



UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.834

(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
l'élément de service d'échange de sécurité**

Recommandation UIT-T X.834

(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
SÉCURITÉ	X.800-X.849
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.834 de l'UIT-T a été approuvé le 5 octobre 1996. Son texte est publié, sous forme identique, comme Norme internationale ISO/CEI 11586-5.

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 dans la Note de bas de page 1) de l'Annexe A.

TABLE DES MATIÈRES

		Page
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 l'élément de service d'échange de sécurité.....		3
A.1	Notations defined for the proforma.....	3
	A.1.1 Status column.....	3
	A.1.2 Support column.....	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.832 ISO/IEC 11586-3 protocol details	5
	A.6.1 ITU-T Rec. X.832 ISO/IEC 11586-3 technical corrigenda implemented.....	5
A.7	Global statement of conformance	5
A.8	Supported APDUs.....	5
A.9	Supported APDU parameters.....	6
	A.9.1 SE-Transfer (SETR).....	6
	A.9.2 SE-U-Abort (SEAB)	6
	A.9.3 SE-P-Abort (SEPA)	6
	A.9.4 Problem codes.....	7
A.10	Abstract syntax.....	7
A.11	Application Context	7
A.12	Security exchanges.....	7
	A.12.1 Class of Security Exchange Supported	7
	A.12.2 Exchange Supported	8
	A.12.3 Directory Authentication Exchange (one way).....	8
	A.12.4 Directory Authentication Exchange (two way).....	8
	A.12.5 Simple Negotiation Exchange.....	8

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 le protocole d'élément de service d'échange de sécurité spécifiée dans la Rec. UIT-T X.832 | ISO/CEI 11586-3 et et pour les échanges de sécurité décrits dans l'Annexe C 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 dont l'objet est de prendre en charge les services de sécurité. La structure de cette série est la suivante:

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

La présente Recommandation | Norme internationale constitue la Partie 5 de cette série.

La Partie 3 définit un protocole pour la communication d'informations d'échange de sécurité 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 le protocole d'élément de service d'échange de sécurité spécifié dans la Partie 3 et les échanges de sécurité définis dans la Partie 1, Annexe C.

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 L'ÉLÉMENT DE SERVICE D'ÉCHANGE DE SÉCURITÉ**

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.832 | ISO/CEI 11586-3 et de l'Annexe C 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.832 | ISO/CEI 11586-3 ou à l'Annexe C 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 étudier 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.210 (1993) | ISO/CEI 10731:1994, *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de référence de base: conventions pour la définition des services de l'interconnexion des systèmes ouverts*.
- 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.832 (1995) | ISO/CEI 11586-3:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Sécurité générique des couches supérieures: spécification du protocole d'élément de service d'échanges de sécurité*.

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 d'interconnexion des systèmes ouverts 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 de 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 d'interconnexion des systèmes ouverts 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 de 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 suivants 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 suivantes 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 descriptives des Conventions pour la définition des services de l'OSI (Rec. UIT-T X.210 | ISO/CEI 10731). L'annexe 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.832 | ISO/CEI 11586-3;
- 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 A¹⁾**Formulaire de déclaration de conformité d'instance de protocole
de l'élément de service d'échange de sécurité**

(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.832 | ISO/IEC 11586-3. The values are as follows:

- M Mandatory support is required.
- O Optional support is permitted for conformance to ITU-T Rec. X.832 | ISO/IEC 11586-3. If implemented, it must conform to the specifications and restrictions contained in ITU-T Rec. X.832 | ISO/IEC 11586-3. These restrictions may affect the optionality of other items.
- n/a The item is not applicable.
- cn* The item is conditional (where *n* 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.
- O.n* The item is optional, but the optionality is qualified (where *n* 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.

¹⁾ **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.4 Date of statement

A.5 Implementation details

- a) supplier, implementation name, operating system, suitable hardware;
- b) system supplier and/or client of the test laboratory that is to test the implementation;
- c) information on whom to contact if there are queries concerning the content of the PICS; and
- d) the relationship between this PICS and the System Conformance Statement for the System (see note).



