



UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

# UIT-T

SECTOR DE NORMALIZACIÓN  
DE LAS TELECOMUNICACIONES  
DE LA UIT

# X.834

(10/96)

SERIE X: REDES DE DATOS Y COMUNICACIÓN  
ENTRE SISTEMAS ABIERTOS

Seguridad

---

**Tecnología de la información – Interconexión  
de sistemas abiertos – Seguridad genérica de  
las capas superiores: Formulario de  
declaración de conformidad de implementación  
de protocolo del elemento de servicio de  
intercambio de seguridad**

Recomendación UIT-T X.834

(Anteriormente «Recomendación del CCITT»)

---

RECOMENDACIONES DE LA SERIE X DEL UIT-T

**REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS**

|                                                                               |                    |
|-------------------------------------------------------------------------------|--------------------|
| REDES PÚBLICAS DE DATOS                                                       | X.1–X.199          |
| Servicios y facilidades                                                       | X.1–X.19           |
| Interfaces                                                                    | X.20–X.49          |
| Transmisión, señalización y conmutación                                       | X.50–X.89          |
| Aspectos de redes                                                             | X.90–X.149         |
| Mantenimiento                                                                 | X.150–X.179        |
| Disposiciones administrativas                                                 | X.180–X.199        |
| INTERCONEXIÓN DE SISTEMAS ABIERTOS                                            | X.200–X.299        |
| Modelo y notación                                                             | X.200–X.209        |
| Definiciones de los servicios                                                 | X.210–X.219        |
| Especificaciones de los protocolos en modo conexión                           | X.220–X.229        |
| Especificaciones de los protocolos en modo sin conexión                       | X.230–X.239        |
| Formularios para declaraciones de conformidad de implementación de protocolo  | X.240–X.259        |
| Identificación de protocolos                                                  | X.260–X.269        |
| Protocolos de seguridad                                                       | X.270–X.279        |
| Objetos gestionados de capa                                                   | X.280–X.289        |
| Pruebas de conformidad                                                        | X.290–X.299        |
| INTERFUNCIONAMIENTO ENTRE REDES                                               | X.300–X.399        |
| Generalidades                                                                 | X.300–X.349        |
| Sistemas de transmisión de datos por satélite                                 | X.350–X.399        |
| SISTEMAS DE TRATAMIENTO DE MENSAJES                                           | X.400–X.499        |
| DIRECTORIO                                                                    | X.500–X.599        |
| GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS | X.600–X.699        |
| Gestión de redes                                                              | X.600–X.629        |
| Eficacia                                                                      | X.630–X.649        |
| Denominación, direccionamiento y registro                                     | X.650–X.679        |
| Notación de sintaxis abstracta uno                                            | X.680–X.699        |
| GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS                                 | X.700–X.799        |
| Marco y arquitectura de la gestión de sistemas                                | X.700–X.709        |
| Servicio y protocolo de comunicación de gestión                               | X.710–X.719        |
| Estructura de la información de gestión                                       | X.720–X.729        |
| Funciones de gestión                                                          | X.730–X.799        |
| <b>SEGURIDAD</b>                                                              | <b>X.800–X.849</b> |
| APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS                            | X.850–X.899        |
| Cometimiento, concurrencia y recuperación                                     | X.850–X.859        |
| Tratamiento de transacciones                                                  | X.860–X.879        |
| Operaciones a distancia                                                       | X.880–X.899        |
| TRATAMIENTO ABIERTO DISTRIBUIDO                                               | X.900–X.999        |

*Para más información, véase la Lista de Recomendaciones del UIT-T.*

## **PREFACIO**

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. En el UIT-T, que es la entidad que establece normas mundiales (Recomendaciones) sobre las telecomunicaciones, participan unos 179 países miembros, 84 empresas de explotación de telecomunicaciones, 145 organizaciones científicas e industriales y 38 organizaciones internacionales.

Las Recomendaciones las aprueban los Miembros del UIT-T de acuerdo con el procedimiento establecido en la Resolución N.º 1 de la CMNT (Helsinki, 1993). Adicionalmente, la Conferencia Mundial de Normalización de las Telecomunicaciones (CMNT), que se celebra cada cuatro años, aprueba las Recomendaciones que para ello se le sometan y establece el programa de estudios para el periodo siguiente.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI. El texto de la Recomendación UIT-T X.834 se aprobó el 5 de octubre de 1996. Su texto se publica también, en forma idéntica, como Norma Internacional ISO/CEI 11586-5.

