

It is also possible that only Sp or SpE is registered. S is present in all cases.

Settings of the terminals for the relevant registrations is a local matter.

The "Security mechanisms" parameter is mandatory because it indicates the selected hash function and/or the selected encipherment algorithm (in case of SpE and/or RpE exchanged).

H.6.2.4.4 Phase 3

The sequence contained in the FIF(s) of the DES is:

Super-tag "Registration mode"	Length of Supergroup	Tag "R"	Length + Content of "R"	Tag "Rp"	Length + Content of "Rp"

Tag "RpE"	Length + Content of "RpE"

Above is an example of registration of Rp and RpE at the same time.

It is also possible that only Rp or RpE is registered. R is present in all cases.

Settings of the terminals for the relevant registrations is local matter.

If the called terminal can find that the S and Sp parameters (and/or [S , SpE]) do not conform with the hash value stored (in case of exchange of hash values out-of-band already made, see H.6.2.1/T.30), it can reject them by the signal FNV.

The reason of the error in FNV is "Registration error for public key or "Registration error for encipherment public key, see Table H.10/T.30.

The use of FNV for such an error indication is explained in H.6.7/T.30.

H.6.2.4.5 Phase 4

The sequence contained in the FIF of the DEC is:

Super-tag "Registration mode"	Length of Supergroup	Tag "Acknowledgment"	Length octet "0000 0000"

If the calling terminal can find that the R and Rp parameters (and/or [R, RpE]) do not conform with the hash value stored (in case of exchange of hash values out-of-band already made, see H.6.2.1/T.30), it can reject them by the signal FNV.

The reason of the error in FNV is "Registration error for public key or "Registration error for encipherment public key, see Table H.10/T.30.

The use of FNV for such an error indication is explained in H.6.7/T.30.

H.6.2.4.6 Phase 5

The sequence contained in the FIF of the DES is:

Super-tag "Registration mode"	Length of Supergroup	Tag "Acknowledgment"	Length octet "0000 0000"

H.6.3 Secure facsimile transmission mode

This mode consists in the transmission of the facsimile document with security features.

Security parameters are transmitted within protocol elements (phases B and D of the T.30 protocol).

As an option, some security parameters are transmitted at the message level (at the message speed, phase C of T.30 protocol): within a special page called "**the security page**".

H.6.3.1 Scheme

See Figure H.5/T.30.

SENDER (S)		RECEIVER (R)
	T.30 call establishment	
	---phase 0--	-------->
	Request of security capabilities *Optional lengths capability* *of the sender*	
<-------------------------	---phase 1--	
	Receiver capabilities: *Security services* *Security mechanisms* *Optional lengths capability* Rra	
(S, Sra, R, *BE* Ss[h(Sra, Rra, R, *BE*), Sia])	---phase 2--	-------->
	+ choice of security features: *Security services* *Security mechanisms*	
(Note 1)		
<-------------------------	---phase 3--	(R, Rra, Rs[h(Rra, Sra, S), Ria])
	---------------------------------Facsimile document---------------------------------	-------->
	---------------------------------optional phase 4-----------------------------------	-------->
		(Note 2)
	Signal containing the digital signature:	(Note 3)
(Note 1)	Srd, UTCd, Lm, Ss[h(Srd, UTCd, Lm, R, *BE*, h(*enc.*document)), Sis]	
<-------------------------	----------------------------------optional phase 5----------------------------------	(Note 2)
	Confirmation of message receipt *containing:* UTCr, Rs[h(Srd, UTCr, Lm, S, *BE*, h(*enc.*document)), Ris]	(Note 1)

Italicized characters indicate optional features.

NOTE 1 – BE (= RpE[S, Ks]) exists in the various tokens only if the service [Message confidentiality + Session Key establishment] has been negotiated between the two parties (with the "Security services" parameter).

NOTE 2 – Phases 4 and 5 exist only if the service [Message integrity + Confirmation of message receipt] has been negotiated between the two parties (with the "Security services" parameter).

NOTE 3 – Additional parameters are present if the security page is used at phase 4.

