



UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

**UIT-T**

SECTEUR DE LA NORMALISATION  
DES TÉLÉCOMMUNICATIONS  
DE L'UIT

**X.835**

(10/96)

SÉRIE X: RÉSEAUX POUR DONNÉES ET  
COMMUNICATION ENTRE SYSTÈMES OUVERTS

Sécurité

---

**Technologies de l'information – Interconnexion  
des systèmes ouverts – Sécurité générique des  
couches supérieures: formulaire de déclaration  
de conformité d'instance de protocole de la  
syntaxe de protection du transfert**

Recommandation UIT-T X.835

(Antérieurement «Recommandation du CCITT»)

---

RECOMMANDATIONS UIT-T DE LA SÉRIE X  
**RÉSEAUX POUR DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS**

RÉSEAUX PUBLICS POUR DONNÉES	X.1-X.199
Services et fonctionnalités	X.1-X.19
Interfaces	X.20-X.49
Transmission, signalisation et commutation	X.50-X.89
Aspects réseau	X.90-X.149
Maintenance	X.150-X.179
Dispositions administratives	X.180-X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200-X.299
Modèle et notation	X.200-X.209
Définitions des services	X.210-X.219
Spécifications des protocoles en mode connexion	X.220-X.229
Spécifications des protocoles en mode sans connexion	X.230-X.239
Formulaires PICS	X.240-X.259
Identification des protocoles	X.260-X.269
Protocoles de sécurité	X.270-X.279
Objets gérés de couche	X.280-X.289
Tests de conformité	X.290-X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300-X.399
Généralités	X.300-X.349
Systèmes de transmission de données par satellite	X.350-X.399
SYSTÈMES DE MESSAGERIE	X.400-X.499
ANNUAIRE	X.500-X.599
RÉSEAUTAGE OSI ET ASPECTS DES SYSTÈMES	X.600-X.699
Réseautage	X.600-X.629
Efficacité	X.630-X.649
Dénomination, adressage et enregistrement	X.650-X.679
Notation de syntaxe abstraite numéro un (ASN.1)	X.680-X.699
GESTION OSI	X.700-X.799
Cadre général et architecture de la gestion-systèmes	X.700-X.709
Service et protocole de communication de gestion	X.710-X.719
Structure de l'information de gestion	X.720-X.729
Fonctions de gestion	X.730-X.799
<b>SÉCURITÉ</b>	<b>X.800-X.849</b>
APPLICATIONS OSI	X.850-X.899
Engagement, concomitance et rétablissement	X.850-X.859
Traitement transactionnel	X.860-X.879
Opérations distantes	X.880-X.899
TRAITEMENT OUVERT RÉPARTI	X.900-X.999

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

## 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. Au sein de l'UIT-T, qui est l'entité qui établit les normes mondiales (Recommandations) sur les télécommunications, participent quelque 179 pays membres, 84 exploitations de télécommunications reconnues, 145 organisations scientifiques et industrielles et 38 organisations internationales.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution n° 1 de la Conférence mondiale de normalisation des télécommunications (CMNT), (Helsinki, 1993). De plus, la CMNT, qui se réunit tous les quatre ans, approuve les Recommandations qui lui sont soumises et établit le programme d'études pour la période suivante.

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. Le texte de la Recommandation X.835 de l'UIT-T a été approuvé le 5 octobre 1996. Son texte est publié, sous forme identique, comme Norme internationale ISO/CEI 11586-6.

---

### 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.

© UIT 1997

Droits de reproduction réservés. Aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'UIT sauf ce qui est indiqué à la Note de bas de page 1) de l'Annexe A.

## TABLE DES MATIÈRES

		<i>Page</i>
1	Domaine d'application.....	1
2	Références.....	1
	2.1 Recommandations   Normes internationales identiques.....	1
	2.2 Paires de Recommandations   Normes internationales équivalentes par leur contenu technique .....	1
3	Définitions.....	2
4	Abréviations.....	2
5	Conventions.....	2
6	Conformité.....	2
Annexe A – Formulaire de déclaration de conformité d'instance de protocole de la syntaxe de protection du transfert .....		
	A.1 Notations defined for the proforma.....	3
	A.2 PICS numbers .....	3
	A.3 Completion of the PICS .....	4
	A.4 Date of statement .....	4
	A.5 Implementation details.....	4
	A.6 ITU-T Rec. X.833   ISO/IEC 11586-4 protocol details .....	5
	A.7 Global statement of conformance .....	5
	A.8 Supported syntax structures .....	5
	A.9 Supported PDV fields .....	6
	A.10 Establishment of encoding for Protecting Transfer Syntax .....	6
	A.11 Security transformations .....	7