---

## **NOTA**

En esta Recomendación, la expresión «Administración» se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

© UIT 1997

Es propiedad. Ninguna parte de esta publicación puede reproducirse o utilizarse, de ninguna forma o por ningún medio, sea éste electrónico o mecánico, de fotocopia o de microfilm, sin previa autorización escrita por parte de la UIT, salvo lo indicado en la nota de pie de página 1) del Anexo A.

# ÍNDICE

|                                                                                                                                                          | <i>Página</i> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| 1 Alcance.....                                                                                                                                           | 1             |
| 2 Referencias normativas .....                                                                                                                           | 1             |
| 2.1 Recomendaciones   Normas Internacionales idénticas.....                                                                                              | 1             |
| 2.2 Recomendaciones   Normas Internacionales de contenido técnico equivalente.....                                                                       | 1             |
| 3 Definiciones .....                                                                                                                                     | 2             |
| 4 Abreviaturas .....                                                                                                                                     | 2             |
| 5 Convenios.....                                                                                                                                         | 2             |
| 6 Conformidad .....                                                                                                                                      | 2             |
| Anexo A – Formulario de enunciado de conformidad de implementación de protocolo (PICS) del elemento de servicio de intercambio de seguridad (SESE) ..... | 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             |

## Resumen

Esta Recomendación | Norma Internacional forma parte de una serie de Recomendaciones sobre seguridad genérica de las capas superiores (GULS, *generic upper layers security*). Se trata del formulario de declaración de conformidad de implementación de protocolo (PICS) para el protocolo del elemento de servicio de intercambio de seguridad especificado en la Rec. UIT-T X.832 | ISO/CEI 11586-3 y los intercambios de seguridad descritos en el Anexo C a la Rec. UIT-T X.830 | ISO/CEI 11586-1. La presente Recomendación | Norma Internacional proporciona la descripción de capacidades y opciones normalizadas de una manera que permite evaluar la conformidad de una implementación determinada.

## Introducción

Esta Recomendación | Norma Internacional pertenece a una serie de Recomendaciones | Norma Internacional multiparte relativas a la prestación de servicios de seguridad. Las partes son las siguientes:

- Parte 1: Sinopsis, modelos y notación
- Parte 2: Definición de servicio del elemento de servicio de intercambio de seguridad
- Parte 3: Especificación del protocolo del elemento de servicio de intercambio de seguridad
- Parte 4: Especificación de la sintaxis de transferencia de protección
- Parte 5: Formulario de PICS del elemento de servicio de intercambio de seguridad
- Parte 6: Formulario de PICS de la sintaxis de transferencia de protección

Esta Recomendación | Norma Internacional constituye la Parte 5 de la serie.

La Parte 3 define un protocolo para las comunicaciones de información de intercambio de seguridad entre sistemas abiertos como parte del funcionamiento de un mecanismo de seguridad. Para evaluar la conformidad de una implementación determinada es necesario tener una descripción de las capacidades y opciones que han sido implementadas. A esa descripción se le denomina declaración de conformidad de implementación de protocolo (PICS). La presente Recomendación | Norma Internacional incluye el formulario de PICS para el protocolo del elemento de servicio de intercambio de seguridad especificado en la Parte 3 y los intercambios de seguridad definidos en el Anexo C a la Parte 1.



## NORMA INTERNACIONAL

## RECOMENDACIÓN UIT-T

**TECNOLOGÍA DE LA INFORMACIÓN – INTERCONEXIÓN DE SISTEMAS  
ABIERTOS – SEGURIDAD GENÉRICA DE LAS CAPAS SUPERIORES:  
FORMULARIO DE DECLARACIÓN DE CONFORMIDAD DE  
IMPLEMENTACIÓN DE PROTOCOLO DEL ELEMENTO DE  
SERVICIO DE INTERCAMBIO DE SEGURIDAD**

**1 Alcance**

Esta Recomendación | Norma Internacional define un formulario de declaración de conformidad de implementación de protocolo (PICS) para la expresión detallada de los requisitos de conformidad de la Rec. UIT-T X.832 | ISO/CEI 11586-3 y el Anexo C a la Rec. UIT-T X.830 | ISO/CEI 11586-1. El formulario de PICS cumple con los requisitos pertinentes y está de acuerdo con las oportunas directrices para un formulario PICS que figuran en la Rec. UIT-T X.291 | ISO/CEI 9646-2. En la presente Recomendación | Norma Internacional se dan los detalles relativos a la utilización de este formulario. Las implementaciones que aleguen conformidad con la Rec. UIT-T X.832 | ISO/CEI 11586-3 o el Anexo C a la Rec. UIT-T X.830 | ISO/CEI 11586-1 deberán rellenar el formulario como parte de los requisitos de conformidad. El nivel de detalle requerido en el formulario supera el de la especificación del protocolo al recabar detalles con los que identificar de manera inequívoca la implementación y al suministrador.