Figure H.5/T.30 – Scheme of secure facsimile transmission mode

H.6.3.2 Use of DER, DES and DEC for secure facsimile transmission mode

H.6.3.2.1 General scheme for secure facsimile transmission mode

For the secure facsimile transmission mode, the signals DER, DES and DEC are used as in Figure H.6/T.30.

```
                  Calling side                                                  Called side


                                   ---------------------------CNG-------------------------->         | (Note 1)
                                   <-------------------------CED----------------------------         |
                                   <------------------(NSF)-(CSI)-DIS--------------------
                                   -------------------DER-----(phase 0)------------------>
                                   <------------------DES-----(phase 1)-------------------
                                   ---------------------------TNR--------------------------->         | (Note 2)
                                   <---------------------------TR-----------------------------         |
                                   -------------------DEC-----(phase 2)------------------>
                                   ——————————— TCF ——————————>
                                   <--------------------------RNR----------------------------         | (Note 3)
                                   -----------------------------RR---------------------------->         |
                                   <------------------DES-----(phase 3)--------------------
                                   ————————————————————————————

                                                                                -------->
                                                    Facsimile data              -------->
                                                                                -------->
                                   ————————————————————————————
                 ----PPS-PSS if phases 4 and 5 are present, PPS-EOP or PPS-EOM otherwise----->
                                   <---------------------------MCF---------------------------
                                   ————————————————————————————

                                                                                -------->         | (Note 4)
                                   Optional phase 4, see Figure H.7/T.30        -------->         |
                                                                                -------->         |
                                   ————————————————————————————
                                   <--------------------------RNR----------------------------         | (Note 3)
                                   -----------------------------RR---------------------------->         |
                                <----Optional phase 5-----MCF appended with octets---         | (Note 4)
                                   ----------------------------DCN--------------------------->
```

The timers used for the signals exchange above are the same ones as those for the standard T.30 protocol and Annex A/T.30 (T1, T2, T4, T5, ...). Upon no response after timer T4, the command from the emitting side (DER, DEC or DNK) is resent (for DER and DEC, only the frames not yet acknowledged).

NOTE 1 – The call establishment CNG/CED which is depicted in the figure is given for example. The other operating methods defined in 3.1 may take place as well.

NOTE 2 – The use of TNR and TR is exactly the same one as the use of RNR/RR but concerns the emitting terminal instead of the receiving terminal. Some optional occurrences of the TNR-TR exchange can permit to the emitting terminal to hold off the receiving terminal during a maximum time of T5 (see Annex A/T.30).

NOTE 3 – Some optional occurrences of the RNR-RR exchange (already defined in Annex A/T.30) can permit to the receiving terminal to hold off the emitting terminal during a maximum time of T5 (see Annex A/T.30).

NOTE 4 – Phases 4 and 5 exist only if the service [Message integrity + Confirmation of message receipt] has been negotiated between the two parties (with the "Security services" parameter).

Figure H.6/T.30 – Signals exchange for secure facsimile transmission mode
Example for a one facsimile page document

H.6.3.2.2 Phase 4

When phase 4 (and then phase 5) is present, two cases exist depending on whether the security page capability has been negotiated between the two parties or not:

Case 1 – When both machines (emitting and receiving) provide the security page capability and the [Message integrity + Confirmation of message receipt] service is invoked, the security page solution (case 1) must be used.

Case 2 – When one of the two machines does not provide the security page capability and the [Message integrity + Confirmation of message receipt] service is invoked, the solution of PPS-EOP or PPS-EOM appended (case 2) must be used.

PPS-EOM (not appended in case 1, appended in case 2) is used if the communication is to be continued by another document.

PPS-EOP (not appended in case 1, appended in case 2) is used in the common case, with only one facsimile document during the communication.

