UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T X.501

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Corrigendum 2
(02/2001)

SERIE X: REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

Directorio

Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Modelos

Corrigendum técnico 2

Recomendación UIT-T X.501 (1997) – Corrigendum 2

(Anteriormente Recomendación del CCITT)

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

REDES PÚBLICAS DE DATOS	
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	
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	
Generalidades	X.300–X.349
Sistemas de transmisión de datos por satélite	X.350–X.369
Redes basadas en el protocolo Internet	X.370–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	
Gestión de redes	X.600–X.629
Eficacia	X.630–X.639
Calidad de servicio	X.640–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	
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 y funciones de arquitectura de gestión distribuida abierta	X.730–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Compromiso, concurrencia y recuperación	X.850–X.859
Procesamiento de transacciones	X.860–X.879
Operaciones a distancia	X.880–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999

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

NORMA INTERNACIONAL ISO/CEI 9594-2
RECOMENDACIÓN UIT-T X.501

Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Modelos

CORRIGENDUM TÉCNICO 2

Orígenes

El corrigendum 2 a la Recomendación UIT-T X.501 (1997), preparado por la Comisión de Estudio 7 (2001-2004) del UIT-T, fue aprobado el 2 de febrero de 2001. Se publica también un texto idéntico como corrigendum técnico 2 a la Norma Internacional ISO/CEI 9594-2.

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. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

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.

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.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB.

ÍNDICE

Página

NORMA INTERNACIONAL
RECOMENDACIÓN UIT-T

Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Modelos

CORRIGENDUM TÉCNICO 2

NOTA – Este corrigendum técnico incluye el resultado de las resoluciones por votación sobre los proyectos de corrigenda técnicos 3 y 4.

1) Informes de defectos tratados en el proyecto de corrigendum técnico 3

(Resoluciones relativas a los informes de defectos 229 y 230.)

1.1) Lo que sigue corrige defectos notificados en los informes de defectos 9594/229-230

En 2.1:

Sustituir:

– Recomendación UIT-T X.525 (1997) | ISO/CEI 9594-8:1999, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Replicación.*

por:

– Recomendación UIT-T X.525 (1997) | ISO/CEI 9594-9:1998, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Replicación.*

En 17.4.3:

En la especificación de **attributeValueSecurityLabelContext**, *sustituir* **SYNTAX** *por* **WITH SYNTAX**

Suprimir el tipo **KeyIdentifier**.

Efectuar los mismos cambios en el anexo P.

En 18.1.2:

Sustituir el cuarto párrafo por:

Las firmas digitales aplicadas a toda la inserción no incluyen atributos operacionales, ni colectivos, ni el propio **attributeIntegrityInfo**. Se incluyen todos los contextos de valor de atributo.

Suprimir el quinto párrafo ("Junto con la firma digital ...").

Cambiar la definición del atributo **attributeIntegrityInfo** *y sus correspondientes definiciones por:*

```
attributeIntegrityInfo ATTRIBUTE  ::=  {
        WITH SYNTAX                    AttributeIntegrityInfo
        ID                             id-at-attributeIntegrityInfo}

AttributeIntegrityInfo  ::=  SIGNED { SEQUENCE  {
        scope           Scope,                          -- Identifies the attributes protected
        signer          Signer      OPTIONAL,           -- Authority or data originators name
        attribsHash     AttribsHash } }                 -- Hash value of protected attributes

Signer  ::=  CHOICE {
        thisEntry   [0]   EXPLICIT ThisEntry,
        thirdParty  [1]   SpecificallyIdentified }
```

```
ThisEntry ::= CHOICE {
        onlyOne  NULL,
        specific IssuerAndSerialNumber }

IssuerAndSerialNumber ::= SEQUENCE {
        issuer       Name,
        serial CertificateSerialNumber }

SpecificallyIdentified ::= SEQUENCE {
        name         GeneralName,
        issuer       GeneralName  OPTIONAL,
        serial       CertificateSerialNumber  OPTIONAL }
        ( WITH COMPONENTS { …, issuer PRESENT, serial PRESENT } |
        ( WITH COMPONENTS { …, issuer ABSENT, serial ABSENT } ) )

Scope ::= CHOICE {
        wholeEntry      [0]   NULL,          -- Signature protects all attribute values in this entry
        selectedTypes   [1]   SelectedTypes
                              -- Signature protects all attribute values of the selected attribute types
        }

SelectedTypes ::= SEQUENCE SIZE (1..MAX) OF AttributeType

AttribsHash ::= HASH { SEQUENCE SIZE (1..MAX) OF Attribute }
                -- Attribute type and values with associated context values for the selected Scope
```