NOTA – Los PICS están relacionadas con Recomendaciones y Normas básicas y solamente con esas Recomendaciones y Normas. La estructura de los PICS podría ampliarse y mejorarse para otros documentos que utilicen las normas básicas (por ejemplo, las ISPICS).

**2 Referencias normativas**

Las siguientes Recomendaciones y Normas Internacionales contienen disposiciones, que mediante su referencia en este texto, constituyen disposiciones de esta Recomendación | Norma Internacional. Al efectuar esta publicación estaban en vigor las ediciones indicadas. Todas las Recomendaciones y Normas son objeto de revisiones por lo que se preconiza que los participantes en acuerdos basados en la presente Recomendación | Norma Internacional investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y Normas citadas a continuación. Los miembros de la CEI y de la ISO mantienen registros de las Normas Internacionales actualmente vigentes. La Oficina de Normalización de las Telecomunicaciones de la UIT mantiene una lista de las Recomendaciones UIT-T actualmente vigentes.

**2.1 Recomendaciones | Normas Internacionales idénticas**

- Recomendación UIT-T X.210 (1993) | ISO/CEI 10731:1994, *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de referencia básico: Convenios para la definición de servicios en la interconexión de sistemas abiertos.*
- Recomendación UIT-T X.830 (1995) | ISO/CEI 11586-1:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Seguridad genérica de capas más altas: Sinopsis, modelos y notación.*
- Recomendación UIT-T X.832 (1995) | ISO/CEI 11586-3:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Seguridad genérica de las capas superiores: Especificación del protocolo del elemento de servicio de intercambio de seguridad.*

**2.2 Recomendaciones | Normas Internacionales de contenido técnico equivalente**

- Recomendación UIT-T X.290 (1995), *Metodología y marco de las pruebas de conformidad de interconexión de sistemas abiertos de las Recomendaciones sobre los protocolos para aplicaciones del UIT-T – Conceptos generales.*
- ISO/IEC 9646-1:1994, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 1: General concepts.*

- Recomendación UIT-T X.291 (1995), *Metodología y marco de las pruebas de conformidad de interconexión de sistemas abiertos de las Recomendaciones sobre los protocolos para aplicaciones del UIT-T: Especificación de sucesiones de pruebas abstractas.*
- ISO/IEC 9646-2:1994, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 2: Abstract Test Suite specification*

### 3 Definiciones

**3.1** Los siguientes términos utilizados en esta Recomendación | Norma Internacional están definidos en la Rec. UIT-T X.290 e ISO/CEI 9646-1:

- a) Declaración de conformidad de implementación de protocolo (PICS).
- b) Formulario de PICS.
- c) Información suplementaria sobre implementación de protocolo para pruebas (PIXIT).

### 4 Abreviaturas

**4.1** Las siguientes abreviaturas, utilizadas en esta Recomendación | Norma Internacional, están definidas en la Rec. UIT-T X.290 e ISO/CEI 9646-1:

- a) PICS: Declaración de conformidad de implementación de protocolo (*protocol implementation conformance statement*).
- b) PIXIT: Información suplementaria sobre implementación de protocolo para pruebas (*protocol implementation extra information for testing*).

### 5 Convenios

La presente Recomendación | Norma Internacional utiliza los convenios descriptivos de servicios OSI de la Rec. UIT-T X.210 | ISO/CEI 10731. El formulario de PICS anexo se ha concebido de manera que sea una sección reparable de la presente Recomendación | Norma Internacional, para su utilización en pruebas y adquisiciones.

### 6 Conformidad

Un formulario PICS conforme deberá ser técnicamente equivalente a un formulario de PICS publicado por el UIT-T | ISO/CEI y mantendrá la numeración y el orden de los ítems del formulario de PICS del UIT-T | ISO/CEI.

Un PICS que se atenga a la presente Recomendación | Norma Internacional deberá:

- a) describir una implementación que esté de acuerdo con la Rec. UIT-T X.832 | ISO/CEI 11586-3;
- b) ser un formulario de PICS conforme, rellenado de acuerdo con las instrucciones que se dan al respecto en A.1 y A.3;
- c) incluir la información necesaria para identificar de manera inequívoca tanto al suministrador como la implementación.