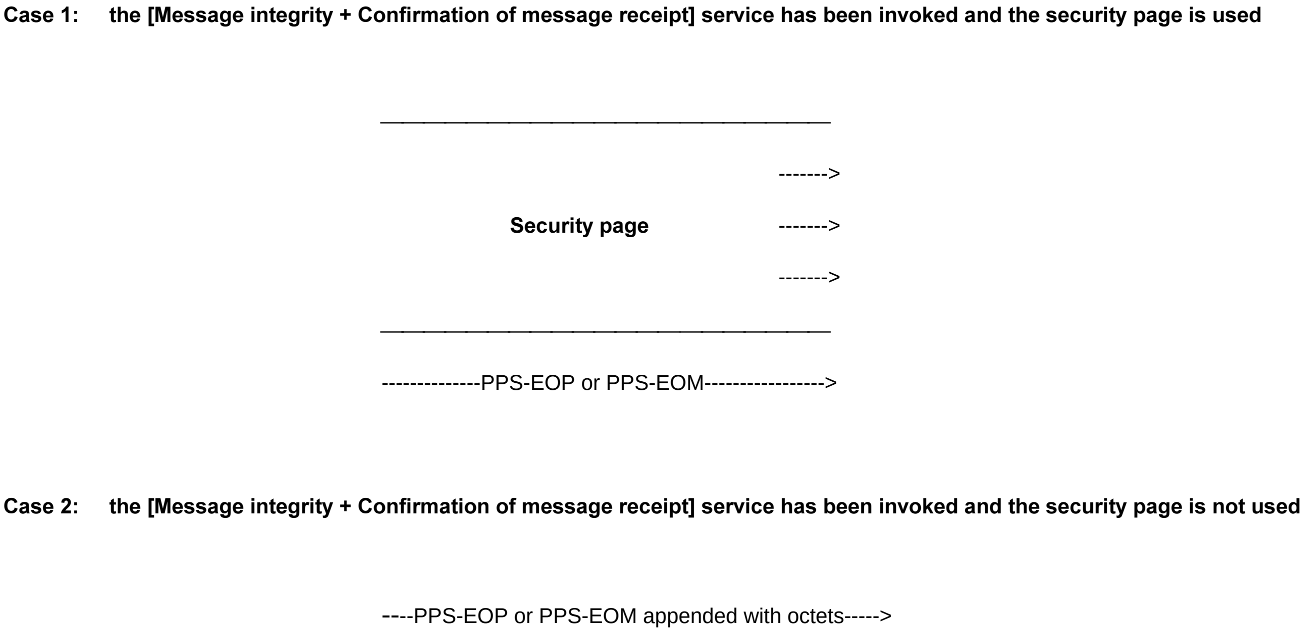

Case 1: the [Message integrity + Confirmation of message receipt] service has been invoked and the security page is used
------->
Security page
------->
------->
-------------PPS-EOP or PPS-EOM---------------->
Case 2: the [Message integrity + Confirmation of message receipt] service has been invoked and the security page is not used
----PPS-EOP or PPS-EOM appended with octets----->

Figure H.7/T.30 – Signals exchange in phase 4

H.6.3.3 Bits allocation in the DIS

The bits allocation in the FIF of the DIS to indicate the security capabilities based on the RSA algorithm is given in Table 2/T.30. Bit No. 82 is used.

The DCS is not emitted in the context of Annex H/T.30; FIF of DCS is included within the new signal "DEC" where the corresponding bit No. 82 must be set to "1".

H.6.3.4 Format of Facsimile Information Field of DER, DES and DEC for secure facsimile transmission mode

H.6.3.4.1 Phase 0

The sequence contained in the FIF(s) of the DER is:

Super-tag "E-F"	Length of Supergroup	Tag "FIF of SUB"	Length + Content of "FIF of SUB"	Tag "FIF of SID"	Length + Content of "FIF of SID"	Tag "FIF of TSI"	Length + Content of "FIF of TSI"

Super-tag "Secure transmission mode"	Length of Supergroup	Tag "Optional lengths capability"	Length + Content of "Optional lengths capability"	Tag "Request of security capabilities"	Length + Content of "Request of security capabilities"

Tag "Unstandardized features"	Length + Content of "Unstandardized features"

If the calling side does not wish to use optional services and optional capabilities, the "Request of security capabilities" parameter is not sent. Secure facsimile transmission mode is carried on with the basic features (Sp, Rp 64 octets long, etc.) with the Mutual authentication service only invoked.

Also, if the calling side cannot handle random numbers of optional lengths (longer than the basic one), it does not have to send the "Optional lengths capability" parameter.

H.6.3.4.2 Phase 1

The sequence contained in the FIF(s) of the DES is:

Super-tag "Secure transmission mode"	Length of Supergroup	Tag "Rra"	Length + Content of "Rra"	Tag "Security services"	Length + Content of "Security services"

Tag "Security mechanisms"	Length + Content of "Security mechanisms"	Tag "Optional lengths capability"	Length + Content of "Optional lengths capability"	Tag "Unstandardized features"	Length + Content of "Unstandardized features"

The optional [tag, length and parameter value] groups are present depending on the requests in phase 0 (bits in the "Request of security capabilities" parameter).

H.6.3.4.3 Phase 2

The sequence contained in the FIF(s) of the DEC is:

Super-tag "E-F"	Length of Super-group	Tag "FIF of DCS"	Length + Content of "FIF of DCS"	Tag "FIF of SUB"	Length + Content of "FIF of SUB"	Tag "FIF of SID"	Length + Content of "FIF of SID"	Tag "FIF of TSI"	Length + Content of "FIF of TSI"

Super-tag "Secure transmission mode"	Length of Supergroup	Tag "S"	Length + Content of "S"	Tag "Sra"	Length + Content of "Sra"	Tag "R"	Length + Content of "R"

Tag "BE"	Length + Content of "BE"	Tag "Token 2" or "Token 2-enc."	Length + Content of "Token 2" or "Token 2-enc."