Añadir el siguiente texto después del ASN.1 anterior:

Un valor de **AttributeIntegrityInfo** puede crearse de tres maneras diferentes:

a) Una autoridad administrativa puede crear y firmar el valor, y la clave pública para verificar que la firma es conocida por medios fuera de línea.

b) El propietario de la inserción, es decir, el objeto representado por la inserción, puede crear y firmar el valor. Si el propietario tiene varios certificados, o se cree que los tendrá en el futuro, el certificado ha de ser identificado por la CA que emite el certificado junto con el número de serie del certificado.

c) Un tercero puede crear y firmar el valor. Se requiere el nombre del firmante, el nombre de la CA que emite el certificado y el número de serie del certificado.

Si el alcance es **wholeEntry**, se ordenarán todos los atributos aplicables como se especifica para el tipo Conjunto-de (set-of) en 6.1 de la Rec. UIT-T X.509 | ISO/CEI 9594-8. Si el alcance es **selectedTypes**, el orden será el mismo indicado en **SelectedTypes**.

NOTA – Si un usuario no recupera todos los atributos completos definidos dentro del tipo de datos **Scope**, no será posible para el usuario verificar la integridad de los atributos.

Suprimir 18.1.2.1.

Los cambios en ASN.1 se efectuarán también en el anexo P.

Sustituir 18.1.3 por:

18.1.3 Contexto para la protección de un valor de atributo único

A continuación se define un contexto para mantener una firma digital junto con la información de control asociada que proporciona la integridad para un valor de atributo único. Cualquier contexto de valor de atributo está incluido en la verificación de integridad, salvo los contextos usados para el mantenimiento de las firmas.

```
attributeValueIntegrityInfoContext  CONTEXT  ::= {
        WITH SYNTAX     AttributeValueIntegrityInfo
        ID              id-avc-attributeValueIntegrityInfoContext }

AttributeValueIntegrityInfo  ::=  SIGNED { SEQUENCE {
        signer          Signer      OPTIONAL,        -- Authority or data originators name
        aVIHash         AVIHash } }                  -- Hash value of protected attribute
```

```
AVIHash  ::=  HASH { AttributeTypeValueContexts }
                -- Attribute type and value with associated context values

AttributeTypeValueContexts ::= SEQUENCE {
      type              ATTRIBUTE.&id ({SupportedAttributes}),
      value             ATTRIBUTE.&Type ({SupportedAttributes}{@type}),
      contextList       SET SIZE (1..MAX) OF Context OPTIONAL }
```

Los atributos **contextList** se ordenarán como se especifica para el tipo Conjunto-de (set-of) en 6.1 de la Rec. X.509 | ISO/CEI 9594-8.

Cambiar la ASN.1 en el anexo P conforme a lo anterior y suprima el tipo de datos **AVIAssertion**.

En el anexo B:

Suprimir la importación **OPTIONALLY-SIGNED** *de* **DirectoryAbstractService**.

En el anexo C:

Sustituir **userApplication** *por* **userApplications** *en el componente* **application** *de* **AttributeTypeInformation**.

En el anexo D:

Añadir **directoryAbstractService** *a la importación de* **UsefulDefinitions**.

Añadir **SupportedAttributes** *a la importación de* **InformationFramework**.

Añadir:

```
Filter
      FROM DirectoryAbstractService directoryAbstractService
```

En el anexo F:

Añadir **enhancedSecurity** *a la importación de* **UsefulDefinitions**

Suprimir **OPTIONALLY-PROTECTED** *y* **DIRQOP** *de la importación de* **EnhancedSecurity**. *Añadir en su lugar* **OPTIONALLY-PROTECTED-SEQ**.

En el anexo P:

Todos los cambios al anexo P se han considerado incluidos por la resolución del informe de defectos 228.

