UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

T.30

Amendement 1
(07/97)

SÉRIE T: TERMINAUX DES SERVICES TÉLÉMATIQUES

Procédures pour la transmission de documents par télécopie sur le réseau téléphonique général commuté

Amendement 1

Recommandation UIT-T T.30 – Amendement 1

(Antérieurement Recommandation du CCITT)

RECOMMANDATIONS UIT-T DE LA SÉRIE T

TERMINAUX DES SERVICES TÉLÉMATIQUES

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

RECOMMANDATION UIT-T T.30

PROCÉDURES POUR LA TRANSMISSION DE DOCUMENTS PAR TÉLÉCOPIE SUR LE RÉSEAU TÉLÉPHONIQUE GÉNÉRAL COMMUTÉ

AMENDEMENT 1

Résumé

La Recommandation T.30 définit les protocoles applicables aux télécopieurs du Groupe 3.

L'Amendement 1 indique les modifications qu'il est proposé d'apporter au corps du texte de la Recommandation T.30 et les modifications couvrant l'introduction des nouvelles Annexes G, H et I.

Les modifications apportées au corps du texte sont les suivantes: introduction des nouveaux signaux fin de sélection (EOS et PPS-EOS, *end of selection*), champ non valable (FNV, *field not valid*), et sous-adresse d'interrogation (PSA, *polling subaddress*); remplacement du mot de passe (PWD, *password*) à transmettre à l'identification de l'émetteur (SID, *sender ID*), et modification de l'introduction des nouvelles annexes.

L'Annexe G décrit l'utilisation du système de gestion de clés HKM, du système de chiffrement HFX40 et du système de hachage HFX40-I (tous trois décrits dans la Recommandation T.36).

L'Annexe H décrit l'utilisation de l'algorithme RSA.

Les procédures proposées dans les Annexes G et H sont fondées sur celles qui sont définies dans le corps du texte ainsi que dans les Annexes A et C de la Recommandation T.30.

L'Annexe I indique les modifications relatives à la transmission d'images polychromes et monochromes avec utilisation de la méthode de codage sans perte définie dans la Recommandation T.43.

Source

L'Amendement 1 à la Recommandation UIT-T T.30, élaboré par la Commission d'études 8 (1997-2000) de l'UIT-T, a été approuvé le 2 juillet 1997 selon la procédure définie dans la Résolution n° 1 de la CMNT.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

La Conférence mondiale de normalisation des télécommunications (CMNT), qui se réunit tous les quatre ans, détermine les thèmes d'études à traiter par les Commissions d'études de l'UIT-T lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution n° 1 de la CMNT.

Dans certains secteurs de la technologie de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un Membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT avait été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

TABLE DES MATIÈRES

Recommandation T.30

PROCÉDURES POUR LA TRANSMISSION DE DOCUMENTS PAR TÉLÉCOPIE SUR LE RÉSEAU TÉLÉPHONIQUE GÉNÉRAL COMMUTÉ

AMENDEMENT 1

(Genève, 1997)

1 Section 1 Introduction de nouveaux signaux et modification de signaux existants

1.1) Modifier le point 5) du 5.3.6.1.2 comme suit:

5) Interrogation sélective (SEP, *selective polling*) – Ce signal facultatif indique que l'information du FIF qui suit est:

a) une sous-adresse pour l'interrogation; ou

b) un numéro de document spécifique.

(Voir 5.3.6.2.9/T.30, format de codage de la SEP.) L'interrogation SEP n'est envoyée que si le bit 47 du signal DIS est activé.

Format: 1000 0101

NOTE – Lorsque la sous-adresse interrogée PSA et l'interrogation SEP sont utilisées ensemble, l'option b) est appliquée.

1.2) Ajouter au 5.3.6.1.2 le nouveau point 6) suivant:

6) Sous-adresse interrogée (PSA, *polled subaddress*) – Ce signal facultatif indique que l'information du FIF qui suit est une sous-adresse pour l'interrogation [voir 5.3.6.2.13/T.30, format de codage pour le sous-adressage (PSA)]. Le signal PSA n'est envoyé que si le bit 35 du signal DIS est activé.

Format: 1000 0110

1.3) Modifier le point 5) du 5.3.6.1.3 comme suit:

"5) Identification de l'émetteur (SID, *sender identification*) – Ce signal facultatif indique que l'information du FIF qui suit est l'identité de l'émetteur (voir 5.3.6.2.11/T.30, format de codage du SID). L'identification de l'émetteur SID n'est envoyée que si le bit 50 du signal DIS est activé.

Format: X100 0101"

1.4) Au 5.3.6.1.6, ajouter dans un point 7) une nouvelle commande postmessage ainsi libellée:

"Format: X111 1000

7) Fin de sélection (EOS, *end of selection*) – Cette commande facultative de l'émetteur pouvant assurer plusieurs interrogations sélectives (SEP) vers le récepteur correspondant sert à indiquer la fin (dernière page ou dernier bloc) du document faisant l'objet de l'interrogation sélective et la nécessité de revenir à la phase B pour engendrer une nouvelle demande de document avec interrogation sélective. La commande EOS ne peut être transmise que si le bit 34 de la commande DTC du récepteur est activé."

1.5) Renuméroter les points 5.3.6.1.6 7) à 5.3.6.1.6 9) existants respectivement en 5.3.6.1.6 8) à 5.3.6.1.6 10)

1.6) Ajouter au 5.3.6.1.8 le nouveau point 3) suivant:

"3) Champ non valable (FNV, *field not valid*) – Ce signal facultatif indique que le dernier signal PWD, SEP, SUB, SID, TSI, PSA ou de télécopie sécurisée (ou toute combinaison de ces signaux) reçu n'est pas valide ou n'est pas accepté. Le signal FNV n'est envoyé que si le bit 33 des signaux DIS/DTC et DCS est activé.

NOTE – Le signal FNV doit être envoyé à la place du signal CFR/FTT lorsque le signal FIF d'un ou de plusieurs signaux facultatifs associés au signal DCS n'est pas valable ou n'est pas accepté. Le champ FNV doit aussi être envoyé en réponse à la commande DTC lorsqu'un ou plusieurs des signaux facultatifs connexes ne sont pas valables ou ne sont pas acceptés. Le champ FNV peut aussi être envoyé en réponse aux signaux DEC, DES, DTR ou DER (définis dans l'Annexe H/T.30).

Format: X101 0011"

1.7) Ajouter le nouveau sous-paragraphe 5.3.6.2.11 suivant:

"**5.3.6.2.11 Format de codage pour l'identification de l'émetteur (SID)**

Le champ d'information pour télécopie du signal SID sera composé de 20 chiffres codés selon le Tableau 3 à l'exclusion du caractère "+". Le bit de poids le plus faible du chiffre de poids le plus faible sera émis en premier. Les octets inutilisés du champ d'information seront remplis par des caractères "espace" et l'information sera justifiée à droite."

1.8) Ajouter le nouveau sous-paragraphe 5.3.6.2.12 suivant:

"**5.3.6.2.12 Format de codage du champ non valable (FNV)**

La structure du champ FIF pour le signal FNV est la suivante:

octets de motif	octet de numéro de trame	octets d'information de diagnostic

Le champ FIF du signal FNV doit comporter au moins un octet de motif. Les autres octets sont facultatifs, mais un octet de numéro de trame est indispensable en cas de présentation de l'un quelconque des octets d'information de diagnostic facultatifs. L'utilisation des octets facultatifs dépend de l'application. Les terminaux qui implémentent le signal FNV doivent pouvoir recevoir ces octets mais n'ont pas à les traiter ou à y répondre.

Format des octets de motif

Le premier octet, dénommé octet de motif, sert à identifier les cas dans lesquels le contenu du champ d'information pour télécopie (FIF, *facsimile information field*) des signaux spécifiés n'est pas valable. Les valeurs applicables à cet octet sont indiquées dans le tableau ci-dessous. Un bit mis à "0" signifie "OK" et un bit mis à "1" signifie "non valable". Le bit 8 est un bit d'extension, qui doit être mis à "1" en présence d'octets de motif supplémentaires dans le champ FIF. Si le bit d'extension est mis à "0", cela signifie qu'il n'y a pas d'octets de motif supplémentaires.

N° du bit	Signification
1	mot de passe (PWD) incorrect
2	référence d'interrogation sélective (SEP) inconnue
3	sous-adresse (SUB) inconnue
4	identité de l'émetteur (SID) inconnue
5	erreur de télécopie sécurisée
6	identification de l'abonné émetteur (TSI) non acceptée
7	sous-adresse interrogée (PSA) inconnue
8	bit d'extension – valeur par défaut "0"
NOTE – La structure binaire des octets de motif supplémentaires définis doit être compatible avec le premier octet de motif. Les sept premiers bits doivent indiquer les motifs (ou être réservés), le huitième bit étant un bit d'extension pour les octets de motif.	

Format du numéro de trame du champ FNV

Il s'agit d'un numéro binaire à huit bits. Le numéro de trame (de 0 à 255 au maximum) sert à identifier le numéro de séquence d'une trame FNV. La trame 0 est la première trame à transmettre dans une série de trames FNV. Le bit de poids le plus faible est transmis en premier.

Format des octets d'information de diagnostic du champ FNV

La présentation de l'information de diagnostic d'un ou de plusieurs signaux est facultative. L'information de diagnostic pour chaque signal est présentée sous la forme d'une série d'octets avec codage du type, de la longueur et de la valeur. Les octets d'information de diagnostic doivent être transmis de gauche à droite dans l'ordre où ils sont imprimés, le bit de poids le plus faible (le plus à droite) devant être transmis en premier, sauf indication contraire (voir ci-dessous les règles applicables aux octets de valeur).

Le format de l'information de diagnostic pour chaque signal est le suivant:

Type	Longueur	Valeur – Contenu du champ FIF non valable ou autre information de diagnostic (nombre variable d'octets)

Type – Spécifié d'après inversion du champ FCF (champ de commande pour télécopie, *facsimile control field*) du signal ou selon une autre désignation spécifique. On utilise normalement des identificateurs à un octet, mais on peut également utiliser une méthode d'extension. Les types sont définis ci-dessous:

Type	**Description**
1100 0001	mot de passe (PWD) incorrect
1010 0001	référence d'interrogation sélective (SEP) inconnue
1100 001X	sous-adresse (SUB) inconnue
1010 001X	identité de l'émetteur (SID) inconnue
0000 1000	erreur de télécopie sécurisée
0100 001X	identification de l'abonné émetteur (TSI) non acceptée
0110 0001	sous-adresse interrogée inconnue
NOTE – X prend la valeur définie au 5.3.6.1/T.30.	

Longueur – Nombre d'octets de la valeur qui suivra. On utilise normalement un seul octet, mais on peut également utiliser une méthode d'extension.

Valeur – Contient la partie du champ FIF qui n'était pas valable pour le type de signal ou une autre information de diagnostic. Dans les cas où la totalité ou une partie d'un champ FIF non accepté est renvoyée, les données, c'est-à-dire les bits et les octets, doivent être présentées dans l'ordre où elles ont été initialement transmises.

Si on dispose d'informations de diagnostic pour plusieurs signaux, l'octet "type" du deuxième signal suivra immédiatement le dernier octet "valeur" du signal précédent. De façon semblable, toutes les informations de diagnostic de tous les signaux doivent être présentées dans le champ FIF du champ FNV jusqu'à ce qu'elles soient toutes transmises. Dans les cas où la quantité d'informations de diagnostic à transmettre dépasse les limites de capacité d'une trame T.30, les informations de diagnostic restantes doivent être placées dans des trames FNV supplémentaires et le numéro de chaque nouvelle trame sera incrementé d'une unité. Pour ces trames supplémentaires, le contenu des octets de motif sera identique à la première trame FNV et le contenu des octets des informations de diagnostic continuera l'information de la trame précédente.

Syntaxe du champ d'information pour télécopie du champ FNV

La syntaxe détaillée du champ d'information pour télécopie du champ non valide (FIF FNV) est présentée ci-dessous [formalisme de Backus Naur (BNF)]. Les symboles utilisés en BNF sont définis au H.6.1.4.5/T.30.

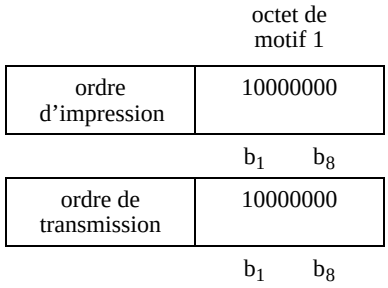
<bit> ::= <0> | <1>
<octet> ::= <bit><bit><bit><bit><bit><bit><bit><bit>
<8_bit_tag> ::= <octet>
<extend_octet> ::= {<1><1><1><1><1><1><1><1>}

<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>]

Exemples de codage des champs d'information pour télécopie du champ FNV

Cas A)

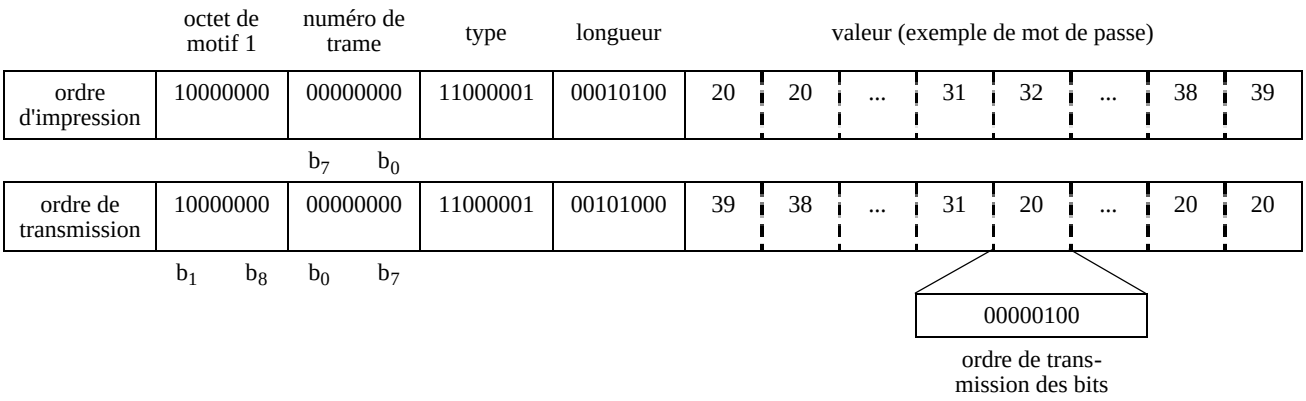
Le mot de passe n'est pas valide et aucune information de diagnostic n'est envoyée.



Cas B)

Le mot de passe n'est pas valide et l'information de diagnostic est envoyée.

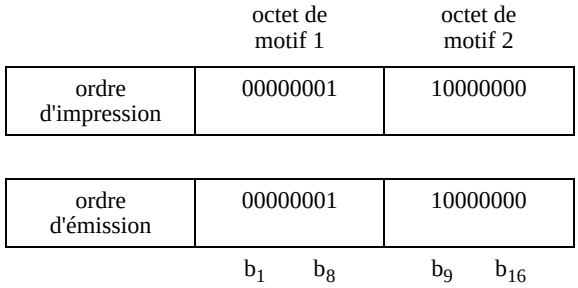
Exemple de mot de passe: "123456789"



Cas C)

De nouveaux bits d'erreur sont définis dans le deuxième octet de motif.

Une erreur se produit dans le bit 1 du deuxième octet de motif et l'information de diagnostic n'est pas envoyée.



Cas D)

Un nouveau bit d'erreur est défini dans le deuxième octet de motif.

Une erreur se produit dans le bit 1 du deuxième octet de motif et l'information de diagnostic est envoyée dans le cas où le champ FIF du signal non valable est renvoyé.

	octet de motif 1	octet de motif 2	numéro de trame		type	longueur	valeur
ordre d'impression	00000001	10000000	00000000		FCF (ordre inverse)	longueur	retour du champ FIF (ordre inverse)
			b_7 b_0				
ordre de transmission	00000001	10000000	00000000		FCF (ordre normal)	longueur	retour du champ FIF (ordre normal)
	b_1 b_8	b_9 b_{16}	b_0 b_7				

Cas E)

De nouveaux bits d'erreur sont définis dans le deuxième octet de motif. Une partie de la sous-adresse n'est pas valide (voir le bit 3) et une erreur est indiquée dans le bit 9 du deuxième octet de motif. L'information de diagnostic est incluse pour les deux erreurs. L'exemple de sous-adresse est "SSSSSSSSSSS1002#2002" et seule l'extension 1002 est rejetée. Une partie de la valeur de l'information de diagnostic pour la deuxième erreur dépassant la limite de la trame, une deuxième trame est transmise avec le reste de la valeur. L'information de diagnostic pour la deuxième erreur n'incluant pas le renvoi d'un champ FIF précédent, l'ordre de transmission des bits suit la règle générale (bit de plus faible poids ou bit de droite transmis en premier).

Première trame

	octet de motif 1	octet de motif 2	numéro de trame	type 1 (SUB)	longueur (4)	valeur (partie renvoyée du champ FIF)			
ordre d'impression	00100001	10000000	00000000	11000011	00000100	31	30	30	32
			b_7 b_0		longueur du premier bloc				
ordre de transmission	00100001	10000000	00000000	11000011	00100000	32	30	30	31
	b_1 b_8	b_9 b_{16}	b_0 b_7						

10001100

ordre de transmission des bits

Première trame (suite)

	type 2	longueur (128)	valeur
ordre d'impression	type	10000000	valeur

ordre de transmission	type (LSB en premier)	00000001	valeur (LSB en premier)

Deuxième trame

	octet de motif 1	octet de motif 2	numéro de trame (2)	valeur (suite)
ordre d'impression	00100001	10000000	00000001	valeur (suite)
			b_7 b_0	
ordre de transmission	00100001	10000000	10000000	valeur (LSB en premier)
	b_1 b_8	b_9 b_{16}	b_0 b_7	

1.9) Ajouter le nouveau sous-paragraphe 5.3.6.2.13 suivant:

"**5.3.6.2.13 Format de codage pour la sous-adresse d'interrogation (PSA)**

Le champ d'information pour télécopie du signal PSA doit être composé de 20 chiffres codés comme indiqué dans le Tableau 3/T.30 à l'exclusion du caractère "+". Le bit de plus faible poids du chiffre de poids le plus faible sera émis en premier. Les octets inutilisés du champ d'information seront remplis par des caractères "espace" et l'information sera justifiée à droite."

1.10) Remplacer le Tableau 2/T.30 existant par le suivant:

Tableau 2/T.30

N° de bit	Signal DIS/DTC	Note	Signal DCS	Note
1	réservé	1	réservé	1
2	réservé	1	réservé	1
3	réservé	1	réservé	1
4	réservé	1	réservé	1
5	réservé	1	réservé	1
6	capacités V.8	23	non valide	24
7	valeurs préférées: 0 = 256 octets 1 = 64 octets	23, 42	non valide	24
8	réservé	1	réservé	1
9	prêt à émettre une télécopie (relève)	18	mis à "0"	
10	fonctionnement du récepteur en mode télécopie	19	fonctionnement du récepteur en mode télécopie	20
11, 12, 13, 14	débit	3	débit	33
0, 0, 0, 0	mode repli V.27 *ter*		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	Rec. V.27 *ter* et V.29		7200 bit/s, Rec. V.29	
0, 0, 1, 0	non utilisé		non valide	31
0, 1, 1, 0	réservé		non valide	31
1, 0, 1, 0	non utilisé		réservé	
1, 1, 1, 0	non valide	32	réservé	
0, 0, 0, 1	non utilisé		14 400 bit/s, Rec. V.17	
0, 1, 0, 1	réservé		12 000 bit/s, Rec. V.17	
1, 0, 0, 1	non utilisé		9600 bit/s, Rec. V.17	
1, 1, 0, 1	Rec. V.27 *ter*, V.29 et V.17		7200 bit/s, Rec. V.17	
0, 0, 1, 1	non utilisé		réservé	
0, 1, 1, 1	réservé		réservé	
1, 0, 1, 1	non utilisé		réservé	
1, 1, 1, 1	réservé		réservé	

Tableau 2/T.30 *(suite)*

N° de bit	Signal DIS/DTC	Note	Signal DCS	Note
15	R8 × 7,7 lignes/mm et/ou 200 × 200 pixels/25,4 mm	10, 11, 13, 25	R8 × 7,7 lignes/mm ou 200 × 200 pixels/25,4 mm	10, 11, 13
16	possibilité de codage bidimensionnel		codage bidimensionnel	
17, 18 (0,0) (0,1) (1,0) (1,1)	capacité de largeur d'enregistrement longueur de ligne de balayage de 215 mm ± 1% longueur de ligne de balayage de 215 mm ± 1%, de 255 mm ± 1% et de 303 mm ± 1% longueur de ligne de balayage de 215 mm ± 1% et de 255 mm ± 1% non valide	27 6	largeur d'enregistrement longueur de ligne de balayage de 215 mm ± 1% longueur de ligne de balayage de 303 mm ± 1% longueur de ligne de balayage de 255 mm ± 1% non valide	27
19, 20 (0,0) (0,1) (1,0) (1,1)	capacité maximale de longueur d'enregistrement A4 (297 mm) illimitée A4 (297 mm) et B4 (364 mm) non valide	2	capacité maximale d'enregistrement A4 (297 mm) illimitée B4 (364 mm) non valide	2
21, 22, 23 (0,0,0) (0,0,1) (0,1,0) (1,0,0) (0,1,1) (1,1,0) (1,0,1) (1,1,1)	temps minimal par ligne d'exploration accepté par le récepteur 20 ms à 3,85 l/mm: $T_{7,7} = T_{3,85}$ 40 ms à 3,85 l/mm: $T_{7,7} = T_{3,85}$ 10 ms à 3,85 l/mm: $T_{7,7} = T_{3,85}$ 5 ms à 3,85 l/mm: $T_{7,7} = T_{3,85}$ 10 ms à 3,85 l/mm: $T_{7,7} = 1/2\ T_{3,85}$ 20 ms à 3,85 l/mm: $T_{7,7} = 1/2\ T_{3,85}$ 40 ms à 3,85 l/mm: $T_{7,7} = 1/2\ T_{3,85}$ 0 ms à 3,85 l/mm: $T_{7,7} = T_{3,85}$	4, 8, 23	temps minimal par ligne d'exploration 20 ms 40 ms 10 ms 5 ms 0 ms	8, 24
24	extension de champ	5	extension de champ	5
25	réservé	1, 41	réservé	1, 41
26	mode sans compression		mode sans compression	
27	mode de correction d'erreurs	9, 17, 23, 25	mode de correction d'erreurs	9, 17, 24, 34
28	mis à "0"		longueur de la trame 0 = 256 octets longueur de la trame 1 = 64 octets	7, 24
29	réservé	1	réservé	1
30	réservé	1	réservé	1
31	possibilité de codage T.6	9, 17	activation du codage T.6	9, 17
32	extension de champ	5	extension de champ	5
33	option champ non valable		option champ non valable	
34	option d'interrogations sélectives multiples		mis à "0"	
35	option PSA	26, 44, 45	mis à "0"	
36	codage T.43	17, 25, 34, 35, 37, 39, 40	codage T.43	17, 25, 34, 35, 37, 39, 40
37	entrelacement des plans	25, 46	entrelacement des plans	25, 46
38	réservé	1	réservé	1
39	réservé	1	réservé	1
40	extension de champ	5	extension de champ	5

Tableau 2/T.30 *(suite)*

N° de bit	Signal DIS/DTC	Note	Signal DCS	Note
41	R8 × 15,4 lignes/mm	10	R8 × 15,4 lignes/mm	10, 34
42	300 × 300 pixels/25,4 mm	34	300 × 300 pixels/25,4 mm	34
43	R16 × 15,4 lignes/mm et/ou 400 × 400 pixels/25,4 mm	10, 12, 13	R16 × 15,4 lignes/mm et/ou 400 × 400 pixels/25,4 mm	10, 12, 13, 34
44	définition préférée en pouce	13, 14	sélection du type de définition "0": définition métrique "1": définition en pouce	13, 14
45	définition métrique préférée	13, 14	sans importance	
46	temps minimal d'exploration de ligne pour les définitions supérieures "0": $T_{15,4} = T_{7,7}$ "1": $T_{15,4} = 1/2\ T_{7,7}$	15	sans importance	
47	interrogation sélective	26, 44	mis à "0"	
48	extension de champ	5	extension de champ	5
49	sous-adressage		transmission du sous-adressage	26
50	mot de passe	26	transmission de l'identification de l'émetteur	26
51	prêt à émettre un fichier de données	17, 21	mis à "0"	
52	réservé	1	réservé	1
53	transfert de fichier binaire (BFT, *binary file transfer*)	16, 17, 21	transfert de fichier binaire (BFT)	16, 17
54	mode de transfert de documents (DTM, *document transfer mode*)	17, 21	mode de transfert de documents (DTM)	17
55	échange de documents informatisés (EDI, *electronic data interchange*)	17	échange de documents informatisés (EDI)	17
56	extension de champ	5	extension de champ	5
57	mode de transfert de base (BTM, *basic transfer mode*)	17, 21	mode de transfert de base (BTM)	17
58	réservé	1	réservé	1
59	prêt à émettre un caractère ou un document en mode mixte (relève)	17, 22	mis à "0"	
60	mode caractère	17, 22	mode caractère	17, 22
61	réservé	1	réservé	1
62	mode mixte (Annexe D/T.4)	17, 22	mode mixte (Annexe D/T.4)	17, 22
63	réservé	1	réservé	1
64	extension de champ	5	extension de champ	5
65	mode retraitable 26 (Rec. T.505)	17, 22	mode retraitable 26 (Rec. T.505)	17, 22
66	capacité du réseau numérique	43	capacité du réseau numérique	43
67 (0) (1)	capacités de fonctionnement en modes duplex et semi-duplex fonctionnement en mode semi-duplex seulement fonctionnement en modes duplex et semi-duplex		capacités de fonctionnement en modes duplex et semi-duplex fonctionnement en mode semi-duplex fonctionnement en mode duplex	
68	codage JPEG	25, 34, 35, 39, 40	codage JPEG	25, 34, 35, 39, 40
69	mode couleur	25, 35	mode couleur	25, 35
70	mis à "0"	36	tables de Huffman préférées	25, 36

Tableau 2/T.30 *(suite)*

N° de bit	Signal DIS/DTC	Note	Signal DCS	Note
71	12 bits/pixel/composante	25, 37	12 bits/pixel/composante	25, 37
72	extension de champ	5	extension de champ	5
73	pas de sous-échantillonnage (1:1:1)	25, 38	pas de sous-échantillonnage (1:1:1)	25, 38
74	illuminant propre à l'utilisateur	25, 39	illuminant propre à l'utilisateur	25, 39
75	gamme de couleurs propre à l'utilisateur	25, 40	gamme de couleurs propre à l'utilisateur	25, 40
76	capacité lettre nord-américain format (215,9 × 279,4 mm)	28	lettre nord-américain (215,9 × 279,4 mm)	
77	capacité légal nord-américain format (215,9 × 355,6 mm)	28	légal nord-américain format (215,9 × 355,6 mm)	
78	capacité de base du codage séquentiel simple (Rec. T.85)	17, 29, 30	codage séquentiel simple (Rec. T.85) de base	17, 29
79	capacité L0 optionnelle du codage séquentiel simple (Rec. T.85)	17, 29, 30	codage séquentiel simple (Rec. T.85) optionnel L0	17, 29
80	extension de champ	5	extension de champ	5
81	fonction de gestion de clés HKM		sélection de la fonction de gestion de clés HKM	
82	fonction de gestion de clés RSA		sélection de la fonction de gestion de clés RSA	47
83	option mode outrepassement		sélection du mode outrepassement	
84	fonction de chiffrement HFX40		sélection de la fonction de chiffrement HFX40	
85	option de chiffrement numéro 2		sélection de l'option de chiffrement numéro 2	
86	option de chiffrement numéro 3		sélection de l'option de chiffrement numéro 3	
87	fonction de hachage HFX40-I		sélection de la fonction de hachage HFX40-I	
88	champ d'extension	5	champ d'extension	5
89	option numéro 2 de système de hachage		sélection de l'option numéro 2 de système de hachage	
90	option numéro 3 de système de hachage		sélection de l'option numéro 3 de système de hachage	
91	réservé pour les futurs éléments de sécurité	1	réservé pour les futurs éléments de sécurité	1
92	réservé	1	réservé	1
93	réservé	1	réservé	1
94	réservé	1	réservé	1
95	réservé	1	réservé	1
96	champ d'extension	5	champ d'extension	5

NOTE 1 – Les bits pour lesquels il est indiqué "réservé" seront mis à "0".

NOTE 2 – Les télécopieurs normalisés conformes à la Recommandation T.4 doivent présenter la capacité suivante: longueur du papier = 297 mm.

NOTE 3 – Lorsque la trame DIS ou DTC définit les capacités de la Recommandation V.27 *ter*, on peut considérer que le télécopieur peut fonctionner à 4800 ou 2400 bit/s.

Lorsque la trame DIS ou DTC définit les capacités V.29, le télécopieur peut fonctionner à 9600 ou à 7200 bit/s conformément à la Recommandation V.29; lorsque la trame en question définit les capacités V.17, le télécopieur peut fonctionner à 14 400 bit/s, 12 000 bit/s, 9600 bit/s ou 7200 bit/s conformément à la Recommandation V.17.

Tableau 2/T.30 *(suite)*

NOTE 4 – Les indications $T_{7,7}$ et $T_{3,85}$ concernent les temps par ligne d'exploration à utiliser quand la définition verticale est de 7,7 lignes/mm (ou 200 lignes/25,4 mm ou 300 lignes/25,4 mm) ou 3,85 lignes/mm respectivement (voir le bit 15 ci-dessus). L'expression $T_{7,7}$ = 1/2 $T_{3,85}$ indique que, lorsque la définition verticale est 7,7 lignes/mm ou 200 lignes/25,4 mm ou 300 lignes/25,4 mm, le temps de la ligne d'exploration peut être divisé par deux.

NOTE 5 – Le champ FIF normal pour les signaux DIS, DTC et DCS a une longueur de 24 bits. Si le(s) bit(s) "extension du champ" correspond(ent) à "1", le champ FIF sera étendu en ajoutant 8 bits supplémentaires.

NOTE 6 – Les télécopieurs existants peuvent émettre la condition non valide (1,1) pour les bits 17 et 18 de leur signal DIS. Si un tel signal est reçu, il doit être interprété comme (0,1).

NOTE 7 – La valeur du bit 28 de la commande DCS n'est valide que lorsque l'indication du mode de correction d'erreurs de la Recommandation T.4 est demandée par le bit 27.

NOTE 8 – Le mode facultatif de correction d'erreurs prévu dans la Recommandation T.4 nécessite 0 ms de la capacité de temps minimal par ligne d'exploration. Les bits 21 à 23 dans les signaux DIS/DTC indiquent le temps minimal par ligne d'exploration d'un récepteur sans tenir compte de la présence du mode de correction des erreurs.

En présence du mode de correction d'erreurs, l'émetteur envoie un signal DCS avec les bits 21 à 23 mis à 1, 1, 1 indiquant une capacité de 0 ms.

En cas de transmission normale, l'émetteur envoie un signal DCS avec les bits 21 à 23 mis aux valeurs appropriées selon les caractéristiques des deux télécopieurs.

NOTE 9 – Le schéma de codage conforme à la Recommandation T.6 tel qu'il est spécifié par le bit 31 est valable uniquement lorsque le bit 27 (mode de correction d'erreurs) est fixé à "1".

NOTE 10 – Les définitions R8 et R16 sont définies de la manière suivante:

R8 = 1728 pixels/(215 mm ± 1%) pour les formats ISO A4, légal et lettre nord-américain.

R8 = 2048 pixels/(255 mm ± 1%) pour le format ISO B4.

R8 = 2432 pixels/(303 mm ± 1%) pour le format ISO A3.

R16 = 3456 pixels/(215 mm ± 1%) pour les formats ISO A4, légal et lettre nord-américain.

R16 = 4096 pixels/(255 mm ± 1%) pour le format ISO B4.

R16 = 4864 pixels/(303 mm ± 1%) pour le format ISO A3.

NOTE 11 – L'interprétation du bit 15 lorsqu'il est mis à "1" dépend des valeurs des bits 44 et 45 de la manière suivante:

bit 44	bit 45	interprétation
0	0	(non valide)
1	0	200 × 200 pixels/25,4 mm
0	1	R8 × 7,7 lignes/mm
1	1	R8 × 7,7 lignes/mm et 200 × 200 pixels/25,4 mm

La valeur "1" du bit 15 sans les bits 41, 42, 43, 44, 45 et 46, indique la définition R8 × 7,7 lignes/mm.

NOTE 12 – L'interprétation du bit 43 lorsqu'il est mis à "1" dépend des valeurs des bits 44 et 45 de la manière suivante:

bit 44	bit 45	interprétation
0	0	(non valide)
1	0	400 × 400 pixels/25,4 mm
0	1	R16 × 15,4 lignes/mm
1	1	R16 × 15,4 lignes/mm et 400 × 400 pixels/25,4 mm

NOTE 13 – Les bits 44 et 45 ne sont utilisés que conjointement aux bits 15 et 43. Le bit 44 du signal DCS, lorsqu'il est utilisé, doit indiquer correctement la définition du document transmis, ce qui signifie que le bit 44 du signal DCS peut ne pas toujours correspondre à la capacité indiquée par les bits 44 et 45 du signal DIS/DTC. Une sélection croisée entraînera la distorsion et la réduction de la zone reproductible.

Si un récepteur indique dans le signal DIS qu'il préfère recevoir des informations basées sur des mesures métriques, tandis que l'émetteur n'a que les informations équivalentes basées sur des mesures en pouce (ou vice versa), la communication se poursuivra.

NOTE 14 – L'utilisation des bits 44 et 45 ne nécessite aucune fonction supplémentaire du télécopieur visant à indiquer à l'usager émetteur ou récepteur si les informations ont été émises ou reçues sur la base de mesures exprimées en mètre-mètre, pouce-pouce, mètre-pouce ou pouce-mètre.

NOTE 15 – $T_{15,4}$ désigne la durée d'une ligne d'exploration à utiliser lorsque la définition verticale est de 15,4 lignes/mm ou 400 lignes/mm.

La relation $T_{15,4}$ = 1/2 $T_{7,7}$ indique que lorsque $T_{7,7}$ est de 10, 20 ou 40 ms, la durée d'une ligne d'exploration peut être réduite de moitié dans un mode de définition supérieure.

Tableau 2/T.30 *(suite)*

Lorsque $T_{7,7}$ est de 5 ms [(bit 21, bit 22, bit 23) = (1, 0, 0), (0, 1, 1)] ou de 0 ms [(1, 1, 1)], le bit 46 du signal DIS/DTC doit être mis à "0" ($T_{15,4} = T_{7,7}$).

NOTE 16 – Le protocole de transfert de fichiers binaires est décrit dans la Recommandation T.434.

NOTE 17 – Lorsque les bits 31, 36, 51, 53, 54, 55, 57, 59, 60, 62, 78 et 79 sont mis à "1", le bit 27 doit être également mis à "1".

NOTE 18 – Le bit 9 indique qu'une télécopie est prête à être émise par le télécopieur qui répond. Il n'indique pas une capacité.

NOTE 19 – Le bit 10 indique que le télécopieur répondeur possède des capacités en réception.

NOTE 20 – Le bit 10 commande au télécopieur récepteur de se mettre en mode réception.

NOTE 21 – Le bit 51 indique qu'un fichier de données est prêt à être émis par le télécopieur qui répond. Il n'indique pas une capacité. Ce bit est utilisé conjointement avec les bits 53, 54 et 57.

NOTE 22 – Le bit 59 indique qu'un document en mode caractères ou en mode mixte est prêt à être relevé par le télécopieur qui répond. Il n'indique pas une capacité. Ce bit est utilisé conjointement avec les bits 60, 62 et 65.

NOTE 23 – Lorsqu'on utilise la procédure facultative définie dans l'Annexe C/T.30, les bits 6 et 7 doivent être mis à "0" et les bits 21 à 23 et 27 doivent être mis à "1" dans les signaux DIS/DTC.

NOTE 24 – Lorsqu'on utilise la procédure facultative définie dans l'Annexe C/T.30, les bits 6, 7 et 28 doivent être mis à "0" et les bits 21 à 23 et 27 doivent être mis à "1" dans le signal DCS.

NOTE 25 – Les protocoles facultatifs pour le mode polychrome et monochrome à modelé continu (mode JPEG) et le mode polychrome et monochrome facultatif à codage sans perte (Recommandation T.43) sont décrits respectivement dans les Annexes E/T.30 et I/T.30. Si le bit 68 de la trame DIS/DTC est mis à "1", cela indique l'option mode JPEG. Si les bits 36 et 68 sont mis à "1", cela indique que le mode T.43 est également disponible. Le bit 36 de la trame DIS/DTC ne doit être mis à "1" que lorsque le bit 68 est lui aussi mis à "1". En outre, les bits 15 et 27 de cette même trame doivent également être mis à "1", si le bit 68 ou les bits 36 et 68 sont mis à "1". Le bit 15 indique l'option de résolution 200 × 200 pixels/25,4 mm, qui est la résolution de base pour la télécopie couleur. Le bit 27 indique l'option mode correction d'erreur, qui est obligatoire pour la télécopie couleur. Les bits 69 à 71 et 73 à 75 ne sont applicables que si le bit 68 est mis à "1". Le bit 73 n'est applicable qu'au mode JPEG. Les bits 69, 71, 74 et 75 sont applicables au mode JPEG et/ou au mode T.43. Le bit 37 n'est applicable que lorsque le bit 36 est mis à "1" – voir aussi les Notes 39 et 40.

NOTE 26 – Pour prévoir un mécanisme de reprise sur erreur, lorsque les trames PWD/SEP/SUB/SID/PSA sont envoyées avec le signal DCS ou la commande DTC, les bits 49 et 50 du signal DCS ou les bits 47, 50 et 35 de la commande DTC doivent être mis à "1". La mise à "1" du bit 47 correspond à l'option d'interrogation sélective pour le signal DIS. La mise à "1" du bit 50 correspond à l'interrogation en vue de l'obtention de la sous-adresse pour la commande DTC et à l'option de sous-adressage pour le signal DIS. La mise à "1" du bit 50 correspond à la transmission du mot de passe pour la commande DTC et au mot de passe ou à l'option d'identification de l'émetteur (Sender ID) pour le signal DIS. La mise à "1" du bit 35 correspond à la transmission de la sous-adresse interrogée pour la commande DTC et à l'option de sous-adresse interrogée pour le signal DIS. Les terminaux conformes aux versions de 1993 de la présente Recommandation peuvent mettre les bits ci-dessus à "0" même si les trames PWD/SEP/SUB sont transmises.

NOTE 27 – Les longueurs des lignes de balayage correspondantes pour les définitions en pouce figurent au 2.2/T.4.

NOTE 28 – Quand il utilise les bits 76 et 77 dans les signaux DIS/DTC, le télécopieur doit avoir la capacité de recevoir les documents ISO A4 dans toute combinaison de bits 76 et 77. Les émetteurs A4, B4 et A3 peuvent ignorer les valeurs attribuées aux bits 76 et 77.

NOTE 29 – La méthode de codage indiquée par les bits 78 et 79 est définie dans la Recommandation T.85.

NOTE 30 – Quand le bit 79 dans la trame DIS est mis à "1", le bit 78 sera également mis à "1".

NOTE 31 – Certains télécopieurs conformes à la version de 1994 ou aux versions antérieures de la présente Recommandation pourraient utiliser cette séquence pour signaler le système de modulation V.33.

NOTE 32 – Certains télécopieurs conformes à la version de 1994 ou aux versions antérieures de la présente Recommandation pourraient utiliser cette séquence pour signaler les capacités V.27 *ter*, V.29 et V.33. Afin de préserver la compatibilité avec de tels dispositifs, un télécopieur qui a la capacité de recevoir en mode V.17 doit aussi être capable de recevoir en mode V.33, et un télécopieur qui a la capacité de recevoir en mode V.33 doit aussi être capable de recevoir en mode V.29.

NOTE 33 – En mode V.34, les bits 11 à 14 de la trame DCS ne sont pas valides et seront mis à "0".