## Résumé

La présente Recommandation | Norme internationale fait partie d'une série de Recommandations sur la sécurité générique des couches supérieures (GULS, *generic upper layers security*). Elle contient le formulaire de déclaration de conformité d'instance de protocole (PICS, *protocol implementation conformance statement*) pour la spécification de la syntaxe de protection du transfert figurant dans la Rec. UIT-T X.833 | ISO/CEI 11586-4 et les transformations de sécurité décrites dans l'Annexe D de la Rec. UIT-T X.830 | ISO/CEI 11586-1. La présente Recommandation | Norme internationale décrit les capacités et options normalisées sous une forme qui permet l'évaluation, aux fins de conformité, d'une réalisation donnée.

## Introduction

La présente Recommandation | Norme internationale appartient à une série de Recommandations | Normes internationales qui fournissent un ensemble de moyens destinés à la réalisation des protocoles des couches supérieures pour prendre en charge les services de sécurité. La structure de cette série est la suivante:

- 1) aperçu général, modèles et notation
- 2) définition du service «Elément de service d'échange de sécurité»
- 3) spécification du protocole «Elément de service d'échange de sécurité»
- 4) spécification de la syntaxe de protection du transfert
- 5) formulaire PICS pour l'élément de service d'échange de sécurité
- 6) formulaire PICS pour la syntaxe de protection du transfert

La présente Recommandation | Norme internationale constitue la Partie 6 de cette série.

La Partie 4 définit une syntaxe de transfert protectrice pour les communications entre systèmes ouverts dans le cadre du fonctionnement d'un mécanisme de sécurité. Pour évaluer la conformité d'une instance donnée, il faut avoir une description des capacités et des options qui ont été mises en œuvre. Une telle description est appelée Déclaration de conformité d'instance de protocole (PICS).

La présente Recommandation | Norme internationale comprend le formulaire PICS pour la syntaxe de transfert protectrice spécifiée dans la Partie 4 et les échanges de sécurité définis dans la Partie 1, Annexe D.



## NORME INTERNATIONALE

## RECOMMANDATION UIT-T

**TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DES SYSTÈMES  
OUVERTS – SÉCURITÉ GÉNÉRIQUE DES COUCHES SUPÉRIEURES:  
FORMULAIRE DE DÉCLARATION DE CONFORMITÉ D'INSTANCE  
DE PROTOCOLE DE LA SYNTAXE DE PROTECTION DU TRANSFERT**

## 1 Domaine d'application

La présente Recommandation | Norme internationale définit un formulaire de déclaration de conformité d'instance de protocole (PICS) qui a pour objet d'indiquer en détail les prescriptions de conformité de la Rec. UIT-T X.833 | ISO/CEI 11586-4 et de l'Annexe D de la Rec. UIT-T X.830 | ISO/CEI 11586-1. Ce formulaire PICS est en conformité avec les prescriptions pertinentes et les lignes directrices correspondantes applicables à un formulaire PICS, comme indiqué dans la Rec. UIT-T X.291 | ISO/CEI 9646-2. Les détails de l'utilisation de ce formulaire figurent dans la présente Recommandation | Norme internationale. Les réalisations qui se déclarent conformes à la Rec. UIT-T X.833 | ISO/CEI 11586-4 ou à l'Annexe D de la Rec. UIT-T X.830 | ISO/CEI 11586-1 doivent remplir le formulaire, dans le cadre des prescriptions de conformité. Le niveau de précision requis dans le formulaire est supérieur à la spécification du protocole, en ce sens que des précisions sont demandées en vue d'identifier sans ambiguïté la réalisation ainsi que le fournisseur.

NOTE – Les formulaires PICS se rapportent aux Recommandations et Normes de base et à elles seulement. La structure des formulaires PICS peut être élargie et précisée pour d'autres documents, à l'aide des Normes de base (par exemple, ISPICS).

## 2 Références normatives

Les Recommandations et les Normes internationales suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Recommandation | Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes Recommandations et Normes sont sujettes à révision et les parties prenantes aux accords fondés sur la présente Recommandation | Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et Normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur. Le Bureau de la normalisation des télécommunications de l'UIT tient à jour une liste des Recommandations de l'UIT-T en vigueur.