Tag "Security services"	Length + Content of "Security services"	Tag "Security mechanisms"	Length + Content of "Security mechanisms"	Tag "Unstandardized features"	Length + Content of "Unstandardized features"

– Tag BE is present only if the service [Message confidentiality + Session Key establishment] is invoked. In such case, this is Token 2-enc. which is sent.

– Tags "Security services" is not present if the transmission is to take place with the Mutual Authentication service only.

– The "Security mechanisms" parameter is mandatory because it indicates the selected hash function.

H.6.3.4.4 Phase 3

The sequence contained in the FIF(s) of the DES is:

Super-tag "Secure transmission mode"	Length of Supergroup	Tag "R"	Length + Content of "R"	Tag "Rra"	Length + Content of "Rra"	Tag "Token 3"	Length + Content of "Token 3"

H.6.3.4.5 Phase 4

Phases 4 and 5 exist only if the service [Message integrity + Confirmation of message receipt] has been negotiated between the two parties.

The signal sent in phase 4 is either the PPS-EOP (or PPS-EOM) signal appended with octets (case 2 depicted in Figure H.7/T.30) or the security page (case 1 depicted in Figure H.7/T.30).

When both machines (emitting and receiving) provide the security page capability and the [Message integrity + Confirmation of message receipt] service is invoked, the security page solution must be used.

The content of the security page is defined in H.6.4/T.30.

In case 2, the structure of the PPS-EOP (or PPS-EOM) appended with octets is the same as that of DER, DES, DEC and DTR (as defined in H.6.1.1/T.30): multi-frames, bit X = 1 for final frame, FIF of 65 octets, frame numbers, ...

The FCF is that already defined in Annex A/T.30 (in A.4.3/T.30.).

The sequence contained in the FIF(s) of the PPS-EOP (or PPS-EOM) appended is:

Super-tag "Secure transmission mode"	Length of Supergroup	Tag "Srd"	Length + Content of "Srd"	Tag "UTCd"	Length + Content of "UTCd"	Tag "Lm"	Length + Content of "Lm"

Tag "Token 4" or "Token 4-enc."	Length + Content of "Token 4" or "Token 4-enc."	Tag "Unstandardized features"	Length + Content of "Unstandardized features"

"Token 4" or "Token 4-enc." is sent depending on whether the service [Message confidentiality + Session Key establishment] has been invoked or not at phase 2.

H.6.3.4.6 Phase 5

Phases 4 and 5 exist only if the service [Message integrity + Confirmation of message receipt] has been negotiated between the two parties.

The signal sent at phase 5 is the MCF signal appended with octets.

The structure of the MCF appended with octets is the same as that of DER, DES, DEC and DTR (as defined in H.6.1.1/T.30): multi-frames, bit X = 1 for final frame, FIF of 65 octets, frame numbers, etc.

The FCF is that already defined for the normal T.30 protocol (in 5.3.6.1.7/T.30).

The sequence contained in the FIF(s) of the MCF appended is:

Super-tag "Secure transmission mode"	Length of Supergroup	Tag "UTCr"	Length + Content of "UTCr"	Tag "Token 5" or "Token 5-enc."	Length + Content of "Token 5" or "Token 5-enc."

"Token 5" or "Token 5-enc." is sent depending on whether the service [Message confidentiality + Session Key establishment] has been invoked or not at phase 2.

H.6.3.4.7 Error-messages

In case of errors detected in phase 1, 2, 3, 4 or 5, the sender or the recipient (depending on the phase) indicates the error with the signal FNV.

The reason of the error is coded in FNV.

Table H.10/T.30 gives the coding of the error value.

The use of FNV for error indication is explained in H.6.7/T.30.

H.6.3.5 Precisions for use of PPS-EOM within a secure document

Within the sequence of partial pages which constitute one secure document, the use of PPS-EOM is allowed (e.g. for changing the image resolution). The procedure after PPS-EOM is quite close as in Annex A/T.30:

```
-----------------------PPS-EOM----------------------->
<-------------------------MCF--------------------------
                                                   T2 elapsed
<------------------(NSF)-(CSI)-DIS-------------------
------------------DEC (with FIF DCS)---------------->
——————————————TCF——————————————>
```

In such a case, for setting the transmission of the remaining pages of the document, the DEC must contain the FIF of DCS [with the relevant bit(s) for security set to "1", as in phase 2]. The security parameters sent in phase 2 are not included in the DEC at this stage; they are valid throughout the transmission of the document.