**Anexo A<sup>1)</sup>****Formulario de enunciado de conformidad de implementación de protocolo (PICS)  
del elemento de servicio de intercambio de seguridad (SESE)**

(Este anexo es parte integrante de esta Recomendación | Norma Internacional)

**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.

<sup>1)</sup> **Comunicado sobre derechos de autor del formulario PICS:**

Los usuarios de esta Recomendación | Norma Internacional pueden reproducir libremente el formulario de PICS de este anexo a fin de que pueda ser utilizado para los fines previstos, y pueden además publicar el PICS cumplimentado.

### A.3 Completion of the PICS

The implementor shall complete all entries in the column marked 'Support'. In certain clauses of the PICS proforma further guidance for completion may be necessary. Such guidance shall supplement the guidance given in this clause and shall have a scope restricted to the clause in which it appears. In addition, other specifically identified information shall be provided by the implementor where requested. No changes shall be made to the proforma except the completion as required. Recognizing that the level of detail required may, in some instances, exceed the space available for responses a number of responses specifically allow for the addition of appendices to the PICS.

#### A.4 Date of statement

Date of statement? (yy-mm-dd)

## A.5 Implementation details

The supplier of the protocol implementation shall specify the information necessary to uniquely identify the implementation and the system in which it may reside. This may include details of:

- 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).

NOTE – The System Conformance Statement is identified in ITU-T Rec. X.290 and ISO/IEC 9646-1. It contains a declaration of the layers of the Reference Model covered by the implementation to be tested.



**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<br>6.2 |         |
| A.8/2 | SE-U-ABORT (SEAB)  | M       |         | M         |         | Part 3<br>6.3 |         |
| A.8/3 | SE-P-ABORT (SEPA)  | M       |         | M         |         | Part3<br>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<br>range |         | M<br>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<br>6.4.1 | M       |         | M         |         |
| A.9.4/2 | Transfer problem codes | Part 3<br>6.4.2 | M       |         | M         |         |
| A.9.4/3 | Abort problem codes    | Part 3<br>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<br>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<br>6.1 | O      |         |
| A.12.1/2 | Arbitrary class of security exchange    | Part 1<br>6.1 | O      |         |

**A.12.2 Exchange Supported**

|                                     |                                                                          | Reference          | Status | Support |
|-------------------------------------|--------------------------------------------------------------------------|--------------------|--------|---------|
| A.12.2/1                            | Directory Authentication Exchange (one way)                              | Part 1<br>Annex C1 | c1     |         |
| A.12.2/2                            | Directory Authentication Exchange (two way)                              | Part 1<br>Annex C2 | c1     |         |
| A.12.2/3                            | Simple Negotiation Exchange                                              | Part 1<br>Annex C3 | c1     |         |
| A.12.2/4                            | What other security exchanges are supported<br>(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 DE RECOMENDACIONES DEL UIT-T

|                |                                                                                                                            |
|----------------|----------------------------------------------------------------------------------------------------------------------------|
| Serie A        | Organización del trabajo del UIT-T                                                                                         |
| Serie B        | Medios de expresión                                                                                                        |
| Serie C        | Estadísticas generales de telecomunicaciones                                                                               |
| Serie D        | Principios generales de tarificación                                                                                       |
| Serie E        | Red telefónica y RDSI                                                                                                      |
| Serie F        | Servicios de telecomunicación no telefónicos                                                                               |
| Serie G        | Sistemas y medios de transmisión                                                                                           |
| Serie H        | Transmisión de señales no telefónicas                                                                                      |
| Serie I        | Red digital de servicios integrados                                                                                        |
| Serie J        | Transmisiones de señales radiofónicas y de televisión                                                                      |
| Serie K        | Protección contra las interferencias                                                                                       |
| Serie L        | Construcción, instalación y protección de los cables y otros elementos de planta exterior                                  |
| Serie M        | Mantenimiento: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales |
| Serie N        | Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión                                   |
| Serie O        | Especificaciones de los aparatos de medida                                                                                 |
| Serie P        | Calidad de transmisión telefónica                                                                                          |
| Serie Q        | Conmutación y señalización                                                                                                 |
| Serie R        | Transmisión telegráfica                                                                                                    |
| Serie S        | Equipos terminales para servicios de telegrafía                                                                            |
| Serie T        | Equipos terminales y protocolos para los servicios de telemática                                                           |
| Serie U        | Conmutación telegráfica                                                                                                    |
| Serie V        | Comunicación de datos por la red telefónica                                                                                |
| <b>Serie X</b> | <b>Redes de datos y comunicación entre sistemas abiertos</b>                                                               |
| Serie Z        | Lenguajes de programación                                                                                                  |