### 2.1 Recommandations | Normes internationales identiques

- Recommandation UIT-T X.830 (1995) | ISO/CEI 11586-1:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Sécurité générique des couches supérieures: aperçu général, modèles et notation.*
- Recommandation UIT-T X.833 (1995) | ISO/CEI 11586-4:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Sécurité générique des couches supérieures: spécification de la syntaxe de protection du transfert.*
- Recommandation UIT-T X.210 (1993) | ISO/CEI 10731:1994 *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de référence de base: conventions pour la définition de l'interconnexion des systèmes ouverts.*

### 2.2 Paires de Recommandations | Normes internationales équivalentes par leur contenu technique

- Recommandation UIT-T X.290 (1995), *Cadre général et méthodologie des tests de conformité OSI pour les Recommandations sur les protocoles pour les applications de l'UIT-T – Concepts généraux.*  
ISO/CEI 9646-1:1994, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadre général et méthodologie des tests de conformité OSI – Partie 1: concepts généraux.*

- Recommandation UIT-T X.291 (1995), *Cadre général et méthodologie des tests de conformité OSI pour les Recommandations sur les protocoles pour les applications de l'UIT-T – Spécification de suite de tests abstraite.*

ISO/CEI 9646-2:1994, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadre général et méthodologie des tests de conformité OSI – Partie 2: spécification des suites de tests abstraites.*

### **3 Définitions**

**3.1** La présente Recommandation | Norme internationale utilise les termes ci-après qui sont définis dans la Rec. UIT-T X.290 et l'ISO/CEI 9646-1:

- a) déclaration de conformité d'instance de protocole (PICS);
- b) formulaire PICS;
- c) informations supplémentaires sur l'instance de protocole destinées au test (PIXIT).

### **4 Abréviations**

**4.1** Les abréviations ci-après qui sont utilisées dans la présente Recommandation | Norme internationale sont définies dans la Rec. UIT-T X.290 et l'ISO/CEI 9646-1:

- a) PICS;
- b) PIXIT.

### **5 Conventions**

La présente Recommandation | Norme internationale utilise les conventions des Conventions pour la définition des services de l'OSI (Rec. UIT-T X.210 | ISO/CEI 10731). L'Annexe A qui contient le formulaire PICS a été conçue comme partie autonome de la présente Recommandation | Norme internationale, aux fins d'utilisation dans les tests et les équipements.

### **6 Conformité**

Tout formulaire PICS dit conforme sera équivalent, sur le plan technique, au formulaire PICS publié par l'UIT-T | ISO/CEI et conservera la numérotation et l'ordre des items du formulaire PICS de l'UIT-T | ISO/CEI.

Un formulaire PICS qui est conforme à la présente Recommandation | Norme internationale:

- a) décrira une instance qui est conforme à la Rec. UIT-T X.833 | ISO/CEI 11586-4;
- b) sera un formulaire PICS conforme, qui a été rempli selon les instructions données à cet effet aux A.1 et A.3;
- c) comprendra les informations nécessaires pour identifier sans ambiguïté le fournisseur et la réalisation.

Annexe A<sup>1)</sup>

## Formulaire de déclaration de conformité d'instance de protocole de la syntaxe de protection du transfert

(Cette annexe fait partie intégrante de la présente Recommandation | Norme internationale)

### A.1 Notations defined for the proforma

In order to reduce the size of tables in the PICS proforma, notations have been introduced that have allowed the use of a multi-column layout, where the columns are headed 'Status', and 'Support'. The definition of each of these follows.

#### A.1.1 Status column

This column indicates the level of support required for conformance to ITU-T Rec. X.833 | ISO/IEC 11586-4. The values are as follows:

M	Mandatory support is required.
O	Optional support is permitted for conformance to ITU-T Rec. X.833   ISO/IEC 11586-4. If implemented it must conform to the specifications and restrictions contained in ITU-T Rec. X.833   ISO/IEC 11586-4. These restrictions may affect the optionality of other items.
n/a	The item is not applicable.
<i>cn</i>	The item is conditional (where <i>n</i> is the number which identifies the condition which is applicable). The definitions for the conditional statements used in this Annex are written under the tables in which they first appear.
<i>O.n</i>	The item is optional, but the optionality is qualified (where <i>n</i> is the number which identifies the qualification which is applicable). The definitions for the qualified optional statements used in this Annex are written under the tables in which they first appear.

#### A.1.2 Support column

The 'Support' column shall be completed by the supplier or implementor to indicate the level of implementation of each feature. The proforma has been designed such that the only entries required in the 'Support' column are:

- Y Yes, the feature has been implemented
- N No, the feature has not been implemented
- Not applicable.

### A.2 PICS numbers

Each line within the PICS proforma which requires implementation detail to be entered is numbered at the left hand edge of the line. This numbering is included as a means of uniquely identifying all possible implementation details within the PICS proforma. The need for such unique referencing has been identified by the testing bodies.