NOTE 34 – La mise à "0" du bit 68 indique que le mode JPEG du terminal appelé et le mode T.43 ne sont pas disponibles et qu'il est impossible de décoder les données codées en mode JPEG ou T.43. Dans une trame DCS, la mise à "1" du bit 68 indique que le mode JPEG du terminal appelant est utilisé et que des données d'image codées en mode JPEG sont envoyées. La mise à "0" du bit 68 et la mise à "1" du bit 36 indiquent que le mode T.43 du terminal appelant est utilisé et que des données d'image codées en mode T.43 sont envoyées. Si le bit 68 ou 36 de la trame DCS est mis à "1", les bits 41 ou 42 ou 43, et le bit 27 de cette même trame doivent aussi être mis à "1". Les bits 42 et 43 indiquent respectivement des résolutions de 300 × 300 et 400 × 400 pixels/25,4 mm. La mise à "0" des bits 68 et 36 indique que ni le mode JPEG ni le mode T.43 ne sont utilisés et que l'image n'est codée ni en mode JPEG ni en mode T.43.

Tableau 2/T.30 *(suite)*

NOTE 35 – Dans la trame DIS/DTC, la mise à "1" du bit 69 indique que le terminal appelé utilise l'option toutes couleurs lui permettant d'accepter des données d'image de toutes les couleurs dans l'espace CIELAB. Si le bit 36 est également mis à "1", le terminal peut aussi accepter les données d'image couleur définies dans la Recommandation T.43. La mise à "0" du bit 69 et la mise à "1" du bit 68 ou des bits 68 et 36 indiquent que le terminal appelé ne fonctionne qu'en mode monochrome, n'acceptant que la composante de brillance (composante L*) dans la représentation CIELAB pour les modes JPEG et T.43 respectivement. Dans une trame DCS, la mise à "1" des bits 68 et 69 indique que le terminal appelant envoie l'image dans la représentation toutes couleurs dans l'espace CIELAB en mode JPEG. Dans une trame DCS, la mise à "1" des bits 36 et 69 indique que le terminal appelant envoie l'image couleur en mode T.43. La mise à "1" du bit 68 ou 36 et la mise à "0" du bit 69 indiquent que le terminal appelant envoie uniquement la composante de brillance (composante L*) dans la représentation CIELAB pour le mode JPEG ou le mode T.43 respectivement. A noter que l'image couleur ne sera transmise que lorsque les bits 68 et 69 ou 36 et 69 seront tous deux mis à "1".

NOTE 36 – Le bit 70 est appelé "Indication des tables de Huffman par défaut". La transmission des tables de Huffman est obligatoire. Il est possible d'indiquer au télécopieur appelé que les tables de Huffman sont les tables par défaut. Celles-ci ne sont spécifiées que pour la définition de saturation d'image par défaut (8 bits/pixel/composante). Les tables de Huffman par défaut doivent être déterminées (par exemple les Tableaux K.3/T.81 à K.6/T.81). Dans une trame DIS/DTC, le bit 70 n'est pas utilisé et est mis à zéro. Dans une trame DCS, le réglage du bit 70 à 0 indique que le télécopieur appelant n'identifie pas comme tables par défaut les tables de Huffman qu'il utilise pour coder les données d'image. Le réglage du bit 70 à 1 indique que le télécopieur appelant identifie comme tables par défaut les tables de Huffman qu'il utilise pour coder les données d'image.

NOTE 37 – Dans la trame DIS/DTC, la mise à "0" du bit 71 indique que le terminal appelé ne peut accepter que des données d'images numérisées à 8 bits/pixel/composante pour le mode JPEG. Cela vaut également pour le mode T.43 si le bit 36 est également mis à "1". La mise à "1" du bit 71 indique que le terminal appelé peut aussi accepter des données d'images numérisées à 12 bits/pixel/composante pour le mode JPEG. Cela vaut également pour le mode T.43 si le bit 36 est lui aussi mis à "1". Dans une trame DCS, la mise à "0" du bit 71 indique que le terminal appelant transmet des données d'images numérisées à 8 bits/pixel/composante pour le mode JPEG. Cela vaut également pour le mode T.43 si le bit 36 est lui aussi mis à "1". La mise à "1" du bit 71 indique que le terminal appelant transmet des données d'images numérisées à 12 bits/pixel/composante pour le mode JPEG. Cela vaut également pour le mode T.43 si le bit 36 est lui aussi mis à "1".

NOTE 38 – Dans une trame DIS/DTC, le réglage du bit 73 à 0 indique que le télécopieur appelé s'attend à des données d'image dont les composantes de chrominance ont été sous-échantillonnées au taux de 4:1:1; ces composantes (a* et b* dans l'espace chromatique CIELAB) sont sous-échantillonnées quatre fois pour chaque échantillonnage de la composante L* (clarté). Les détails sont décrits dans l'Annexe E/T.4. Le réglage du bit 73 à 1 indique que le télécopieur appelé peut accepter, sur option, l'absence de sous-échantillonnage des composantes de chrominance contenues dans les données d'image. Dans une trame DCS, le réglage du bit 73 à 0 indique que le télécopieur appelé utilise un taux de sous-échantillonnage de 4:1:1 pour les composantes a* et b* des données d'image. Le réglage du bit 73 à 1 indique que le télécopieur appelé n'effectue pas de sous-échantillonnage.

NOTE 39 – Dans une trame DIS/DTC, la mise à 0 du bit 74 indique que le terminal appelé s'attend à ce que l'illuminant D50 normalisé par la CIE soit utilisé dans les données d'images couleur, comme indiqué dans la Recommandation T.42. La mise à 1 du bit 74 indique que le terminal appelé peut aussi accepter d'autres types d'illuminants que l'illuminant D50. La mise à 1 du bit 68 indique que le terminal utilise l'option de codage JPEG comme indiqué dans l'Annexe E/T.4. La mise à 1 du bit 36 indique que le terminal utilise l'option de codage couleur, décrite dans la Recommandation T.43. Dans une trame DCS, la mise à 0 du bit 74 et la mise à "1" du bit 68 ou du bit 36, indiquent que le terminal appelant utilise l'illuminant D50 pour la représentation des données d'images couleur, comme indiqué dans la Recommandation T.42. La mise à 1 du bit 74 indique qu'un autre type d'illuminant est utilisé. Lorsque les bits 68 et 74 sont mis à "1", la spécification est intégrée dans la syntaxe JPEG décrite dans l'Annexe E/T.4. Lorsque les bits 36 et 74 sont mis à "1", la spécification est intégrée dans la syntaxe T.43 décrite dans la Recommandation T.43.

NOTE 40 – Dans une trame DIS/DTC, la mise à 0 du bit 75 indique que le terminal appelé s'attend à ce que les données d'images couleur soient représentées à l'aide de la gamme de valeurs par défaut spécifiée dans la Recommandation T.42. La mise à 1 du bit 75 indique que le terminal appelé peut aussi accepter d'autres gammes de valeurs. La mise à 1 du bit 68 indique que le terminal utilise l'option de codage JPEG décrite dans l'Annexe E/T.4. La mise à 1 du bit 36 indique que le terminal utilise l'option de codage couleur décrite dans la Recommandation T.43. Dans une trame DCS, la mise à 0 du bit 75 et la mise à "1" du bit 68 ou du bit 36 indiquent que le terminal appelant utilise la gamme de valeurs par défaut spécifiée dans la Recommandation T.42. La mise à "1" du bit 75 indique que le terminal appelant utilise une gamme de valeurs différente. Lorsque les bits 68 et 75 sont mis à "1", la spécification est intégrée dans la syntaxe JPEG décrite dans l'Annexe E/T.4. Lorsque les bits 36 et 75 sont mis à "1", la spécification est intégrée dans la syntaxe T.43 décrite dans la Recommandation T.43.

NOTE 41 – Certains télécopieurs qui sont conformes aux versions de la présente Recommandation datant d'avant 1996 peuvent mettre ce bit à "1". Ils donneront une séquence de réponse conforme aux indications figurant dans la Figure III.2/T.30.

NOTE 42 – Il est entendu que, pour assurer la rétrocompatibilité, un télécopieur émetteur peut ignorer la demande visant la trame de 64 octets; le télécopieur récepteur doit donc être prêt à prendre en charge, d'une façon ou d'une autre, des trames de 256 octets.

NOTE 43 – Voir C.7.2/T.30.

NOTE 44 – Des précisions sur l'utilisation de l'interrogation sélective pour les valeurs d'activation du bit 47 et du bit 35 sont données à l'alinéa 5) du 5.3.6.1.2/T.30.

NOTE 45 – Des précisions sur l'utilisation d'une sous-adresse d'interrogation pour les valeurs d'activation du bit 35 sont données à l'alinéa 6) du 5.3.6.1.2/T.30.

Tableau 2/T.30 *(fin)*

NOTE 46 – Dans une trame DIS/DTC, la mise à "0" du bit 37 indique que le terminal appelé ne peut accepter que les données d'images utilisant l'entrelacement des bandes (128 lignes/bande ou moins). La mise à "1" du bit 37 indique que le terminal appelé peut aussi accepter des données d'images avec entrelacement des plans. Dans une trame DCS, la mise à "0" du bit 37 indique que les données d'images du terminal appelant utilisent l'entrelacement des bandes. La mise à "1" du bit 37 indique que les données d'images du terminal appelant utilisent l'entrelacement des plans. Ces deux méthodes d'entrelacement sont décrites en détail dans la Recommandation T.43.

NOTE 47 – Le signal DCS n'est pas émis dans le contexte de l'Annexe H/T.30, le champ FIF du signal DCS est incorporé dans le nouveau signal "DEC" (commande numérique enrichie, *digital extended command*) (voir H.6.1/T.30) dont le bit correspondant 82 doit être mis à "1".

1.11) Dans la Figure A.1/T.30, modifier la description de FCF2 comme suit:

FCF2 Champ de commande pour télécopie 2: commande après transmission du message (NULL, MPS, EOM, EOP, EOS et PRI-Q)

1.12) Définition du signal PPS-EOS

Réviser la Note 1 du A.4.3, Figure A.1/T.30, comme suit:

FCF2	Signification
0000 0000	Code NULL qui indique la limite de la page partielle
1111 0000	EOM dans le mode facultatif de correction d'erreurs de la Recommandation T.4
1111 0010	MPS dans le mode facultatif de correction d'erreurs de la Recommandation T.4
1111 0100	EOP dans le mode facultatif de correction d'erreurs de la Recommandation T.4
1111 1000	EOS dans le mode facultatif de correction d'erreurs de la Recommandation T.4
1111 1001	PRI-EOM dans le mode facultatif de correction d'erreurs de la Recommandation T.4
1111 1010	PRI-MPS dans le mode facultatif de correction d'erreurs de la Recommandation T.4
1111 1100	PRI-EOP dans le mode facultatif de correction d'erreurs de la Recommandation T.4

2 Section 2

Ajouter une nouvelle Annexe G comme suit:

Annexe G

Procédures pour la transmission sécurisée de documents de télécopie du Groupe 3 utilisant les systèmes HKM et HFX

G.1 Introduction

G.1.1 La présente annexe décrit le protocole utilisé pour les terminaux de télécopie du Groupe 3 afin de sécuriser les communications en utilisant les systèmes HKM et HFX. Les procédures utilisées se réfèrent à celles définies dans les Annexes A/T.30 et C/T.30 ainsi que dans le corps de la présente Recommandation.

G.1.2 L'utilisation de la présente annexe est facultative.

G.1.3 La correction d'erreurs définie dans les Annexes A/T.30 ou C/T.30 (selon le cas) est obligatoire.

G.2 Caractéristiques de la procédure de transmission sécurisée de documents de télécopie

G.2.1 Les systèmes HKM et HFX donnent les possibilités suivantes pour les transmissions sécurisées de documents entre des entités (terminaux ou opérateurs de terminaux):

- authentification mutuelle d'entités;
- élaboration d'une clé secrète de session;
- confidentialité des documents;
- confirmation de réception;
- confirmation ou réfutation de l'intégrité du document.

G.2.2 Fonctions

Le système HKM défini dans l'Annexe B/T.36 permet la gestion de clé. Deux procédures sont définies, la première étant l'enregistrement et la seconde la transmission sécurisée d'une clé secrète. L'enregistrement élabore des secrets mutuels et permet d'effectuer en toute sécurité l'ensemble des transmissions ultérieures. Dans les transmissions ultérieures, le système HKM permet l'authentification mutuelle, l'utilisation d'une clé de session secrète pour la confidentialité et la sécurité des documents, de même que la confirmation de réception, la confirmation ou la réfutation de l'intégrité du document.

Le système de chiffrement défini dans l'Annexe D/T.36 permet de garantir la confidentialité des documents. Le système de chiffrement utilise une clé à 12 chiffres décimaux qui équivaut à peu près à 40 bits.

Le système défini dans l'Annexe E/T.36 assure l'intégrité du document. La Recommandation T.36 définit l'algorithme de hachage, y compris les calculs associés et l'échange d'informations.

G.2.3 Principe

Dans le mode d'enregistrement, les deux terminaux échangent des informations permettant aux entités de s'identifier réciproquement de façon unique. Cette méthode est basée sur l'accord entre les utilisateurs d'une clé secrète utilisée une seule fois. Chaque entité mémorise un nombre à 16 chiffres qui est associé de façon unique à l'entité avec laquelle l'enregistrement a été effectué.

Quand il est nécessaire d'envoyer un document secrètement, le terminal émetteur envoie un nombre secret de 16 chiffres associé à l'entité réceptrice, de même qu'un nombre aléatoire et une clé de session chiffrée pour mettre à l'épreuve l'entité de réception. Le terminal récepteur répond en émettant la clé de 16 chiffres associée à l'entité d'émission, de même qu'un nombre aléatoire et une version chiffrée à nouveau de la mise à l'épreuve provenant de l'entité émettrice. Il émet en même temps un nombre aléatoire et une clé de session chiffrée comme mise à l'épreuve pour l'entité émettrice. Le terminal émetteur répond par un nombre aléatoire et une version chiffrée à nouveau de la mise à l'épreuve de l'entité réceptrice. Cette procédure permet à deux entités de s'authentifier réciproquement. Au même moment, le terminal émetteur émet un nombre aléatoire, de même que la clé de session chiffrée devant être utilisée pour le chiffrement et pour le hachage.

Après la transmission du document, le terminal émetteur émet un nombre aléatoire et une clé de session chiffrée comme mise à l'épreuve à l'entité réceptrice. Au même moment, il envoie un nombre aléatoire et une valeur chiffrée de hachage permettant à l'entité réceptrice de vérifier l'intégrité du document reçu. Le terminal récepteur émet un nombre aléatoire, de même que la version chiffrée à nouveau de la mise à l'épreuve provenant de l'entité émettrice. En même temps, il envoie un nombre aléatoire et un nombre d'intégrité chiffré pour confirmer ou réfuter l'intégrité du document reçu.

L'algorithme de hachage utilisé pour l'intégrité du document est appliqué à l'ensemble du document.

On dispose d'un mode de prise de contrôle manuel n'impliquant pas l'échange de signaux de sécurité entre les deux terminaux. Les utilisateurs conviennent de l'introduction manuelle d'une clé de session secrète pour l'échange qui sera utilisée une fois. Cette clé est utilisée par le terminal émetteur pour chiffrer le document et par le terminal de réception pour le déchiffrer.

G.3 Références normatives

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui de ce fait en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée.

– Recommandation UIT-T T.4 (1996), *Normalisation des télécopieurs du Groupe 3 pour la transmission de documents.*

– Recommandation UIT-T T.36 (1997), *Capacités de sécurité destinées à être utilisées avec des télécopieurs du Groupe 3.*

G.4 Définitions

G.4.1 Fonctionnement sur le réseau RTPC utilisant les systèmes de modulation V.27 *ter*, V.29, V.17 et V.34 (mode à l'alternat)

Les signaux et les définitions utilisés avec les procédures de transmission de documents par télécopie sécurisée sont ceux utilisés à l'Annexe A/T.30 et dans le corps de la présente Recommandation, et ceux détaillés au G.6.1/T.30.

G.4.2 Fonctionnement sur le réseau RTPC utilisant le système de modulation V.34 (mode duplex) et sur le RNIS

Les signaux et les définitions utilisés avec les procédures de transmission de documents par télécopie sécurisée sont ceux qui sont définis à l'Annexe C/T.30, et ceux indiqués au G.6.1/T.30.

G.5 Abréviations

G.5.1 Les abréviations utilisées pour les procédures de transmission de documents par télécopie sécurisée sont celles qui sont définies aux Annexes A/T.30 et C/T.30 et dans le corps de la présente Recommandation, ou celles spécifiées ci-dessous.

ESHx valeur de hachage embrouillée et chiffrée provenant de l'émetteur (*encrypted scrambled hash value from the transmitter*)

ESIMy message d'intégrité embrouillé et chiffré provenant du récepteur (*encrypted scrambled integrity message from the receiver*)

ESSC1x clé d'épreuve secrète embrouillée et chiffrée provenant de l'émetteur (*encrypted scrambled secret challenge key from the transmitter*)

ESSC1y clé d'épreuve secrète embrouillée et chiffrée provenant du récepteur (*encrypted scrambled secret challenge key from the receiver*)

ESSC2x clé d'épreuve secrète embrouillée et chiffrée provenant de l'émetteur (*encrypted scrambled secret challenge key from the transmitter*)

ESSR1x clé de réponse secrète embrouillée et chiffrée provenant de l'émetteur (*encrypted scrambled secret response key from the transmitter*)

ESSR1y clé de réponse secrète embrouillée et chiffrée provenant du récepteur (*encrypted scrambled secret response key from the receiver*)

ESSR2y clé de réponse secrète embrouillée et chiffrée provenant du récepteur (*encrypted scrambled secret response key from the receiver*)

ESSS1x clé de session secrète embrouillée et chiffrée provenant de l'émetteur (*encrypted scrambled secret session key from the transmitter*)

RCNx nombre chiffré enregistré (16 chiffres décimaux dans 16 octets) associé à l'émetteur [*registered crypt number (16 decimal digits in 16 octets) associated with the transmitter*]

RCNy nombre chiffré enregistré (16 chiffres décimaux dans 16 octets) associé au récepteur [*registered crypt number (16 decimal digits in 16 octets) associated with the receiver*]

RK clés du récepteur (*receiver keys*) – voir G.6.1/T.30

RNC1x nombre aléatoire associé à une épreuve secrète provenant de l'émetteur (*random number associated with a secret challenge from the transmitter*)

RNC1y nombre aléatoire associé à une épreuve secrète provenant du récepteur (*random number associated with a secret challenge from the receiver*)

RNC2x nombre aléatoire associé à une épreuve secrète provenant de l'émetteur (*random number associated with a secret challenge from the transmitter*)

RNIMy nombre aléatoire associé à un message d'intégrité provenant du récepteur (*random number associated with an integrity message from the receiver*)

RNSR1x nombre aléatoire associé à une réponse secrète provenant de l'émetteur (*random number associated with a secret response from the transmitter*)

RNSR1y nombre aléatoire associé à une réponse secrète provenant du récepteur (*random number associated with a secret response from the receiver*)

RNSR2y nombre aléatoire associé à une réponse secrète provenant du récepteur (*random number associated with a secret response from the receiver*)

RNSS1x nombre aléatoire associé à une clé de session secrète provenant de l'émetteur (*random number associated with a secret session key from the transmitter*)

RTC retour à la commande (*return to control*) – comme défini dans la Recommandation T.4

TK clés de l'émetteur (*transmitter keys*) – voir G.6.1/T.30

TKx clé de transfert fournie par l'émetteur (*transfer key provided by the transmitter*)

TKy clé de transfert fournie par le récepteur (*transfer key provided by the receiver*)

TNR émetteur non prêt (*transmitter not ready*) – voir G.6.1/T.30

TR émetteur prêt (*transmitter ready*) – voir G.6.1/T.30

NOTE 1 – Toutes les valeurs des nombres aléatoires sont des valeurs à 4 chiffres décimaux dans 4 octets.

NOTE 2 – Toutes les valeurs embrouillées et chiffrées sont des valeurs à 12 chiffres décimaux dans 12 octets.

G.6 Procédures de télécopie

G.6.1 Champ de commande de télécopie

Le système de gestion de clé de chiffrement HKM utilise des trames d'émetteur (TK) et de récepteur (RK) selon T.30. Le contenu des champs FIF de ces signaux diffère selon l'utilisation et est énuméré au point G.6.2/T.30. A chaque signal TK et RK est ajouté un chiffre pour faire référence aux organigrammes et aux diagrammes de séquences de signaux dans la présente annexe.

Chaque clé de chiffrement transférée (différente de celle de l'enregistrement) est en format embrouillé et chiffré (ES, *encrypted scrambled*) et s'accompagne d'un nombre aléatoire associé (RN, *random number*).

1) *Emetteur non prêt (TNR)* – ce signal est utilisé pour indiquer que l'émetteur n'est pas encore prêt à émettre.

   Format:
   X101 0111

2) *Emetteur prêt (TR)* – ce signal est utilisé pour demander l'état de l'émetteur.

   Format:
   X101 0110

3) *Clés de l'émetteur (TK)* – ce signal est utilisé pour transmettre les clés de sécurité, etc. de l'émetteur du document vers le récepteur du document. Le contenu des champs FIF du signal est défini ultérieurement dans la présente annexe et dépendra des circonstances dans lesquelles il est utilisé.

   Format:
   1101 0010

4) *Clés du récepteur (RK)* – ce signal est utilisé pour transmettre les clés de sécurité, etc. du récepteur du document vers l'émetteur du document. Le contenu des champs FIF de ce signal est défini ultérieurement dans la présente annexe et dépendra des circonstances dans lesquelles il est utilisé.

   Format:
   0101 0010

G.6.2 Champs d'information de télécopie

Le codage des clés devra être identique à celui indiqué au Tableau 3/T.30 et le bit de plus faible poids du chiffre de poids faible devra être le premier bit transmis.

G.6.2.1 Enregistrement mutuel et authentification mutuelle

Voir le Tableau G.1/T.30.

Tableau G.1/T.30

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

G.6.2.2 Signaux préliminaires à la transmission du message: authentification mutuelle et échange de clé de session secrète

Voir le Tableau G.2/T.30.

Tableau G.2/T.30

Signal	Octets FIF	Contenu FIF
TK8	1 2 longueur 3-18 19-22 23-34	0000 1100 0010 0000 RCNy RNC1x ESSC1x
RK9	1 2 longueur 3-18 19-22 23-34 35-38 39-50	0000 1001 0011 0000 RCNx RNSR1y ESSR1y RNC1y ESSC1y
TK10	1 2 longueur 3-6 7-18 19-21 23-34	0000 1010 0010 0000 RNSR1x ESSR1x RNSS1x ESSS1x
NOTE – Si le document n'est pas chiffré, tous les chiffres des champs RNC1x et ESSS1x sont mis à zéro.		

G.6.2.3 Procédure pendant le message

De l'émetteur vers le récepteur. Les formats et les signaux spécifiques de procédure pendant le message devront être conformes à ceux définis à l'Annexe A/T.4.

G.6.2.4 Signaux postérieurs à la transmission du message: confirmation et intégrité du document (transmission normale)

Voir le Tableau G.3/T.30.

Tableau G.3/T.30

Signal	Octets FIF	Contenu FIF
TK16	1 2 longueur 3-6 7-18 19-42	0001 0000 0010 1000 RNC2x ESSC2x ESHx
RK17	1 2 longueur 3-6 7-18 19-22 23-34	0001 0001 0010 0000 RNSR2y ESSR2y RNIMy ESIMy
NOTE 1 – Si le document n'a pas de contrôle d'intégrité, tous les chiffres des champs ESHx, RNIMy et ESIMy sont mis à zéro. NOTE 2 – La trame TK16 n'est pas fournie si DCS indique l'absence de hachage. NOTE 3 – La trame RK17 n'est pas fournie en l'absence de TK16.		

G.6.2.5 Notes générales

1) Durant l'étape d'enregistrement, les épreuves et les réponses sont obligatoires. Le mécanisme d'épreuve/réponse est défini dans la Recommandation T.36.

2) Durant les appels normaux, toutes les épreuves et toutes les réponses valables doivent avoir un nombre aléatoire différent de zéro. Les nombres aléatoires mis à zéro dans les épreuves ou les réponses indiquent que l'authentification mutuelle n'est pas acceptée.

3) Les trames TK16/RK17 sont normalement utilisées avec/après PPS-EOP sauf dans le cas de relève cyclique quand elles peuvent être envoyées avec/après PPS-EOM.

4) L'emploi du hachage et du chiffrement est déterminé par le premier appel DIS/DCS et s'applique à tout document transmis dans cette session.

G.7 Organigrammes

G.7.1 Fonctionnement sur le réseau RTPC utilisant les systèmes de modulation V.27 *ter*, V.29, V.17 et V.34 (mode semi-duplex)

Les organigrammes de la Figure G.7-1/T.30 indiquent l'étape B correspondant aux procédures préliminaires à la transmission du message, l'étape C correspondant à la procédure de message, l'étape D correspondant à la procédure suivant la transmission du message et l'étape E correspondant à la libération d'appel, à la fois pour le terminal émetteur et pour le terminal récepteur.

Il convient également de se référer aux procédures définies dans la Recommandation T.36.

G.7.2 Règles relatives aux organigrammes

Les organigrammes suivent deux règles simples:

1) Tous les traits ont une flèche pointée uniquement vers la destination.

2) Il n'y a pas de croisements de traits.

G.7.3 Temporisateurs utilisés dans les organigrammes

T1	35 s ± 5 s
T2	6 s ± 1 s
T3	10 s ± 5 s
T4	4,5 s ± 15% pour les postes manuels
T4	3,0 s ± 15% pour les postes automatiques
T5	60 s ± 5 s

G.7.4 Abréviations et descriptions utilisées dans les organigrammes

Sauf spécification contraire ci-après, la définition des termes des organigrammes est indiquée dans le corps de la Recommandation et/ou l'Annexe A/T.30.

Besoin d'authentification? — Vérifier que l'authentification mutuelle est nécessaire au début de la transmission.

NOTE 1 – Une fois que l'authentification mutuelle a été effectuée, il convient de toujours suivre la sortie "non" à l'intérieur de la même session.

Mode enregistrement? — Vérifier que l'enregistrement de sécurité est nécessaire.

Première page? — Vérifier que l'authentification mutuelle est nécessaire au début de la transmission.

NOTE 2 – Une fois effectuée l'authentification mutuelle, il convient de toujours suivre la sortie "non" à l'intérieur de la même session.

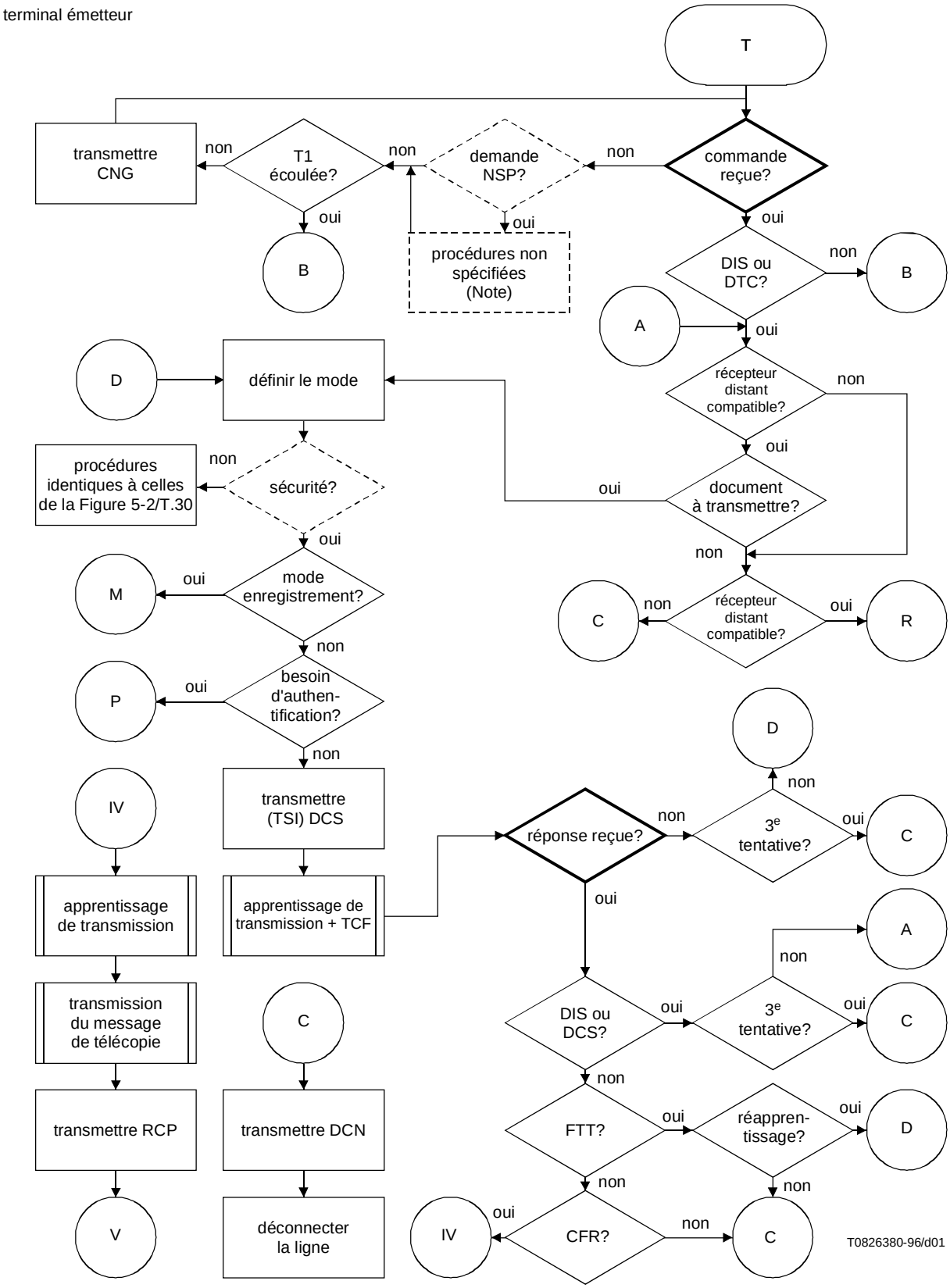
G.8 Organigrammes

G.8.1 Fonctionnement sur le réseau RTPC utilisant le système de modulation V.34 (mode duplex) et sur le RNIS

Le fonctionnement de la télécopie de document sécurisée sur le réseau RTPC utilisant le système de modulation V.34 (mode duplex) et sur le RNIS est exactement identique à celui défini dans l'Annexe C/T.30, sauf pour les exceptions indiquées par les organigrammes ci-dessous.

Les organigrammes de la Figure G.8/T.30 indiquent l'étape B correspondant aux procédures préliminaires à la transmission de message, l'étape D correspondant à la procédure postérieure à la transmission de message et l'étape E correspondant à la libération de l'appel, à la fois pour les terminaux émetteur et récepteur.

Il convient de se référer également aux procédures définies dans la Recommandation T.36.



NOTE – La procédure non spécifiée (NSP) correspond à une procédure qui s'exécute en moins de 6 secondes. Il ne s'agit pas nécessairement d'une séquence définissable de signaux.

Figure G.7-1/T.30 (feuillet 1 de 20)

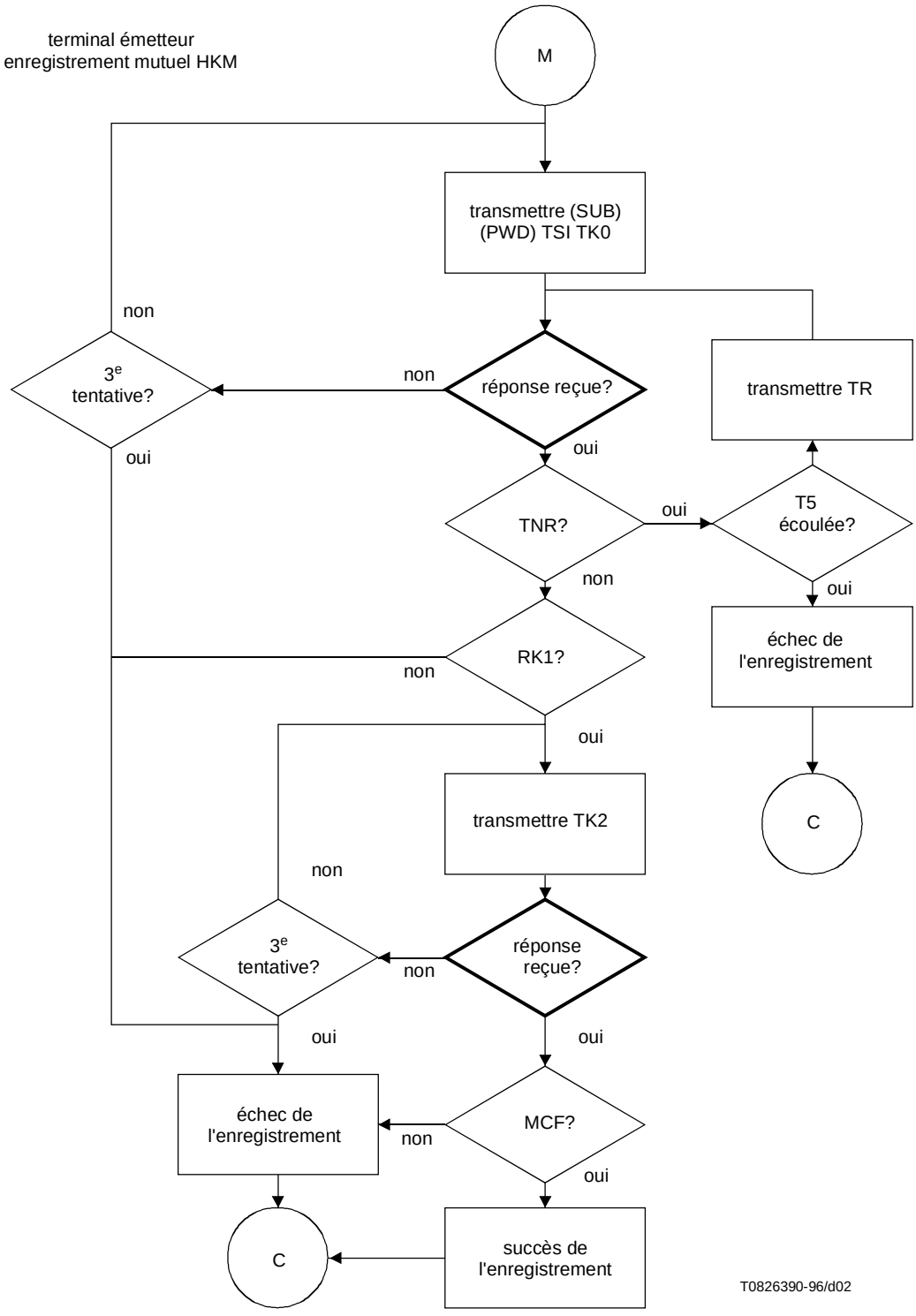


Figure G.7-1/T.30 (feuillet 2 de 20)

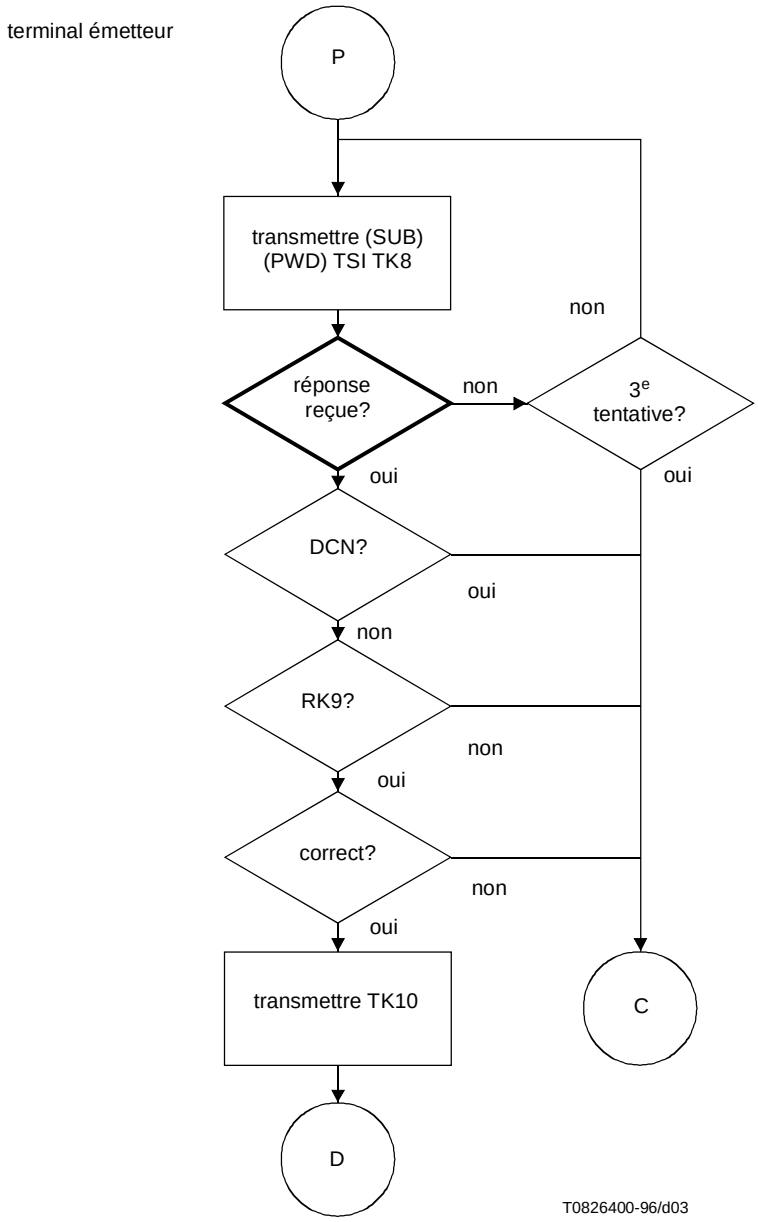


Figure G.7-1/T.30 (feuillet 3 de 20)

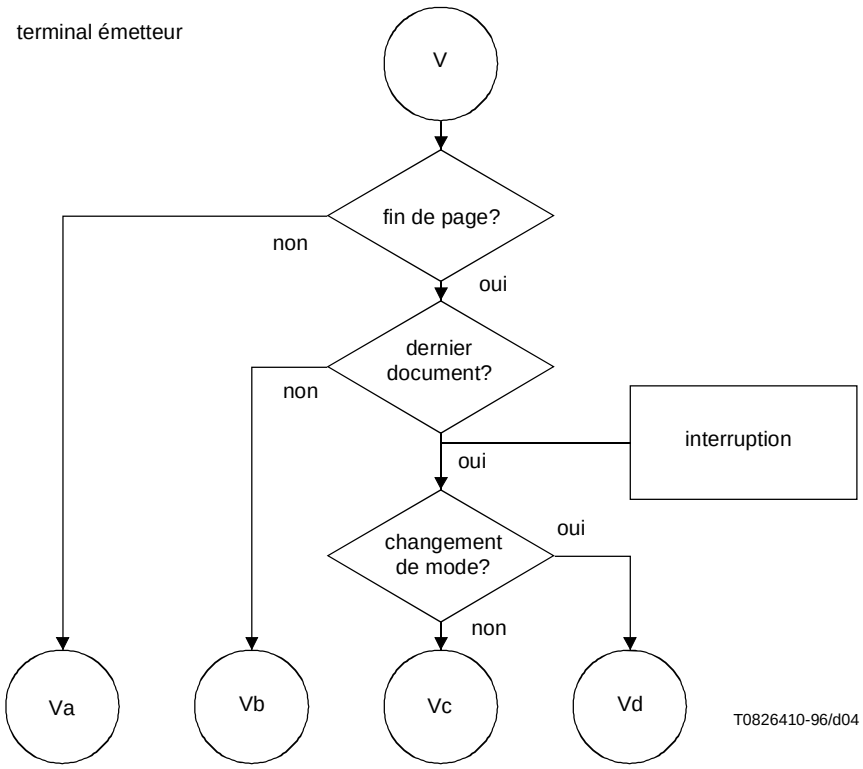


Figure G.7-1/T.30 (feuillet 4 de 20)