H.6.4 At the message level: Security page

The use of the security page is defined in case 1 of Figure H.7/T.30.

When both machines (emitting and receiving) provide the security page capability and the [Message integrity + Confirmation of message receipt] service is invoked, the security page solution must be used.

H.6.4.1 Content of the security page

The "security page" contains the following security parameters defined in Tables H.1/T.30 and H.5/T.30:

Security-page-indicator : Indicates the block contains the security page.

S : Identity of the sender.

Sp : Public Key of the sender.

R : Identity of the recipient.

Srd : Random number created by the sender for the digital signature.

UTCd : Date/time chosen by the sender (date/time of the generation/signature of the document).

Lm : Length of the document.

"Security services" parameter : See definition in Table H.6/T.30.

"Security mechanisms" parameter : See definition in Table H.8/T.30.

BE : RpE[S, Ks].

Token 4 or Token 4-enc. : See definition in Table H.5/T.30.

Security-Page-Type-Identification : Indicates the version number of the security page. In the next versions of this Annex, other types of security pages may be allowed, they will be given other version numbers.

Certification path : Certificate of the public key of the sender. The precise definition of the certification path is for further study.

Unstandardized features : Unstandardized features.

The bit order transmission within the security page follows the same rules as defined for FIF of DES/DEC/DER/DTR in H.4.8.3/T.30 and specified in Table H.1/T.30.

H.6.4.1.1 Coding of the "Security-page-indicator" parameter

This tag (and the relevant parameter) indicates the block contains the security page.

The length octet is "0000 1000" (8 octets).

The contain is (in hexadecimal):

0x01 0x23 0x45 0x67 0x89 0xAB 0xCD 0xEF

H.6.4.1.2 Coding of the "Security-Page-Type-Identification" parameter

This parameter is optional in the security page.

The length octet is "0000 0001" (1 octet).

The contain is the version number of the security page. In this version of this Annex, only one version of the security page exists, the version number is: 0x00.

H.6.4.2 Format of the security page

The security page has exactly the same kind of format as the sequences within the DER, DES, DEC and DTR signals (super-tags, tags and parameters values), except that in this case, the sequence is not placed in the series of FIF of DER, DES, DEC or DTR, but in the ECM frames.

Within the sequence of tags introduced by the super-tag, **the order is unfixed**, except the Security-page-indicator which is the first one.

The sequence is the following:

Super-tag "Secure transmission mode"	Length of Supergroup	Tag "Security-page-indicator"	Length + Content of "Security-page-indicator"	Tag "S"	Length + Content of "S"	Tag "Sp"	Length + Content of "Sp"

Tag "R"	Length + Content of "R"	Tag "Srd"	Length + Content of "Srd"	Tag "UTCd"	Length + Content of "UTCd"	Tag "Lm"	Length + Content of "Lm"

Tag "Security services"	Length + Content of "Security services"	Tag "Security mechanisms"	Length + Content of "Security mechanisms"

Tag "BE"	Length octet + Content of "BE"

Tag "Token 4" or "Token 4-enc."	Length + Content of "Token 4" or "Token 4-enc."	Tag "Security-Page-Type-Identification"	Length + Content of "Security-Page-Type-Identification"

Tag "Certification path"	Length + Content of "Certification path"	Tag "Unstandardized features"	Length + Content of "Unstandardized features"

NOTE 1 – The bits in the Security services and Security mechanisms parameters are set in conformance with respectively Table H.6/T.30 and Table H.8/T.30 [version of the security system, bit indicating the hash function used, bit indicating the encipherment algorithm used (if document enciphered)].

NOTE 2 – Parameter BE is present only if the service [Message confidentiality + Session Key establishment] has been invoked.

NOTE 3 – The format of the certification path is for further study.

H.6.5 Rules for hashing the document – Rules for enciphering the document

H.6.5.1 Rules for hashing the document

The data of the document which are part of the bit string which is hashed are all the octets contained in the FIF of all the ECM data frames except the first octet of each frame (which is the frame number). Therefore, any fill bits and pad bits (as described in A.3.6.2/T.4 and in 2.4.1.2/T.6) are part of the data which pass through the hash function.

The bit stream entering in the hashing process for producing h(document) or h(enc.document) (in case of encipherment) can be represented as the bit string contained in the rectangle depicted in Figure H.8/T.30.

For each octet, this bit string has the same bit order in the hashing process as the data bits of each octet when transmitted over the line.