The means of referencing individual responses should be to specify the following sequence:

- a) a reference to the smallest subclause enclosing the relevant item;
- b) a solidus character, '/';
- c) the reference number of the row in which the response appears;
- d) if, and only if, more than one response occurs in the row identified by the reference number, then each possible entry is implicitly labelled a, b, c, etc., from left to right, and this letter is appended to the sequence.

---

<sup>1)</sup> **Droits de reproduction du formulaire PICS**

Les utilisateurs de la présente Recommandation | Norme internationale sont autorisés à reproduire le formulaire PICS de la présente annexe pour utiliser celui-ci conformément à son objet. Ils sont également autorisés à publier le formulaire une fois celui-ci complété.



**A.6 ITU-T Rec. X.833 | ISO/IEC 11586-4 protocol details**

**A.6.1 ITU-T Rec. X.833 | ISO/IEC 11586-4 technical corrigenda implemented**

**A.7 Global statement of conformance**

Are all mandatory features implemented? (Yes or no)

NOTE – If a positive response is not given to this box, then the implementation does not conform to ITU-T Rec. X.833 | ISO/IEC 11586-4.

**A.8 Supported syntax structures**

	Syntax structure	Sending		Receiving		Reference	Comment
		Status	Support	Status	Support		
A.8/1	First PDV explicit	O		O	Part 4 5.4, 6		
A.8/2	First PDV external	O		O	Part 4 5.4, 6		
A.8/3	Subsequent PDV	O		O	Part 4 5.4, 6		

**A.9 Supported PDV fields****A.9.1 First PDV explicit**

	Field	Sending		Receiving	
		Status	Support	Status	Support
A.9.1/1	Transformation Id	c1		c1	
A.9.1/2	Static Unprotected parameters	c2		c2	
A.9.1/3	Dynamic Unprotected parameters	c2		c2	
A.9.1/4	Xformed Data	c1		c1	
c1: if [ A.8/1 ] then M else n/a					
c2: if [ A.8/1 ] then O else n/a					

**A.9.2 First PDV external**

	Field	Sending		Receiving	
		Status	Support	Status	Support
A.9.2/1	External Context Id	c3		c3	
A.9.2/2	Dynamic Unprotected parameters	c4		c4	
A.9.2/3	Xformed Data	c3		c3	
c3: if [ A.8/2 ] then M else n/a					
c4: if [ A.8/2 ] then O else n/a					

**A.9.3 Subsequent PDV**

	Field	Sending		Receiving	
		Status	Support	Status	Support
A.9.3/1	Dynamic Unprotected parameters	c6		c6	
A.9.3/2	Xformed Data	c5		c5	
c5: if [ A.8/3 ] then M else n/a					
c6: if [ A.8/3 ] then O else n/a					

**A.10 Establishment of encoding for Protecting Transfer Syntax**

		Ref	Status	Support
A.10/1	Specific encoding / decoding rules implied	Part 4 5.2 a)	O	
A.10/2	Specific encoding / decoding rules not implied	Part 4 5.2 b)	O	

**A.11 Security transformations****A.11.1 Security Transformations Supported**

		Ref	Status	Support
A.11.1/1	Directory Encrypted Transformation	Part 1 Annex D1	O	
A.11.1/2	Directory Signed Transformation	Part 1 Annex D2	O	
A.11.1/3	Directory Signature Transformation	Part 1 Annex D3	O	
A.11.1/4	GULS Signed Transformation	Part 1 Annex D4	O	
A.11.1/5	GULS Signature Transformation	Part 1 Annex D5	O	

**A.11.2 Directory Encrypted Transformation****A.11.2.1 Parameters**

No parameters defined.

**A.11.2.2 Other information**

		Status	Support	
A.11.2.2/1	Associated Protection Mapping	c7	ASN.1 name	
A.11.2.2/2	Initial Encoding Rules	c7	BER / DER / Canonical Other	
c7: if [A.11.1/1] then O else n/a				

**A.11.3 Directory Signed Transformation****A.11.3.1 Parameters**

		Sending		Receiving	
		Status	Support	Status	Support
A.11.3.1/1	(data) to be signed	c8		c8	
A.11.3.1/2	Algorithm	c9		c9	
A.11.3.1/3	Other algorithm specific parameters	c9		c9	
A.11.3.1/4	Enciphered Hash	c8		c8	
c8: if [ A.9.1/2 ] then M else n/a c9: if [ A.9.1/2 ] then O else n/a					

**A.11.3.2 Other information**

		Status	Support	
A.11.3.2/1	Associated Protection Mapping	c9	ASN.1 name	
A.11.3.2/1	Initial Encoding Rules	c9	DER	