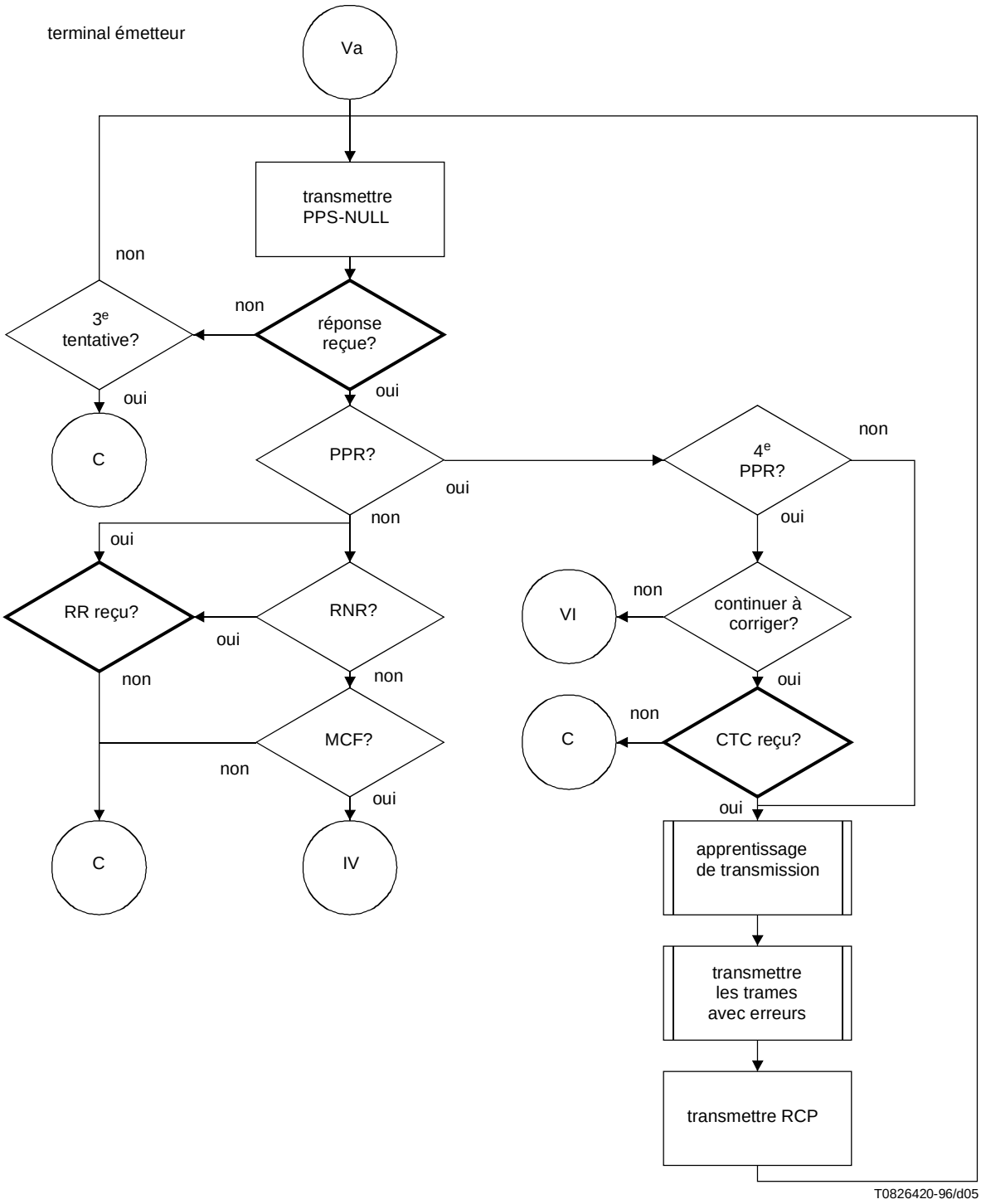


Figure G.7-1/T.30 (feuillet 5 de 20)

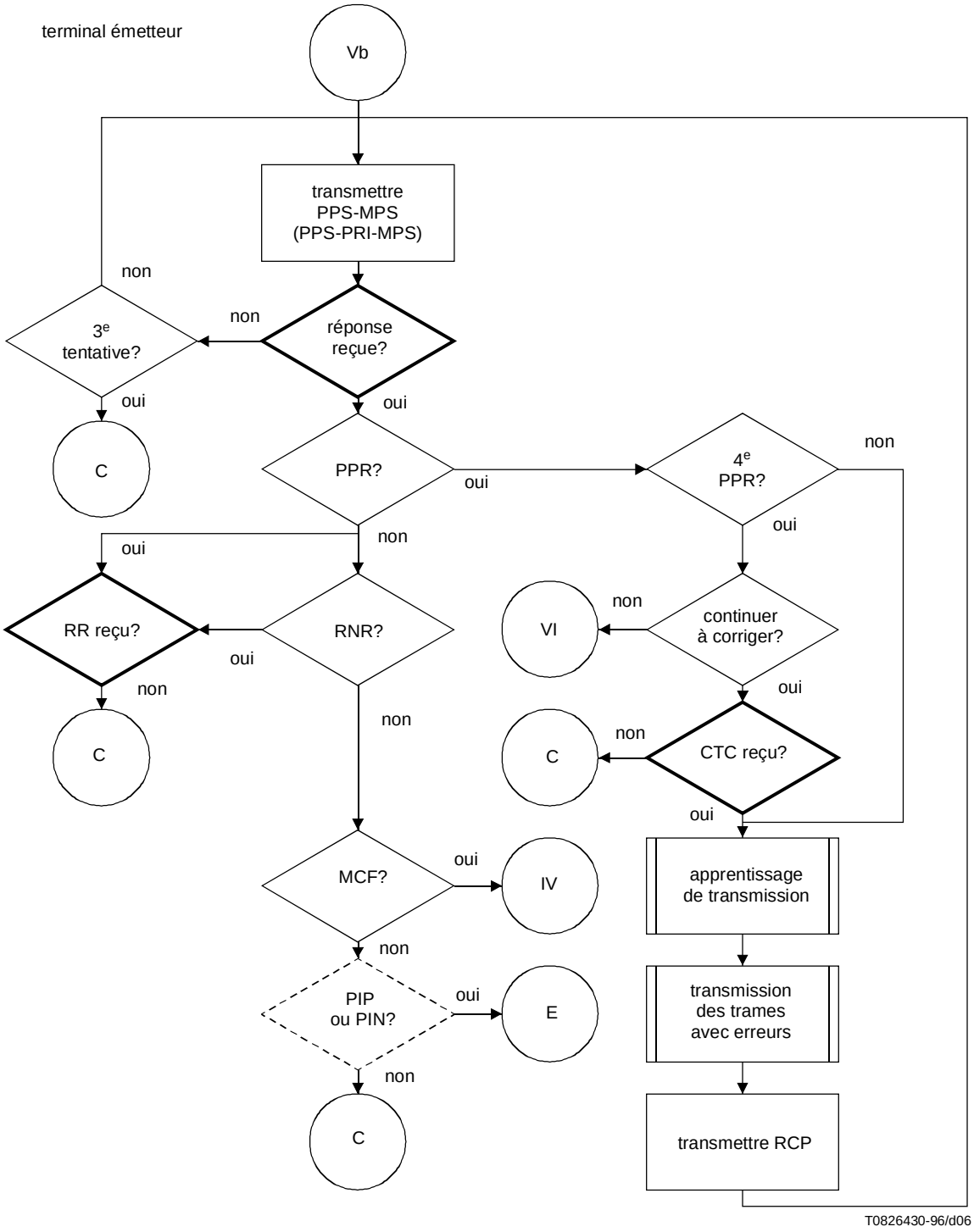


Figure G.7-1/T.30 (feuillet 6 de 20)

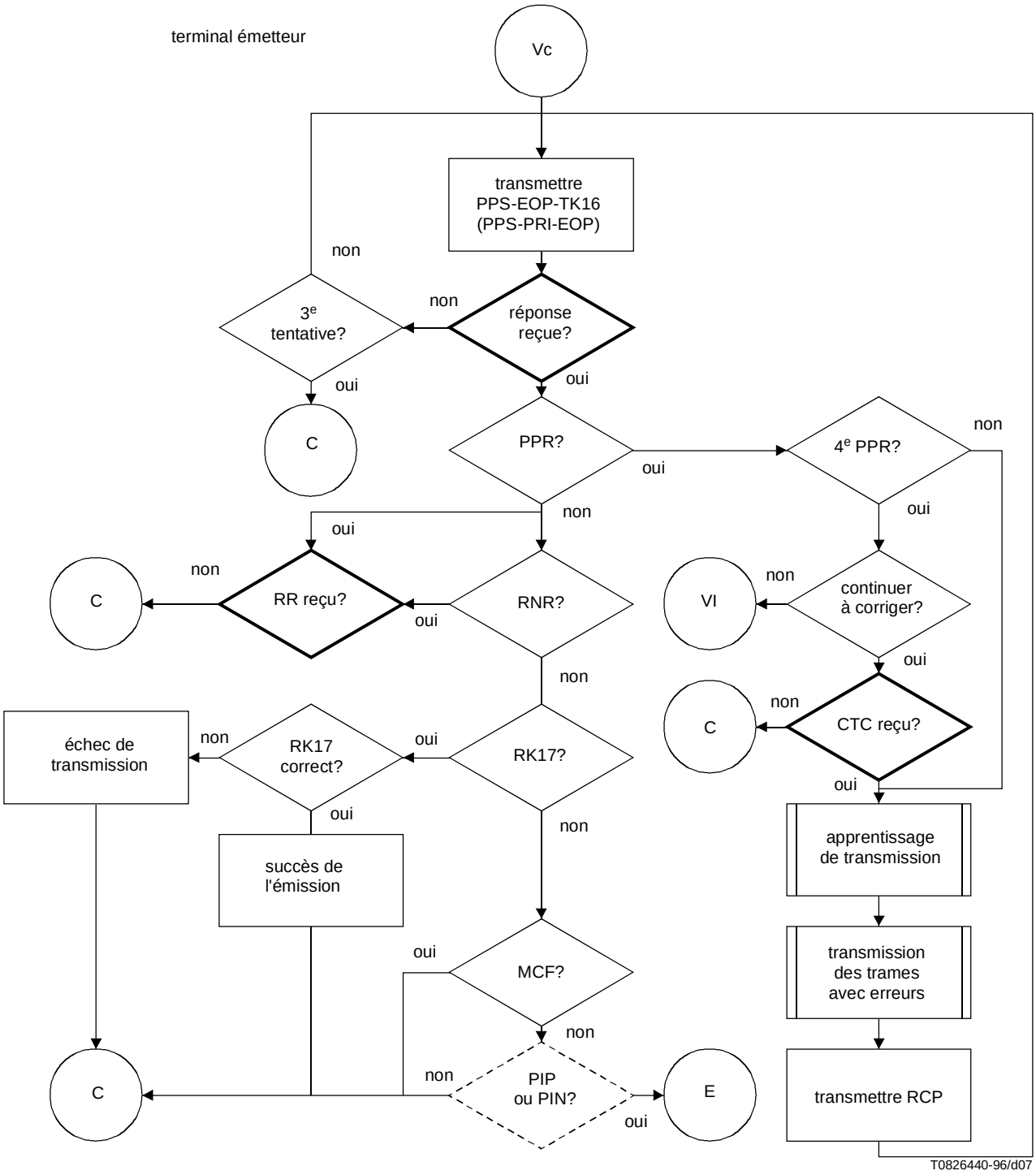


Figure G.7-1/T.30 (feuillet 7 de 20)

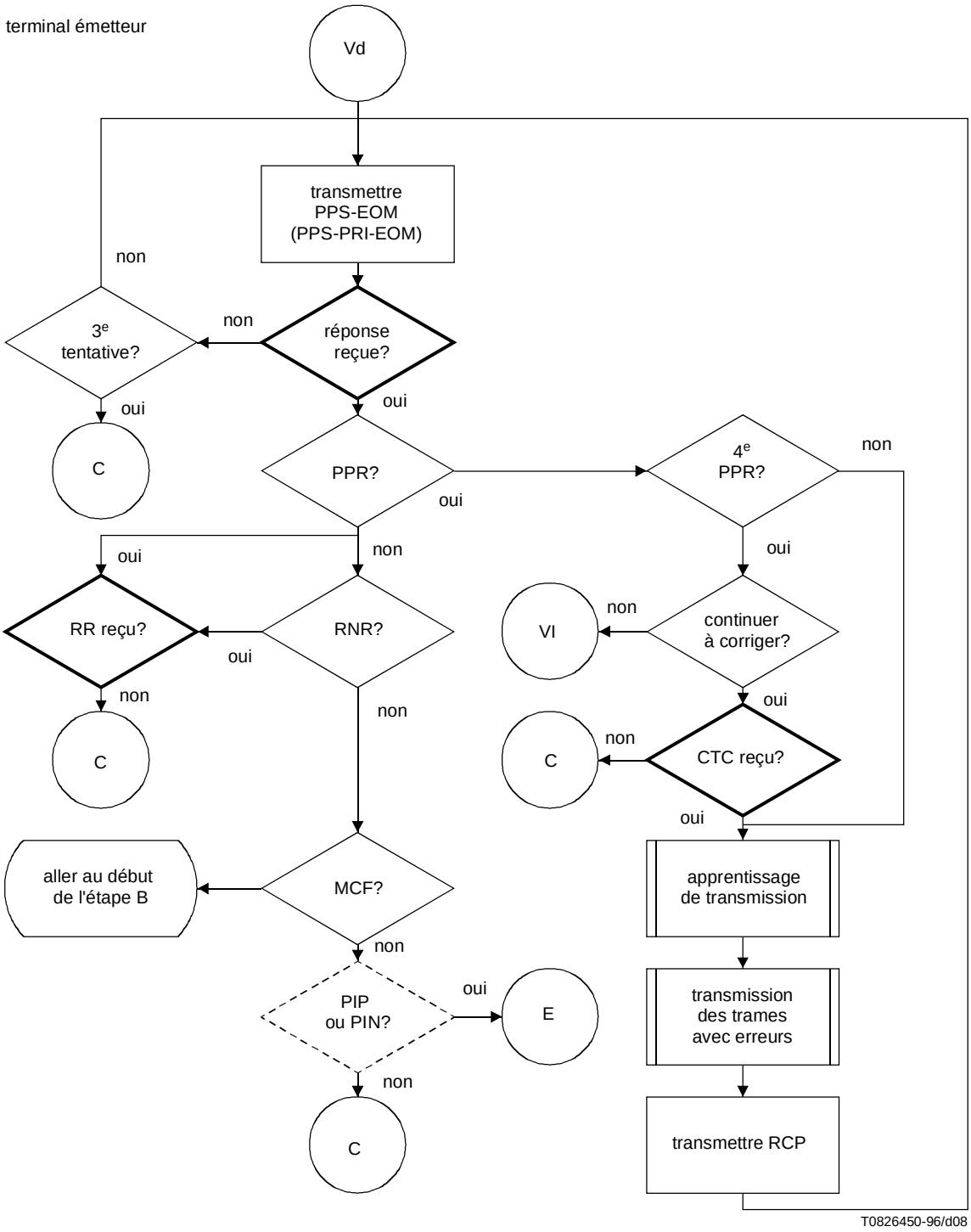


Figure G.7-1/T.30 (feuillet 8 de 20)

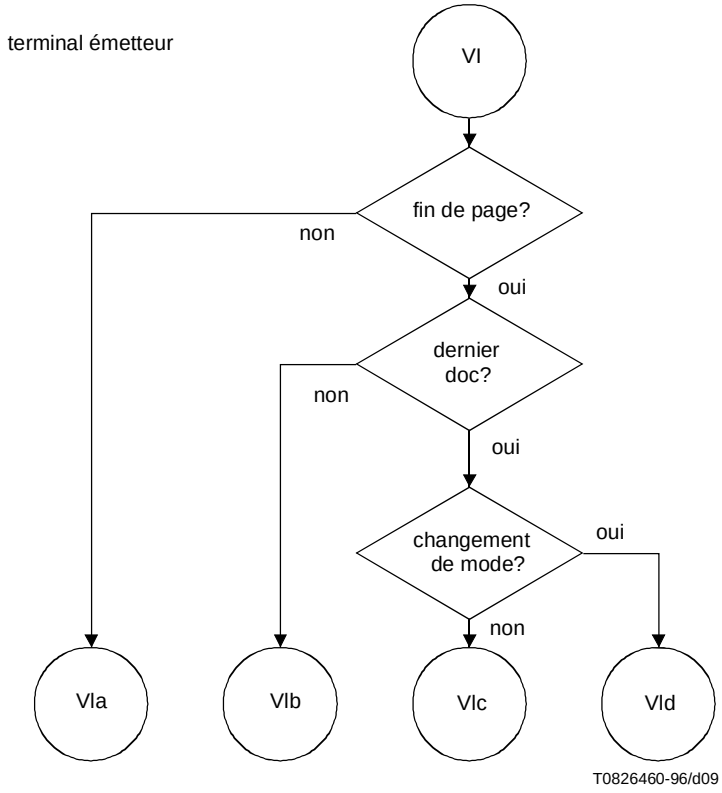


Figure G.7-1/T.30 (feuillet 9 de 20)

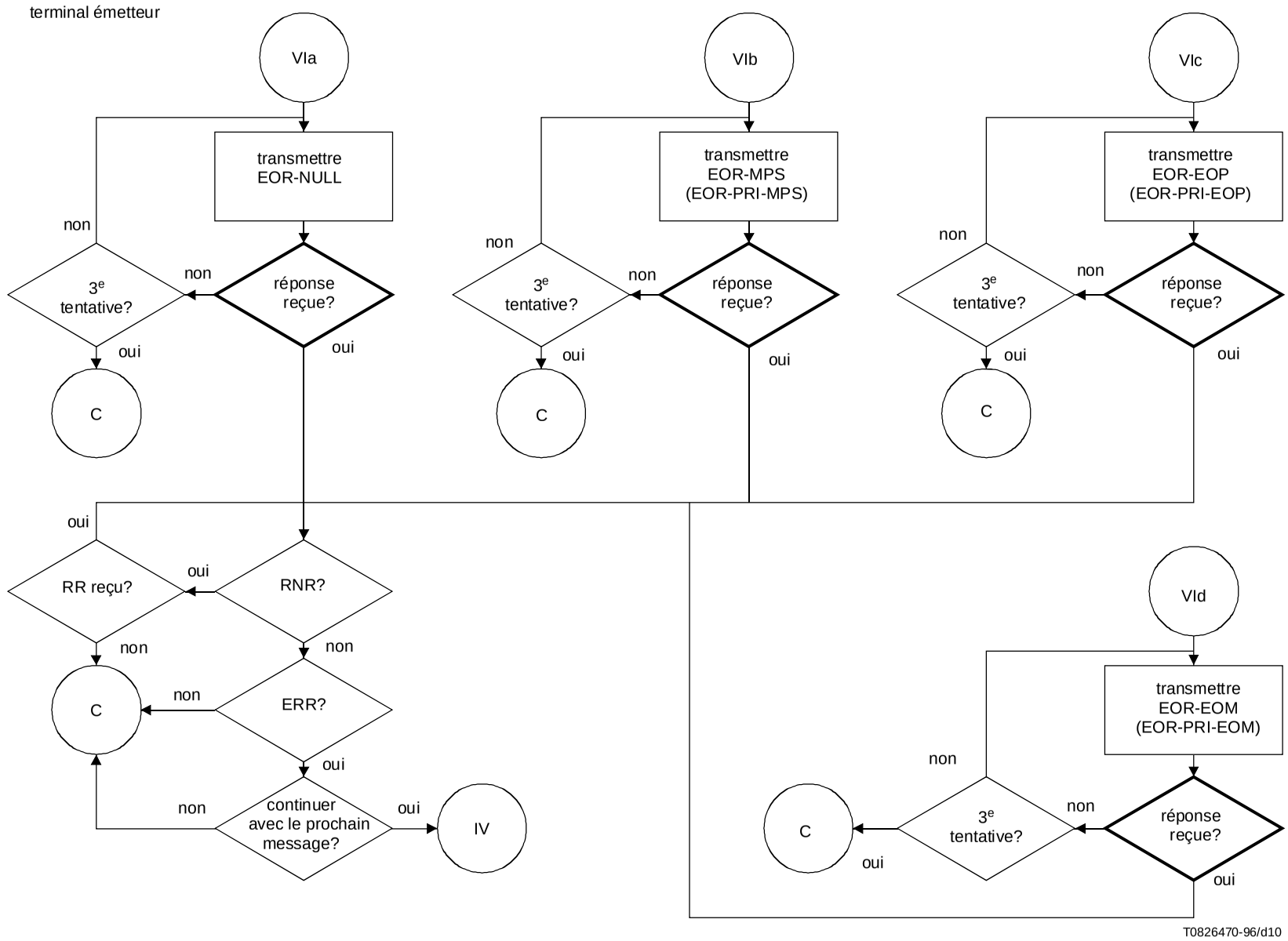


Figure G.7-1/T.30 (feuillet 10 de 20)

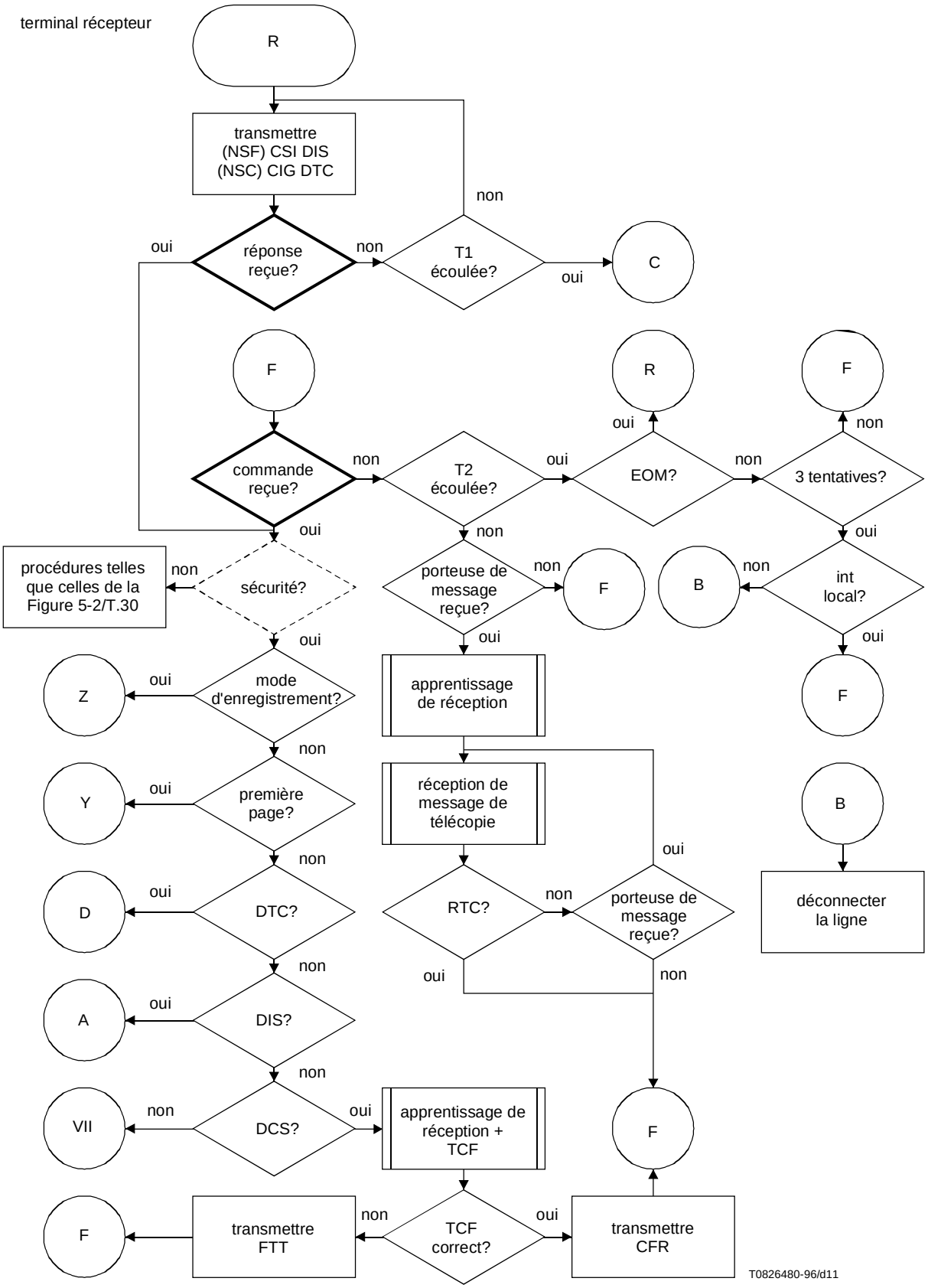


Figure G.7-1/T.30 (feuillet 11 de 20)

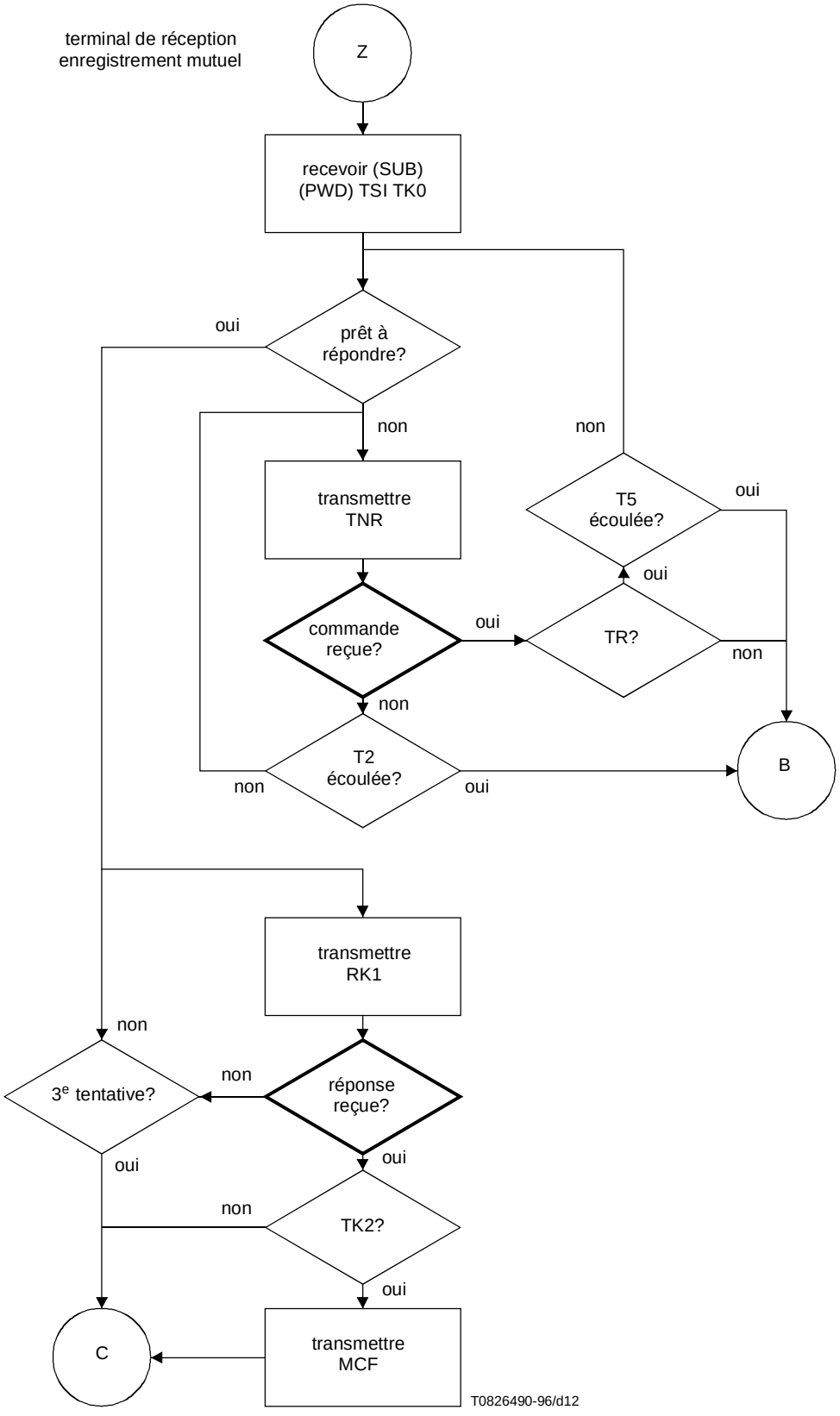


Figure G.7-1/T.30 (feuillet 12 de 20)

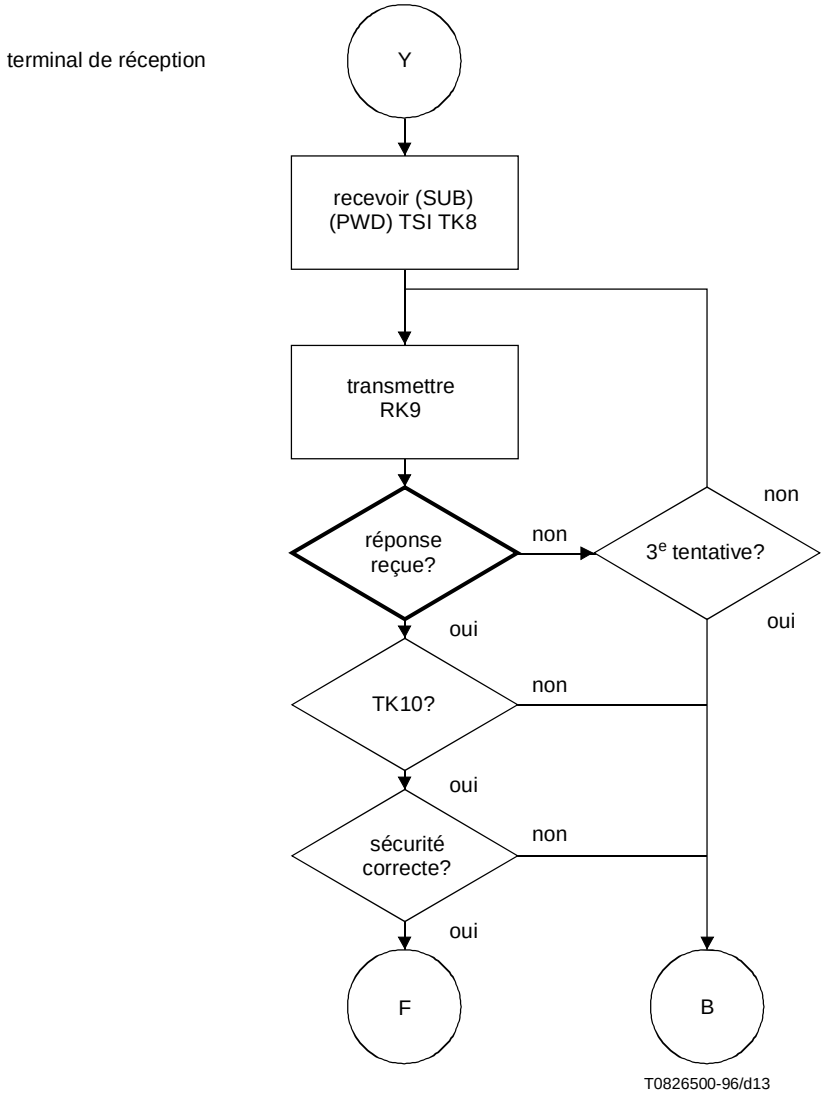


Figure G.7-1/T.30 (feuillet 13 de 20)

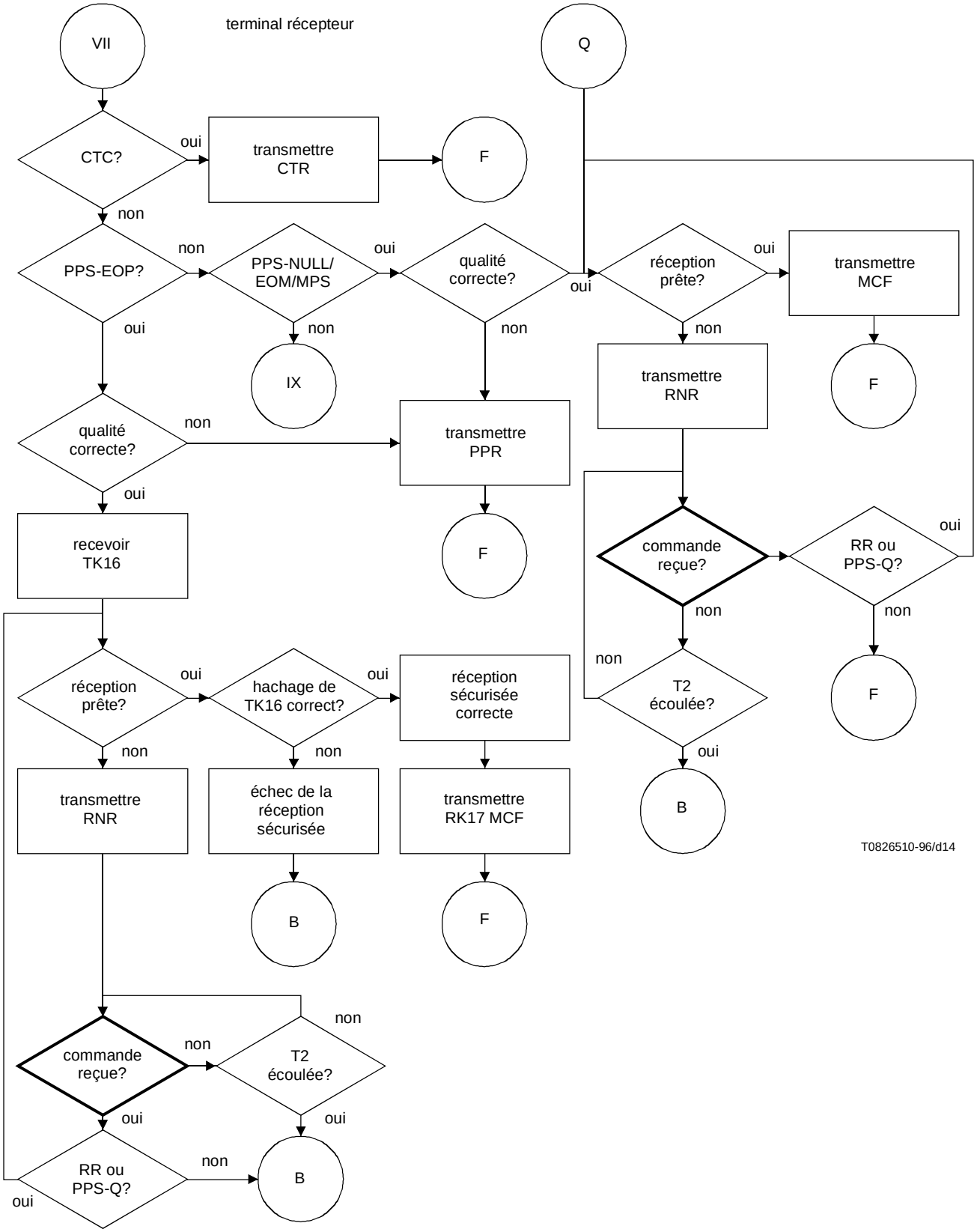


Figure G.7-1/T.30 (feuillet 14 de 20)

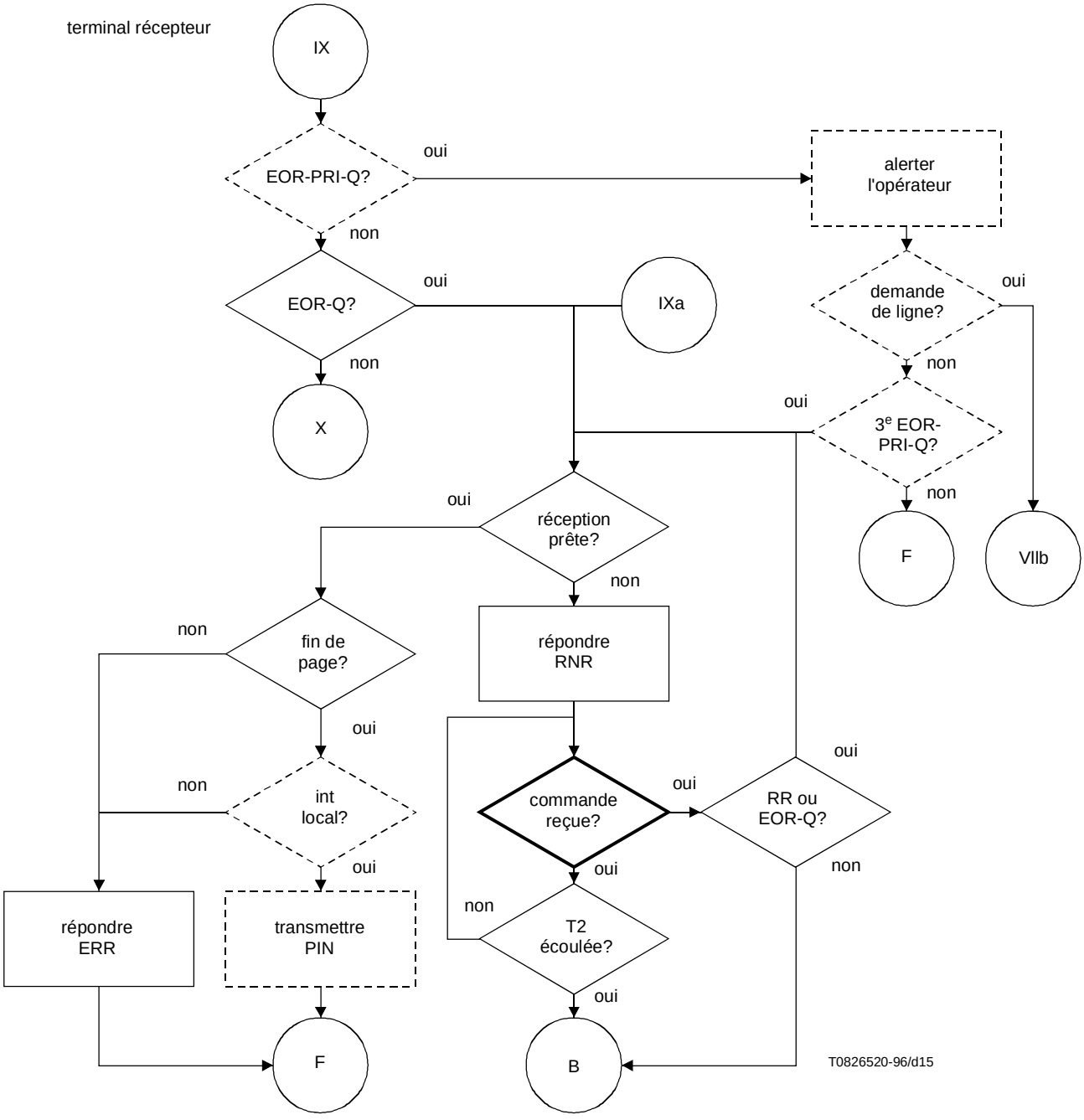


Figure G.7-1/T.30 (feuillet 15 de 20)

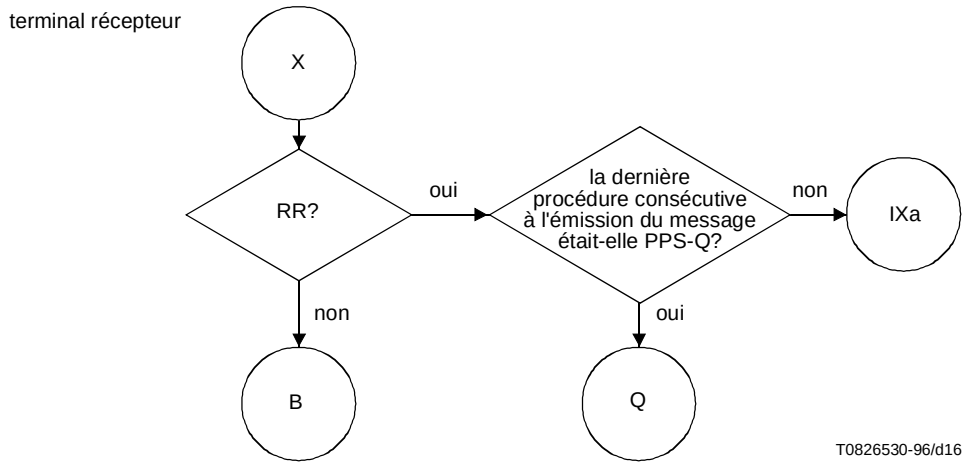


Figure G.7-1/T.30 (feuillet 16 de 20)