2) Informes de defectos tratados en el proyecto de corrigendum técnico 4

(Trata las resoluciones relativas a los informes de defectos 228, 242, 255, 260, 261, 267 y 269.)

2.1) Lo que sigue corrige defectos notificados en los informes de defectos 9594/228

Añadir al comienzo de 15.3 inmediatamente antes de 15.3.1:

Advertencia – Se sabe que 15.3.1 y 15.3.2 contienen especificaciones no válidas, por lo cual se desaprueban estas subcláusulas. En una edición futura se suprimirán las especificaciones desaprobadas o se proporcionará texto actualizado.

Se suministran las siguientes especificaciones para preservar la capacidad opcionalmente firmada prevista en la edición 2 de estas Especificaciones de directorio y para permitir que la capacidad se extienda a todas las operaciones y a todos los errores:

OPTIONALLY-PROTECTED es un tipo de datos parametrizado en el cual el parámetro es un tipo de datos cuyos valores pueden, a opción del generador, estar acompañados de su firma digital. Esta capacidad se especifica por medio del siguiente tipo:

```
OPTIONALLY-PROTECTED { Type }  ::=  CHOICE {
      unsigned          Type,
      signed            SIGNED {Type} }
```

OPTIONALLY-PROTECTED-SEQ se utiliza en lugar de **OPTIONALLY-PROTECTED** cuando el tipo de datos protegido es un tipo de datos en secuencia no rotulado.

```
OPTIONALLY-PROTECTED-SEQ { Type } ::= CHOICE {
        unsigned        Type,
        signed    [0]   SIGNED { Type } }
```

El tipo de datos parametrizado **SIGNED**, que describe la forma del formulario firmado de la información, se especifica en la Rec. UIT-T X.509 | ISO/CEI 9594-8.

Añadir al comienzo de 18.2 inmediatamente antes de 18.2.1:

Advertencia – Se sabe que esta subcláusula contiene especificaciones no válidas, por lo cual se desaprueba esta subcláusula. En una edición futura se suprimirán las especificaciones desaprobadas o se proporcionará texto actualizado.

En el anexo A, añadir el siguiente punto de comentario ASN.1:

```
-- securityExchange                 ID    ::=   {ds 32}
-- directorySecurityExchanges       ID    ::=   {module directorySecurityExchanges (29) 1}
-- id-se                            ID    ::=   securityExchange
```

En la cláusula 26, suprima toda aparición de:

,

DIRQOP.&…-QOP{@dirqop}

y cambie toda aparición de:

OPTIONALLY-PROTECTED

por:

OPTIONALLY-PROTECTED-SEQ

Se introducirán los mismos cambios en el anexo F.

Sustituir el anexo P por:

Anexo P

Seguridad ampliada

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

Se sabe que este módulo contiene especificaciones no válidas, por lo cual se desaprueba parte de este módulo. La parte desaprobada se indica mediante puntos de comentario ASN.1. En una edición futura se suprimirán las especificaciones desaprobadas o se proporcionarán especificaciones actualizadas.

```
EnhancedSecurity { joint-iso-itu-t ds(5) modules(1) enhancedSecurity(28) 1 }
DEFINITIONS IMPLICIT TAGS  ::=
BEGIN

-- EXPORTS All --

IMPORTS

-- from ITU-T Rec. X.501 | ISO/IEC 9594-2

      authenticationFramework, basicAccessControl, certificateExtensions, id-at, id-avc, id-mr,
      informationFramework, upperBounds
            FROM UsefulDefinitions { joint-iso-itu-t ds(5) module(1) usefulDefinitions(0) 3 }

      Attribute, ATTRIBUTE, AttributeType, Context, CONTEXT, MATCHING-RULE, Name,
      objectIdentifierMatch, SupportedAttributes
            FROM InformationFramework informationFramework

      AttributeTypeAndValue
            FROM BasicAccessControl basicAccessControl

-- from ITU-T Rec. X.509 | ISO/IEC 9594-8

      AlgorithmIdentifier, CertificateSerialNumber, ENCRYPTED{}, HASH{}, SIGNED{}
            FROM AuthenticationFramework authenticationFramework

      GeneralName, KeyIdentifier
            FROM CertificateExtensions certificateExtensions

      ub-privacy-mark-length
            FROM UpperBounds upperBounds ;
-- from GULS
-- SECURITY-TRANSFORMATION, PROTECTION-MAPPING, PROTECTED
--      FROM Notation { joint-iso-ccitt genericULS (20) modules (1) notation (1) }

-- dirSignedTransformation, KEY-INFORMATION
--      FROM GulsSecurityTransformations { joint-iso-ccitt genericULS (20) modules (1)
--            gulsSecurityTransformations (3) }

-- signed
--      FROM GulsSecurityTransformations { joint-iso-ccitt genericULS (20) modules (1)
--            dirProtectionMappings (4) };

-- The "signed" Protection Mapping and associated "dirSignedTransformations" imported
-- from the Generic Upper Layers Security specification (ITU-T Rec. X.830 | ISO/IEC 11586-1)
-- results in identical encoding as the same data type used with the SIGNED as defined in
-- ITU-T REC. X.509 | ISO/IEC 9594-8

-- The three statements below are provided temporarily to allow signed operations to be supported as in edition 3.
```

```
OPTIONALLY-PROTECTED { Type } ::= CHOICE {
        unsigned        Type,
        signed          SIGNED {Type} }

OPTIONALLY-PROTECTED-SEQ { Type } ::= CHOICE {
        unsigned        Type,
        signed    [0]   SIGNED { Type } }
-- The following out-commented ASN.1 specifications are known to be erroneous and are therefore deprecated.

-- genEncryptedTransform {KEY-INFORMATION: SupportedKIClasses } SECURITY-TRANSFORMATION ::=
--      {
--      IDENTIFIER                  { enhancedSecurity gen-encrypted(2) }
--      INITIAL-ENCODING-RULES      { joint-iso-itu-t asn1(1) ber(1) }
                                    -- This default for initial encoding rules may be overridden
                                    -- using a static protected parameter (initEncRules).
--      XFORMED-DATA-TYPE           SEQUENCE {
--              initEncRules        OBJECT IDENTIFIER DEFAULT { joint-iso-itu-t asn1(1) ber(1) },
--              encAlgorithm        AlgorithmIdentifier OPTIONAL, --  -- Identifies the encryption algorithm,
--              keyInformation      SEQUENCE {
--                      kiClass     KEY-INFORMATION.&kiClass ({SupportedKIClasses}),
--                      keyInfo     KEY-INFORMATION.&KiType ({SupportedKIClasses} {@kiClass})
--                                  } OPTIONAL,
                        -- Key information may assume various formats, governed by supported members
                        -- of the KEY-INFORMATION information object class (defined in ITU-T
                        -- Rec. X.830 | ISO/IEC 11586-1)
--              encData     BIT STRING ( CONSTRAINED BY {
                        -- the encData value must be generated following
                        -- the procedure specified in 17.3.1-- })
--              }
--      }

-- encrypted PROTECTION-MAPPING ::= {
--      SECURITY-TRANSFORMATION { genEncryptedTransform } }

-- signedAndEncrypt PROTECTION-MAPPING ::= {
--      SECURITY-TRANSFORMATION { signedAndEncryptedTransform } }

-- signedAndEncryptedTransform {KEY-INFORMATION: SupportedKIClasses}
--      SECURITY-TRANSFORMATION ::= {
--          IDENTIFIER                  { enhancedSecurity dir-encrypt-sign (1) }
--          INITIAL-ENCODING-RULES      { joint-iso-itu-t asn1 (1) ber-derived (2) distinguished-encoding (1) }