**A.11.4 Directory Signature Transformation**

**A.11.4.1 Parameters**

		Sending		Receiving	
		Status	Support	Status	Support
A.11.4.1/1	Algorithm	c10		c10	
A.11.4.1/2	Other algorithm specific parameters	c10		c10	
A.11.4.1/3	Enciphered Hash	c11		c11	
c10: if [ A.11.1/3 ] then O else n/a c11: if [ A.11.1/3 ] then M else n/a					

**A.11.4.2 Other information**

		Status	Support	
A.11.4.2/1	Associated Protection Mapping	c10	ASN.1 name	
A.11.4.2/2	Initial Encoding Rules	c10	DER	

**A.11.5 GULS Signed Transformation**

**A.11.5.1 Parameters**

		Sending		Receiving	
		Status	Support	Status	Support
A.11.5.1/1	Unprotected item	c12		c12	
A.11.5.1/2	Initial Encoding Rules	c13		c13	
A.11.5.1/3	Sign or Seal Algorithm	c13		c13	
A.11.5.1/4	Hash Algorithm	c13		c13	
A.11.5.1/5	Key Information	c13		c13	
A.11.5.1/6	Appendix	c12		c12	
c12: if [ A.11.1/4 ] then M else n/a c13: if [ A.11.1/4 ] then O else n/a					

**A.11.5.2 Other information**

		Status	Support	
A.11.5.2/1	Associated Protection Mapping	c13	ASN.1 name	
A.11.5.2/2	Initial Encoding Rules	c13	Canonical If N, specify	
A.11.5.2/3	Direct encoding (see Part 1, 8.1)	c14	Supported	
A.11.5.2/4	Embedded encoding (see Part 1, 8.1)	c14	Supported	
A.11.5.2/5	Protecting transfer syntax (see Part 4, clause 9)	c15	GULS General If N, specify	
c14: if not [ A.11.1/4 ] then n/a else either Direct or embedded encoding must be selected c15: if not [ A.11.1 ] then n/a else if [ A.11.5.2/3 ] then GULS General is m else o				

**A.11.6 GULS signature transformation****A.11.6.1 Parameters**

		Sending		Receiving	
		Status	Support	Status	Support
A.11.6.1/1	Initial Encoding Rules	c16		c16	
A.11.6.1/2	Sign or Seal Algorithm	c16		c16	
A.11.6.1/3	Hash Algorithm	c16		c16	
A.11.6.1/4	Key Information	c16		c16	
A.11.6.1/5	Appendix	c17		c17	
c16: if [ A.11.1/5 ] then O else n/a c17: if [ A.11.1/5 ] then M else n/a					

**A.11.6.2 Other information**

		Status	Support	
A.11.6.2/1	Associated Protection Mapping	c16	ASN.1 name	
A.11.6.2/2	Initial Encoding Rules	c16	Canonical If N, specify	
A.11.6.2/3	Direct encoding (see Part 1, 8.1)	c18	Supported	
A.11.6.2/4	Embedded encoding (see Part 1, 8.1)	c18	Supported	
A.11.6.2/5	Protecting transfer syntax (see Part 4, clause 9)	c19	GULS General If N, specify	
c18: if not [ A.11.1/5 ] then n/a else either Direct or embedded encoding must be selected c19: if not [ A.11.1/5 ] then n/a else if [ A.11.5.2/3 ] then GULS General is M else O				



## SERIES DES RECOMMANDATIONS UIT-T

- Série A Organisation du travail de l'UIT-T
- Série B Moyens d'expression
- Série C Statistiques générales des télécommunications
- Série D Principes généraux de tarification
- Série E Réseau téléphonique et RNIS
- Série F Services de télécommunication non téléphoniques
- Série G Systèmes et supports de transmission
- Série H Transmission des signaux autres que téléphoniques
- Série I Réseau numérique à intégration de services
- Série J Transmission des signaux radiophoniques et télévisuels
- Série K Protection contre les perturbations
- Série L Construction, installation et protection des câbles et autres éléments des installations extérieures
- Série M Maintenance: systèmes de transmission, de télégraphie, de télécopie, circuits téléphoniques et circuits loués internationaux
- Série N Maintenance: circuits internationaux de transmission radiophoniques et télévisuels
- Série O Spécifications des appareils de mesure
- Série P Qualité de transmission téléphonique
- Série Q Commutation et signalisation
- Série R Transmission télégraphique
- Série S Equipements terminaux de télégraphie alphabétique
- Série T Equipements terminaux et protocoles 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