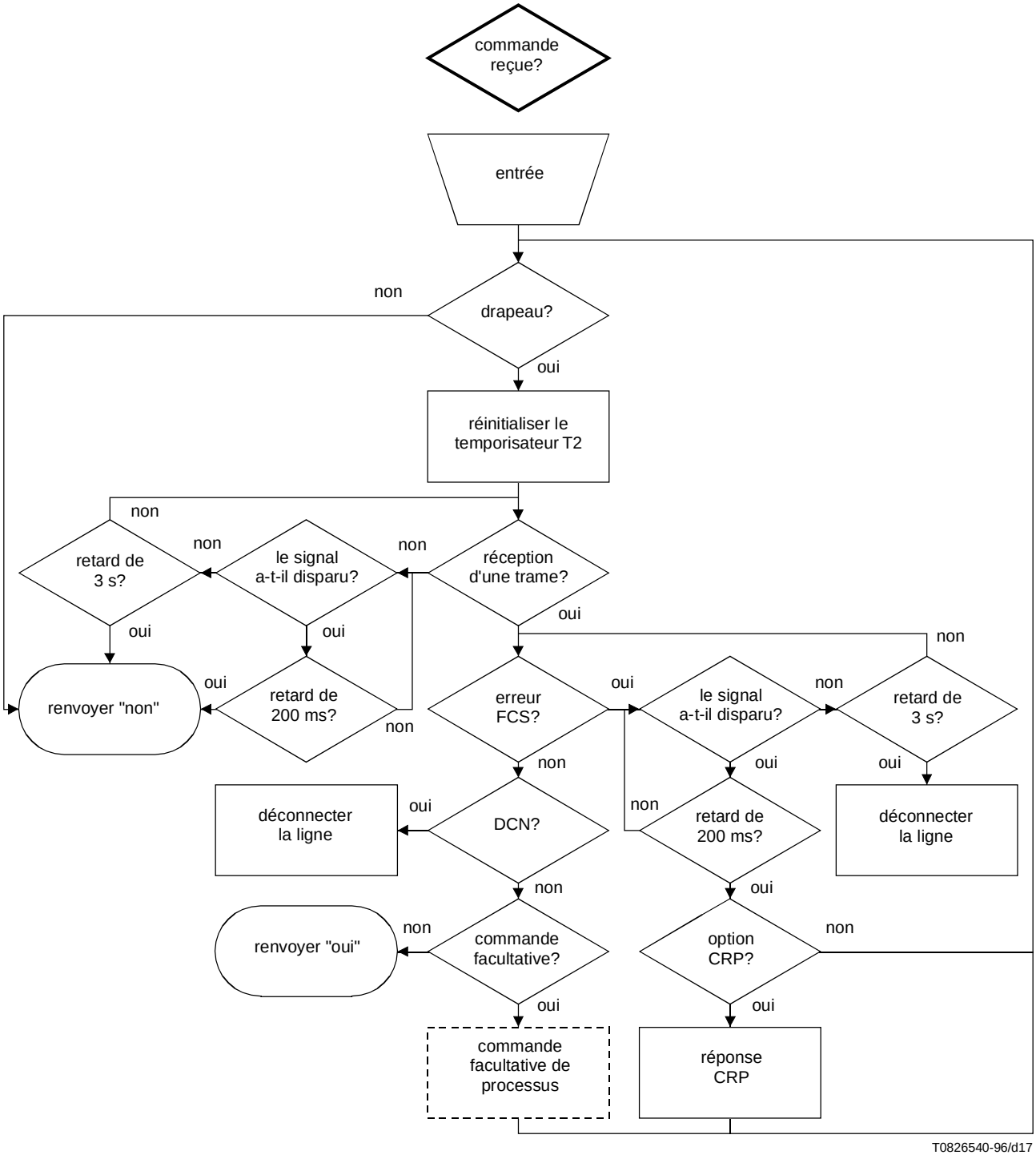


Figure G.7-1/T.30 (feuillet 17 de 20)

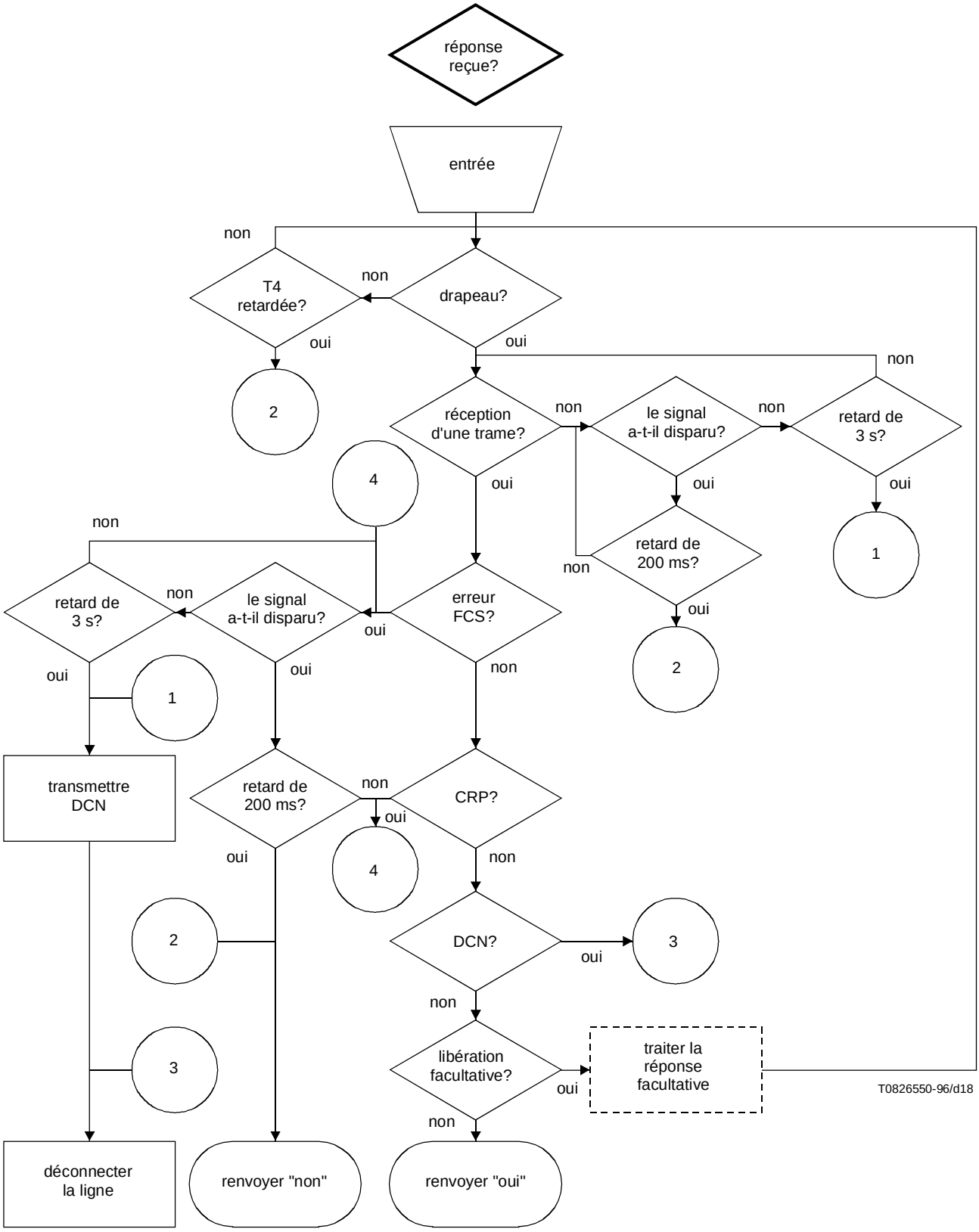


Figure G.7-1/T.30 (feuillet 18 de 20)

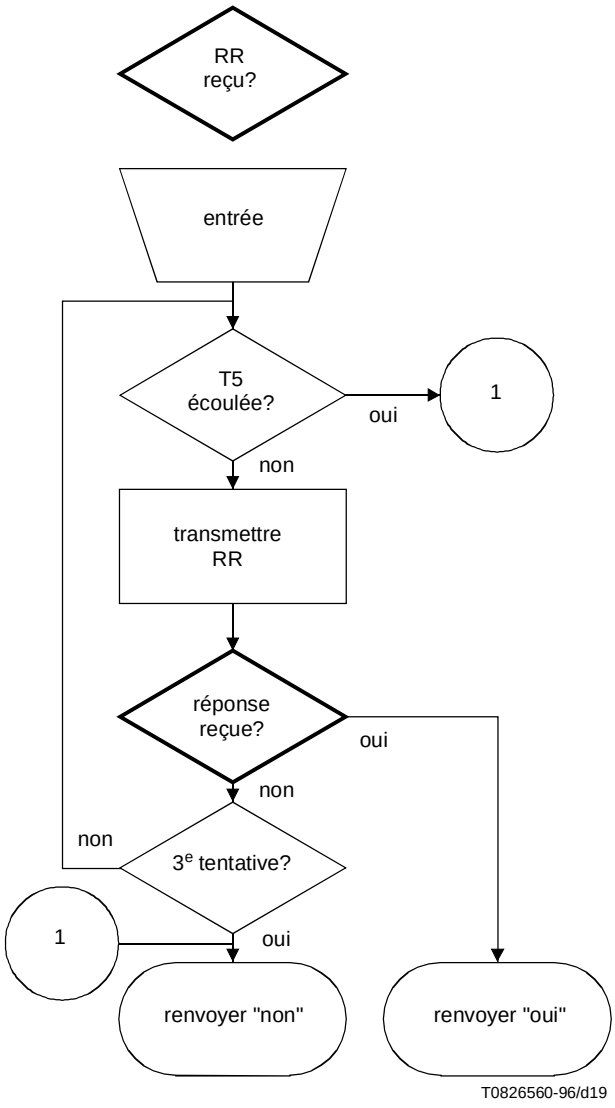


Figure G.7-1/T.30 (feuillet 19 de 20)

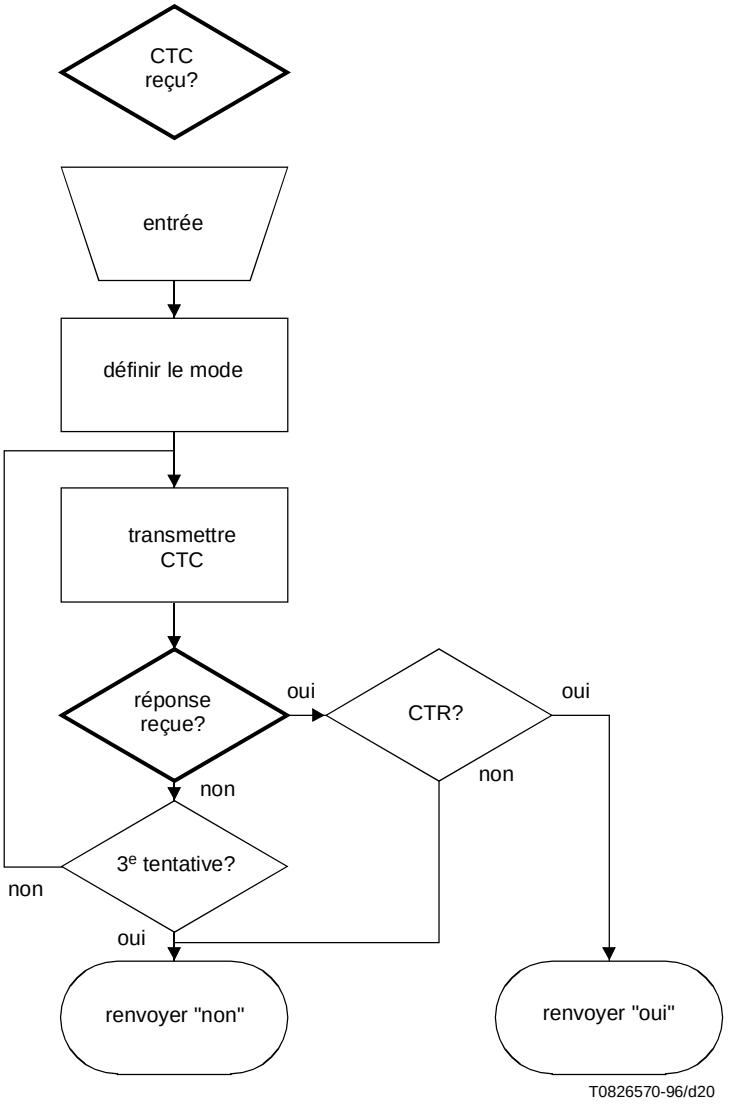


Figure G.7-1/T.30 (feuillet 20 de 20)

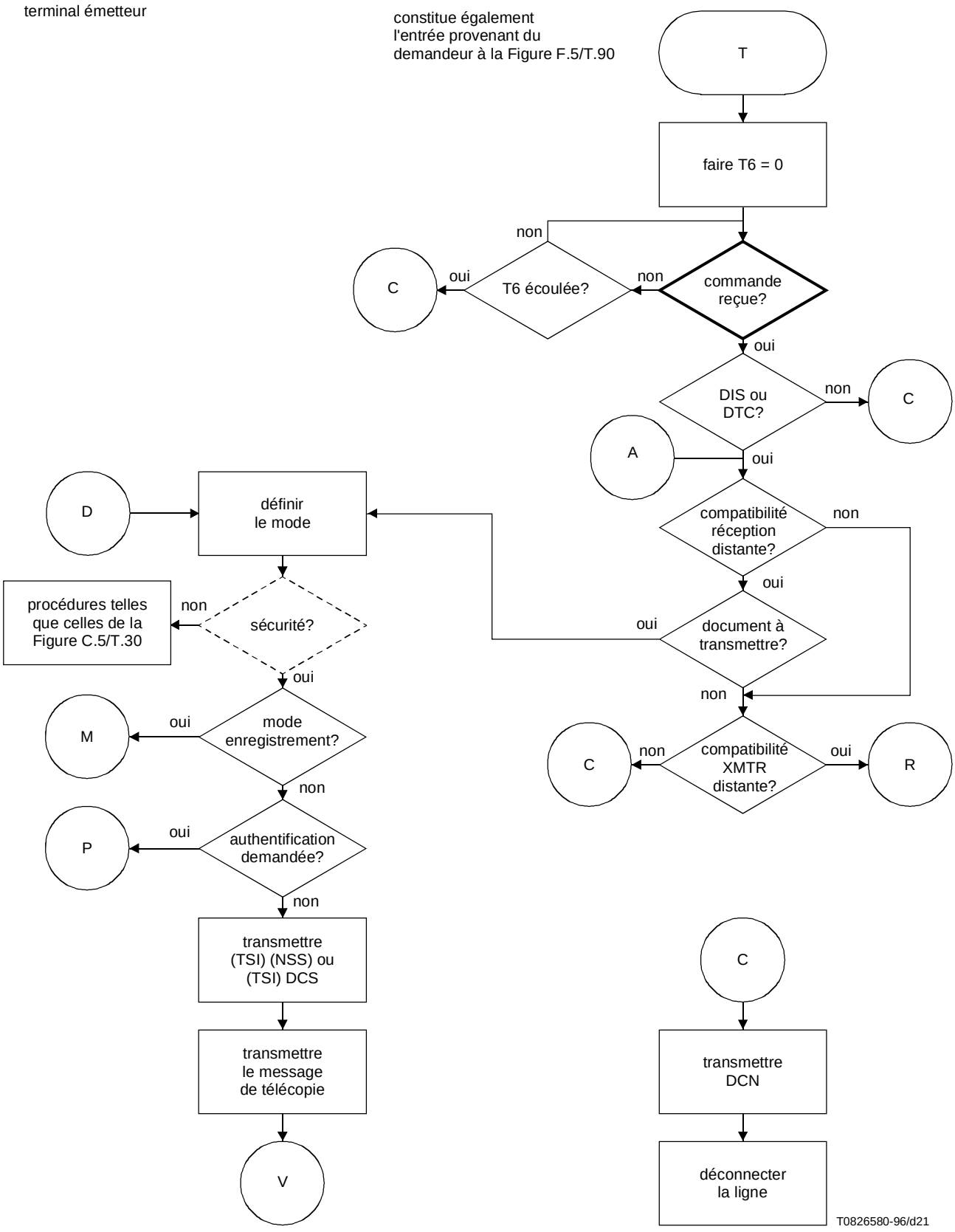


Figure G.8-1/T.30 (feuillet 1 de 3) (Utilisée à la place de la Figure C.5/T.30) mode duplex

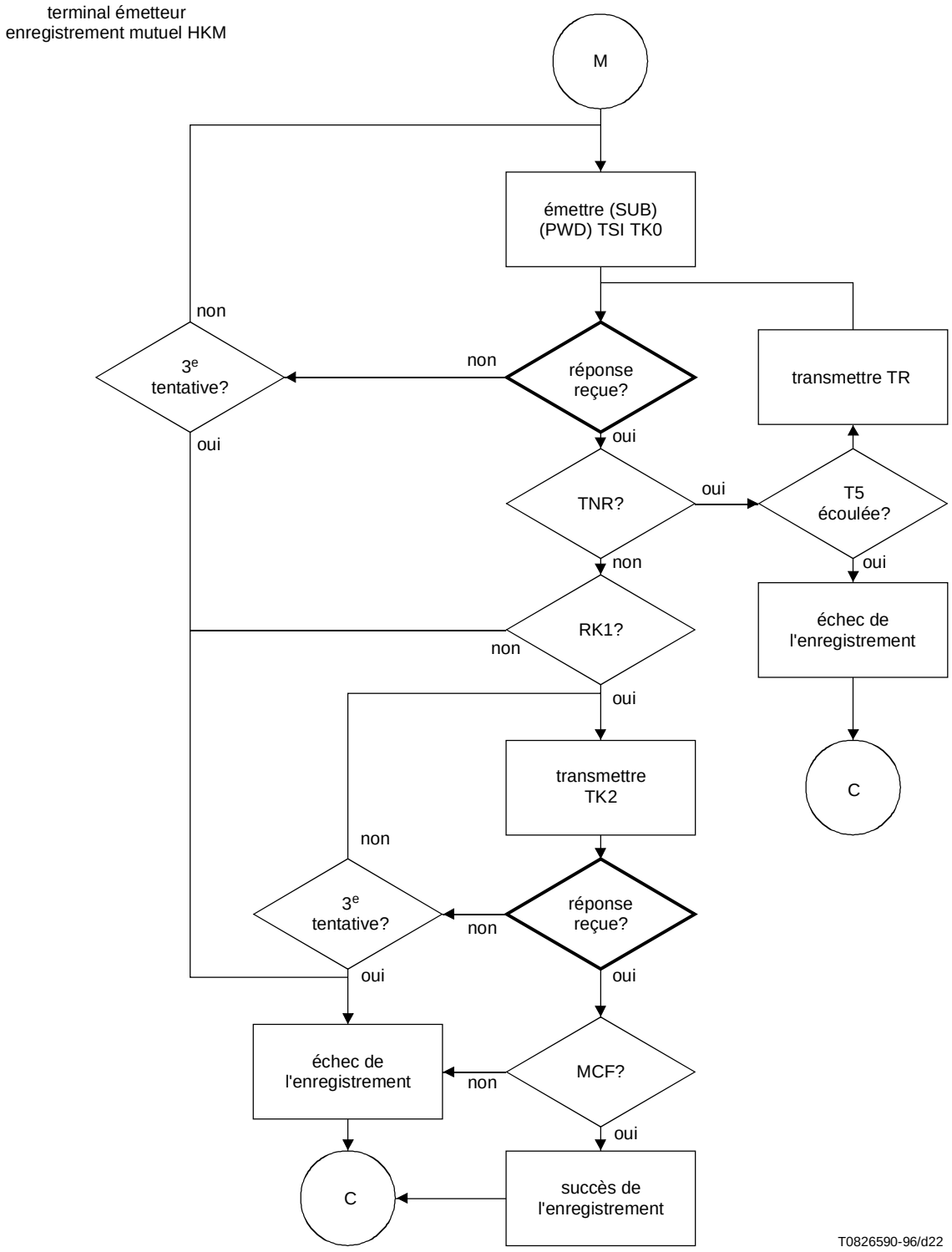


Figure G.8-1/T.30 (feuillet 2 de 3) (Utilisée à la place de la Figure C.5/T.30) mode duplex

terminal émetteur

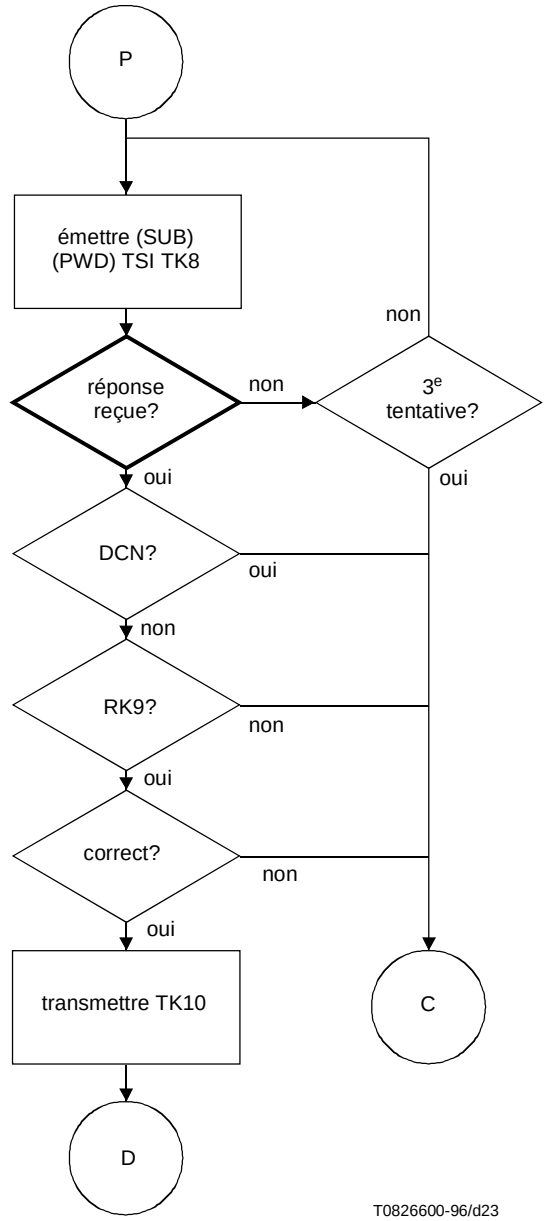


Figure G.8-1/T.30 (feuillet 3 de 3) (Utilisée à la place de la Figure C.5/T.30) mode duplex

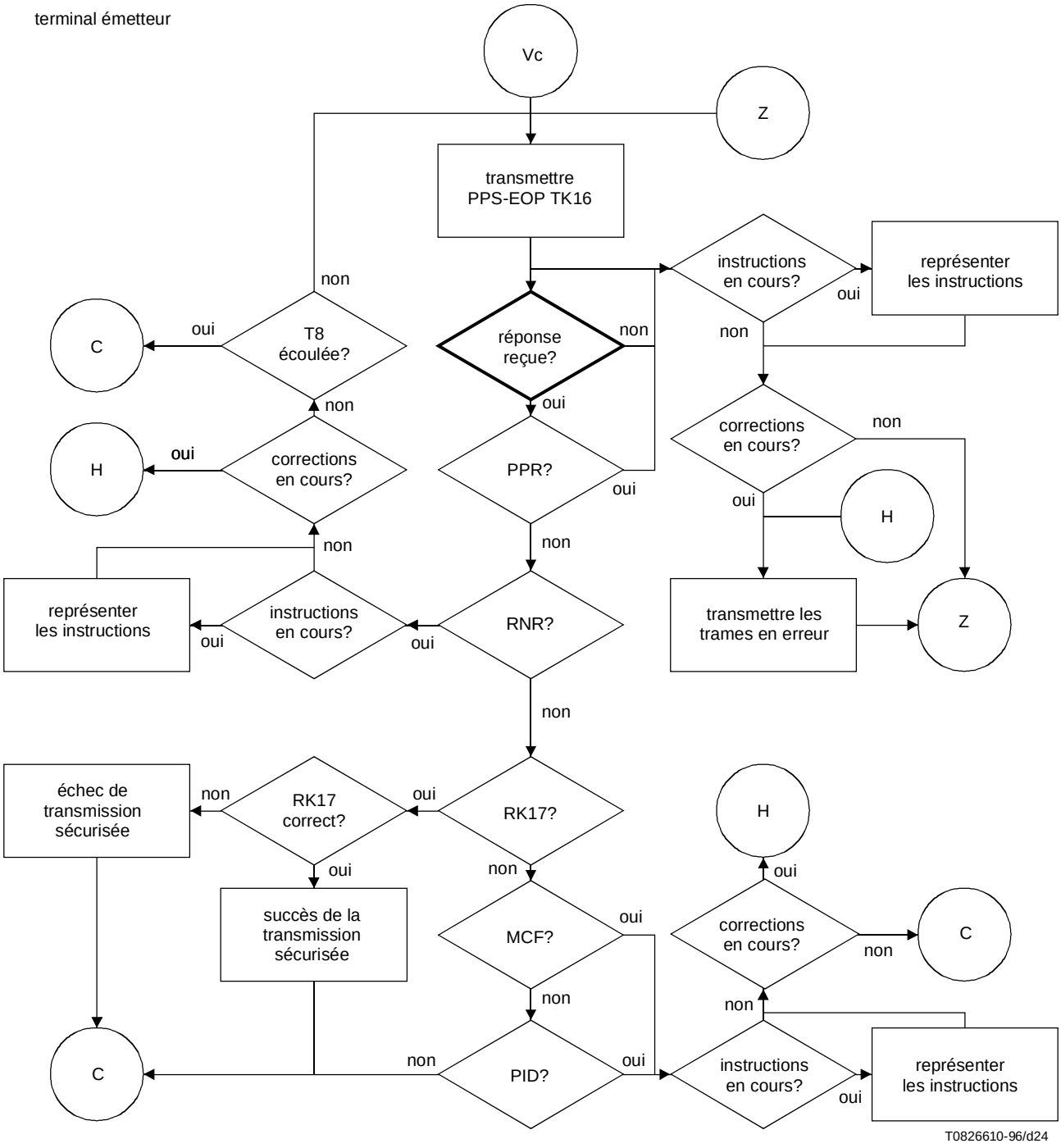


Figure G.8-2/T.30 (Utilisée à la place de la Figure C.9/T.30) mode duplex

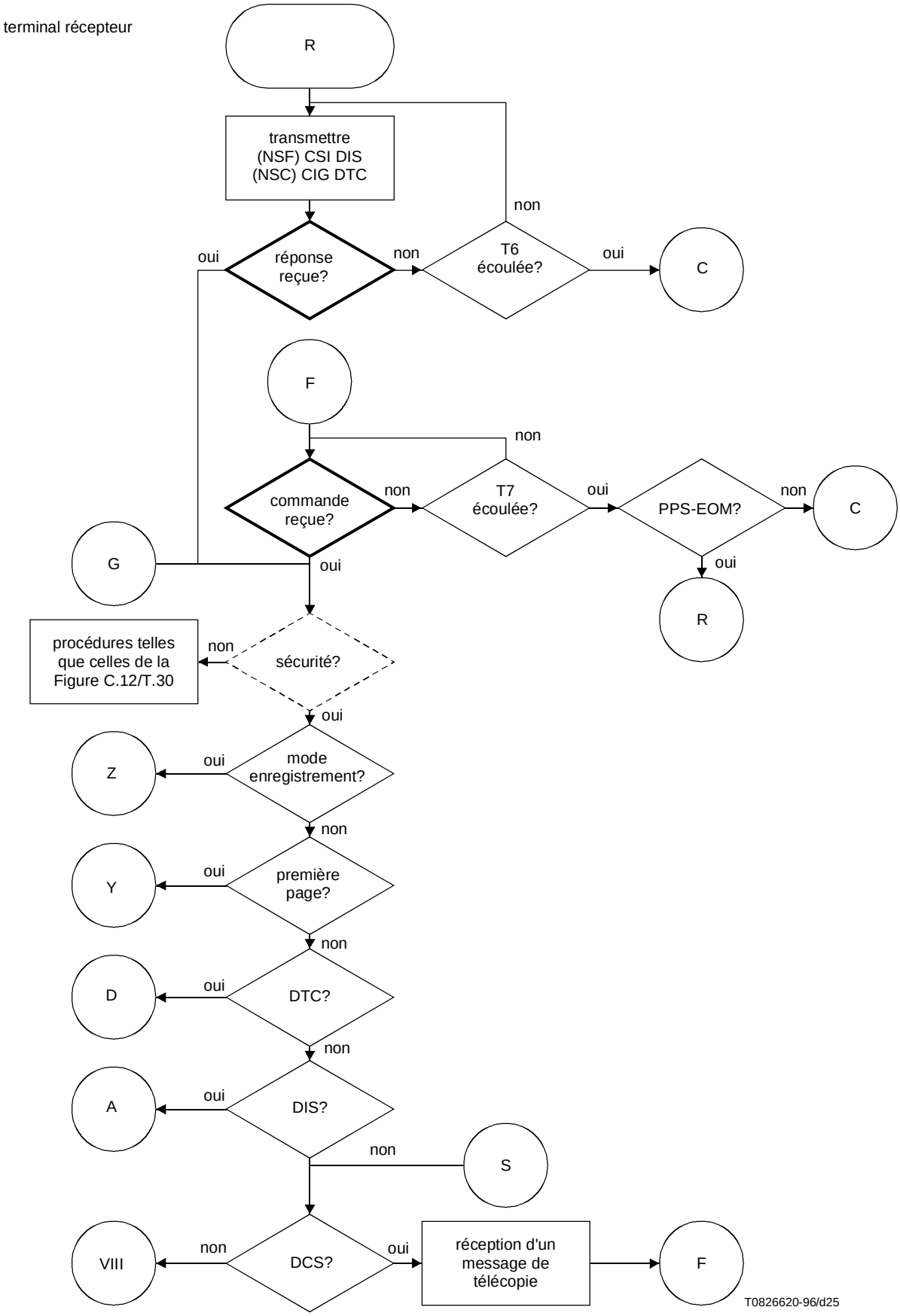


Figure G.8-3/T.30 (feuillet 1 de 3) (Utilisée à la place de la Figure C.12/T.30) mode duplex

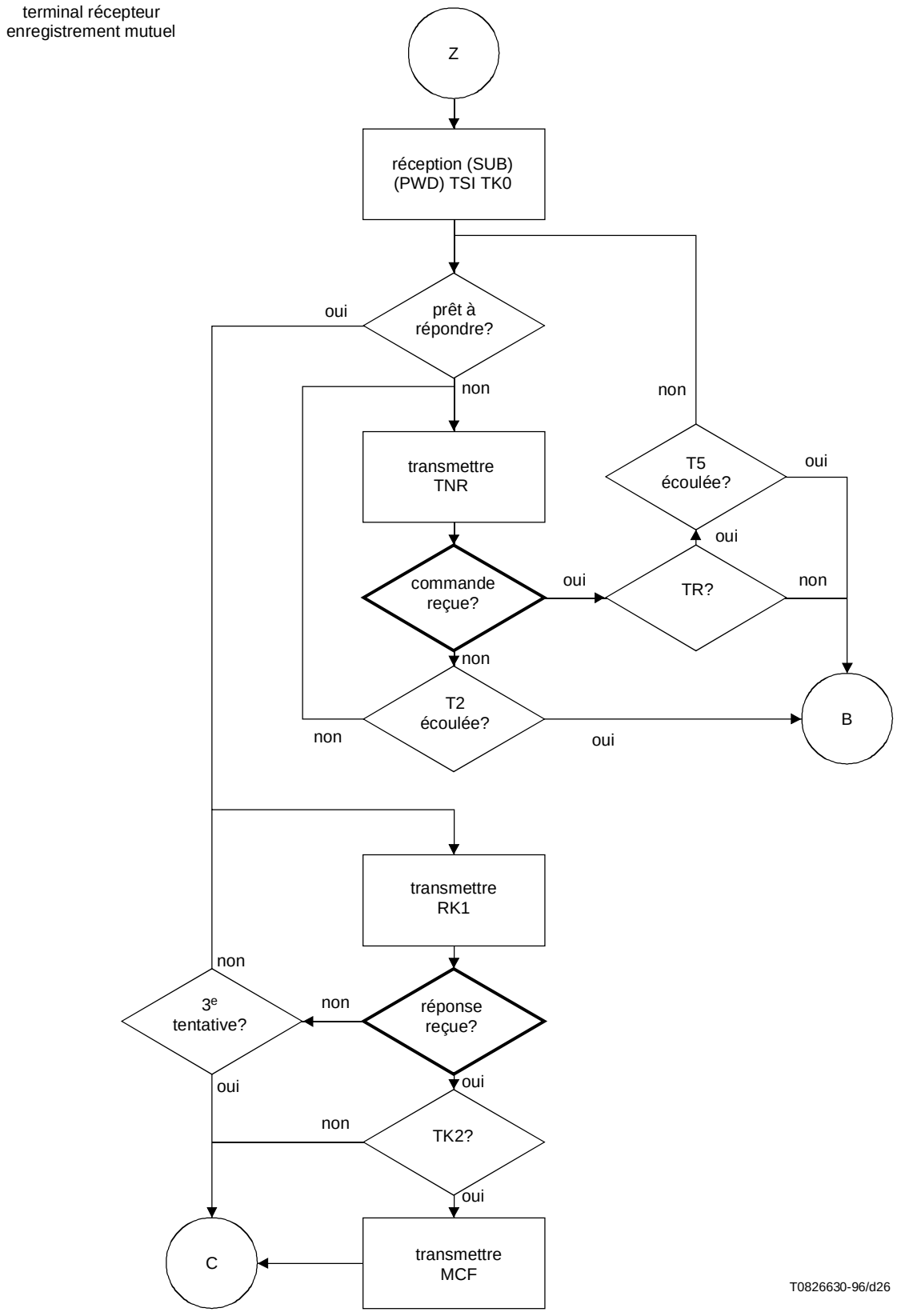


Figure G.8-3/T.30 (feuillet 2 de 3) (Utilisée à la place de la Figure C.12/T.30) mode duplex

terminal récepteur

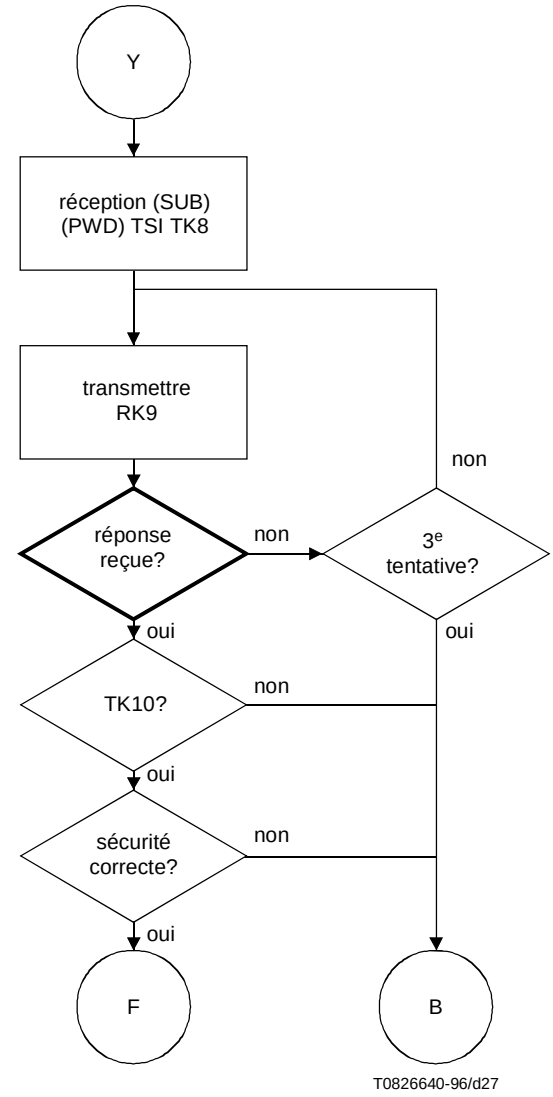


Figure G.8-3/T.30 (feuillet 3 de 3) (Utilisée à la place de la Figure C.12/T.30) mode duplex

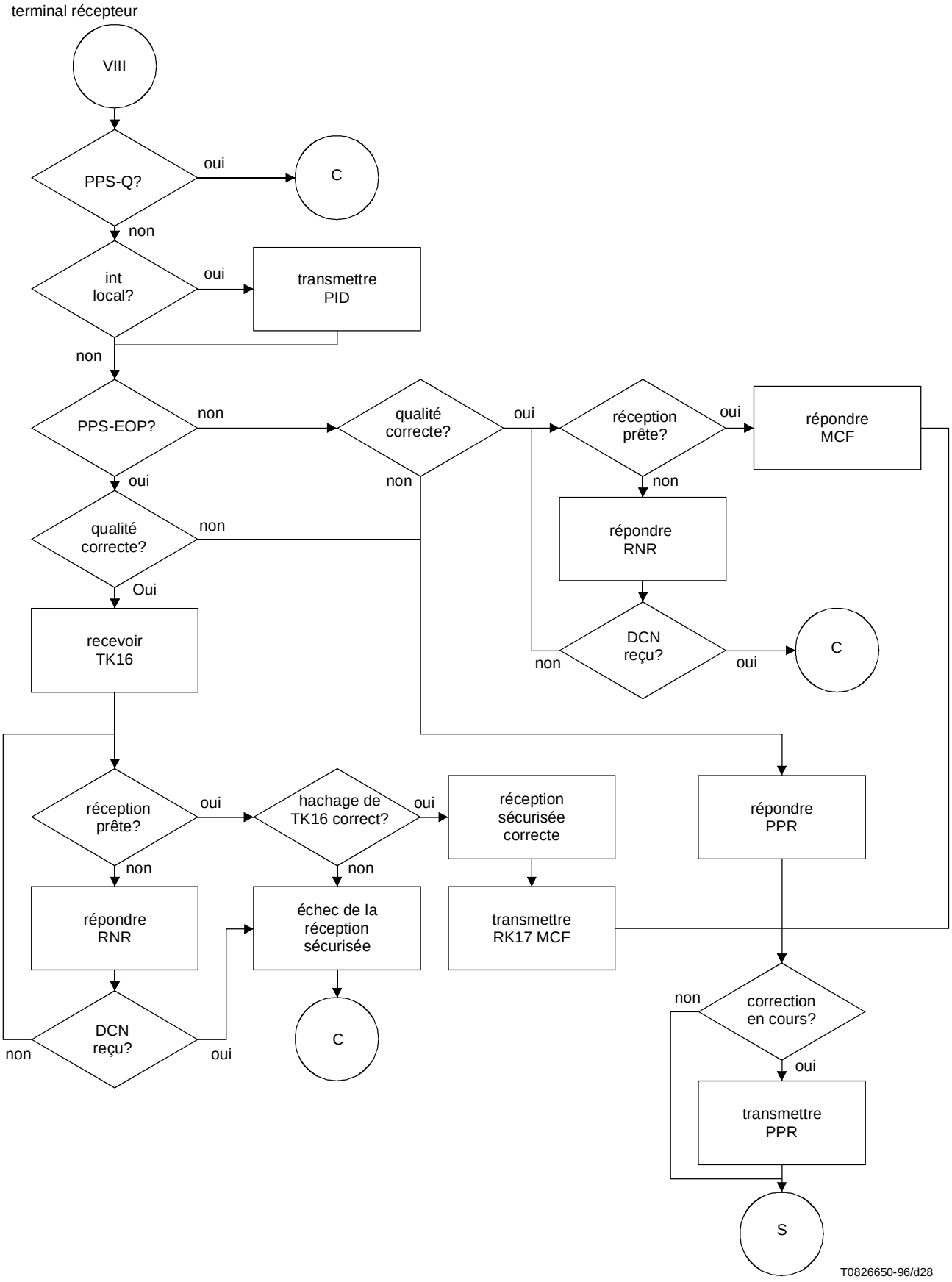


Figure G.8-4/T.30 (Utilisée à la place de la Figure C.13/T.30) mode duplex

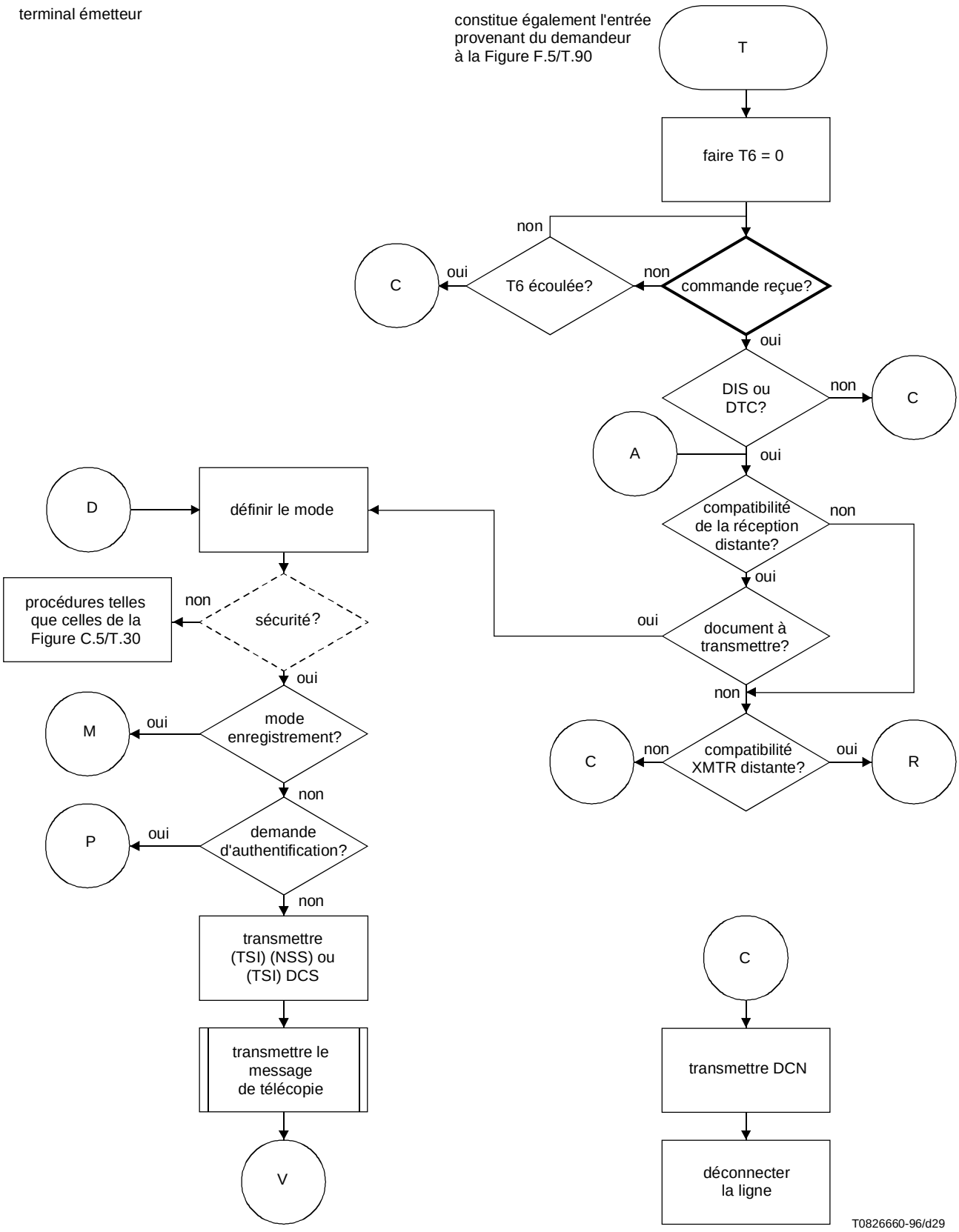


Figure G.8-5/T.30 (feuillet 1 de 3) (Utilisée à la place de la Figure C.14/T.30) mode duplex