A.6 ITU-T Rec. X.832 | ISO/IEC 11586-3 protocol details**A.6.1 ITU-T Rec. X.832 | ISO/IEC 11586-3 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.832 | ISO/IEC 11586-3.

A.8 Supported APDUs

	APDU	Sending		Receiving		Reference	Comment
		Status	Support	Status	Support		
A.8/1	SE-TRANSFER (SETR)	M		M		Part 3 6.2	
A.8/2	SE-U-ABORT (SEAB)	M		M		Part 3 6.3	
A.8/3	SE-P-ABORT (SEPA)	M		M		Part3 6.4	

A.9 Supported APDU parameters**A.9.1 SE-Transfer (SETR)**

	Parameter	Sending		Receiving	
		Status	Support	Status	Support
A.9.1/1	SE Identifier	M		M	
A.9.1/2	Item Identifier	M		M	
A.9.1/3	SE Item	M		M	
A.9.1/4	Invocation Id (specify range supported)	O range		M range	
A.9.1/5	Start Flag	M		M	
A.9.1/6	End Flag	M		M	

A.9.2 SE-U-Absort (SEAB)

	Parameter	Sending		Receiving	
		Status	Support	Status	Support
A.9.2/1	Invocation Id	c0		M	
A.9.2/2	Item Identifier	M		M	
A.9.2/3	Errors	M		M	
c0: if A.9.1/4 supported then M else n/a					

A.9.3 SE-P-Absort (SEPA)

	Parameter	Sending		Receiving	
		Status	Support	Status	Support
A.9.3/1	Invocation Id	c0		M	
A.9.3/2	Item Identifier	M		M	
A.9.3/3	Problem Code	M		M	

A.9.4 Problem codes

	Problem code	Reference	Sending		Receiving	
			Status	Support	Status	Support
A.9.4/1	General problem codes	Part 3 6.4.1	M		M	
A.9.4/2	Transfer problem codes	Part 3 6.4.2	M		M	
A.9.4/3	Abort problem codes	Part 3 6.4.3	M		M	

A.10 Abstract syntax

What is the abstract syntax supported ? (Give object identifier)

A.11 Application Context

		Reference	Status	Support
A.11/1	Basic SESE Application Context	Part 1 Annex B	O	
A.11/2	If not give object identifier for application context supported			

A.12 Security exchanges**A.12.1 Class of Security Exchange Supported**

		Reference	Status	Support
A.12.1/1	Alternating class of security exchanges	Part 1 6.1	O	
A.12.1/2	Arbitrary class of security exchange	Part 1 6.1	O	

A.12.2 Exchange Supported

		Reference	Status	Support
A.12.2/1	Directory Authentication Exchange (one way)	Part 1 Annex C1	c1	
A.12.2/2	Directory Authentication Exchange (two way)	Part 1 Annex C2	c1	
A.12.2/3	Simple Negotiation Exchange	Part 1 Annex C3	c1	
A.12.2/4	What other security exchanges are supported (give object identifiers)			
c1: if [A.12.1/1] then O else n/a				

A.12.3 Directory Authentication Exchange (one way)

	Security Exchange Item	Sending		Receiving	
		Status	Support	Status	Support
A.12.3/1	Directory Credentials	c2		c2	
c2: if [A.12.2/1] then M else n/a					

A.12.4 Directory Authentication Exchange (two way)

	Security Exchange Item	Sending		Receiving	
		Status	Support	Status	Support
A.12.4/1	Initiator Credentials	c3		c3	
A.12.4/2	Responder Credentials	c3		c3	
A.12.4/3	Authentication Failure	c3		c3	
c3: if [A.12.2/2] then M else n/a					

A.12.5 Simple Negotiation Exchange

	Security Exchange Item	Sending		Receiving	
		Status	Support	Status	Support
A.12.5/1	Offered Ids	c4		c4	
A.12.5/2	Accepted Ids	c4		c4	
c4: if [A.12.2/3] then M else n/a					

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
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