First page		
First block:		
First frame FIF	: frame number	first data octet . . . . last octet of FIF
Second frame FIF	: frame number	first data octet . . . . last octet of FIF
. . .		
Last frame FIF	: frame number	first data octet . . . . last octet of FIF
Second block:		
First frame FIF	: frame number	first data octet . . . . last octet of FIF
Second frame FIF	: frame number	first data octet . . . . last octet of FIF
. . .		
Last frame FIF	: frame number	first data octet . . . . last octet of FIF
. . .		
. . .		
. . .		
Last block:		
First frame FIF	: frame number	first data octet . . . . last octet of FIF
Second frame FIF	: frame number	first data octet . . . . last octet of FIF
. . .		
Last frame FIF	: frame number	first data octet . . . . last octet of FIF
Second page		
. . .		
. . .		
. . .		
Last page		
. . .		
. . .		
Last block:		
First frame FIF	: frame number	first data octet . . . . last octet of FIF
Second frame FIF	: frame number	first data octet . . . . last octet of FIF
. . .		
Last frame FIF	: frame number	first data octet . . . . last octet of FIF

Figure H.8/T.30 – Rules for hashing the document

H.6.5.2 Rules for enciphering the document

The data of the document which will be encrypted are the octets contained in the FIF of the ECM data frames except the first octet of each frame (which is the frame number).

The input bit order to the encryption function is the same order as the one when the facsimile data is transmitted over the line without encryption.

NOTE – For FEAL-32, these data are aligned every 64 bits in order from the left to the right and are input to FEAL-32 function.

Every 64 bits of the encrypted data from FEAL-32 function are aligned in order from the left to the right, and the left-most bit is transmitted first.

H.6.6 Secure polling mode

H.6.6.1 Simple polling

The use and the coding of the signals in the secure polling mode follows the same rules as for the secure facsimile transmission mode.

The signals exchange is depicted in Figure H.9/T.30.

```
              Calling side                                    Called side


                          ------------------------------CNG------------------------------>      | (Note)
                          <----------------------------CED--------------------------------      |
                          <---------------------(NSF)-(CSI)-DIS-----------------------
                          --------------------DTR-----(phase 00)-------------------->
                          <--------------------DER-----(phase 0)----------------------
                          ---------------------DES-----(phase 1)--------------------->
                          <-----------------------------TNR-------------------------------
                          --------------------------------TR------------------------------->
                          <---------------------DEC-----(phase 2)---------------------
                      <——————————————————————TCF———————————————————————
                          --------------------------------RNR------------------------------>
                          <-------------------------------RR---------------------------------
                          ----------------------DES-----(phase 3)--------------------->
                          ______________________________________________________
                          <-------
                          <-------               Facsimile data
                          <-------
                          ______________________________________________________
              <--- PPS-PSS if phases 4 and 5 are present, PPS-EOP or PPS-EOM otherwise ----
                          ---------------------------------MCF----------------------------->
                          ______________________________________________________
                          <-------
                          <------- Optional phase 4, see Figure H.7/T.30
                          <-------
                          ______________________________________________________
                          ---------------------------------RNR---------------------------->
                          <--------------------------------RR------------------------------
                         ----- Optional phase 5---- MCF appended with octets --->
                          <-------------------------------DCN---------------------------->
```

Figure H.9/T.30 – Signals exchange for secure polling mode
Example for a one facsimile page document

NOTE – The call establishment CNG/CED which is depicted in the figure is given for example. The other operating methods defined in 3.1/T.30 may take place as well.

Phases 0, 1, 2, 3 and 4 are the same ones as for the secure facsimile transmission mode.

For phase 00, the sequence contained in the FIF(s) of the DTR is:

Super-tag "E-F"	Length of Supergroup	Tag "FIF of PWD"	Length + Content of "FIF of PWD"	Tag "FIF of PSA"	Length + Content of "FIF of PSA"	Tag "FIF of SEP"	Length + Content of "FIF of SEP"

Tag "FIF of CIG"	Length + Content of "FIF of CIG"	Tag "FIF of DTC"	Length + Content of "FIF of DTC"

Super-tag "Secure transmission mode"	Length of Supergroup	Tag "Unstandardized features"	Length + Content of "Unstandardized features"

H.6.6.2 Turn-around polling

In case of turnaround polling, after DIS received, the sequence of phases (00, 0, 1, 2, 3 and 4) takes place exactly as for simple polling.

```
              document emission =====>                    |
------------------------PPS-EOM----------------------->   | (Note)
<------------------------MCF-----------------------------

                                                            T2 time-out

<-------------------(NSF)-(CSI)-DIS-------------------
--------------------DTR-----(phase 00)---------------->

           the rest is the same as for simple polling
```

NOTE – If the document sent before the turnaround polling is sent with secure facsimile transmission mode, the rules in H.6.3.2/T.30 apply: if phases 4 and 5 are present, the security page is sent or the PPS-EOM appended with octets is sent and the response MCF is appended with octets.