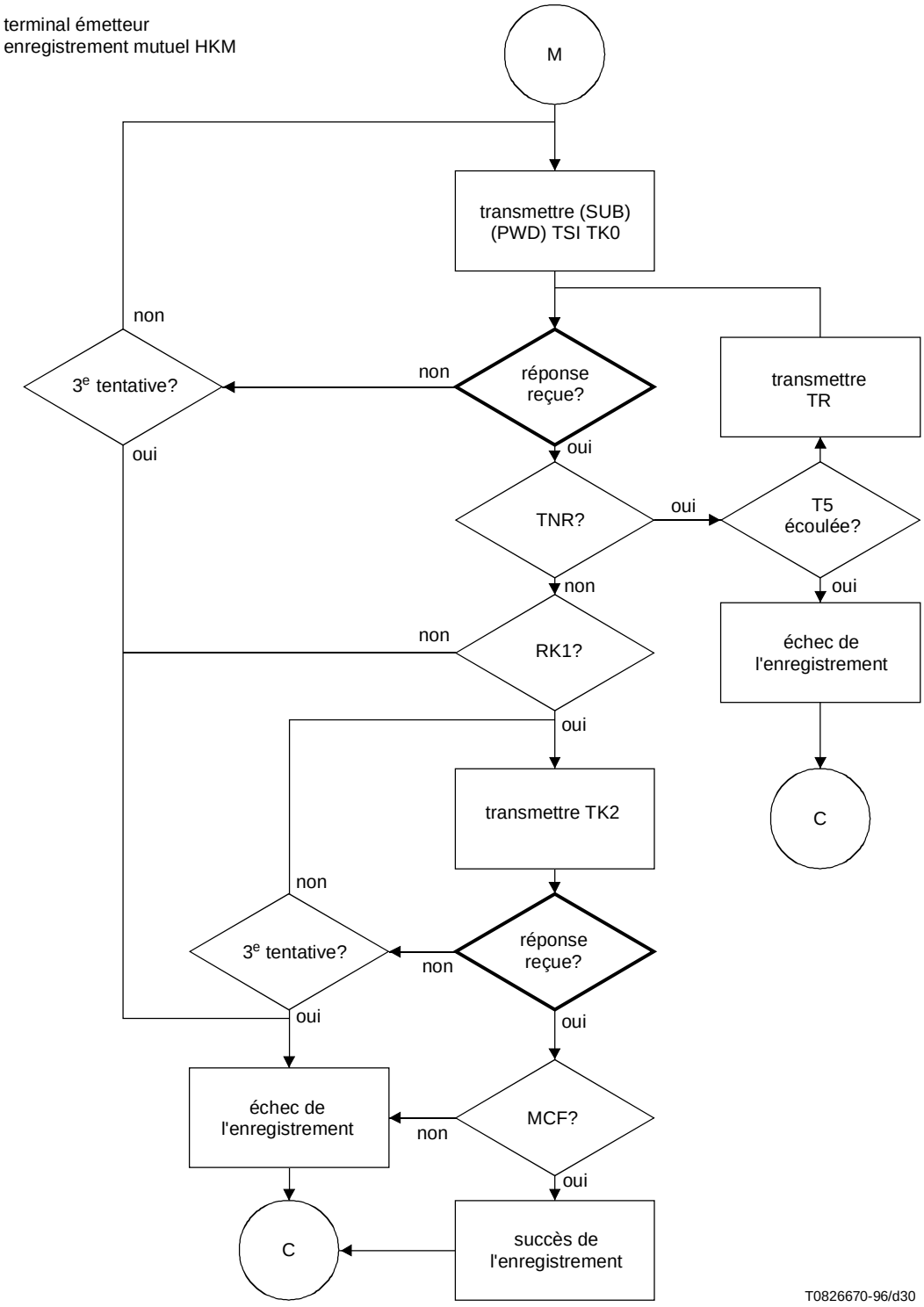


Figure G.8-5/T.30 (feuillet 2 de 3) (Utilisée à la place de la Figure C.14/T.30) mode duplex

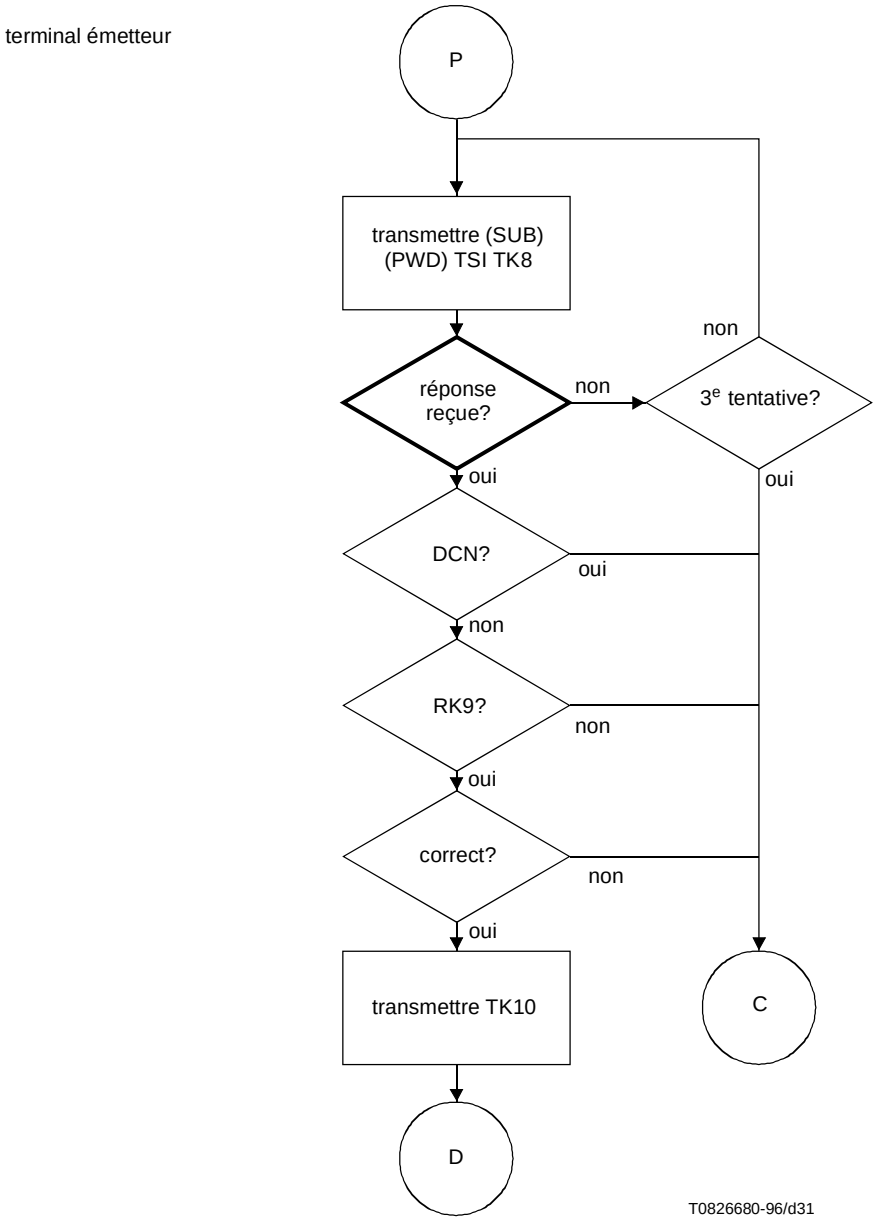


Figure G.8-5/T.30 (feuillet 3 de 3) (Utilisée à la place de la Figure C.14/T.30) mode duplex

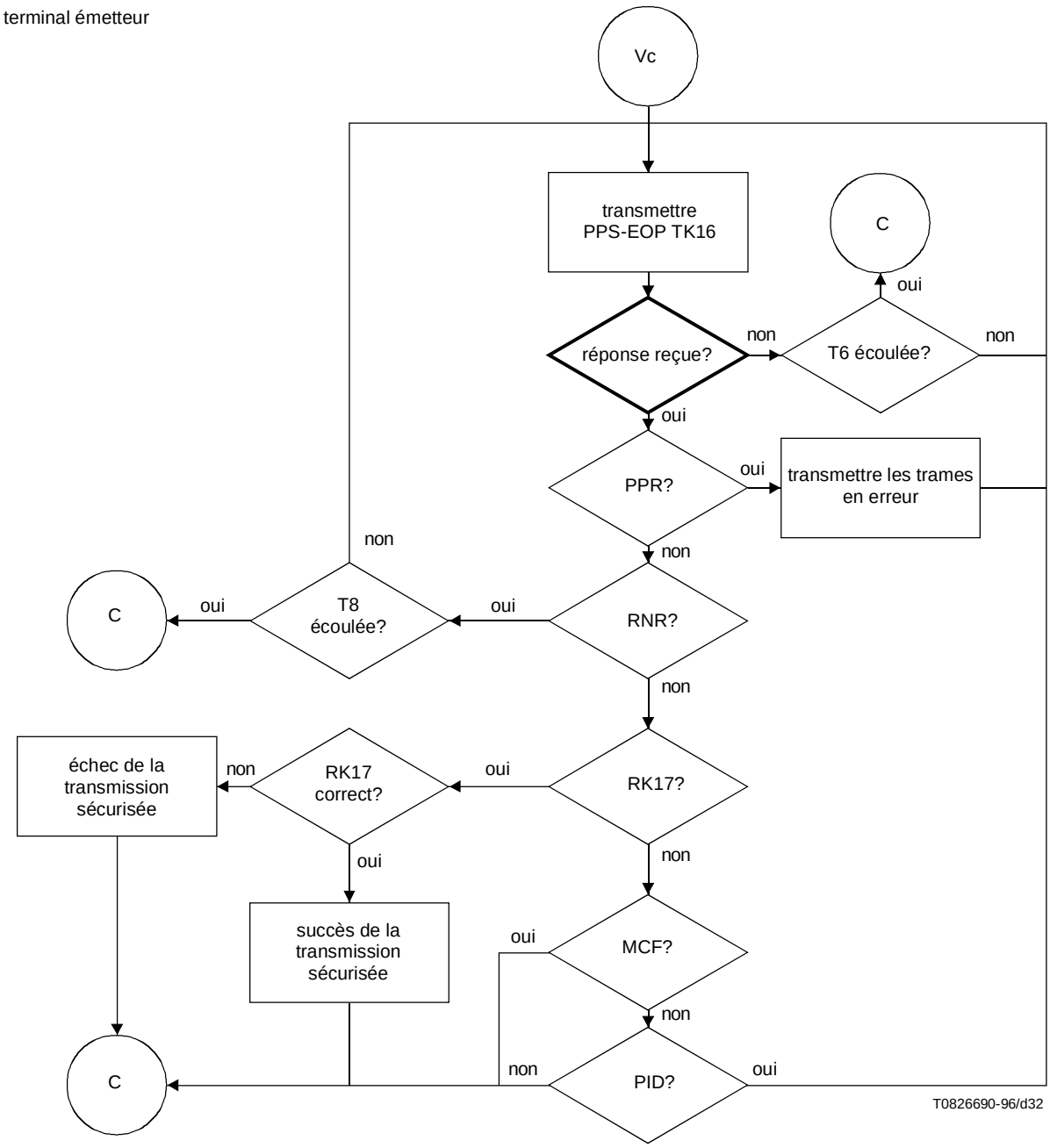


Figure G.8-6/T.30 (Utilisée à la place de la Figure C.18/T.30) mode duplex

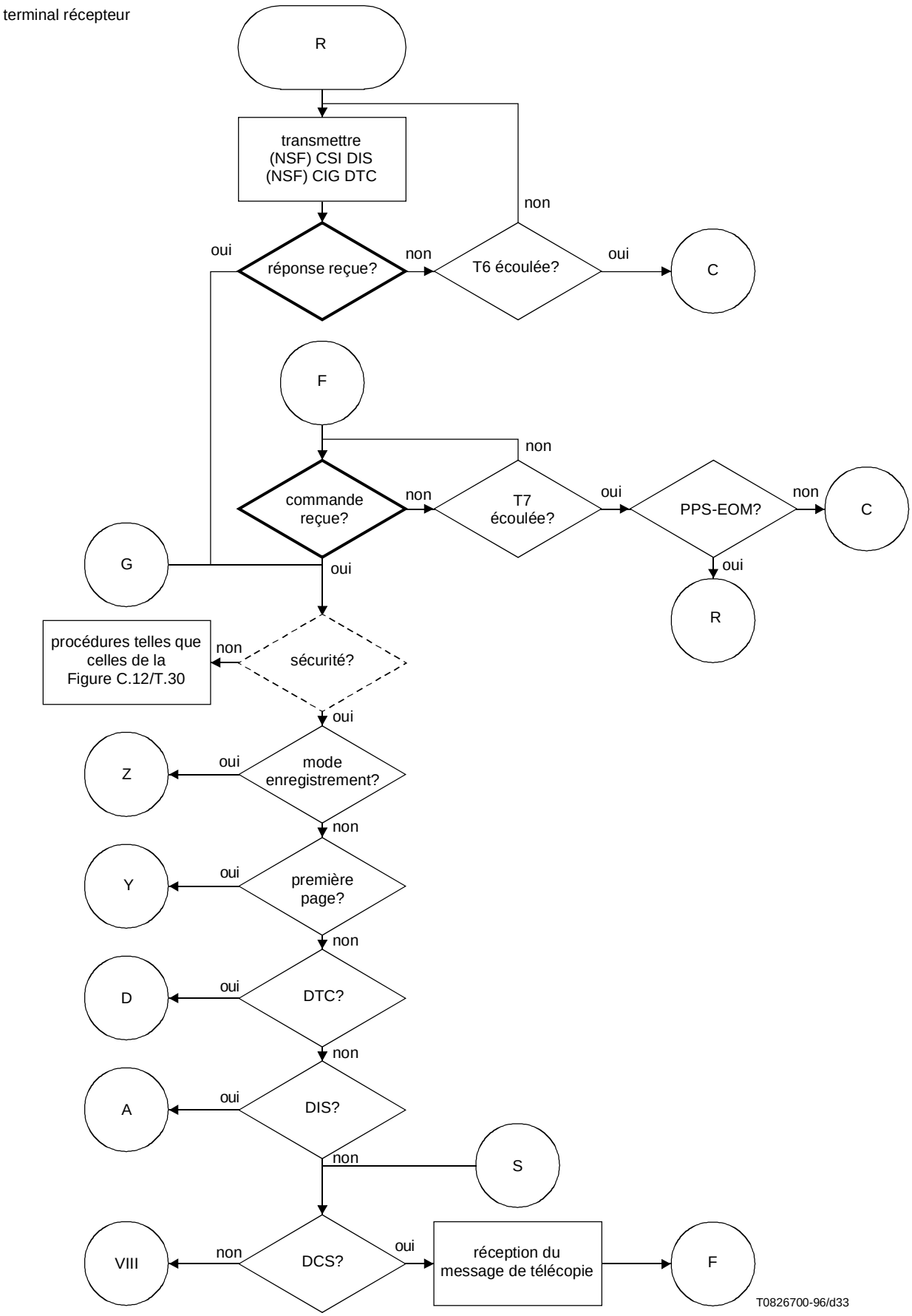


Figure G.8-7/T.30 (Utilisée à la place de la Figure C.21/T.30) mode duplex

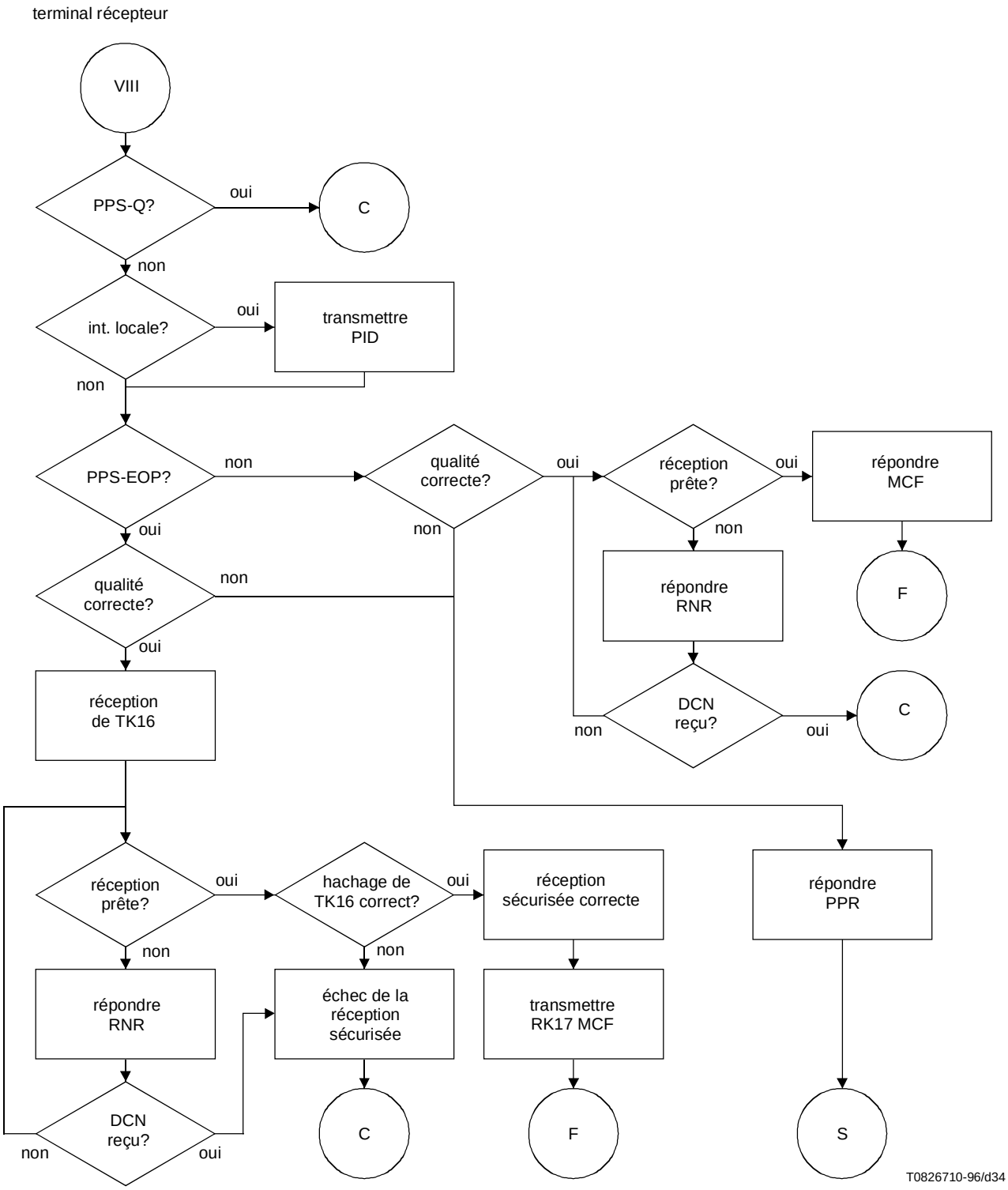


Figure G.8-8/T.30 (Utilisée à la place de la Figure C.22/T.30) mode duplex

G.8.2 Règles s'appliquant aux organigrammes

Les organigrammes suivent deux règles simples:

1) tous les traits ont une flèche pointée vers la destination uniquement;

2) les traits ne se croisent pas.

G.8.3 Temporisateurs utilisés dans les organigrammes

T1	35 s ± 5 s
T2	6 s ± 1 s
T3	10 s ± 5 s
T4	4,5 s ± 15% pour les postes manuels
T4	3,0 s ± 15% pour les postes automatiques
T5	60 s ± 5 s
T6	5 s ± 0,5 s
T7	6 s ± 1 s
T8	10 s ± 1 s
T9	durée de 256 drapeaux

G.8.4 Abréviations et descriptions utilisées dans les organigrammes

A moins que cela ait été défini différemment ci-dessous, la définition des termes de l'organigramme est donnée dans le corps de la Recommandation et/ou à l'Annexe A/T.30.

Authentification demandée? Vérifier que l'authentification mutuelle est nécessaire au début de la transmission.

NOTE 1 – Une fois que l'authentification mutuelle a été effectuée avec succès, la sortie "non" doit toujours être suivie pendant toute la session.

Mode enregistrement? Vérifier que l'enregistrement de sécurité est nécessaire.

Première page? Vérifier que l'authentification mutuelle est nécessaire au début de la transmission.

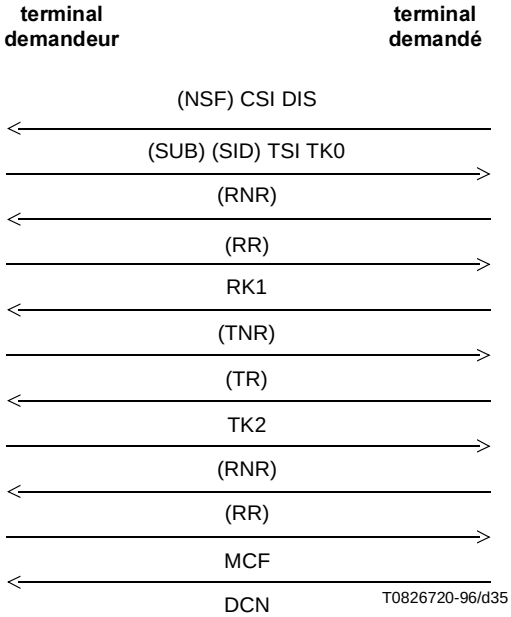
NOTE 2 – Une fois que l'authentification mutuelle a été achevée avec succès, la sortie "non" doit toujours être suivie pendant toute la session.

G.9 Exemples de séquences de signaux dans le cas de la procédure de télécopie

Les exemples de la Figure G.9-1/T.30-G.9-2/T.30 font référence aux organigrammes et sont donnés uniquement à des fins d'illustration et à des fins didactiques. Ils ne doivent pas être interprétés comme définissant ou limitant le protocole. L'échange des différents signaux et des différentes réponses est limité uniquement par les règles spécifiées dans la présente Recommandation.

NOTE – Les signaux de suspension RNR/RR et TNR/TR peuvent être utilisés à tout moment pour permettre à l'émetteur et au récepteur d'avoir le temps, pendant l'étape B et l'étape D, d'effectuer n'importe quel traitement impliquant le calcul de valeurs de sécurité ou permettant d'obtenir des clés à partir de l'enregistrement ou, dans le cas de l'enregistrement, à partir de l'opérateur.

G.9.1 Enregistrement mutuel HKM



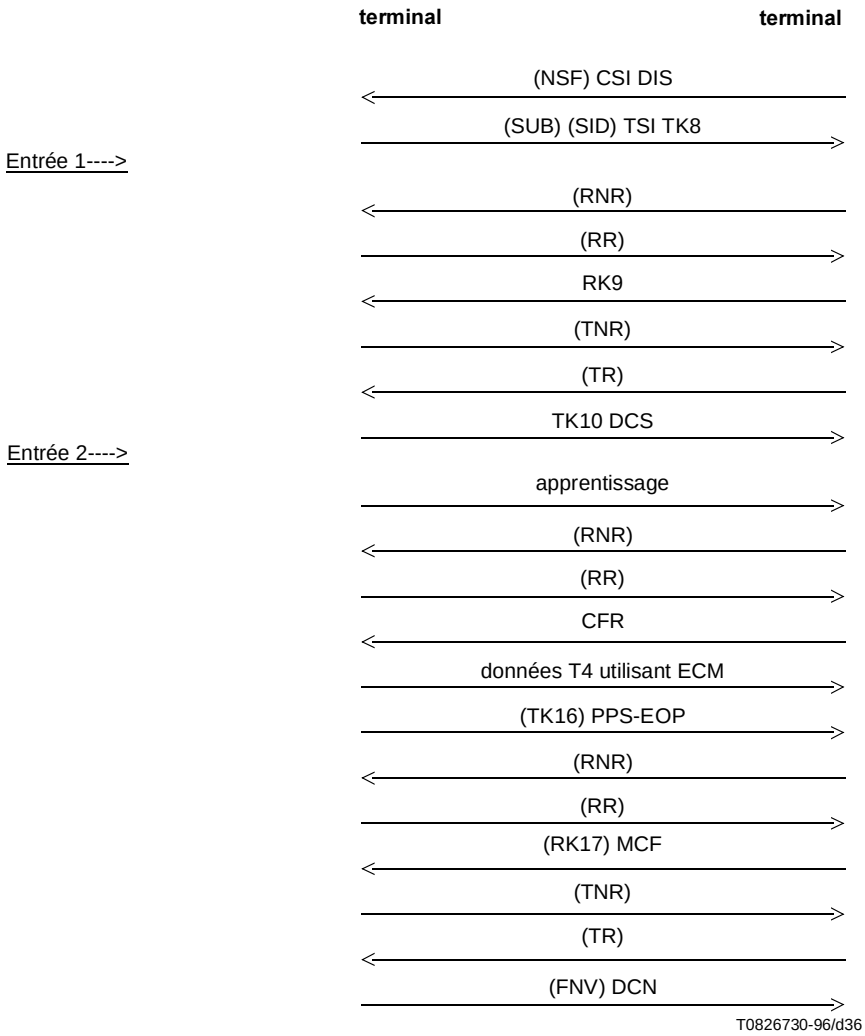
NOTE 1 – L'opérateur ou le terminal demandé peut avoir besoin de temps pour composer les chiffres de la clé utilisée une fois. S'ils sont composés manuellement, les signaux RNR et RR sont utilisés pour mettre le terminal demandeur en pause. Les signaux RNR et RR donnent une temporisation allant jusqu'à 65 secondes.

NOTE 2 – Le signal SUB peut être utilisé pour identifier un individu dans le domaine du terminal demandé pour lequel l'enregistrement est demandé.

NOTE 3 – Le signal d'identification de l'émetteur, ou SID, peut être utilisé pour identifier un individu dans le domaine du terminal demandeur à partir duquel l'enregistrement est demandé.

Figure G.9-1/T.30

G.9.2 Transmission sécurisée HKM avec chiffrement et hachage facultatifs



NOTE 1 – Le signal SUB peut être utilisé pour identifier un individu dans le domaine du terminal demandé pour recevoir le document de télécopie sécurisée.

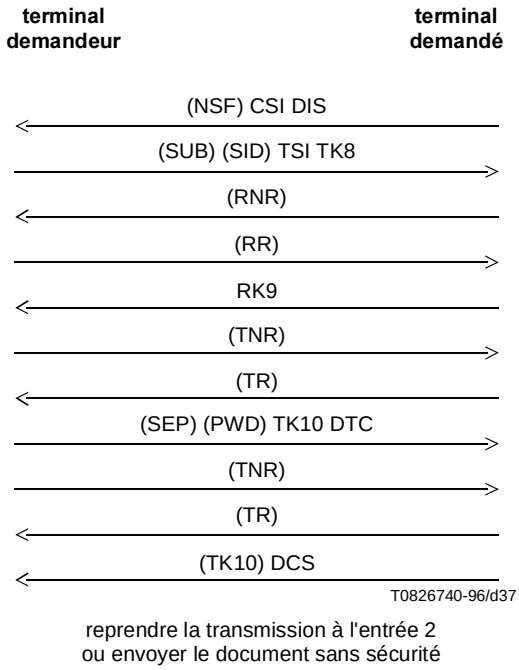
NOTE 2 – Le signal d'identification d'émetteur (SID) peut être utilisé pour identifier un individu dans le domaine du terminal demandeur qui envoie le document de télécopie sécurisée.

NOTE 3 – Les données devant être transmises doivent avoir exactement le format qu'elles auraient si le chiffrement n'était pas utilisé, c'est-à-dire normal y compris le remplissage, etc. Le chiffrement précède immédiatement la transmission effective de ces données. Le déchiffrement des données par le terminal récepteur est effectué immédiatement avant le traitement normal.

Figure G.9-2/T.30

G.9.3 Relève HKM sécurisée avec chiffrement et hachage facultatifs

Voir la Figure G.9-3/T.30.



NOTE 1 – Le signal SUB peut être utilisé pour identifier un individu dans le domaine du terminal demandé pour recevoir le document de télécopie sécurisée.

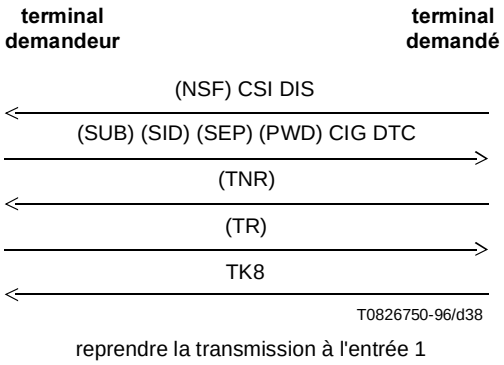
NOTE 2 – Le signal d'identification d'émetteur (SID) peut être utilisé pour identifier un individu dans le domaine du terminal demandeur qui envoie le document de télécopie sécurisée.

NOTE 3 – Les données devant être transmises doivent avoir exactement le format qu'elles auraient si le chiffrement n'était pas utilisé, c'est-à-dire normal y compris le remplissage, etc. Le chiffrement précède immédiatement la transmission effective de ces données. Le déchiffrement des données par le terminal récepteur est effectué immédiatement avant le traitement normal.

Figure G.9-3/T.30

G.9.4 Relève sécurisée HKM (déclenchée par le système de relève) avec chiffrement et hachage facultatifs

Voir la Figure G.9-4/T.30.



NOTE 1 – Le signal SUB peut être utilisé pour identifier un individu dans le domaine du terminal demandé pour fournir le document de télécopie sécurisée.

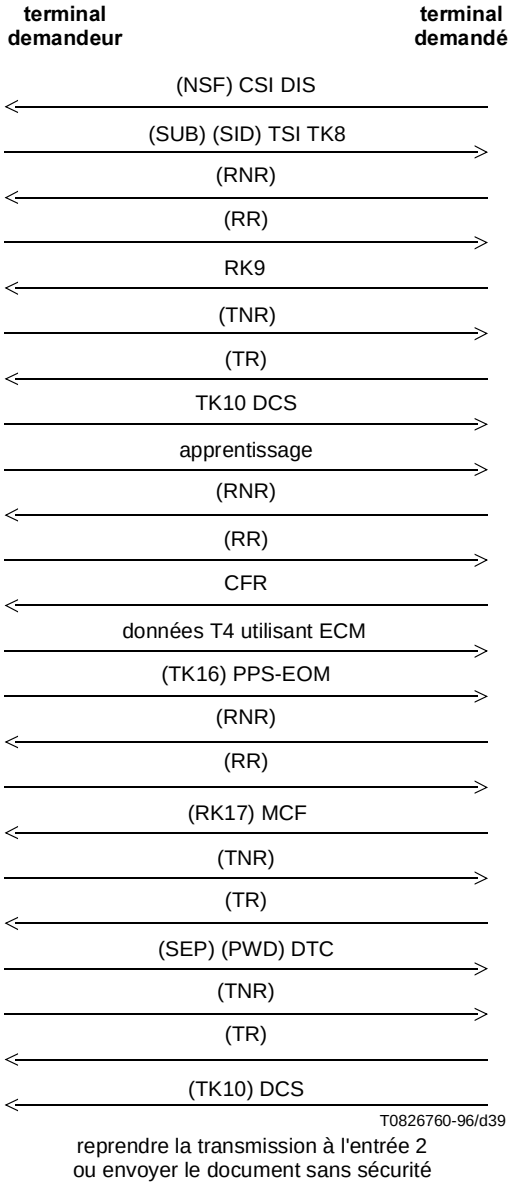
NOTE 2 – Le signal d'identification d'émetteur (SID) peut être utilisé pour identifier un individu dans le domaine du terminal demandeur qui relève le document de télécopie sécurisée.

NOTE 3 – Les données devant être transmises doivent avoir exactement le format qu'elles auraient si le chiffrement n'était pas utilisé, c'est-à-dire normal y compris le remplissage, etc. Le chiffrement précède immédiatement la transmission effective de ces données. Le déchiffrement des données par le terminal récepteur est effectué immédiatement avant le traitement normal.

Figure G.9-4/T.30

G.9.5 Relève cyclique HKM sécurisée avec chiffrement et hachage facultatifs

Voir la Figure G.9-5/T.30.



NOTE 1 – Le signal SUB peut être utilisé pour identifier un individu dans le domaine du terminal demandé pour recevoir le document de télécopie sécurisée.

NOTE 2 – Le signal d'identification d'émetteur (SID) peut être utilisé pour identifier un individu dans le domaine du terminal demandeur qui envoie le document de télécopie sécurisée.

NOTE 3 – Les données devant être transmises doivent avoir exactement le format qu'elles auraient si le chiffrement n'était pas utilisé, c'est-à-dire normal avec le remplissage, etc. Le chiffrement précède immédiatement la transmission effective de ces données. Le déchiffrement des données par le terminal récepteur est effectué immédiatement avant le traitement normal.

NOTE 4 – TK10 est facultatif et, le cas échéant, contiendra une nouvelle clé de session avec les valeurs réponses mises à zéro.

Figure G.9-5/T.30

3 Section 3

Ajouter une nouvelle Annexe H comme suit:

Annexe H

Sécurisation de la télécopie G3 sur la base de l'algorithme RSA

H.1 Préambule

(Le préambule est volontairement omis.)

H.2 Introduction

La présente annexe spécifie les mécanismes qui permettent de proposer des éléments de sécurité fondés sur l'usage du mécanisme cryptographique RSA. N'importe lequel des systèmes de codage définis dans les Recommandations T.4 et T.30 (Huffmann modifié, MR, MMR, mode caractères selon l'Annexe D/T.4, BFT, autre mode de transfert de fichier selon l'Annexe C/T.4, etc.) est applicable dans le cas d'un document transmis sous couvert d'éléments de sécurité.

H.3 Références normatives

– ISO/CEI 9796:1991, *Technologies de l'information – Techniques de sécurité – Schéma de signature numérique rétablissant le message*.

  Annexe A: RSA: R.L. Rivest, A. Shamir, L. Adleman: A method for obtaining digital signatures and public-key cryptosystems (Une méthode pour l'obtention de signatures numériques et de systèmes cryptographiques à clé publique), *CACM (Communications of the ACM*, Vol. 21, N° 2, p. 120-126, 1978).

– ISO/CEI 10118-3[1], *Technologies de l'information – Techniques de sécurité – Fonctions de brouillage – Partie 3: Fonctions de hachage dédiées*.

  Référence: ISO/CEI JTC 1/SC27 N1108:

  SHA-1 (Secure Hash Algorithm – Algorithme de hachage sûr), décrit dans *Secure Hash Standard,* FIPS (federal information processing standard) PUB 180-1, avril 1995, un algorithme en provenance du NIST (National Institute of Standardization), Etats-Unis d'Amérique.

– MD-5 (RFC 1321): *Message digest algorithm*.

– ISO/CEI 9979:1991, *Techniques cryptographiques – Procédures pour l'enregistrement des algorithmes cryptographiques*.

H.4 Mécanismes de sécurité

H.4.1 Mécanisme de signature numérique et gestion des clés

L'algorithme de base sur lequel est fondée la signature numérique (pour des services des types authentification et intégrité) est le **RSA**.

Le couple de clés utilisé à cette fin est "clé publique"/"clé secrète".

Lorsque le service facultatif de confidentialité est offert, le jeton qui contient la clé de session "Ks" utilisée pour chiffrer le document, est chiffré, lui aussi, par usage de l'algorithme RSA. Le couple de clés utilisé à cette fin, appelé "clé publique de chiffrement"/"clé secrète de chiffrement", n'est pas le même que celui qui sert aux services des types authentification et intégrité. Cette distinction a pour but de découpler les deux sortes d'usage.

L'implémentation du RSA qu'utilise la présente annexe est décrite dans l'ISO/CEI 9796 ("Schéma de signature numérique rétablissant le message").

---

[1] Actuellement à l'état de projet.

En ce qui concerne le chiffrement du jeton qui contient la clé de session, les règles de redondance applicables au traitement de l'algorithme RSA sont les mêmes que celles que spécifie l'ISO/CEI 9796.

NOTE – Certaines Administrations peuvent exiger qu'en plus du RSA, mécanisme de base dans le contexte de la présente annexe, soit implémenté un mécanisme facultatif, le DSA (norme de signature numérique).

Références

– ISO/CEI CD 14883-3:1995.

Référence: ISO/CEI JTC 1/SC27 N1113.

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

H.4.2 Longueurs des clés publiques, des clés secrètes et des signatures numériques

La caractéristique de base des clés publiques, des clés secrètes et des signatures numériques est d'avoir une longueur de **512 bits**. Des longueurs plus élevées sont possibles à titre facultatif. Elles sont alors négociées au moyen du protocole (voir ci-après).

H.4.3 Longueur de l'exposant public du RSA

Aux fins de signature numérique, la valeur de l'exposant est fixe et égale à 3.

Aux fins de chiffrement du jeton qui contient la clé de session "Ks", l'exposant public a une valeur fixe égale à $2^{16} + 1$. La clé de session sert en cas de chiffrement du document (voir ci-après).

H.4.4 Autorités de certification

Par défaut, il n'est pas fait appel à des autorités de certification.

Facultativement, il est permis de faire appel à des autorités de certification pour certifier la validité de la clé publique de l'émetteur du message de télécopie. Il est loisible en ce cas de certifier la clé publique selon les règles spécifiées dans la Recommandation X.509.

La présente annexe décrit les moyens à mettre en œuvre pour transmettre le certificat attaché à la clé publique de l'émetteur, mais le format précis du certificat est laissé pour étude ultérieure (il sera inclus dans des versions ultérieures de la présente annexe).

Le protocole permet de négocier la transmission effective du certificat.

H.4.5 Mode enregistrement

A titre de caractéristique **obligatoire**, il est fourni un *mode enregistrement.* Celui-ci donne à l'émetteur et au récepteur le moyen d'enregistrer et de conserver de manière fiable les clés publiques du partenaire avant que ne s'engage entre les deux partenaires la transmission sécurisée de télécopie.

Ce mode permet d'éviter que l'utilisateur n'ait à entrer manuellement les clés publiques du correspondant, qui sont assez longues (64 octets au moins).

Comme le mode enregistrement permet d'échanger les clés publiques et de les conserver dans les équipements terminaux, il n'est pas nécessaire de transmettre ces clés au cours des communications de télécopie.

Le mécanisme du mode enregistrement est détaillé plus loin dans la présente annexe.

H.4.6 Fonction de hachage

Ainsi que le décrit la présente annexe, certaines signatures s'appliquent au résultat d'une "fonction de hachage".

La fonction de hachage utilisée est soit le SHA-1 (algorithme de hachage sûr, *secure hash algorithm*, en provenance du NIST, aux Etats-Unis), soit le MD-5 (RFC 1321).

Dans le cas de SHA-1, la longueur du résultat du processus de hachage est de **160 bits**.

Dans le cas de MD-5, la longueur du résultat du processus de hachage est de **128 bits**.

Un équipement terminal est libre d'implémenter soit le SHA-1, soit le MD-5, soit les deux.

L'emploi de l'un ou l'autre algorithme fait l'objet de négociation dans le protocole (voir ci-après).

D'autres fonctions de hachage facultatives pourront être ajoutées dans l'avenir à la présente annexe.

H.4.7 Chiffrement

H.4.7.1 Généralités

Le chiffrement des données aux fins d'usage d'un service de confidentialité est facultatif. Dans le cadre de la présente annexe, sont enregistrés cinq mécanismes de chiffrement facultatifs:

FEAL-32, SAFER K-64, RC5, IDEA et HFX40 (selon la Recommandation T.36). Des règlements nationaux sont susceptibles d'en contraindre l'usage dans certains pays.

D'autres algorithmes facultatifs pourraient être enregistrés à l'avenir.

Il est aussi permis d'employer d'autres algorithmes facultatifs, choisis en accord avec l'ISO/CEI 9979 ("Procédure pour l'enregistrement des algorithmes cryptographiques").

La capacité que possède un équipement terminal à manipuler l'un de ces algorithmes ainsi que l'emploi effectif de l'un d'entre eux au cours d'une communication donnée font l'objet de négociation dans le protocole.

Une clé de session, appelée "**Ks**", est utilisée pour le chiffrement.

La longueur de base de la clé Ks est de 40 bits.

– Pour les algorithmes qui utilisent une clé de session de 40 bits (par exemple HFX40), la clé de session Ks est celle qui est effectivement utilisée dans l'algorithme de chiffrement.

– Pour les algorithmes qui nécessitent des clés d'une longueur supérieure à 40 bits (par exemple FEAL-32, IDEA, SAFER K-64 qui nécessitent des débits respectifs de: 64 bits, 128 bits et 64 bits), un mécanisme de redondance est mis en œuvre pour obtenir la longueur nécessaire. La clé ainsi obtenue est appelée la "clé de session redondante". La "clé de session redondante" est la clé qui est effectivement utilisée dans l'algorithme de chiffrement.

Le mécanisme de redondance est décrit dans le sous-paragraphe suivant.

Le jeton "BE" qui contient Ks (voir ci-après) est chiffré par la "clé publique de chiffrement" du récepteur et lui est envoyée par l'émetteur.

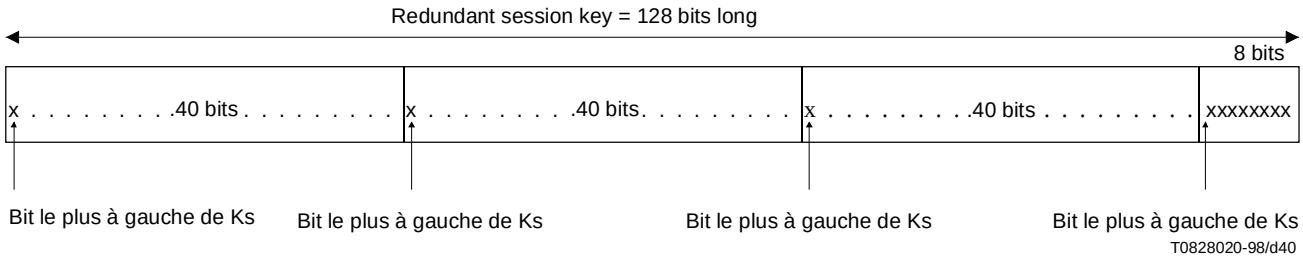
Lorsqu'une clé de redondance est nécessaire, le terminal de réception la régénère à partir du jeton "BE" reçu en provenance du terminal d'émission.

H.4.7.2 Mécanisme de redondance permettant d'obtenir la clé de session redondante lorsqu'il y a lieu

Lorsqu'une "clé de session redondante" est nécessaire (l'algorithme de chiffrement nécessitant une clé d'une longueur supérieure à 40 bits), cette entité est générée comme indiqué ci-dessous:

Le schéma de bits de Ks est répété autant de fois que nécessaire pour obtenir la longueur nécessaire voulue pour l'algorithme. Si besoin est, une partie du schéma de bits (commençant par le bit le plus à gauche) est ajoutée à la fin pour correspondre à la longueur correcte.

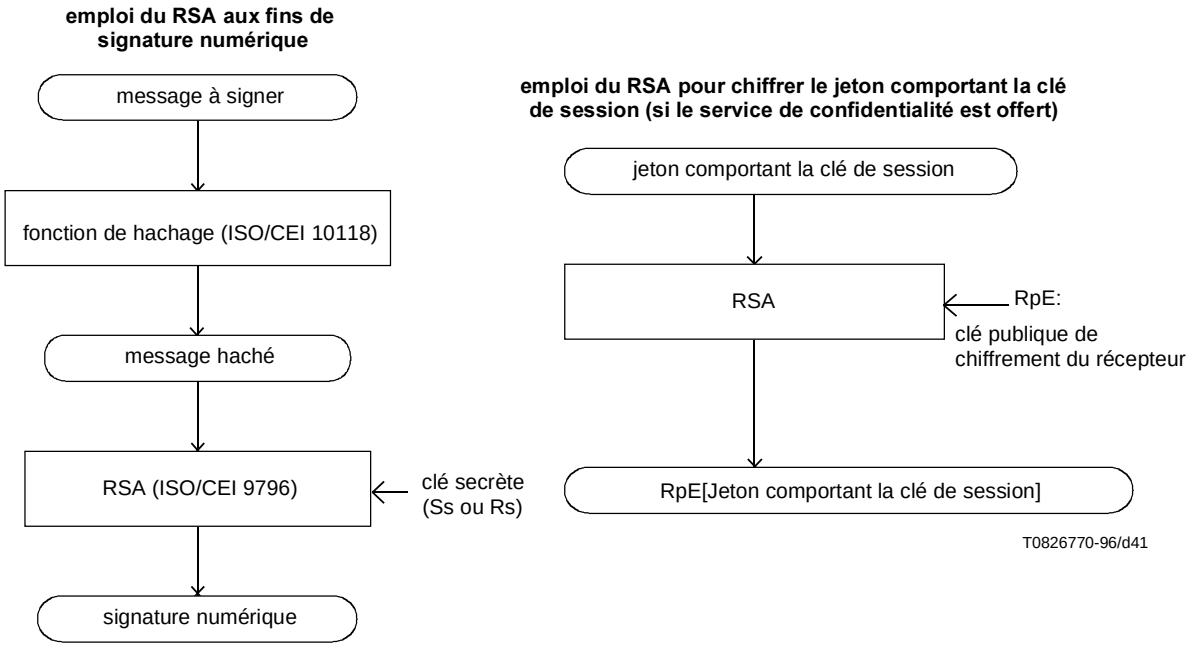
Ce principe est illustré sur l'exemple ci-dessous où l'algorithme exige 128 bits (par exemple IDEA).



H.4.8 Emploi de la fonction de hachage et de l'algorithme RSA

H.4.8.1 Mécanisme général

Voir la Figure H.1/T.30.



NOTE – L'ISO/CEI 9796 a été conçue afin de signer par le RSA un court élément de données qui est soit le message à signer (s'il est court), soit le résultat de hachage du message à signer (si le message est trop long), voir l'ISO/CEI 9796.

Figure H.1/T.30

H.4.8.2 Ordre de transmission des bits

Tout au long de la présente annexe:

1) toutes les séquences d'octets sont transmises de telle sorte que l'octet le plus à gauche (selon la représentation de la présente annexe) soit transmis en premier;

   la règle relative à la transmission des bits au sein de chaque octet est la suivante;

2) à l'exception du contenu du champ **FIF** des signaux DES, DEC, DER et DTR définis ci-après, les bits de chacun des octets représentés dans la présente annexe sont transmis de gauche à droite comme ils sont imprimés. Tel est le cas, par exemple, pour les codes du FCF;

3) en ce qui concerne le champ **FIF** des signaux DES, DEC, DER et DTR:

   3a) il existe une règle générale, qui est la suivante:

   le bit de plus faible poids de chaque octet est transmis en premier.

   En cas de numérotation dans les tableaux, le bit de plus faible poids est numéroté "bit nº 0".

   Par exemple, l'octet "1 0 1 1 0 0 1 1"

   numéroté (s'il l'est):

```
bit nº 7 6 5 4 3 2 1 0
       1 0 1 1 0 0 1 1
```

   sera transmis comme suit:

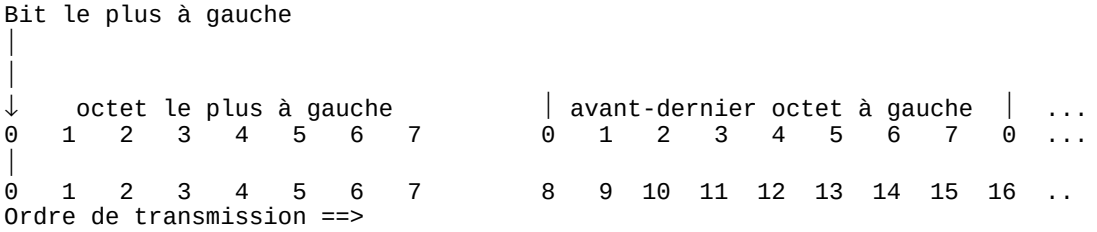
   Ordre de transmission ==>

   1 1 0 0 1 1 0 1

   3b) dans les cas où le contenu du champ FIF des signaux existants de T.30 est enchâssé au sein d'une structure étiquetée (voir H.6.1.4.7 "Supergroupe des trames enchâssées"), la cohérence est maintenue avec l'ordre de transmission des octets et des bits du champ FIF tel qu'il a été défini précédemment pour ces signaux (voir 5.3 et 5.3.6.2);

3c) au sein des champs FIF des signaux DES, DEC, DER et DTR, il existe une exception à la règle générale pour le cas de paramètres pour lesquels le Tableau H.1/T.30 indique "codage binaire". Pour ces paramètres, la règle suivante s'applique:

le premier bit transmis sur la ligne est le bit le plus à gauche de l'octet le plus à gauche:



H.4.8.3 Ordre des bits dans les processus de hachage et RSA

Les normes de fonctions de hachage (SHA-1 et MD-5) définissent une chaîne de bits à laquelle s'applique la fonction de hachage et une chaîne de bits qui constitue le résultat du hachage.

Le premier bit de ces chaînes est celui qui apparaît le plus à gauche dans les figures de ces normes.

La présente annexe définit divers paramètres auxquels s'applique la fonction de hachage. Certains résultats de hachage sont transmis sur la ligne. Les règles applicables à l'ordre des bits sur la ligne et à l'ordre des bits pour l'application de la fonction de hachage sont les mêmes:

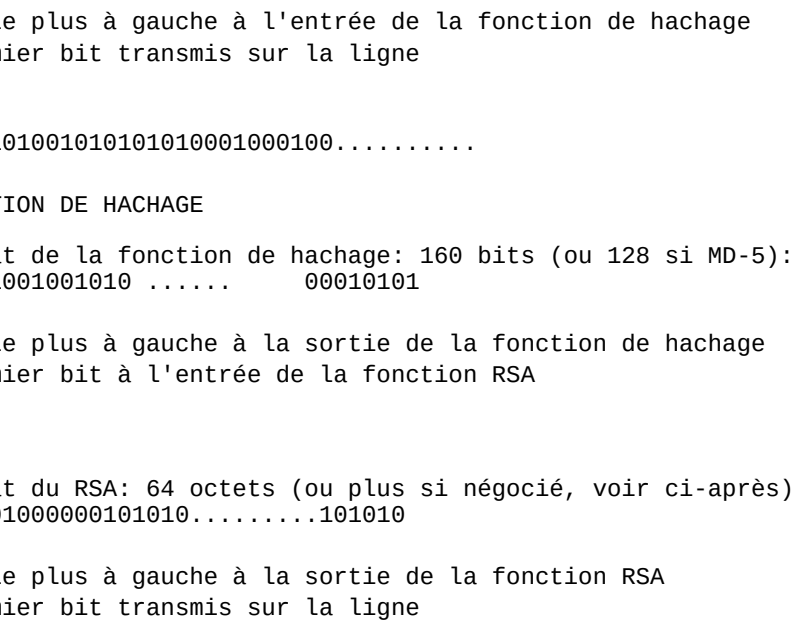
– le premier bit à passer dans la fonction de hachage est le bit le plus à gauche de l'octet le plus à gauche.

Si la fonction de hachage est appliquée à plusieurs entités concaténées, par exemple h(a,b,c,...), la chaîne de bits à hacher est la chaîne de bits [a] immédiatement suivie de la chaîne de bits [b], etc.

En ce qui concerne la fonction RSA, le même principe s'applique:

le premier bit à passer dans la fonction RSA est le bit le plus à gauche de l'octet le plus à gauche.

Le dessin suivant illustre l'ordre de passage des bits à travers les fonctions de hachage et RSA (les chaînes de bits représentées n'ont qu'une valeur d'exemple).



Le principe est valable aussi pour les paramètres qui entrent directement dans la fonction RSA sans passer par le hachage (par exemple le jeton qui comporte la clé de session "Ks").

Si le RSA est appliqué à plusieurs entités concaténées, par exemple (a,b,c,...), la chaîne de bits à traiter par le RSA est la chaîne de bits [a] suivie immédiatement de la chaîne de bits [b], etc.

H.5 Paramètres de sécurité

Le Tableau H.1/T.30 définit les divers paramètres de sécurité. Certains d'entre eux sont échangés entre les partenaires.

Il est défini pour tous les paramètres une longueur de base, qu'il est obligatoire de prendre en charge.

De plus, certains paramètres admettent des longueurs facultatives négociables dans le protocole.

Le Tableau H.1/T.30 indique aussi le type de codage (binaire, ASCII, etc.) applicable aux paramètres.

Plus loin, la présente annexe spécifie comment sont transportés ces paramètres dans les signaux DES, DEC, DER et DTR.

Tableau H.1/T.30 – Paramètres de sécurité

Abréviation	Description	Longueur de base	Plus grandes longueurs facultatives	Codage du champ
S	identité de l'émetteur	20 octets	pour étude ultérieure	codage IA5 (Note 1)
Sp	clé publique de l'émetteur	64 octets	possible	codage binaire (Note 2)
Ss	clé secrète de l'émetteur	64 octets	comme Sp	codage binaire (Note 2)
SpE	clé publique de chiffrement de l'émetteur (pour le chiffrement du jeton comportant la clé de session)	64 octets	possible	codage binaire (Note 2)
SsE	clé secrète de chiffrement de l'émetteur (pour le déchiffrement du jeton chiffré comportant la clé de session)	64 octets	comme SpE	codage binaire (Note 2)
Sra	nombre aléatoire créé par l'émetteur aux fins d'authentification du récepteur	8 octets	possible	codage binaire (Note 2)
Srd	nombre aléatoire créé par l'émetteur aux fins de signature numérique	8 octets	possible	codage binaire (Note 2)
R	identité du récepteur	20 octets	pour étude ultérieure	codage IA5 (Note 1)
Rp	clé publique du récepteur	64 octets	possible	codage binaire (Note 2)
Rs	clé secrète du récepteur	64 octets	comme Rp	codage binaire (Note 2)
RpE	clé publique de chiffrement du récepteur (pour le chiffrement du jeton comportant la clé de session)	64 octets	possible	codage binaire (Note 2)
RsE	clé secrète de chiffrement du récepteur (pour le déchiffrement du jeton chiffré comportant la clé de session)	64 octets	comme RpE	codage binaire (Note 2)
Rra	nombre aléatoire créé par le récepteur aux fins d'authentification de l'émetteur	8 octets	possible	codage binaire (Note 2)
Ks	clé de session	40 bits	pour étude ultérieure	codage binaire (Note 2)
BE	BE = RpE[S, Ks] = chiffrement par RpE de la concaténation de l'identité de l'émetteur et de la clé de session	64 octets	comme RpE	codage binaire (Note 2)
UTCd	date/heure choisies par l'émetteur (date et heure de création et signature du document)	8 octets	pour étude ultérieure	YY MM DD HH MM SS décalage GMT codage BCD (Note 3)
UTCr	date/heure choisies par le récepteur (date et heure de confirmation de réception du message)	8 octets	pour étude ultérieure	YY MM DD HH MM SS décalage GMT codage BCD (Note 3)
Lm	longueur du document	4 octets	pour étude ultérieure	correspond au nombre d'octets de la totalité du document transmis (données + bits de remplissage, voir H.6.5/T.30) codage BCD (Note 4)

Tableau H.1/T.30 – Paramètres de sécurité *(fin)*

Abréviation	Description	Longueur de base	Plus grandes longueurs facultatives	Codage du champ
h(...)	résultat du hachage de l'entité entre parenthèses	160 ou 128 bits selon la fonction de hachage choisie	pour étude ultérieure	codage binaire (Note 2)
Rs[h(...)]	signature par le récepteur du résultat du hachage de l'entité entre parenthèses	64 octets	comme Rp	codage binaire (Note 2)
Ss[h(...)]	signature par l'émetteur du résultat du hachage de l'entité entre parenthèses	64 octets	comme Sp	codage binaire (Note 2)
Sia	indicateur dans le jeton utilisé pour l'authentification de l'émetteur	1 octet	non	octet égal à: "00000000" (Note 5)
Ria	indicateur dans le jeton utilisé pour l'authentification du récepteur	1 octet	non	octet égal à: "00000001" (Note 5)
Sis	indicateur dans le jeton utilisé pour la signature numérique	1 octet	non	octet égal à: "00000010" (Note 5)
Ris	indicateur dans le jeton utilisé pour la confirmation de réception du message	1 octet	non	octet égal à: "00000011" (Note 5)
document	document envoyé en mode transmission sécurisée de télécopie	variable	non applicable	non applicable
document chiffré	document envoyé en mode transmission sécurisée de télécopie lorsque est invoqué le service de confidentialité. Le chiffrement du document utilise la clé de session Ks (ou la clé de session redondante si l'algorithme nécessite pour fonctionner plus de bits que la clé Ks)	variable	non applicable	non applicable

NOTE 1 – La règle générale relative au FIF de DES/DEC/DER/DTR s'applique: le bit de plus faible poids de chaque octet est transmis en premier.

NOTE 2 – La règle applicable à la transmission des éléments codés en binaire est donnée au H.4.8.2/T.30.

NOTE 3 – Exemple: pour le 24 mars 1995, 8 h 25 05 s, après-midi, décalage 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
```

La règle générale relative au FIF de DES/DEC/DER/DTR s'applique: le bit le plus à droite de chaque octet est transmis en premier.

NOTE 4 – Exemple: pour un document d'une longueur de 123456 octets:

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

La règle générale relative au FIF de DES/DEC/DER/DTR s'applique: le bit le plus à droite de chaque octet est transmis en premier.

NOTE 5 – La règle générale relative au FIF de DES/DEC/DER/DTR s'applique: le bit le plus à droite de chaque octet est transmis en premier.

H.6 Echange des paramètres de sécurité

Le mode correction d'erreurs (ECM) décrit à l'Annexe A/T.30 doit être employé pour pouvoir offrir des services de sécurité fondés sur le RSA.

Il est nécessaire de transmettre certains paramètres de sécurité pendant la communication de télécopie au niveau du protocole (étapes B et D du protocole T.30). A titre facultatif (voir plus loin "page sécuritaire"), certains paramètres de sécurité sont transmis au niveau du message (étape C du protocole T.30).

H.6.1 Echange de paramètres de sécurité au niveau du protocole

Les huit nouveaux signaux employés sont les suivants:

– DER: demande numérique enrichie (*digital extended request*)

Cette commande est envoyée par le terminal émetteur. Elle a le pouvoir d'établir des paramètres de sécurité pour la session; elle peut aussi demander des détails complémentaires sur les capacités du dispositif récepteur en matière de sécurité.

– DES: signal numérique enrichi (*digital extended signal*)

Cette commande est envoyée par le dispositif récepteur; elle en donne les capacités en matière de sécurité.

– DEC: commande numérique enrichie (*digital extended command*)

Cette commande est envoyée par le terminal émetteur en réponse à DES ou à DTR.

Elle contient toutes les valeurs établies pour la communication en cours.

DEC remplace DCS qui n'est pas émis. L'information normalement contenue dans le FIF de DCS se trouve dans DEC. DEC contient aussi les divers paramètres de sécurité envoyés du terminal émetteur au terminal récepteur.

– DTR: demande numérique de retournement (*digital turnaround command*)

Cette commande peut être envoyée par le terminal appelant en réponse à DIS ou à DES. Elle s'emploie pour demander une relève ou retourner la transmission.

DTR remplace DTC qui n'est pas émise. L'information normalement contenue dans le FIF de DTC se trouve dans DTR. DTR contient aussi les divers paramètres de sécurité envoyés du terminal récepteur au terminal émetteur.

– DNK: accusé de non-réception numérique (*digital not acknowledge*)

DER, DES, DEC et DTR sont structurés sous forme de trames HDLC.

DNK indique que la commande précédente (DER, DES, DEC ou DTR) n'a pas été reçue de manière satisfaisante et qu'il est nécessaire de retransmettre les trames spécifiées dans le FIF de DNK. Aussi bien le terminal émetteur que le terminal récepteur a le droit d'émettre DNK (contrairement à PPR de l'Annexe A/T.30 qui ne peut être émis que par le terminal émetteur).

DNK sert aussi à rejeter TCF.

– TNR: transmetteur non prêt (*transmitter not ready*)

Ce signal sert à indiquer que le transmetteur n'est pas encore prêt à transmettre.

Format:

FCF: X101 0111 (X est le bit défini au 5.3.6.1/T.30).

– TR: transmetteur prêt? (*transmitter ready?*)

Ce signal sert à demander l'état du transmetteur.

Format:

FCF: X101 0110 (X est le bit défini au 5.3.6.1/T.30).

– PPS-PSS: signal de page partielle-signal de signature présente (*partial page signal-present signature signal*)

Ce signal sert à indiquer une fin du document suivie de signature numérique.

Format:

FCF1: X111 1101 (X est le bit défini au 5.3.6.1/T.30).

FCF2: 1111 1000.

De plus amples renseignements sur le codage particulier de DER, DES, DEC, DTR et DNK sont donnés dans la présente annexe.

H.6.1.1 Structure de DER, DES, DEC et DTR

H.6.1.1.1 Généralités

Les signaux DER, DES, DEC et DTR sont structurés sous forme de trames HDLC.

La structure de la séquence de trames respecte les mêmes règles que celles déjà établies pour les commandes multitrames dans la Recommandation T.30 (par exemple pour NSF-CSI-DIS). Ces règles sont décrites aux 5.3.1, 5.3.3, 5.3.4 et 5.3.5 de la Recommandation T.30.

H.6.1.1.2 FCF (champ de commande de télécopie, *facsimile control field*)

Le FCF des trames est:

– trames DES: 0000 0101

– trames DEC: 1100 1001

– trames DER: 1100 1010

– trames DTR: 1000 1000

H.6.1.1.3 FIF (champ d'information de télécopie, *facsimile information field*)

Dans le contexte de l'Annexe H, les spécifications applicables au FIF de DES, DEC, DER et DTR sont les suivantes:

La longueur maximale du FIF d'une trame est de 65 octets. Si une trame est une trame intermédiaire (pas la dernière), son FIF doit avoir une longueur de 65 octets, **sauf lorsque le contenu de la trame est "FIF de DCS"** (voir ci-après). Dans ce dernier cas, la trame n'a que la longueur nécessaire pour contenir les octets du FIF, mais pas plus (aucun octet de remplissage n'est autorisé).

S'il s'agit de la dernière trame, la longueur du FIF peut être inférieure à 65 octets en fonction du nombre d'octets de données à transporter. Aucun octet de remplissage n'est autorisé.

Le premier octet du FIF de chaque trame contient le numéro de trame, puis vient le champ de données. Le numéro de trame est un nombre binaire de huit bits. La règle générale relative au FIF de DES/DEC/DER/DTR est applicable: le bit de plus faible poids du numéro de trame (bit le plus à droite) est transmis en premier.

La trame numérotée "0" est transmise la première.

Ces principes sont illustrés dans la Figure H.2/T.30.

NOTE – L'usage de trames transportant un FIF qui dépasserait 65 octets est pour étude ultérieure.

Préambule	Adresse HDLC	Champ de commande	Champ de commande de télécopie	FIF		FCS	Fanion(s)	Adresse HDLC	Champ de commande	Champ de commande de télécopie	FIF		FCS	Fanion(s)
fanions	1111 1111	1100 X000 X = 0 (trame non finale)	DEC = 1100 1001	numéro de trame 0000 0000	champ de données 64 octets	FCS	au moins un fanion	1111 1111	1100 X000 X = 1 (trame finale)	DEC = 1100 1001	numéro de trame 0000 0001	champ de données ≤ 64 octets	FCS	au moins un fanion

NOTE 1 – Le FCF est transmis comme le présente la figure: le bit le plus à gauche est transmis en premier.

NOTE 2 – Le numéro de trame est transmis en sens inverse de la présentation sur la figure: le bit le plus à droite est transmis en premier.

Dans l'exemple, pour le numéro de trame de la seconde trame:

1000 0000

ordre de transmission ==>

NOTE 3 – **Le champ de données de la trame "0" peut comporter moins de 64 octets s'il contient le "FIF de DCS".**

Figure H.2/T.30 – Exemple d'un DEC constitué de deux trames

H.6.1.2 Usage et structure de DNK

H.6.1.2.1 Structure de DNK

Définition

Dans la suite de la présente annexe, les expressions "signal X" ou "X" désignent l'un des signaux DER, DES, DEC ou DTR.

DNK permet de demander la retransmission particulière de trames de "signal X" dans lesquelles des erreurs sont détectées à la réception.

DNK sert aussi à rejeter TCF (voir ci après).

NOTE – Lorsque toutes les trames d'un signal X ont été reçues correctement, la réponse normale que spécifie la présente annexe sert d'accusé de réception implicite, sauf s'il est nécessaire de rejeter TCF. DNK sert à ce rejet.

DNK consiste en une trame HDLC dont la structure respecte les mêmes règles que celles qui s'appliquent aux autres signaux de T.30 (ces règles sont décrites aux 5.3.1, 5.3.3, 5.3.4 et 5.3.5 de la Recommandation T.30).

H.6.1.2.2 FCF de DNK

Le FCF est: X101 1001

La définition du bit X se trouve au 5.3.6.1/T.30.

H.6.1.2.3 FIF de DNK

H.6.1.2.3.1 Généralités

Le FIF comporte un nombre entier d'octets.

Pour chaque octet du FIF de DNK, le bit le plus à gauche du texte imprimé est transmis en premier. Il porte le numéro de bit "0".

L'ordre de transmission correspondant à la numérotation des bits est:

numéro de bit 01234567 01234567 01234567 ...

ordre de transmission ========>

Le premier octet de DNK sert à rejeter TCF en cas de besoin (si TCF est corrompu à la réception).

Les autres octets servent à demander la retransmission des trames incorrectement reçues.

H.6.1.2.3.2 Nouvelle demande de trames incorrectement reçues

Dès le début du second octet du FIF, chaque bit correspond à une trame de la commande ou de la réponse émise précédemment: le premier bit correspond à la première trame, etc. Pour les trames bien reçues, le bit correspondant sera obligatoirement mis à "0". Les bits correspondant aux trames incorrectement reçues seront obligatoirement mis à "1". Des bits de remplissage de valeur "1" seront ajoutés si nécessaire pour respecter l'alignement avec la frontière du dernier octet.

Comme dans le mode ECM que décrit l'Annexe A/T.30, mais ici à la vitesse de modulation du protocole, si plus d'un DNK est transmis (à la suite d'une série de tentatives infructueuses de transmission de trames X), le bit correspondant à une trame X qui a déjà été reçue correctement doit toujours être mis à "0".

NOTE 1 – Il peut arriver que DNK soit émis à nouveau avec un FIF de taille différente.

Soit par exemple un signal X si fortement corrompu à la réception qu'il semble ne contenir que 7 trames alors qu'il a en réalité une longueur de 9 trames. En ce cas, le FIF de DNK ne contiendra que deux octets (le premier servant à rejeter le TCF – voir ci-après – et le second qui suffit à indiquer les trames trouvées erronées). Après retransmission du signal X, l'équipement récepteur découvre que le signal X a une longueur de 9 trames. S'il arrive encore que des trames soient erronées, un nouveau DNK avec un FIF de 3 octets est émis. Cet exemple est illustré ci-dessous.

NOTE 2 – Il est à noter que le terminal qui reçoit le signal X est en mesure de localiser la dernière trame au moyen du bit "x" du champ de commande HDLC dont la valeur est "1".

Exemple avec un DEC incorrectement reçu (les mêmes principes s'appliquent en cas de corruption des signaux DES, DER ou DTR)

---------->

DEC

9 trames <----------

DNK avec un FIF long de 2 octets:

```
Bit n°   0123   4567   01234567
         xxxx   xxx0   10101111
```

premier octet: rejet de TCF
(voir explication ci-après)
trames 0, 2, 4, 5 et 6 incorrectement reçues
trames 7 et 8 non reçues
(le dernier bit à "1" ne sert qu'à l'alignement de l'octet)

---------->

DEC

trames 0, 2, 4, 5, 6, 7 et 8 <----------

DNK avec un FIF long de 3 octets:

```
Bit n°   0123   4567   01234567  01234567
         xxxx   xxx0   10000000  01111111
```

seule la trame 0 est incorrectement reçue

---------->

DEC

trame 0 <----------

trame correctement reçue
réponse normale = accusé de réception implicite
(dépendant du contexte)

H.6.1.2.3.3 Période maximale de retransmission de signal X sur occurrence de DNK

En ce qui concerne la retransmission de signal X sur occurrence de DNK, il est défini un temporisateur Tx de "défaillance sécurisée".

– Le temporisateur Tx est défini de la manière suivante:

  Tx = 60 s ± 5 s.

– Le transmetteur du signal X démarre le temporisateur Tx lorsqu'il reconnaît DNK pour la première fois. Il l'arrête lorsqu'il reconnaît la réponse normale ou FNV.

– En cas d'expiration du temporisateur Tx, l'émetteur du signal X envoie une commande DCN pour libérer la communication.

H.6.1.2.3.4 Rejet spécifique par DNK

Le bit le plus à gauche du premier octet du FIF de DNK (numéroté "n° 0" dans le Tableau H.2/T/30) sert à rejeter le TCF (TCF corrompu). Ce rôle équivaut à celui de FTT en T.30 normal.

Il est impossible de combiner le rejet de TCF défini par le Tableau H.2/T.30 avec l'indication de réception erronée de trames X que définit le H.6.1.2.3.2/T.30.

Le processus de rejet se déroule selon la séquence suivante:

1) dans un premier temps, toutes les trames altérées du signal DEC (DES, DER ou DTR) sont demandées par le signal DNK. Le bit 7 et le bit 0 du premier octet du signal DNK sont mis à "0" (le bit 0 n'étant pas significatif à ce stade);

2) une fois que toutes les trames ont été corrigées, le contenu du signal DEC (DES, DER ou DTR) peut être rejeté par FNV si besoin est (voir ci-après).

   Si le contenu de DEC est correct et dans le cas où le TCF qui suit le DEC est altéré, le TCF est rejeté par le premier octet de DNK.

Tableau H.2/T.30 – Rejet spécifique par le premier octet du FIF de DNK

Rejet spécifique	Codage du premier octet du FIF de DNK
TCF corrompu (équivalent de FTT en mode normal)	bit n° 0 1 2 3 4 5 6 7 1 x x x x x x x
Les bits 1 à 6 sont réservés pour un usage ultérieur	bit n° 0 1 2 3 4 5 6 7 x x x x x x x x
Le bit 7 doit être mis à "1" si toutes les trames ont été correctement reçues et si le DNK n'est envoyé que pour rejet de TCF. Si le bit 7 est mis à 1, les octets suivant le premier ne sont pas envoyés.	bit n° 0 1 2 3 4 5 6 7 x x x x x x x 1

Précisions:

– comme le précise la présente annexe, les bits du FIF de DCS sont placés dans la première trame HDLC du DEC;

– pour ce qui est des autres trames, la trame 0 d'un DEC contenant le FIF de DCS n'est réémise que lorsqu'elle est demandée par le DNK (si cette trame a été incorrectement reçue). Il y a une exception à cette règle lorsque TCF est rejeté. Dans ce cas, la trame 0 doit toujours être envoyée avec le TCF (voir exemple ci-après).

Exemple d'un DEC suivi de TCF

---------->

DEC 3 trames

———————>

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

DNK avec un FIF long de 2 octets:

Bit n° 01234567 01234567

00000000 01011111

trame 1 incorrectement reçue
trames 0 et 2 bien reçues

---------->

DEC 1 trame:
trame 1

———————>

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

DNK avec un FIF long de 1 octet:

Bit n° 01234567

10000001

trame 1 bien reçue, rejet de TCF

---------->

DEC 1 trame:

trame 0 (contenant le FIF de DCS)

———————>

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

trame 0 correctement reçue et TCF correct
réponse normale = accusé de réception implicite
(dépendant du contexte)

H.6.1.3 Précisions relatives à l'usage de FNV dans l'Annexe H

FNV, défini au 5.3.6.2.12/T.30, ne sert qu'après que la condition suivante a été satisfaite:

– il n'y a pas de trame de signal X en attente de correction.

Exemple

---------->

DEC 3 trames

———————>

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

DNK avec un FIF long de 2 octets:

```
Bit n°   01234567   01234567
         00000000   01011111
```

trame 1 incorrectement reçue
trames 0 et 2 bien reçues

---------->

DEC 1 trame:
trame 1

———————>

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

trame 1 correctement reçue
FNV (à cause d'une erreur dans le contenu des paramètres)

H.6.1.4 Codage des données contenues dans le FIF de DER, DES, DEC et DTR

H.6.1.4.1 Supergroupes et groupes

La séquence des champs d'information de télécopie des signaux DER, DES, DEC et DTR est structurée sous forme de groupes et supergroupes.

Les groupes sont des collections d'attributs de terminal ou de session similaires ou apparentés qu'il sera souvent nécessaire de négocier simultanément.

Les supergroupes offrent un niveau hiérarchique additionnel permettant de rassembler des groupes d'attributs apparentés.

La séquence générale de supergroupes et groupes qu'il est possible de présenter dans la séquence des champs d'information de télécopie des signaux DER, DES, DEC et DTR prend l'apparence suivante:

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

où SG signifie supergroupe et G, groupe.

Les supergroupes sont repérés par des étiquettes de supergroupe, aussi appelées dans la présente annexe "superétiquettes".

Les supergroupes contiennent des groupes repérés par des étiquettes de groupe, aussi appelées plus simplement dans la présente annexe "étiquettes".

Une superétiquette est suivie de la longueur du supergroupe qu'elle identifie, puis par la séquence des groupes du supergroupe.

Pour chaque groupe, l'étiquette qui identifie le groupe est suivie de la longueur du groupe puis par le contenu du groupe.

Notation

– Dans la présente annexe, le contenu d'un groupe est appelé "paramètre".

– La longueur du groupe est appelée "longueur de la valeur paramétrique".

– Le contenu du groupe est appelé "valeur du paramètre".

H.6.1.4.2 Affectation des étiquettes

1) Les superétiquettes ont une longueur de huit bits.

   Une valeur d'étiquette commençant par FF (hexadécimal) indique une extension de huit autres bits, ce qui pourra servir dans des versions ultérieures de la présente annexe.

2) Les étiquettes ont une longueur de huit bits. Le principe d'extension établi pour les superétiquettes s'applique de même aux étiquettes.

H.6.1.4.3 Longueur des supergroupes – longueur des groupes

L'unité pour ce décompte est l'octet. Le premier octet qui suit la superétiquette ou l'étiquette contient le nombre des octets suivants. Si le premier octet du compte a la valeur 0, alors les deux octets suivants donnent le nombre des octets suivants.

Exemple: pour une valeur de paramètre de longueur égale à 20 octets, l'octet de longueur sera: "00010100".

Exemple: pour une valeur de paramètre de longueur égale à 257 octets, les octets de longueur seront: "0000 0000 0000 0001 0000 0001".

La règle générale relative au FIF de DES/DEC/DER/DTR s'applique: le bit le plus à droite de chaque octet tel qu'il est imprimé (bit de plus faible poids) est transmis en premier.

H.6.1.4.4 Règles de codage

Une description formelle des règles applicables au codage des champs d'information de télécopie des signaux DER, DES, DEC et DTR est donnée ci-dessous dans le formalisme de Backus-Naur (BNF):

RÈGLES POUR LA SYNTAXE DE CODAGE DES ÉTIQUETTES DE TÉLÉCOPIE

<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 – La donnée "Tag_Encoded_Data" peut recouvrir plusieurs trames (voir H.6.1.4.6/T.30).

H.6.1.4.5 Description de la BNF

Les éléments syntaxiques du formalisme Backus-Naur utilisés dans ce qui précède sont décrits ci-après.

Symbole	Emploi
libellé	Un élément (ou un composant) est dénoté par un libellé.
::=	Opérateur d'affectation de production.
|	Ce symbole sépare des éléments ou groupes d'éléments constituant une alternative.
< >	Un élément non terminal est dénoté par un libellé encadré par les caractères "<" et ">".
[ ]	Un élément ou groupe d'éléments facultatif est encadré par les caractères "[" et "]".
{ }	Un élément ou groupe d'éléments encadré par "{" et "}" peut être répété 0 fois, une fois, ou plus.

H.6.1.4.6 Relation entre le codage des FIF et la structure dans les trames HDLC

La structuration en superétiquettes, étiquettes et paramètres décrite ci-dessus est indépendante de la structure des trames HDLC décrite au H.6.1.1/T.30. La série d'octets qui constitue la séquence des superétiquettes, étiquettes et des paramètres correspondants est insérée en ordre dans les FIF des trames HDLC, en remplissant d'abord le FIF de la première trame (trame "0") puis le FIF de la seconde trame (trame "1") et ainsi de suite.

H.6.1.4.7 Supergroupe des trames enchâssées

Il est créé un supergroupe rassemblant tous les groupes qui contiennent le FIF des trames classiques suivantes de T.30: DCS, TSI, SUB, SID, DTC, CIG, SEP, PWD, PSA.

Ce supergroupe est dénommé "supergroupe des trames encapsulées".

La superétiquette qui l'identifie est 0000 0001.

H.6.1.4.8 Les deux supergroupes de sécurité

Il est créé deux supergroupes relatifs à la sécurité:

– un pour le mode enregistrement;

– un pour le mode transmission sécurisée.

H.6.1.4.9 Liste des superétiquettes

Voir le Tableau H.3/T.30.

Tableau H.3/T.30 – Liste des superétiquettes

Code de la superétiquette	Nom de la superétiquette	Description
0000 0001	trame enchâssée (abréviation "E-F" encapsulated frame)	cette superétiquette est celle du supergroupe de trames enchâssées qui réunit tous les groupes contenant le FIF des trames T.30 classiques.
0000 0010	mode enregistrement	cette superétiquette est celle du supergroupe qui réunit tous les groupes transmis en mode enregistrement.
0000 0011	mode transmission sécurisée	cette superétiquette est celle du supergroupe qui réunit tous les groupes transmis en mode transmission sécurisée de télécopie.

H.6.1.4.10 Liste des étiquettes du supergroupe des trames enchâssées

Voir le Tableau H.4/T.30.

H.6.1.4.11 Liste des étiquettes afférentes aux caractéristiques de sécurité

Les étiquettes qui suivent peuvent être introduites par:

- les superétiquettes de sécurité "mode enregistrement"; et
- "mode transmission sécurisée".

Certains de ces paramètres ne sont utilisés qu'au niveau du message ("page sécuritaire", voir ci-après); un astérisque "*" permet de les repérer dans le Tableau H.5/T.30.

H.6.1.4.12 Ordre des superétiquettes et des étiquettes

Dans la séquence des superétiquettes, étiquettes et valeurs de paramètres, l'ordre est le suivant:

– le supergroupe des trames enchâssées est transmis avant les supergroupes de sécurité;

– au sein de chaque supergroupe, l'ordre des étiquettes n'est pas fixé, sauf que:

  - au sein du supergroupe de trames enchâssées, l'étiquette "**FIF de DCS**", si elle est présente, **doit être transmise en premier**. Cette règle a pour but de faciliter les opérations en cas de retransmission sur rejet de TCF [le champ de données de la première trame qui contient (et ne contient que) "FIF de DCS" **a une longueur inférieure à 64 octets**];

– au sein de chaque séquence d'étiquettes et de valeurs de paramètres introduite par les superétiquettes de sécurité, l'ordre des étiquettes n'est pas fixé.

Tableau H.4/T.30 – Liste des étiquettes appartenant au supergroupe des trames enchâssées

Code de l'étiquette	Nom de l'étiquette	Description
1000 0011	FIF de DCS	cette étiquette délimite la zone dans laquelle sont placés les bits qui correspondent au FIF de DCS (bits du Tableau 2/T.30).
0100 0011	FIF de TSI	cette étiquette délimite la zone dans laquelle sont placés les bits qui correspondent au FIF de TSI (quand il est employé).
1100 0011	FIF de SUB	cette étiquette délimite la zone dans laquelle sont placés les bits qui correspondent au FIF de SUB (quand il est employé).
1010 0011	FIF de SID	cette étiquette délimite la zone dans laquelle sont placés les bits qui correspondent au FIF de SID (quand il est employé).
1000 0001	FIF de DTC	cette étiquette délimite la zone dans laquelle sont placés les bits qui correspondent au FIF de DTC (quand il est employé).
0100 0001	FIF de CIG	cette étiquette délimite la zone dans laquelle sont placés les bits qui correspondent au FIF de CIG (quand il est employé).
1100 0001	FIF de PWD	cette étiquette délimite la zone dans laquelle sont placés les bits qui correspondent au FIF de PWD (quand il est employé).
1010 0001	FIF de SEP	cette étiquette délimite la zone dans laquelle sont placés les bits qui correspondent au FIF de SEP (quand il est employé).
0110 0001	FIF de PSA	cette étiquette délimite la zone dans laquelle sont placés les bits qui correspondent au FIF de PSA (quand il est employé).

H.6.1.4.13 Codage du paramètre "services de sécurité"

Le Tableau H.6/T.30 donne le codage des valeurs du paramètre qui fait suite à l'étiquette "services de sécurité" et à l'octet de longueur afférent.

L'octet de longueur prend la valeur "0000 0001" car la longueur du paramètre n'est que d'un octet. Ce paramètre pourrait être plus long dans des versions ultérieures de la présente annexe.

Tableau H.5/T.30 – Liste des étiquettes afférentes aux caractéristiques de sécurité

Code de l'étiquette		Nom de l'étiquette	Description
0001 0001		S	identité de l'émetteur
0001 0010		Sp	clé publique de l'émetteur
0001 0011		Ss	clé secrète de l'émetteur
0001 0100		SpE	clé publique de chiffrement de l'émetteur
0001 0101		SsE	clé secrète de chiffrement de l'émetteur
0001 0110		R	identité du récepteur
0001 0111		Rp	clé publique du récepteur
0001 1000		Rs	clé secrète du récepteur
0001 1001		RpE	clé publique de chiffrement du récepteur
0001 1010		RsE	clé secrète de chiffrement du récepteur
0001 1011		Srd/Rra	nombres aléatoires créés respectivement par l'émetteur aux fins de signature numérique et par le récepteur aux fins d'authentification de l'émetteur
0001 1100		BE = RpE[S, Ks]	chiffrement par RpE de l'identité de l'émetteur et de la clé de session
0001 1101		UTCd	date et heure choisies par l'émetteur (date et heure de création et de signature du document)
0001 1110		UTCr	date et heure choisies par le récepteur (date et heure de confirmation de réception du message)
0001 1111		Lm	longueur du document
0010 0000		jeton 2 = Ss[h(Sra, Rra, R), Sia]	jeton utilisé pour authentifier l'émetteur quand le service [confidentialité de message + établissement de clé de session] n'a pas été invoqué
0010 0001		jeton 2-chiffré = Ss[h(Sra, Rra, R, BE), Sia]	jeton utilisé pour authentifier l'émetteur quand le service [confidentialité de message + établissement de clé de session] a été invoqué
0010 0010		jeton 3 = Rs[h(Rra, Sra, S), Ria]	jeton utilisé pour authentifier le récepteur
0010 0011		jeton 4 = Ss[h(Srd, UTCd, Lm, R, h(document)), Sis]	jeton utilisé aux fins d'intégrité du message quand le service [confidentialité de message + établissement de clé de session] n'a pas été invoqué
0010 0100		jeton 4-chiffré = Ss[h(Srd, UTCd, Lm, R, BE, h(document chiffré)), Sis]	jeton utilisé aux fins d'intégrité du message quand le service [confidentialité de message + établissement de clé de session] a été invoqué
0010 0101		jeton 5 = Rs[h(Srd, UTCr, Lm, S, h(document)), Ris]	jeton utilisé pour confirmer la réception du message quand le service [confidentialité de message + établissement de clé de session] n'a pas été invoqué
0010 0110		jeton 5-chiffré = Rs[h(Srd, UTCr, Lm, S, BE, h(document chiffré)), Ris]	jeton utilisé pour confirmer la réception du message quand le service [confidentialité de message + établissement de clé de session] a été invoqué
0010 0111		services de sécurité	services de sécurité
0010 1000		mécanismes de sécurité	mécanismes de gestion de clés, fonctions de hachage, algorithmes de chiffrement
0010 1001		capacité de longueurs facultatives	capacité de longueurs facultatives
0010 1010		demande des capacités de sécurité	par usage de cette étiquette (et du paramètre correspondant), le terminal demande au terminal distant d'indiquer ses capacités en matière de sécurité
0010 1011		accusé de réception	accusé de réception utilisé en mode enregistrement
0010 1100	*	indicateur de page sécuritaire	indique que la page est la page sécuritaire
0010 1101	*	identification du type de page sécuritaire	indique le numéro de version de la page sécuritaire Il se peut que d'autres types de pages de sécurité soient autorisés dans des versions ultérieures de la présente annexe. D'autres numéros de version seront alloués
0010 1110	*	chemin de certification	chemin de certification
0010 1111		éléments non normalisés	éléments non normalisés
NOTE – L'étiquette facultative "éléments non normalisés" peut être utilisée en cas de reconnaissance de codes d'identification dans NSF. Les informations contenues dans les premiers octets de la valeur du paramètre "éléments non normalisés" doivent être compatibles avec les règles d'identification définies au 5.3.6.2.7/T.30 [capacités non normalisées (NSF, NSC, NSS)].			

Tableau H.6/T.30 – Paramètre "services de sécurité"

Services de sécurité	Statut	Codage du champ
authentification mutuelle	obligatoire	bit n° 7 6 5 4 3 2 1 0 x x x x x x x x Il n'est pas nécessaire d'affecter de bit puisque le service est obligatoire
service de sécurité comprenant: • authentification mutuelle • intégrité de message • confirmation de réception de message	facultatif	bit n° 7 6 5 4 3 2 1 0 x x x x x x x 1
service de sécurité comprenant: • authentification mutuelle • confidentialité de message (chiffrement) • établissement de clé de session	facultatif	bit n° 7 6 5 4 3 2 1 0 x x x x x x 1 x
service de sécurité comprenant: • authentification mutuelle • intégrité de message • confirmation de réception de message • confidentialité de message (chiffrement) • établissement de clé de session	facultatif	bit n° 7 6 5 4 3 2 1 0 x x x x x x 1 1
NOTE 1 – Le service d'enregistrement, obligatoire, ne nécessite pas d'affectation de bit. NOTE 2 – S'il n'y a pas de services facultatifs, l'affectation des bits est "0000 0000". NOTE 3 – Si l'émetteur ne choisit que le service "authentification mutuelle" pour le mode transmission sécurisée de télécopie, le paramètre "services de sécurité" n'est pas envoyé, puisque le service "authentification mutuelle" est le service de base.		

Les quatre groupes de services décrits dans le Tableau H.6/T.30 sont présentés dans le Tableau H.7/T.30 sous forme de profils de service:

Tableau H.7/T.30 – Profils de sécurité de l'Annexe H

Services de sécurité	Profils de service			
	1	2	3	4
authentification mutuelle	X	X	X	X
• intégrité de message • confirmation de réception de message		X		X
• confidentialité de message (chiffrement) • établissement de clé de session			X	X

H.6.1.4.14 Codage du paramètre "mécanismes de sécurité"

Le Tableau H.8/T.30 donne le codage des valeurs du paramètre qui fait suite à l'étiquette "mécanismes de sécurité" et à l'octet de longueur afférent.

La valeur de l'octet de longueur dépend du nombre d'algorithmes de chiffrement facultatifs qui sont indiqués (voir le Tableau H.8/T.30).

Pour la négociation:

– si le terminal émetteur le lui demande, le terminal récepteur indique les mécanismes de sécurité qu'il accepte en envoyant le paramètre "mécanismes de sécurité";

– le terminal émetteur choisit les mécanismes de sécurité à appliquer durant la session: une fonction de hachage, aucun ou un algorithme de chiffrement.

Dans la page sécuritaire (voir ci-après), le paramètre "mécanismes de sécurité" indique aussi quels mécanismes de sécurité ont été choisis pour la session.

Tableau H.8/T.30 – Paramètre "mécanismes de sécurité"

Mécanismes	Statut	Codage du champ
version du système de sécurité	obligatoire	bit n° 7 6 5 4 3 2 1 0 x x x x x x 0 0 (Note)
SHA-1 (fonction de hachage)	facultatif	bit n° 7 6 5 4 3 2 1 0 x x x x x 1 x x
MD-5 (fonction de hachage)	facultatif	bit n° 7 6 5 4 3 2 1 0 x x x x 1 x x x
page sécuritaire	facultatif	bit n° 7 6 5 4 3 2 1 0 x x x 1 x x x x
SAFER K-64 (algorithme de chiffrement)	facultatif	bit n° 7 6 5 4 3 2 1 0 x x 1 x x x x x
FEAL-32 (algorithme de chiffrement)	facultatif	bit n° 7 6 5 4 3 2 1 0 x 1 x x x x x x
RC5 (algorithme de chiffrement)	facultatif	bit n° 7 6 5 4 3 2 1 0 1 x x x x x x x
second octet	facultatif	
IDEA (algorithme de chiffrement)	facultatif	bit n° 7 6 5 4 3 2 1 0 x x x x x x x 1
HFX40	facultatif	bit n° 7 6 5 4 3 2 1 0 x x x x x x 1 x
DSA (gestion de clé)	facultatif	bit n° 7 6 5 4 3 2 1 0 x x x x x 1 x x
bits 3 à 7 réservés pour usage ultérieur (mis à "0")		bit n° 7 6 5 4 3 2 1 0 x x x x x x x x
.....	facultatif	bit n° 7 6 5 4 3 2 1 0 x x x x x x x x
dernier octet	facultatif	bit n° 7 6 5 4 3 2 1 0 x x x x x x x x

NOTE – A mesure que de nouvelles versions du système de sécurité de l'Annexe H/T.30 seront introduites, il conviendra de maintenir la compatibilité amont.

Le second octet est facultatif.

Les octets allant du troisième au dernier sont facultatifs eux aussi. Ils peuvent ne pas être présents.

Chacun de ces octets code un algorithme de chiffrement facultatif disponible dans le terminal de réception. L'octet prend pour valeur le numéro d'un algorithme de chiffrement tel qu'enregistré dans l'index des entrées de l'Appendice 2 à l'ISO/CEI 9979 (Procédures pour l'enregistrement des algorithmes cryptographiques). Ce numéro est codé en binaire (par exemple, "0000 0000" pour l'entrée numéro 00).

Lorsque le terminal émetteur choisit les mécanismes, le paramètre "mécanismes de sécurité" n'est long que d'un ou de deux octets. Le troisième octet n'est requis qu'en cas de sélection d'un algorithme de chiffrement enregistré dans l'ISO/CEI 9979 qui ne soit ni SAFER K-64, ni FEAL-32, ni RC5, ni IDEA, ni HFX40. Le troisième octet indique alors quel algorithme a été choisi.

H.6.1.4.15 Codage du paramètre "capacité de longueurs facultatives"

H.6.1.4.15.1 Principe

L'étiquette "capacité de longueurs facultatives", l'octet de longueur et la valeur correspondante du paramètre sont émis pour indiquer la capacité à traiter des longueurs facultatives.

H.6.1.4.15.2 Codage du paramètre "capacité de longueurs facultatives"

Les principes suivants s'appliquent à ce codage:

– des indicateurs permettent de préciser les longueurs maximales que peut traiter le terminal.

  Ces indicateurs sont codés en binaire sur 4 ou 8 bits selon le paramètre considéré;

– ces indicateurs sont employés dans un ordre déterminé:

Octet n° 0							
bit n°	7	6	5	4	3	2	1	0
			indicateur a		indicateur b			
Octet n° 1							
bit n°	7	6	5	4	3	2	1	0
			indicateur c		réservé			

D'abord vient l'octet 0 qui contient:

– en premier, l'indicateur "a" (4 bits) pour indiquer la longueur maximale acceptée pour les clés publiques et secrètes;

– puis l'indicateur "b" (4 bits) pour indiquer la longueur acceptée pour les nombres aléatoires (Sra, Srd, Rra),

puis l'octet 1 (facultatif) qui contient:

– l'indicateur "c" (4 bits) pour indiquer la longueur maximale acceptée pour les clés publiques et secrètes de chiffrement.

Il s'ensuit que l'octet de longueur du paramètre "capacité de longueurs facultatives" prend soit la valeur "0000 0001" (longueur d'un octet si le service [confidentialité de message + établissement de clé de session] n'est pas offert), soit la valeur "0000 0010" (deux octets si le service [confidentialité de message + établissement de clé de session] est offert). A l'avenir, dans des versions ultérieures de la présente annexe, le paramètre pourra être plus long.

H.6.1.4.15.3 Règles d'utilisation des indicateurs

Longueur maximale en octets des clés publiques et secrètes =

64 (longueur de base) + ([indicateur a] × 16) octets

avec 0 ≤ indicateur a ≤ 4 octets

Le terminal doit être capable de traiter toutes les longueurs comprises entre la longueur de base et la longueur maximale, par incréments de 16 octets.

Longueur maximale en octets des nombres aléatoires =

8 (longueur de base) + [indicateur b] octets

avec 0 ≤ indicateur b ≤ 8 octets

Le terminal doit être capable de traiter toutes les longueurs comprises entre la longueur de base et la longueur maximale.

Longueur maximale en octets des clés publiques et secrètes de chiffrement =

64 (longueur de base) + ([indicateur c] × 16) octets

avec 0 ≤ indicateur c ≤ 4 octets

Le terminal doit être capable de traiter toutes les longueurs comprises entre la longueur de base et la longueur maximale, par incréments de 16 octets.

H.6.1.4.15.4 Exemples

Exemple 1

Octet n° 0								
bit n°	7	6	5	4	3	2	1	0
	0	0	0	1	0	0	0	0
Octet n° 1								
bit n°	7	6	5	4	3	2	1	0
	0	0	0	1	0	0	0	0

Dans cet exemple:

– longueur maximale des clés publiques et secrètes = 64 + 16 × 1 = 80 octets

– longueur maximale des nombres aléatoires = 8 + 0 = 8 octets (pas de prise en charge de longueurs facultatives)

– longueur maximale des clés publiques et secrètes de chiffrement = 64 + 16 × 1 = 80 octets

Exemple 2

Octet n° 0								
bit n°	7	6	5	4	3	2	1	0
	0	0	0	0	0	0	0	0

Dans cet exemple, le terminal indique les seules capacités de base.

H.6.1.4.16 Codage du paramètre "demande des capacités de sécurité"

Par l'usage de cette étiquette et du paramètre afférent, le terminal demande au terminal distant de lui indiquer quelles sont ses capacités en matière de sécurité. Voir le Tableau H.9/T.30

L'octet de longueur prend la valeur "0000 0001" (la longueur du paramètre n'est que d'un octet). A l'avenir, dans de prochaines versions de la présente annexe, ce paramètre pourrait être plus long.

Tableau H.9/T.30 – Paramètre "demande des capacités de sécurité"

Indication de capacités demandées	Statut	Codage du champ
demande de "services de sécurité"	facultatif	bit n° 7 6 5 4 3 2 1 0 x x x x x x x 1
demande de "mécanismes de sécurité"	facultatif	bit n° 7 6 5 4 3 2 1 0 x x x x x x 1 x
demande de "capacité de longueurs facultatives"	facultatif	bit n° 7 6 5 4 3 2 1 0 x x x x x 1 x x
demande d'"éléments non normalisés"	facultatif	bit n° 7 6 5 4 3 2 1 0 x x x x 1 x x x
NOTE – Si le paramètre "demande des capacités de sécurité" est utilisé, l'un au moins des bits doit être mis à "1". Sinon, il ne sert à rien d'utiliser ce paramètre dans la session considérée.		

H.6.2 Mode enregistrement

H.6.2.1 Mécanisme

La Figure H.3/T.30 décrit le mécanisme du mode enregistrement, qui comporte deux étapes:

– *Etape une*

[Le terminal émetteur hache l'identité et la clé publique de l'émetteur.

Le terminal récepteur hache l'identité et la clé publique du récepteur.]

OU/(INCLUSIVEMENT)

[Le terminal émetteur hache l'identité et la clé publique de chiffrement de l'émetteur.]

OU/(INCLUSIVEMENT)

[Le terminal récepteur hache l'identité et la clé publique de chiffrement du récepteur.]

Les résultats de ces hachages sont échangés hors bande (directement de la main à la main, par courrier, téléphone, etc.) et mémorisés dans les terminaux.

– *Etape 2*

Echange entre les partenaires, au moyen de protocoles T.30, des identités et des clés publiques. Celles-ci sont mémorisées dans les terminaux.

L'ordre des deux étapes n'est pas fixé.

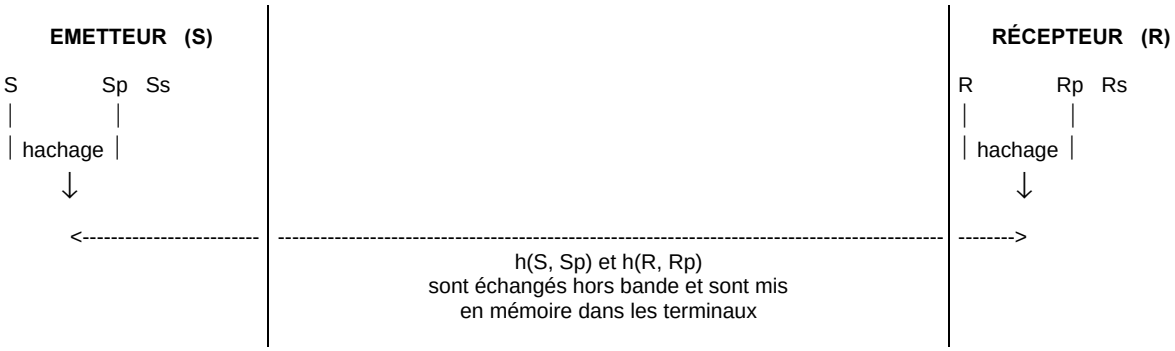
La comparaison des résultats de hachage reçus hors bande avec ceux qui résultent du hachage des données transmises via le protocole permet de déterminer la validité de l'identité et de la clé ou des clés du partenaire.

Après validation, ces valeurs, identité et clé publique (ou clés publiques) du partenaire, sont conservées dans les terminaux. Elles serviront à sécuriser les futures communications avec ce partenaire.

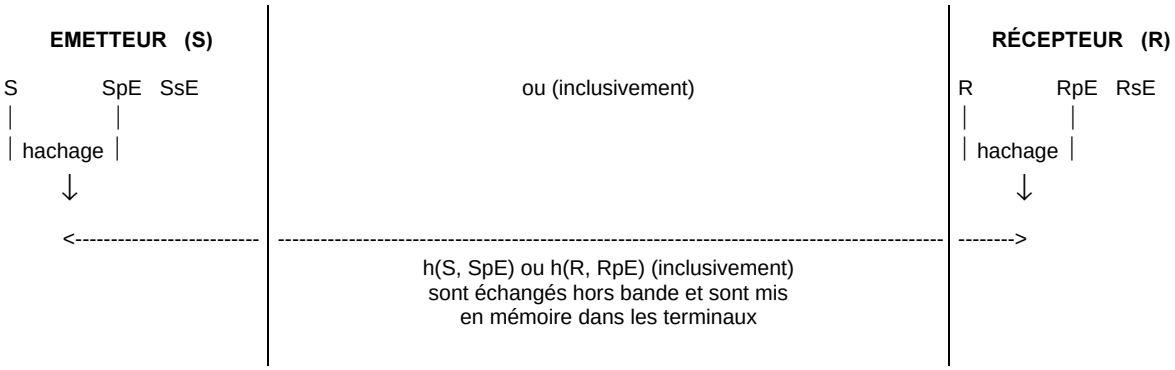
C'est un accord entre les utilisateurs des deux terminaux qui détermine si l'enregistrement concernera soit les clés publiques, soit les clés publiques de chiffrement, soit les deux. Pour les clés publiques de chiffrement, l'enregistrement peut ne concerner qu'un seul utilisateur, ou intéresser les deux.

Les moyens d'enregistrement dans les terminaux sont du ressort de ces derniers.

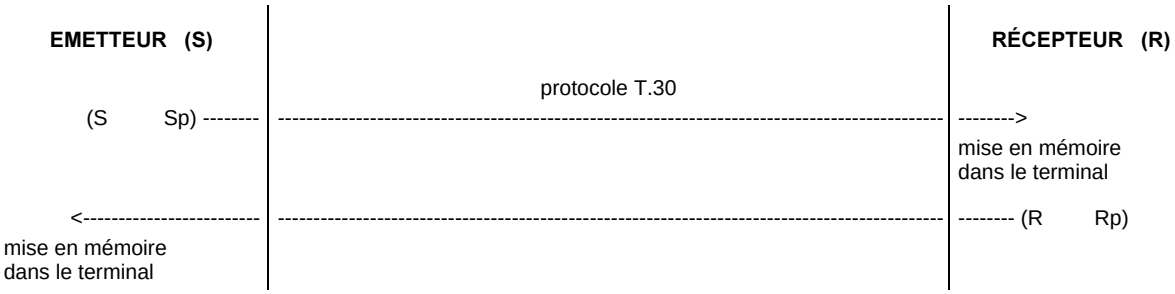
Echange hors bande des résultats de hachage et mise en mémoire dans les terminaux.



Au lieu de [S, Sp, h(S, Sp)] et [R, Rp, h(R, Rp)] ou en plus de ces quantités, l'opération ci-dessus peut intéresser [S, SpE, h(S, SpE)] ou [R, RpE, h(R, RpE)] ou les deux:



Etablissement de la communication T.30, échange des identités et des clés publiques au moyen du protocole T.30.



Au lieu de [S, Sp] et [R, Rp] ou en plus de ces quantités, l'opération ci-dessus peut intéresser [S, SpE] ou [R, RpE], ou les deux:

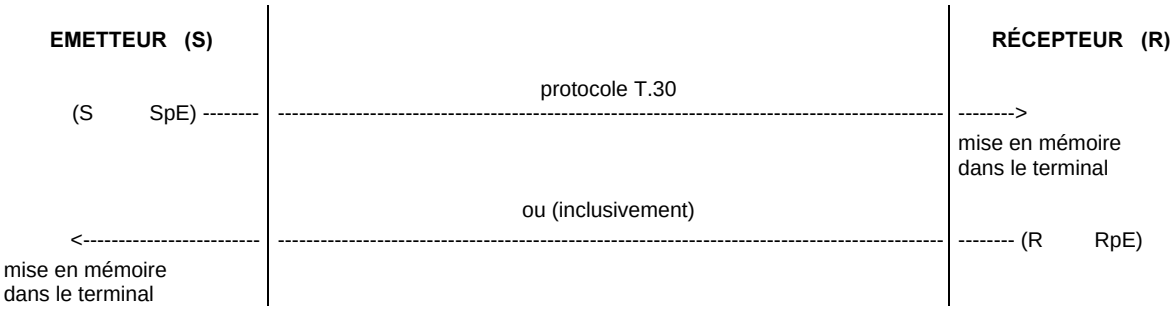
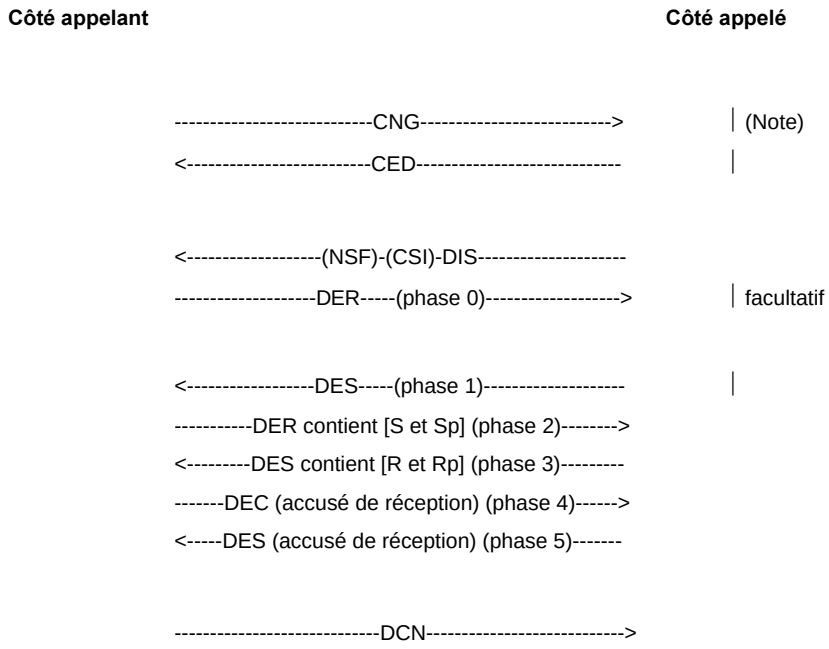


Figure H.3/T.30 – Mécanisme du mode enregistrement

H.6.2.2 Usage de DER, DES et DEC en mode enregistrement

Au cours de la seconde étape du mode enregistrement, les signaux DER, DES et DEC sont utilisés dans la Figure H.4/T.30.



NOTE – L'établissement de la communication par CNG/CED qu'illustre la figure n'est donné qu'à titre d'exemple.

Les autres méthodes opératoires définies au 3.1 peuvent aussi se présenter.

Au lieu de Sp et de Rp, ou en plus de ces valeurs, l'opération ci-dessus peut intéresser SpE ou RpE ou les deux.

Les temporisateurs mis en œuvre lors des échanges de signaux présentés ci-dessus sont les mêmes que ceux qu'utilise le protocole T.30 normal (T1, T2, T4, etc.). En l'absence de réponse sur temporisateur T4, la commande du côté émetteur (DER, DEC ou DNK) est émise à nouveau (dans le cas de DER et de DEC, seules sont émises à nouveau les trames non acquittées).

Figure H.4/T.30 – Echange des signaux en mode enregistrement

H.6.2.3 Assignation des bits du DIS

L'assignation des bits servant à indiquer dans le FIS du DIS les capacités de sécurité fondées sur l'algorithme RSA est donnée dans le Tableau 2/T.30. Le bit n° 82 est utilisé.

H.6.2.4 Format des champs d'information de télécopie de DER, DES et DEC en mode enregistrement

Convention

Dans les figures de la présente annexe, des groupes composés d'une étiquette, de l'octet de longueur et de la valeur de paramètre afférents sont représentés dans des cases à fond grisé. L'usage de telles étiquettes est facultatif.

Lorsque le fond des cases est blanc, l'usage de l'étiquette est obligatoire.

H.6.2.4.1 Phase 0 FACULTATIVE

Si le côté appelant ne désire pas utiliser de capacités facultatives, la phase 0 est facultative. Le mode enregistrement s'exécute avec les caractéristiques de base (Sp et Rp ont une longueur de 64 octets, il n'y a pas d'échange de clés publiques de chiffrement).

La séquence contenue dans le ou les FIF du DER est:

super-étiquette "E-F"	longueur du supergroupe	étiquette "FIF de SUB"	longueur + contenu du "FIF de SUB"	étiquette "FIF de SID"	longueur + contenu du "FIF de SID"	étiquette "FIF de TSI"	longueur + contenu du "FIF de TSI"

superétiquette "mode enregistrement"	longueur du supergroupe	étiquette "demande des capacités de sécurité"	longueur + contenu de "demande des capacités de sécurité"

étiquette "éléments non normalisés"	longueur + contenu d'"éléments non normalisés"

Conventions

Pour des raisons de simplicité, les représentations des séquences superétiquettes, étiquettes, octets de longueur et valeurs de paramètres ne montrent pas la structure HDLC interne du signal (préambule, fanions, adresses, commande, ..., FCS, fanions).

Il se peut qu'une séquence se trouve représentée par plusieurs rangées de cases. Ceci n'est qu'affaire de commodité, la séquence, elle, est continue.

Ces remarques s'appliquent à toutes les représentations de séquences de ce type dans la présente annexe.

H.6.2.4.2 Phase 1 FACULTATIVE

Il n'y a de phase 1 que s'il existe une phase 0.

La séquence contenue dans le ou les FIF du DES est:

superétiquette "mode enregistrement"	longueur du supergroupe	étiquette "services de sécurité"	longueur + contenu de "services de sécurité"

étiquette "mécanismes de sécurité"	longueur + contenu de "mécanismes de sécurité"	étiquette "capacité de longueurs facultatives"	longueur + contenu de "capacité de longueurs facultatives"	étiquette "éléments non normalisés"	longueur + contenu de "éléments non normalisés

Les groupes facultatifs [étiquette, octet de longueur et valeur de paramètre] sont présents si la demande en a été faite lors de la phase 0 par le positionnement des bits dans le paramètre "demande des capacités de sécurité".

H.6.2.4.3 Phase 2

La séquence contenue dans le ou les FIF du DER est:

super-étiquette "E-F"	longueur du supergroupe	étiquette "FIF de SUB"	longueur + contenu du "FIF de SUB"	étiquette "FIF de SID"	longueur + contenu du "FIF de SID"	étiquette "FIF de TSI"	longueur + contenu du "FIF de TSI"

superétiquette "mode enregistrement"	longueur du supergroupe	étiquette "S"	longueur + contenu de "S"	étiquette "Sp"	longueur + contenu de "Sp"

étiquette "SpE"	octet de longueur + contenu de "SpE"	étiquette "mécanismes de sécurité"	octet de longueur + contenu de "mécanismes de sécurité"	étiquette "éléments non normalisés"	longueur + contenu de "éléments non normalisés"

Dans l'exemple ci-dessus, Sp et SpE sont enregistrés en même temps.

Il est aussi possible de n'enregistrer que Sp ou que SpE. S est présent dans tous les cas.

Il est du ressort des terminaux de déterminer comment ils enregistrent les informations correspondantes.

Le paramètre "mécanismes de sécurité" est obligatoire car il indique le choix de la fonction de hachage, ou de l'algorithme de chiffrement (ou des deux) lorsqu'il y a eu échange de SpE ou de RpE (ou des deux).

H.6.2.4.4 Phase 3

La séquence contenue dans le ou les FIF du DES est:

superétiquette "mode enregistrement"	longueur du supergroupe	étiquette "R"	longueur + contenu de "R"	étiquette "Rp"	longueur + contenu de "Rp"

étiquette "RpE"	longueur + contenu de "RpE"

Dans l'exemple ci-dessus, Rp et RpE sont enregistrés en même temps.

Il est aussi possible ne n'enregistrer que Rp ou que RpE. R est présent dans tous les cas.

Il est du ressort des terminaux de déterminer comment ils enregistrent les informations correspondantes.

Si le terminal demandé découvre que les paramètres S et Sp (ainsi que, le cas échéant, [S, SpE]) ne concordent pas avec les valeurs hachées enregistrées dans le cas où l'échange hors bande des valeurs hachées a déjà eu lieu (voir H.6.2.1/T.30), il peut les rejeter par usage du signal FNV.

La cause d'erreur dans FNV est "erreur d'enregistrement de clé publique" ou "erreur d'enregistrement de clé publique de chiffrement" (voir le Tableau H.10/T.30).

L'emploi de FNV pour indiquer des erreurs de cette sorte est expliqué au H.6.7/T.30.

H.6.2.4.5 Phase 4

La séquence contenue dans le FIF du DEC est:

superétiquette "mode enregistrement"	longueur du supergroupe	étiquette "accusé de réception"	octet de longueur "0000 0000"

Si le terminal appelant découvre que les paramètres R et Rp (ainsi que, le cas échéant, [R, RpE]) ne concordent pas avec les valeurs hachées enregistrées dans le cas où l'échange hors bande des valeurs hachées a déjà eu lieu (voir H.6.2.1/T.30), il peut les rejeter par usage du signal FNV.

La cause d'erreur dans FNV est "erreur d'enregistrement de clé publique" ou "erreur d'enregistrement de clé publique de chiffrement" (voir le Tableau H.10/T.30).

L'emploi de FNV pour indiquer des erreurs de cette sorte est expliqué au H.6.7/T.30.

H.6.2.4.6 Phase 5

La séquence contenue dans le FIF du DES est:

superétiquette "mode enregistrement"	longueur du supergroupe	étiquette "accusé de réception"	octet de longueur "0000 0000"

H.6.3 Mode transmission sécurisée de télécopie

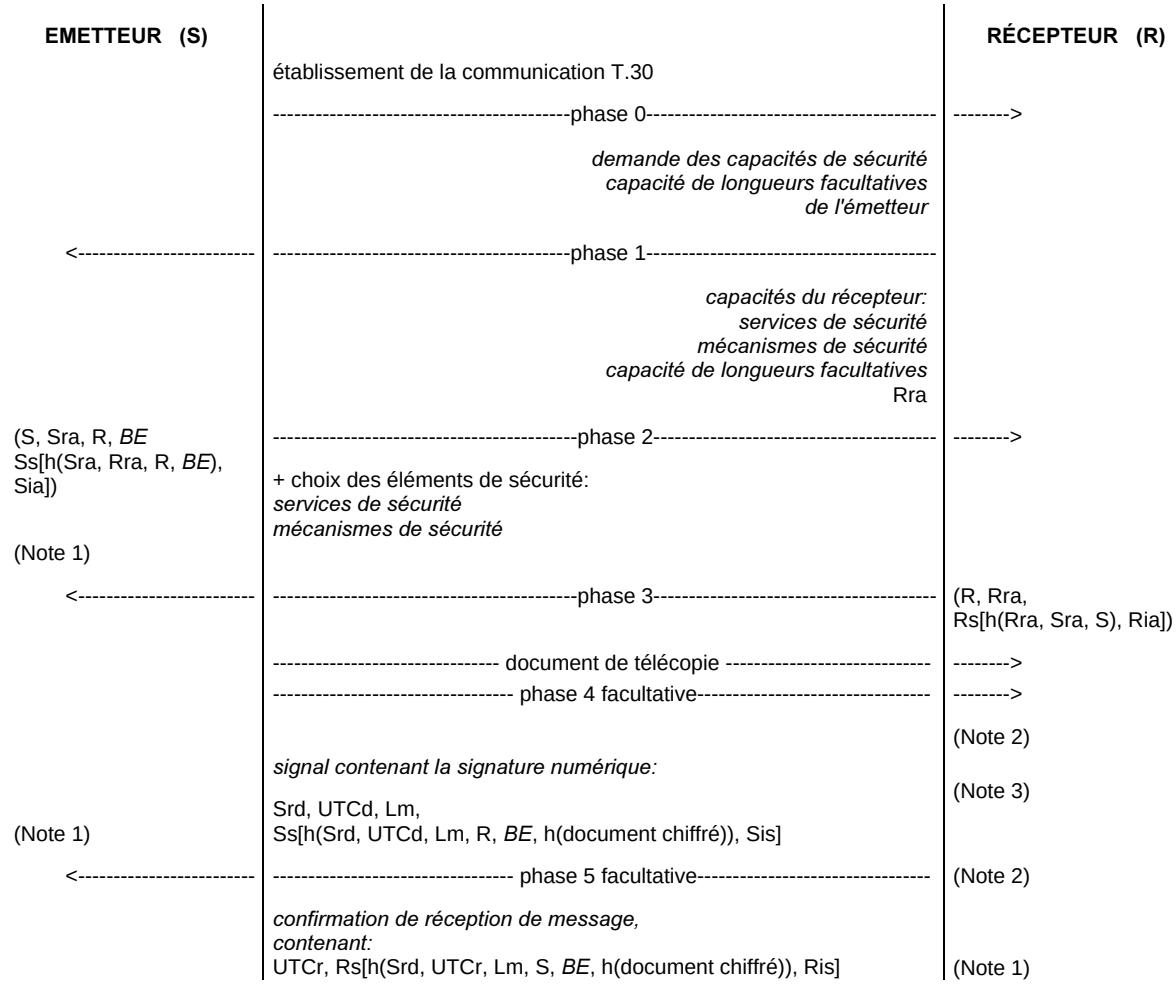
Ce mode assortit de moyens de sécurité la transmission du document de télécopie.

Les paramètres de sécurité sont transmis au sein d'éléments de protocole au cours des étapes B et D du protocole T.30.