H.6.7 Error-messages

H.6.7.1 Error messages

When an error message is to be indicated, the bit No. 5 of the Reason octet of FNV (bit indicating "Secure Fax Error") must be set to 1.

FNV is defined in 5.3.6.2.12/T.30.

The error reason is contained in the Diagnostic Information Octets of FNV.

The Type octet for error messages is "Secure Fax Error" as defined in 5.3.6.2.12/T.30.

Table H.10/T.30 specifies the octets contained in the Value field of "Secure Fax Error".

Table H.10/T.30 – Error reasons coded in the value field of Secure Fax Error in FNV

Coding of the value octets in FNV	Error reasons
	First octet

`Bit No. 7 6 5 4 3 2 1 0`
`        x x x x x x x 1`
	Registration error for public key

`Bit No. 7 6 5 4 3 2 1 0`
`        x x x x x x 1 x`
	Registration error for encipherment public key

`Bit No. 7 6 5 4 3 2 1 0`
`        x x x x x 1 x x`
	Service not supported

`Bit No. 7 6 5 4 3 2 1 0`
`        x x x x 1 x x x`
	Party not registered

`Bit No. 7 6 5 4 3 2 1 0`
`        x x x 1 x x x x`
	Authentication failure

`Bit No. 7 6 5 4 3 2 1 0`
`        x x 1 x x x x x`
	Receipt not confirmed (Srd non valid)
	The Random number received is rejected by the recipient (e.g. in case of replay detected)

`Bit No. 7 6 5 4 3 2 1 0`
`        x 1 x x x x x x`
	Receipt not confirmed (UTCd non valid)
	The recipient does not accept the UTCd received from the sender (the criteria are implementation matter)

`Bit No. 7 6 5 4 3 2 1 0`
`        1 x x x x x x x`
	Receipt not confirmed (Lm non valid)
	The length indicated by the sender does not correspond to the actual length of the document received

	Second octet

`Bit No. 7 6 5 4 3 2 1 0`
`        x x x x x x x 1`
	Receipt not confirmed (Token 4 or Token 4-enc. non valid)
	The recipient finds the digital signature by the sender not correct

`Bit No. 7 6 5 4 3 2 1 0`
`        x x x x x x 1 x`
	Receipt not valid (Token 5 or Token 5-enc. non valid)

NOTE 1 – Several reasons may be indicated together (several bits set to "1"). NOTE 2 – In next versions of this annex, more additional octets may be defined to code other error reasons. NOTE 3 – For each octet, the least significant bit (right-most bit) is the first one transmitted.	

H.6.7.2 Use of FNV for error indication

Once the FNV indicating the Secure Fax error has been sent, the terminal which has received it "acknowledges" it in sending DCN and disconnects the line.

An example is given below where authentication of the recipient at phase 3 of the secure facsimile transmission fails.

Calling side **Called side**

<------------------DES-----(phase 3)-------------------

authentication failure

---------------------------FNV------------------------->

indication of authentication
failure by FNV

<--------------------------DCN---------------------------

disconnection

(the document is not sent)

4 Section 4

Add a new Annex I to read as follows:

Annex I

Procedure for the Group 3 document facsimile transmission of colour and gray-scale images using T.43

I.1 Introduction

This Annex describes the additions to Recommendation T.30 to enable the transmission of colour and gray-scale images using lossless coding method defined by Recommendation T.43 for Group 3 facsimile mode of operation.

This Recommendation is an optional colour and gray-scale mode which shall only be implemented if the associated base colour and gray-scale mode defined in Annex E/T.4 is also implemented. Implementation of the gray-scale mode of Recommendation T.43 requires implementation of the associated gray-scale mode of Annex E/T.4. Similarly implementation of the colour mode of Recommendation T.43 requires implementation of the associated colour mode of Annex E/T.4.

The objective is to enable the efficient transmission of a wide variety of images, from a simple document such as containing Red or Blue characters to high quality full-colour/gray-scale images over the general switched telephone network and other networks. The images are normally obtained by scanning the original sources with scanners of 200 pels/25.4 mm or higher. The original sources are typically business documents underlined with assorted colour, computer-generated business graph, palettized colour images and high definition continuous-tone colour and gray-scale images.