A titre d'option facultative, certains paramètres de sécurité peuvent être transmis au niveau du message (à la vitesse du message) au cours de l'étape C du protocole T.30, au sein d'une page spéciale appelée "**page sécuritaire**".

H.6.3.1 Mécanisme

Voir la Figure H.5/T.30.



Les caractères italiques indiquent les éléments facultatifs.

NOTE 1 – BE (= RpE[S, Ks]) ne se trouve dans les divers jetons que si les deux partenaires se sont mis d'accord par négociation (via le paramètre "services de sécurité") pour faire usage du service [confidentialité de message + établissement de clé de session].

NOTE 2 – Il n'y a présence des phases 4 et 5 que si les deux partenaires se sont mis d'accord par négociation (via le paramètre "services de sécurité") pour faire usage du service [intégrité de message + confirmation de réception de message].

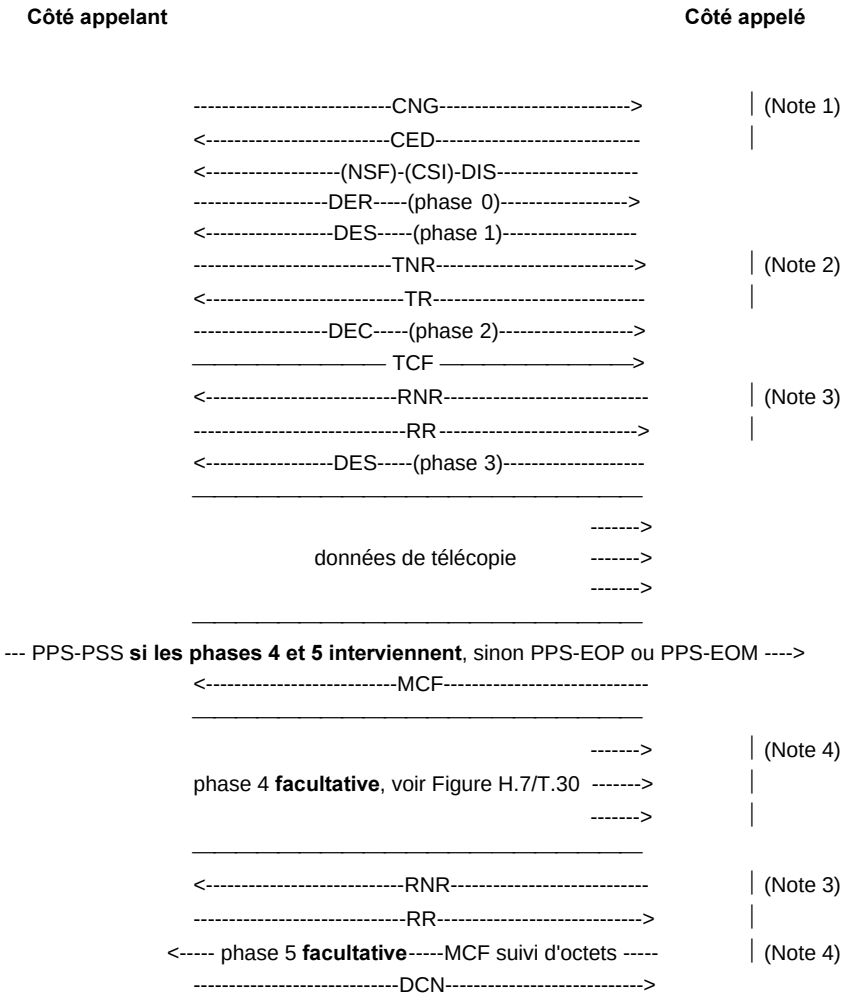
NOTE 3 – D'autres paramètres apparaissent si la page sécuritaire est employée en phase 4.

Figure H.5/T.30 – Mécanisme du mode transmission sécurisée de télécopie

H.6.3.2 Usage de DER, DES et DEC en mode transmission sécurisée de télécopie

H.6.3.2.1 Mécanisme général du mode transmission sécurisée de télécopie

En mode transmission sécurisée de télécopie, les signaux DER, DES et DEC sont utilisés dans la Figure H.6/T.30:



Les temporisateurs mis en œuvre lors des échanges de signaux présentés ci-dessus sont les mêmes que ceux qu'utilisent le protocole T.30 normal et l'Annexe A/T.30 (T1, T2, T4, T5, etc.). En l'absence de réponse sur le temporisateur T4, la commande du côté émetteur (DER, DEC ou DNK) est émise à nouveau (dans le cas de DER et de DEC, seules sont émises à nouveau les trames non acquittées).

NOTE 1 – L'établissement de la communication par CNG/CED qu'illustre la figure n'est donné qu'à titre d'exemple. Les autres méthodes opératoires définies au 3.1 peuvent aussi se présenter.

NOTE 2 – L'usage de TNR et TR est identique à celui de RNR/RR mais s'applique au terminal émetteur au lieu du terminal récepteur. Des occurrences facultatives de l'échange TNR-TR permettent au terminal émetteur d'arrêter le terminal récepteur pour une période de temps dont la durée maximale est donnée par T5 (voir l'Annexe A/T.30).

NOTE 3 – Des occurrences facultatives de l'échange RNR-RR (comme le définit déjà l'Annexe A/T.30) permettent au terminal récepteur d'arrêter le terminal émetteur pour une période de temps dont la durée maximale est donnée par T5 (voir l'Annexe A/T.30).

NOTE 4 – Les phases 4 et 5 n'interviennent que si les deux partenaires se sont mis d'accord par négociation (via le paramètre "services de sécurité") pour faire usage du service [intégrité de message + confirmation de réception de message].

Figure H.6/T.30 – Echange de signaux en mode transmission sécurisée de télécopie
Exemple relatif à un document de télécopie d'une page

H.6.3.2.2 Phase 4

Lorsque la phase 4 (et par suite la phase 5) intervient, il existe deux cas de figure selon que les deux partenaires ont ou n'ont pas négocié l'usage de la page sécuritaire:

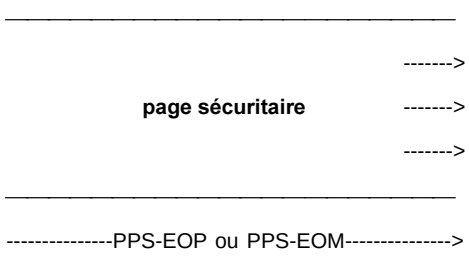
Cas 1 – Lorsque les deux équipements (émetteur et récepteur) ont la capacité de traiter la page sécuritaire et que le service [intégrité de message + confirmation de réception de message] est invoqué, il faut utiliser la solution de la page sécuritaire (cas 1).

Cas 2 – Lorsque l'un des deux équipements n'a pas la capacité de traiter la page sécuritaire et que le service [intégrité de message + confirmation de réception de message] est invoqué, il faut utiliser la solution PPS-EOP ou PPS-EOM suivi d'octets (cas 2).

PPS-EOM (sans suite au cas 1, avec suite au cas 2) s'emploie si la communication doit se continuer avec un autre document.

PPS-EOP (sans suite au cas 1, avec suite au cas 2) s'emploie ordinairement, lorsque la communication ne concerne qu'un seul document de télécopie.

Cas 1: il a été fait appel au service [intégrité de message + confirmation de réception de message] et la page sécuritaire est employée:



Cas 2: il a été fait appel au service [intégrité de message + confirmation de réception de message] mais la page sécuritaire n'est pas employée:

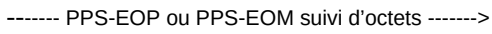


Figure H.7/T.30 – Echange de signaux en phase 4

H.6.3.3 Assignation des bits du DIS

L'assignation des bits servant à indiquer dans le FIF du DIS les capacités de sécurité fondées sur l'algorithme RSA est donnée dans le Tableau 2/T.30. Le bit n° 82 est utilisé.

Dans le contexte de l'Annexe H/T.30, le DCS n'est pas émis. Le FIF de DCS est inclus dans le nouveau signal "DEC" dont le bit correspondant n° 82 doit être mis à "1".

H.6.3.4 Format des champs d'information de télécopie de DER, DES et DEC en mode transmission sécurisée de télécopie

H.6.3.4.1 Phase 0

La séquence contenue dans le ou les FIF du DER est:

super-étiquette "E-F"	longueur du supergroupe	étiquette "FIF de SUB"	longueur + contenu du "FIF de SUB"	étiquette "FIF de SID"	longueur + contenu du "FIF de SID"	étiquette "FIF de TSI"	longueur + contenu du "FIF de TSI"

superétiquette "mode de transmission sécurisée"	longueur du supergroupe	étiquette "capacité de longueurs facultatives"	longueur + contenu de "capacité de longueurs facultatives"	étiquette "demande des capacités de sécurité"	longueur + contenu de "demande des capacités de sécurité"

étiquette "éléments non normalisés"	longueur + contenu de "éléments non normalisés"

Si le côté appelant ne souhaite utiliser ni services facultatifs ni capacités facultatives, il n'envoie pas le paramètre "demande des capacités de sécurité". Le mode transmission sécurisée de télécopie est mis en œuvre par emploi des caractéristiques de base (Sp, Rp de 64 octets, etc.), seul étant invoqué le service d'authentification mutuelle.

Si, de plus, le côté appelant est incapable de manipuler des valeurs quelconques de longueurs facultatives autres que les valeurs de base, il n'est pas tenu d'émettre le paramètre "capacité de longueurs facultatives".

H.6.3.4.2 Phase 1

La séquence contenue dans le ou les FIF du DES est:

superétiquette "mode transmission sécurisée"	longueur du supergroupe	étiquette "Rra"	longueur + contenu de "Rra"	étiquette "services de sécurité"	longueur + contenu de "services de sécurité"

étiquette "mécanismes de sécurité"	longueur + contenu de "mécanismes de sécurité"	étiquette "capacité de longueurs optionnelles"	longueur + contenu de "capacité de longueurs optionnelles"	étiquette "éléments non normalisés"	longueur + contenu de "éléments non normalisés"

Les groupes facultatifs [étiquette, longueur et valeur de paramètre] sont présents si la demande en a été faite lors de la phase 0 par le positionnement des bits dans le paramètre "demande des capacités de sécurité".

H.6.3.4.3 Phase 2

La séquence contenue dans le ou les FIF du DEC est:

super-étiquette "E-F"	longueur du supergroupe	étiquette "FIF de DCS"	longueur + contenu du "FIF de DCS"	étiquette "FIF de SUB"	longueur + contenu du "FIF de SUB"	étiquette "FIF de SID"	longueur + contenu du "FIF de SID"	étiquette "FIF de TSI"	longueur + contenu du "FIF de TSI"

superétiquette "mode transmission sécurisée"	longueur du supergroupe	étiquette "S"	longueur + contenu de "S"	étiquette "Sra"	longueur + contenu de "Sra"	étiquette "R"	longueur + contenu de "R"

étiquette "BE"	longueur + contenu de "BE"	étiquette "jeton 2" ou "jeton 2-chiffré"	longueur + contenu de "jeton 2" ou de "jeton 2-chiffré"

étiquette "services de sécurité"	octet de longueur + contenu de "services de sécurité"	étiquette "mécanismes de sécurité"	octet de longueur + contenu de "mécanismes de sécurité"	étiquette "éléments non normalisés"	longueur + contenu de "éléments non normalisés"

– L'étiquette "BE" ne figure que si le service [confidentialité de message + établissement de clé de session] est invoqué. En ce cas, c'est jeton 2-chiffré qui est émis.

– L'étiquette "services de sécurité" ne figure pas si la transmission ne doit s'effectuer qu'avec le seul appel au service d'authentification mutuelle.

– Le paramètre "mécanismes de sécurité" est obligatoire car il indique quelle fonction de hachage a été choisie.

H.6.3.4.4 Phase 3

La séquence contenue dans le ou les FIF du DES est:

superétiquette "mode transmission sécurisée"	longueur du supergroupe	étiquette "R"	longueur + contenu de "R"	étiquette "Rra"	longueur + contenu de "Rra"	étiquette "jeton 3"	longueur + contenu de "jeton 3"

H.6.3.4.5 Phase 4

Les phases 4 et 5 n'interviennent que si les deux partenaires se sont mis d'accord par négociation pour faire usage du service [intégrité de message + confirmation de réception de message].

Le signal émis en phase 4 est soit PPS-EOP (ou PPS-EOM) suivi d'octets (cas 2 de la Figure H.7/T.30) soit la page sécuritaire (cas 1 de la Figure H.7/T.30).

Lorsque les deux équipements (émetteur et récepteur) ont la capacité de traiter la page sécuritaire et qu'il est fait appel au service [intégrité de message + confirmation de réception de message], il faut utiliser la solution de la page sécuritaire (cas 1).

Le contenu de la page sécuritaire est défini au H.6.4/T.30.

Dans le cas 2, la structure de PPS-EOP (ou de PPS-EOM) suivi d'octets est la même que celle que donne le H.6.1.1/T.30 pour DER, DES, DEC et DTR: trames multiples, bit X valant 1 pour la dernière trame, FIF de 65 octets, numéros de trames, etc.

Le FCF est celui déjà défini dans l'Annexe A/T.30 (en A.4.3/T.30).

La séquence contenue dans le ou les FIF de PPS-EOP (ou de PPS-EOM) avec suite est:

superétiquette "mode transmission sécurisée"	longueur du supergroupe	étiquette "Srd"	longueur + contenu de "Srd"	étiquette "UTCd"	longueur + contenu de "UTCd"	étiquette "Lm"	longueur + contenu de "Lm"

étiquette "jeton 4" ou "jeton 4-chiffré"	longueur + contenu de "jeton 4" ou "jeton 4-chiffré"	étiquette "éléments non normalisés"	longueur + contenu de "éléments non normalisés"

"jeton 4-chiffré" ou "jeton 4" est émis selon qu'il a été fait appel ou non au service [confidentialité de message + établissement de clé de session] au cours de la phase 2.

H.6.3.4.6 Phase 5

Les phases 4 et 5 n'interviennent que si les deux partenaires se sont mis d'accord par négociation pour faire usage du service [intégrité de message + confirmation de réception de message].

Le signal émis en phase 5 est MCF suivi d'octets.

La structure de MCF suivi d'octets est la même que celle de DER, DES, DEC et DTR, dont la définition est donnée au H.6.1.1/T.30: trames multiples, bit X valant 1 pour la dernière trame, FIF de 65 octets, numéros de trames, etc.

Le FCF est celui déjà défini pour le protocole T.30 normal (voir 5.3.6.1.7/T.30).

La séquence contenue dans le ou les FIF de MCF (ou de PPS-EOM) avec suite est:

superétiquette "mode transmission sécurisée"	longueur du supergroupe	étiquette "UTCr"	longueur + contenu de "UTCr"	étiquette "jeton 5" ou "jeton 5-chiffré"	longueur + contenu de "jeton 5" ou "jeton 5-chiffré"

"jeton 5-chiffré" ou "jeton 5" est émis selon qu'il a été fait appel ou non au service [confidentialité de message + établissement de clé de session] au cours de la phase 2.

H.6.3.4.7 Messages d'erreur

S'il détecte des erreurs au cours des phases 1, 2, 3, 4 ou 5, l'émetteur ou le récepteur, selon la phase, indique l'erreur au moyen du signal FNV.

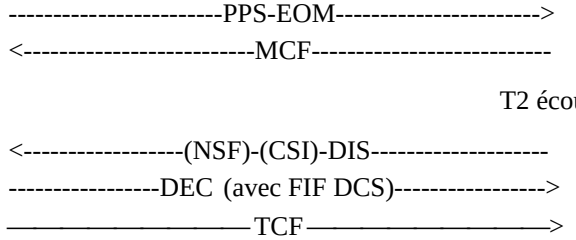
La cause de l'erreur est codée au sein de FNV.

Le Tableau H.10/T.30 donne le codage des causes d'erreur.

Le sous-paragraphe H.6.7/T.30 explique comment utiliser FNV pour indiquer les erreurs.

H.6.3.5 Précision sur l'usage de PPS-EOM au sein d'un document sécurisé

Il est permis d'utiliser PPS-EOM au cours de la séquence de pages partielles qui constituent un document sécurisé pour, par exemple, changer la résolution d'image. La procédure qui s'applique après PPS-EOM est très proche de celle que donne l'Annexe A/T.30:



Pour pouvoir paramétrer dans ce cas la transmission des pages résiduelles du document, DEC doit contenir le FIF de DCS, avec le ou les bits de sécurité adéquats mis à "1" comme dans la phase 2. Les paramètres de sécurité validés au cours de la phase 2 ne sont pas inclus dans le DEC à ce moment, car ils sont valables pour l'ensemble de la transmission du document.

H.6.4 Au niveau du message: la page sécuritaire

L'usage de la page sécuritaire est présenté au cas 1 de la Figure H.7/T.30.

Lorsque les deux équipements (émetteur et récepteur) ont la capacité de traiter la page sécuritaire et qu'il est fait appel au service [intégrité de message + confirmation de réception de message], il faut utiliser la solution de la page sécuritaire.

H.6.4.1 Contenu de la page sécuritaire

La page sécuritaire contient les paramètres de sécurité suivants, qui sont définis dans les Tableaux H.1/T.30 et H.5/T.30:

indicateur de page sécuritaire	:	indique que le bloc contient une page sécuritaire.
S	:	identité de l'émetteur.
Sp	:	clé publique de l'émetteur.
R	:	identité du récepteur.
Srd	:	nombre aléatoire créé par l'émetteur aux fins de signature numérique.
UTCd	:	date et heure choisies par l'émetteur (date et heure de création et de signature du document).
Lm	:	longueur du document.
paramètre "services de sécurité"	:	voir définition au Tableau H.6/T.30.
paramètre "mécanismes de sécurité"	:	voir définition au Tableau H.8/T.30.
BE	:	RpE[S, Ks].
jeton 4 ou jeton 4-chiffré	:	voir définition au Tableau H.5/T.30.
identification de type de page sécuritaire	:	indique le numéro de version de la page de sécurité. Des versions ultérieures de la présente annexe pourraient autoriser d'autres types de pages de sécurité, qui se verraient attribuer d'autres numéros de version.
chemin de certification	:	la définition précise du chemin de certification est pour étude ultérieure.
éléments non normalisés	:	éléments non normalisés.

L'ordre de transmission des bits de la page sécuritaire respecte les règles définies pour le FIF de DES/DEC/DER/DTR au H.4.8.3/T.30 et que précise le Tableau H.1/T.30.

H.6.4.1.1 Codage du paramètre "indicateur de page sécuritaire"

Cette étiquette, avec le paramètre associé, indique que le bloc contient une page sécuritaire.

L'octet de longueur a la valeur "0000 1000" (8 octets).

Le contenu exprimé en hexadécimal est:

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

H.6.4.1.2 Codage du paramètre "identification du type de page sécuritaire"

Ce paramètre est facultatif dans la page sécuritaire.

L'octet de longueur a la valeur "0000 0001" (1 octet).

Le contenu est le numéro de version de la page sécuritaire. Dans la version de la présente annexe, il n'existe qu'une seule version de la page sécuritaire. Le numéro de version est: 0x00.

H.6.4.2 Format de la page sécuritaire

La page sécuritaire se présente exactement sous le même format que les séquences contenues dans les signaux DER, DES, DEC et DTR (superétiquettes, étiquettes et valeurs de paramètres), sauf que dans le cas présent la séquence n'est pas localisée dans la série des FIF de DER, DES, DEC ou DTR mais dans les trames ECM.

Au sein de la séquence d'étiquettes présentée par la superétiquette, **l'ordre n'est pas fixé**, à l'exception de l'indicateur de page sécuritaire qui vient en premier.

La séquence est la suivante:

superétiquette "mode transmission sécurisée"	longueur du supergroupe	étiquette "indicateur de page sécuritaire"	longueur + contenu de "indicateur de page sécuritaire"	étiquette "S"	longueur + contenu de "S"	étiquette "Sp"	longueur + contenu de "Sp"

étiquette "R"	longueur + contenu de "R"	étiquette "Srd"	longueur + contenu de "Srd "	étiquette "UTCd"	longueur + contenu de "UTCd"	étiquette "Lm"	longueur + contenu de "Lm"

étiquette "services de sécurité"	longueur + contenu de "services de sécurité"	étiquette "mécanismes de sécurité"	longueur + contenu de "mécanismes de sécurité"

étiquette "BE"	octet de longueur + contenu de "BE"

étiquette "jeton 4" ou "jeton 4-chiffré"	longueur + contenu de "jeton 4" ou "jeton 4-chiffré"	étiquette "identification de type de page sécuritaire"	longueur + contenu de "identification de type de page sécuritaire"

étiquette "chemin de certification"	longueur + contenu de "chemin de certification"	étiquette "éléments non normalisés"	longueur + contenu de "éléments non normalisés"

NOTE 1 – Les valeurs des bits des paramètres "services de sécurité" et "mécanismes de sécurité" sont conformes aux Tableaux H.6/T.30 et H.8/T.30, respectivement (version du système de sécurité, bit indiquant quelle fonction de hachage est utilisée, bit indiquant quel algorithme de sécurité est utilisé si le document est chiffré).

NOTE 2 – Le paramètre "BE" ne figure que si le service [confidentialité de message + établissement de clé de session] a été invoqué.

NOTE 3 – Le format de "chemin de certification" est pour étude ultérieure.

H.6.5 Règles relatives au hachage du document – règles relatives au chiffrement du document

H.6.5.1 Règles relatives au hachage du document

Les données qui dans le document font partie de la chaîne de bits soumise à la fonction de hachage sont tous les octets contenus dans le FIF de toutes les trames de données ECM à l'exception du premier octet de chaque trame, celui qui porte le numéro de trame. Par conséquent, tous les bits de bourrage et de remplissage décrits au A.3.6.2/T.4 et au 2.4.1.2/T.6 font partie des données qui passent dans la fonction de hachage.

La chaîne de bits qui entre dans le processus de hachage pour donner h(document) ou, s'il y a eu chiffrement, h(document chiffré), est représentable sous la forme de la chaîne de données présentée dans le cadre de la Figure H.8/T.30.

Pour chacun des octets, cette chaîne de bits se présente au processus de hachage avec les bits dans le même ordre que les bits de données de chacun des octets lors de la transmission sur la ligne.

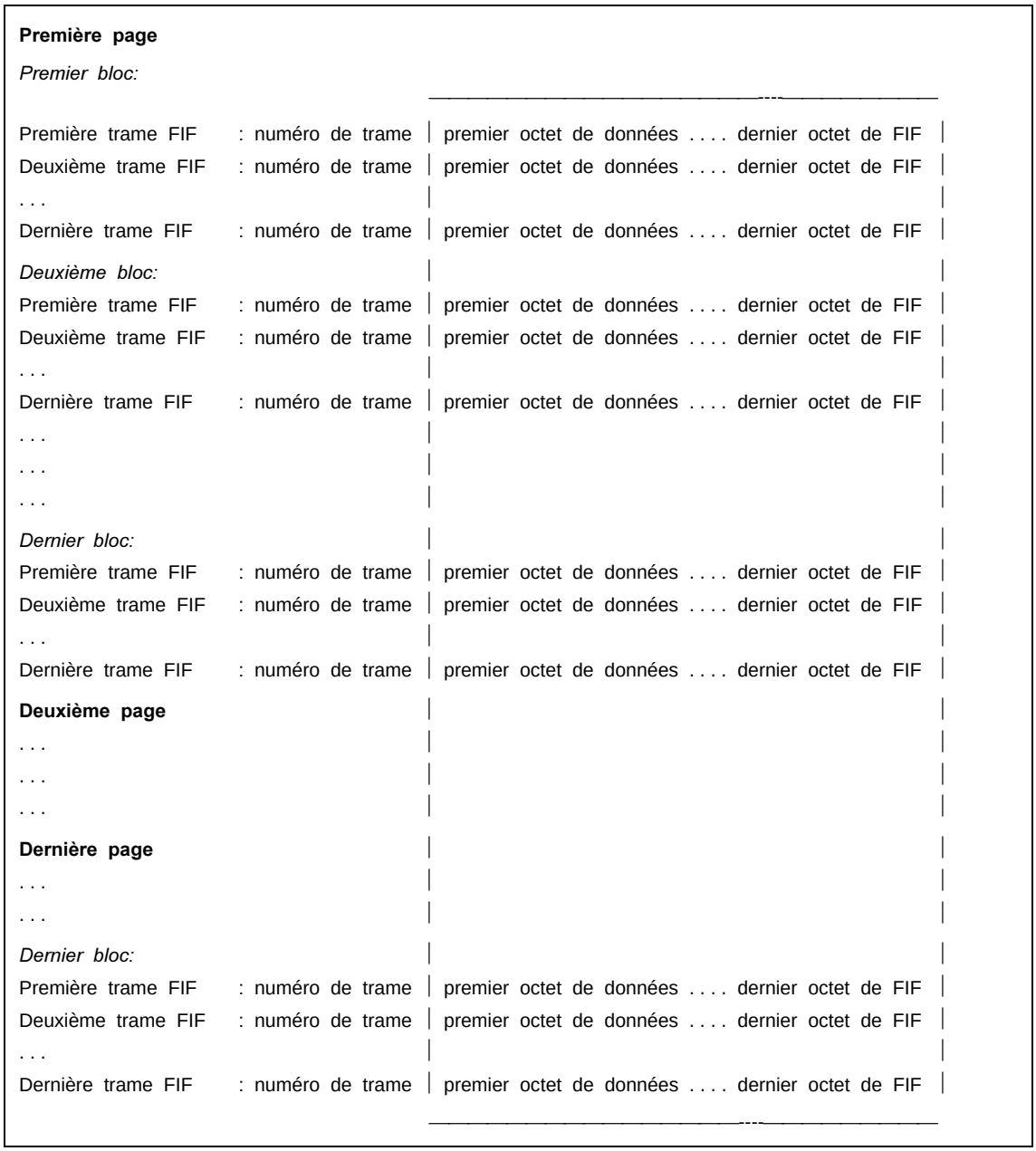


Figure H.8/T.30 – Règles relatives au hachage du document

H.6.5.2 Règles relatives au chiffrement du document

Les données qui dans le document sont soumises à la fonction de chiffrement sont tous les octets contenus dans le FIF de toutes les trames de données ECM à l'exception du premier octet de chaque trame, celui qui porte le numéro de trame.

Les bits se présentent à l'entrée de la fonction de chiffrement dans le même ordre que sur la ligne quand il n'y a pas chiffrement à la transmission de la télécopie.

NOTE – Dans le cas de FEAL-32, les données sont alignées par 64 bits ordonnés de gauche à droite puis entrés dans la fonction FEAL-32.

Les bits en sortie de la fonction FEAL-32 sont alignés par 64, ordonnés de gauche à droite. Le bit le plus à gauche est transmis en premier.

H.6.6 Mode relève sécurisée

H.6.6.1 Relève simple

Les règles relatives à l'usage et au codage des signaux utilisés dans le mode relève sécurisée sont les mêmes que celles qui s'appliquent au mode transmission sécurisée de télécopie.

La Figure H.9/T.30 illustre l'échange des signaux.

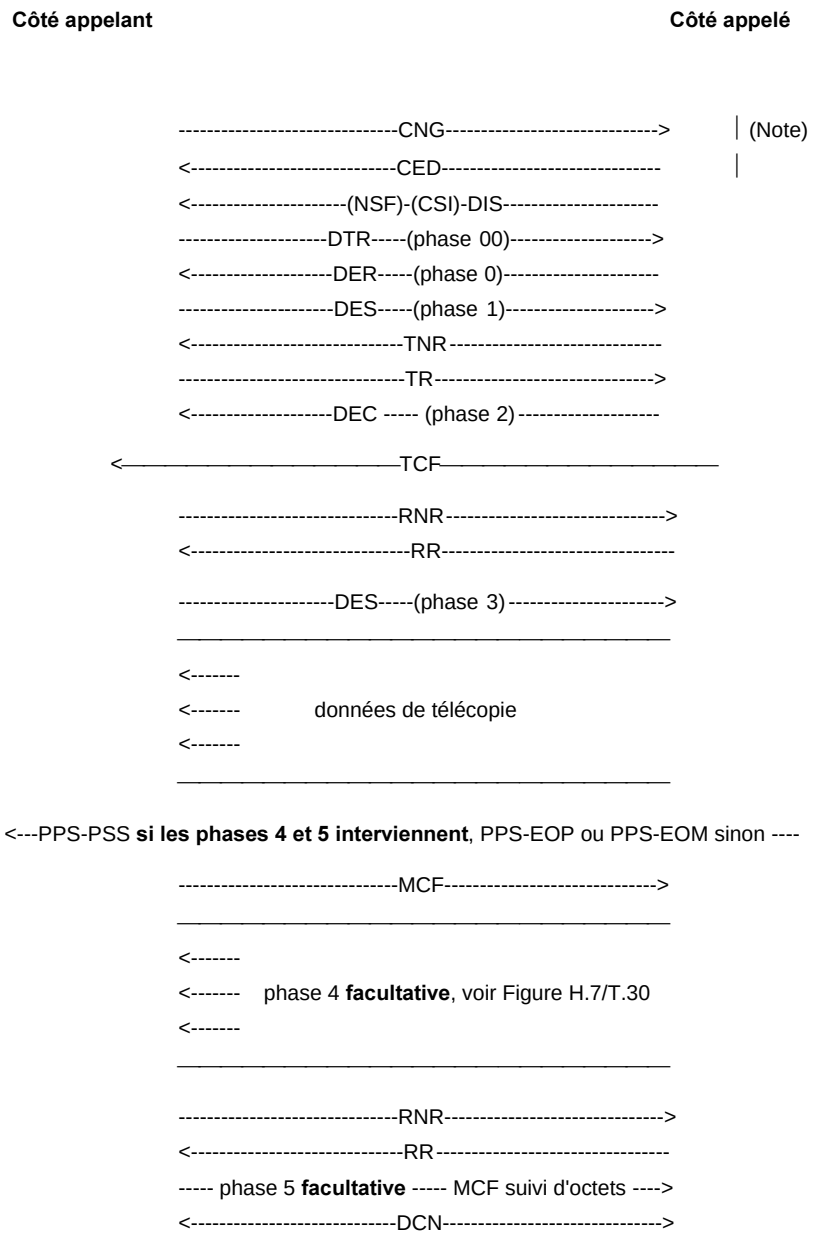


Figure H.9/T.30 – Echange de signaux en mode relève sécurisée
Exemple relatif à un document de télécopie d'une page

NOTE – L'établissement de la communication par CNG/CED qu'illustre la figure n'est donné qu'à titre d'exemple. Les autres méthodes opératoires définies au 3.1/T.30 peuvent aussi se présenter.

Les phases 0, 1, 2, 3 et 4 sont les mêmes qu'en mode transmission sécurisée de télécopie.

Pour la phase 00, la séquence contenue dans le ou les FIF du DTR est:

superétiquette "E-F"	longueur du supergroupe	étiquette "FIF de PWD"	longueur + contenu de "FIF de PWD"	étiquette "FIF de PSA"	longueur + contenu de "FIF de PSA"	étiquette "FIF de SEP"	longueur + contenu de "FIF de SEP"

étiquette"FIF de CIG"	longueur + contenu de "FIF de CIG"	étiquette "FIF de DTC"	longueur + contenu de "FIF de DTC"

superétiquette "mode transmission sécurisée"	longueur du supergroupe	étiquette "éléments non normalisés"	longueur + contenu de "éléments non normalisés"

H.6.6.2 Relève avec retournement

Dans le cas de relève avec retournement, la même séquence de phases (00, 0, 1, 2, 3 et 4) que dans le cas de relève simple intervient après réception de DIS.

émission du document =====>

----------PPS-EOM----------> (Note)

<----------MCF----------

T2 écoulé

<----------(NSF)-(CSI)-DIS----------

----------DTR-----(phase 00)---------->

la suite est comme pour la relève simple

NOTE – Si le document envoyé avant la relève avec retournement l'est en mode transmission sécurisée de télécopie, les règles du H.6.3.2/T.30 sont applicables: si les phases 4 et 5 interviennent, la page sécuritaire est émise, ou bien PPS-EOM suivi d'octets et la réponse MCF est suivie d'octets.

H.6.7 Messages d'erreur

H.6.7.1 Messages d'erreur

S'il faut indiquer un message d'erreur, le bit n° 5 de l'octet cause de FNV, qui indique "erreur de télécopie sécurisée", doit prendre la valeur "1".

La définition de FNV se trouve au 5.3.6.2.12/T.30.

La cause d'erreur se trouve dans les octets information de diagnostic de FNV.

Selon le 5.3.6.2.12/T.30, l'octet type des messages d'erreur est "erreur de télécopie sécurisée".

Le Tableau H.10/T.30 spécifie les octets que contient le champ valeurs de "erreur de télécopie sécurisée".

Tableau H.10/T.30 – Codage des "causes d'erreur" dans le champ valeurs de "erreur de télécopie sécurisée" de FNV

Codage des octets de valeur dans FNV	Causes d'erreur
	Premier octet
bit n° 7 6 5 4 3 2 1 0 x x x x x x x 1	erreur d'enregistrement de clé publique
bit n° 7 6 5 4 3 2 1 0 x x x x x x 1 x	erreur d'enregistrement de clé publique de chiffrement
bit n° 7 6 5 4 3 2 1 0 x x x x x 1 x x	service non pris en charge
bit n° 7 6 5 4 3 2 1 0 x x x x 1 x x x	partenaire non enregistré
bit n° 7 6 5 4 3 2 1 0 x x x 1 x x x x	échec de l'authentification
bit n° 7 6 5 4 3 2 1 0 x x 1 x x x x x	réception non confirmée (Srd non valable) le nombre aléatoire reçu est rejeté par le récepteur (par exemple en cas de détection de rejeu)
bit n° 7 6 5 4 3 2 1 0 x 1 x x x x x x	réception non confirmée (UTCd non valable) modification sans objet dans le texte français (dans le texte anglais, remplacer "received by the sender" par "received from the sender")
bit n° 7 6 5 4 3 2 1 0 1 x x x x x x x	réception non confirmée (Lm non valable) la longueur indiquée par l'émetteur ne correspond pas à celle du document reçu
	Second octet
bit n° 7 6 5 4 3 2 1 0 x x x x x x x 1	réception non confirmée (jeton 4 ou jeton 4-chiffré non valable) le récepteur trouve incorrecte la signature numérique de l'émetteur
bit n° 7 6 5 4 3 2 1 0 x x x x x x 1 x	réception non confirmée (jeton 5 ou jeton 5-chiffré non valable)
NOTE 1 – Il est possible d'indiquer plusieurs causes simultanément, plusieurs bits prenant la valeur "1". NOTE 2 – Dans les versions ultérieures de la présente annexe, il pourra être défini d'autres octets pour coder d'autres causes. NOTE 3 – Pour chaque octet, le bit de plus faible poids (le plus à droite) est transmis en premier.	

H.6.7.2 Usage de FNV pour l'indication des erreurs

Après que FNV indiquant une erreur de télécopie sécurisée a été émis, le terminal qui l'a reçu en accuse réception par envoi de DCN, puis déconnecte la ligne.

Un échec de l'authentification du récepteur au cours de la phase 3 de la transmission sécurisée de télécopie est présenté dans l'exemple ci-dessous:

Côté appelant **Côté appelé**

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

échec de l'authentification

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

indication de l'échec
de l'authentification par FNV

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

déconnexion

(le document n'est pas émis)

4 Section 4

Ajouter une nouvelle Annexe I comme suit:

Annexe I

Procédure pour la transmission des images polychromes et monochromes par télécopie du Groupe 3 en utilisant la Recommandation T.43

I.1 Introduction

La présente annexe décrit les extensions à la Recommandation T.30 pour permettre la transmission d'images polychromes et monochromes en utilisant le mode de codage sans perte défini dans la Recommandation T.43 pour le mode de fonctionnement de télécopie du Groupe 3.

La présente Recommandation spécifie un mode polychrome ou monochrome facultatif qui ne doit être implémenté que si le mode polychrome ou monochrome de base associé, défini dans l'Annexe E/T.4, est lui aussi implémenté. L'implémentation du mode monochrome de la Recommandation T.43 exige l'implémentation du mode monochrome associé de l'Annexe E/T.4. De même, l'implémentation du mode polychrome de la Recommandation T.43 exige l'implémentation du mode polychrome associé de l'Annexe E/T.4.

L'objectif est de permettre la transmission efficace sur le réseau public commuté et d'autres réseaux d'une grande variété d'images, depuis les documents simples contenant par exemple des caractères rouges ou bleus jusqu'aux images de haute qualité demi-tons polychromes. Les images sont normalement obtenues par balayage des documents source par des lecteurs d'une précision de 200 pixels/25,4 mm ou plus. Les documents source sont en général des documents commerciaux soulignés de diverses couleurs, des dessins produits par ordinateurs, des images à couleurs palettisées et des images polychromes et monochromes demi-tons à haute définition.

Dans la présente annexe, trois types d'images sont pris en considération: les images à un bit par couleur CMY(K) ou RVB, les images à couleurs palettisées et les images polychromes demi-tons ou monochromes demi-teintes. Les images à un bit par couleur CMY(K) ou RVB, sont représentées à l'aide d'une palette chromatique et constituent un cas particulier des images à couleurs palettisées où chaque couleur serait représentée par une information d'un bit de couleur originale imprimable. La représentation des informations d'images polychromes repose sur les Recommandations T.42 et T.43. La méthode fondamentale est une représentation de l'espace chromatique indépendante de l'appareil, l'espace CIELAB, permettant les échanges d'informations sans ambiguïté. La décomposition et le codage des plans binaires selon la Recommandation T.82 sont également décrits dans la Recommandation T.43.

La présente annexe décrit la procédure de négociation des capacités de transmission des images polychromes et monochromes. Elle stipule les définitions et les spécifications des nouvelles entrées du champ d'information de télécopie des trames DIS/DTC et DCS du protocole de la Recommandation T.30.

Les informations relatives aux possibilités du récepteur, à celles du mode polychrome, de la précision d'amplitude de l'image dans la numérisation (bits/composante), le mode d'entrelacement, l'éclairement individuel et la gamme de valeurs font l'objet de négociations à l'étape préliminaire de la transmission de message du protocole T.30.

La présente annexe ne traite ni de la sémantique ni de la syntaxe du codage des images polychromes et monochromes lors du codage sans perte. De telles informations sont données dans la Recommandation T.43.

L'utilisation du mode avec correction d'erreurs (ECM) pour la transmission sans erreur est obligatoire dans la procédure décrite dans la présente annexe. Dans le mode de transmission avec correction d'erreurs, la séquence des informations de l'image codée est imbriquée dans la partie des données codées de la télécopie (FCD) contenue dans les trames de transmission HDLC (procédure de commande de liaison de données à haut niveau, *high-level data link control*) spécifiées à l'Annexe A/T.30.

I.2 Définitions

I.2.1 espace CIE (L*a*b*) (CIELAB): espace couleur défini par la CIE (Commission internationale de l'éclairage), tel que des couleurs ayant des différences visuelles perceptibles égales soient représentées par des points situés à des distances égales les uns des autres partout dans cet espace. Les trois composantes sont L* (luminosité), a* et b* (chrominances).

I.2.2 groupe mixte d'experts sur les images en deux tons (JBIG, *joint bi-level image experts group*) et également notation abrégée pour le mode de codage décrit dans la Recommandation T.82 et défini par ce groupe.

I.3 Références normatives

– Recommandation UIT-T T.4 (1996), *Normalisation des télécopieurs du Groupe 3 pour la transmission de documents.*

– Recommandation UIT-T T.82 (1993) | ISO/CEI 11544:1993, *Technologies de l'information – Représentation codée des images et du son – Compression progressive des images en deux tons. (Cette norme étant généralement appelée norme JBIG.)*

– Recommandation UIT-T T.42 (1996), *Méthode de représentation des demi-teintes polychromes en télécopie.*

– Recommandation UIT-T T.43 (1997), *Représentation d'images demi-tons polychromes et monochromes utilisant l'algorithme de codage sans perte pour la télécopie.*

I.4 Procédure de négociation

La négociation pour émettre et recevoir des images polychromes et monochromes par le codage de plans binaires sans perte dans le protocole de télécopie du Groupe 3 est invoquée par le positionnement des bits dans les trames DIS/DTC et DCS de la procédure préliminaire à la transmission du message (étape B) du protocole T.30.

Les trois types d'images ci-dessus sont en outre divisés en 7 classes de sous-mode de codage comme cela est spécifié dans le Tableau G.1/T.4. La relation des 4 classes de mode de codage et des 7 classes de sous-mode de codage à utiliser est indiquée dans le Tableau G.2/T.4.

La relation des 7 classes de sous-mode de codage et des 4 classes de mode de codage, indiquées par la combinaison des bits X par X + 2, est indiquée dans le Tableau I.1/T.30.

Dans le Tableau I.1/T.30, la possibilité de codage sans perte monochrome/polychrome, le nombre d'indices de palette et le nombre de bits de précision sont explicitement décrits. Les paramètres à négocier se trouvent dans le Tableau I.2/T.30.

Tableau I.1/T.30 – Correspondance entre les classes de sous-mode de codage et les bits DIS/DTC/DCS

Classe de sous-mode de codage		**Espace couleur**	**Bit 36 Codage T.43**	**Bit 69 Mode polychrome**	**Bit 71 Mode 12 bits**	
Type image	**Nombre de plans binaires**					
image à un bit par couleur	(3,4)		1	1	0	(Note)
image à couleurs palettisées	représentation de base – précision 8 bits: (1-12) x 1	Lab	1	1	0	
	représentation étendue – précision 12 bits: (1-12) x 1 précision 8 ou 12 bits: (13-16) x 1	Lab	1	1	1	
image demi-tons	demi-tons de gris 2-8 9-12	 L L	 1 1	 0 0	 0 1	
	couleur (2-8) x 3 (9-12) x 3	 Lab Lab	 1 1	 1 1	 0 1	
NOTE – Ce sous-mode de codage est un cas particulier de palette de sous-mode polychrome, auquel cas chaque plan binaire correspond à CMY(K) ou aux couleurs primaires RVB. Le nombre de plans (3 ou 4) sera désigné par l'entrée G3FAX0.						

Tableau I.2/T.30 – Capacités obligatoires et optionnelles

Obligatoires	Optionnelles
demi-tons de gris T.43	T.43 chromatique
mode 8 bits	mode 12 bits
entrelacement de bandes	entrelacement de plans
norme illuminant D50 de la CIE	illuminant individualisé
gamme de valeurs par défaut	gamme de valeurs individualisées

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série B	Moyens d'expression: définitions, symboles, classification
Série C	Statistiques générales des télécommunications
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	RGT et maintenance des réseaux: systèmes de transmission, de télégraphie, de télécopie, circuits téléphoniques et circuits loués internationaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	**Terminaux des services télématiques**
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux pour données et communication entre systèmes ouverts
Série Z	Langages de programmation

12813

Imprimé en Suisse
Genève, 1998