In this Annex, three types of images are supported. They are one-bit per colour CMY(K)/RGB image, palettized colour image and continuous-tone colour and gray-scale image. One-bit per colour CMY(K)/RGB image is also represented using colour palette table, and is a special case of palettized colour image in which every colour is represented by one bit information of original printable colour. The representation of colour image data is based on Recommendations T.42 and T.43. The basic way is a device-independent colour space representation, the CIELAB space, which enables unambiguous exchange of colour information. The bit-plane decomposition and coding using Recommendation T.82 is also described in Recommendation T.43.

This Annex describes the procedure for negotiation of the capabilities for transmission of colour and gray-scale images. It specifies the definitions and the specifications of new entries to the Facsimile Information field of the DIS/DTC and DCS frames of Recommendation T.30.

Information pertaining to receiver capability, colour mode capability, image amplitude precision in digitization (bits/component), interleave method, custom illumination, and custom gamut are subject to negotiation in the pre-message phase of T.30 protocol.

This Annex does not address the semantics and syntax of the actual encoding of the colour and gray-scale images by lossless coding. Such information is included in Recommendation T.43.

The use of Error Correction Mode (ECM) for error free transmission is mandatory in the procedure described by this Annex. Under the error correction mode of transmission, the encoded image data sequence is embedded in the Facsimile Coded Data (FCD) part of the HDLC (High-level Data Link Control) transmission frames specified by Annex A/T.30.

I.2 Definitions

I.2.1 CIE (L* a* b*) space (CIELAB): A colour space defined by the CIE (Commission internationale de l'éclairage), having approximately equal visually perceptible difference between equally spaced points throughout the space. The three components are L* (in Lightness), a* and b* (both in chrominance).

I.2.2 Joint Bi-level Image experts Group (JBIG), and also shorthand for the encoding method, described in Recommendation T.82, which was defined by this group.

I.3 Normative references

- ITU-T Recommendation T.4 (1996), *Standardization of Group 3 facsimile apparatus for document transmission.*
- ITU-T Recommendation T.82 (1993) | ISO/IEC 11544:1993, *Information Technology – Coded representation of picture and audio information – Progressive Bi-level Image Compression. (Commonly referred to as JBIG standard.)*
- ITU-T Recommendation T.42 (1996), *Continuous-tone colour representation method for facsimile.*
- ITU-T Recommendation T.43 (1997), *Colour and gray-scale image representations using lossless coding scheme for facsimile.*

I.4 Negotiation procedure

The negotiation to transmit and receive encoded colour and gray-scale images by lossless bit-plane coding under the Group 3 facsimile protocol is invoked through the setting of the bits in the DIS/DTC and DCS frames during the pre-message procedure (Phase B) of T.30 protocol.

The above three image types are further divided into 7 coding submode classes as specified in Table G.1/T.4. The relation of 4 coding mode classes and 7 coding submode classes to be supported are shown in Table G.2/T.4.

The relation of 7 coding submode classes and 4 coding mode classes, which are given by the combination of bits X through X + 2, are given in Table I.1/T.30.

In Table I.1/T.30, the capability of lossless gray-scale/colour coding, number of palette indices, and the number of bit precision are explicitly described. Parameters to be negotiated can be found in Table I.2/T.30.

Table I.1/T.30 – The correspondence of coding submode classes and DIS/DTC/DCS bits

Coding submode class		**Colour space**	**Bit 36 T.43 coding**	**Bit 69 Colour mode**	**Bit 71 12-bit mode**	
Image type	**# of bit plane**					
One bit per colour image	(3,4)		1	1	0	(Note)
Palettized colour image	Basic (1-12) x 1 8 bits precision	Lab	1	1	0	
	Extended (1-12) x 1 12 bits precision or (13-16) x 1 8 or 12 bits precision	Lab	1	1	1	
Continuous-tone image	Gray-scale					
	2-8	L	1	0	0	
	9-12	L	1	0	1	
	Colour					
	(2-8) x 3	Lab	1	1	0	
	(9-12) x 3	Lab	1	1	1	
NOTE – This coding submode is a special case of palettized colour submode, in which each bit plane corresponds to CMY(K) or RGB primaries. The number of planes (3 or 4) will be distinguished by G3FAX0 Entry.						

Table I.2/T.30 – Mandatory and optional capabilities

Mandatory	Optional
T.43 gray-scale	T.43 colour
8-bit mode	12-bit mode
Stripe interleave	Plane interleave
CIE standard illuminant D50	Custom illuminant
Default gamut range	Custom gamut range

ITU-T RECOMMENDATIONS SERIES

Series A	Organization of the work of the ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	**Terminals for telematic services**
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communication
Series Z	Programming languages

12812

Printed in Switzerland
Geneva, 1998