--          XFORMED-DATA-TYPE
--              PROTECTED
--              {
--                  PROTECTED
--                  {
--                  ABSTRACT-SYNTAX.&Type,
--                  signed
--                  },
--              encrypted
--              }
--      }

-- OPTIONALLY-PROTECTED {ToBeProtected, PROTECTION-MAPPING:generalProtection} ::=
--      CHOICE {
--          toBeProtected   ToBeProtected,
                                -- no DIRQOP specified for operation
--          signed          PROTECTED {ToBeProtected, signed},
                                -- DIRQOP is Signed
--          protected       [APPLICATION 0]
--                              PROTECTED { ToBeProtected, generalProtection } }
                                -- DIRQOP is other than Signed
```

```
-- defaultDirQop ATTRIBUTE  ::=  {
--      WITH SYNTAX                     OBJECT IDENTIFIER
--      EQUALITY MATCHING RULE          objectIdentifierMatch
--      USAGE                           directoryOperation
--      ID                              id-at-defaultDirQop }


-- DIRQOP  ::=  CLASS
-- This information object class is used to define the quality of protection
-- required throughout directory operation.
-- The Quality Of Protection can be signed, encrypted, signedAndEncrypt
--  {
--      &dirqop-Id                                  OBJECT IDENTIFIER UNIQUE,
--      &dirBindError-QOP                           PROTECTION-MAPPING:protectionReqd,
--      &dirErrors-QOP                              PROTECTION-MAPPING:protectionReqd,
--      &dapReadArg-QOP                             PROTECTION-MAPPING:protectionReqd,
--      &dapReadRes-QOP                             PROTECTION-MAPPING:protectionReqd,
--      &dapCompareArg-QOP                          PROTECTION-MAPPING:protectionReqd,
--      &dapCompareRes-QOP                          PROTECTION-MAPPING:protectionReqd,
--      &dapListArg-QOP                             PROTECTION-MAPPING:protectionReqd,
--      &dapListRes-QOP                             PROTECTION-MAPPING:protectionReqd,
--      &dapSearchArg-QOP                           PROTECTION-MAPPING:protectionReqd,
--      &dapSearchRes-QOP                           PROTECTION-MAPPING:protectionReqd,
--      &dapAbandonArg-QOP                          PROTECTION-MAPPING:protectionReqd,
--      &dapAbandonRes-QOP                          PROTECTION-MAPPING:protectionReqd,
--      &dapAddEntryArg-QOP                         PROTECTION-MAPPING:protectionReqd,
--      &dapAddEntryRes-QOP                         PROTECTION-MAPPING:protectionReqd,
--      &dapRemoveEntryArg-QOP                      PROTECTION-MAPPING:protectionReqd,
--      &dapRemoveEntryRes-QOP                      PROTECTION-MAPPING:protectionReqd,
--      &dapModifyEntryArg-QOP                      PROTECTION-MAPPING:protectionReqd,
--      &dapModifyEntryRes-QOP                      PROTECTION-MAPPING:protectionReqd,
--      &dapModifyDNArg-QOP                         PROTECTION-MAPPING:protectionReqd,
--      &dapModifyDNRes-QOP                         PROTECTION-MAPPING:protectionReqd,
--      &dspChainedOp-QOP                           PROTECTION-MAPPING:protectionReqd,
--      &dispShadowAgreeInfo-QOP                    PROTECTION-MAPPING:protectionReqd,
--      &dispCoorShadowArg-QOP                      PROTECTION-MAPPING:protectionReqd,
--      &dispCoorShadowRes-QOP                      PROTECTION-MAPPING:protectionReqd,
--      &dispUpdateShadowArg-QOP                    PROTECTION-MAPPING:protectionReqd,
--      &dispUpdateShadowRes-QOP                    PROTECTION-MAPPING:protectionReqd,
--      &dispRequestShadowUpdateArg-QOP             PROTECTION-MAPPING:protectionReqd,
--      &dispRequestShadowUpdateRes-QOP             PROTECTION-MAPPING:protectionReqd,
--      &dopEstablishOpBindArg-QOP                  PROTECTION-MAPPING:protectionReqd,
--      &dopEstablishOpBindRes-QOP                  PROTECTION-MAPPING:protectionReqd,
--      &dopModifyOpBindArg-QOP                     PROTECTION-MAPPING:protectionReqd,
--      &dopModifyOpBindRes-QOP                     PROTECTION-MAPPING:protectionReqd,
--      &dopTermOpBindArg-QOP                       PROTECTION-MAPPING:protectionReqd,
--      &dopTermOpBindRes-QOP                       PROTECTION-MAPPING:protectionReqd
-- }
-- WITH SYNTAX
--  {
--      DIRQOP-ID                       &dirqop-Id
--      DIRECTORYBINDERROR-QOP          &dirBindError-QOP
--      DIRERRORS-QOP                   &dirErrors-QOP
--      DAPREADARG-QOP                  &dapReadArg-QOP
--      DAPREADRES-QOP                  &dapReadRes-QOP
--      DAPCOMPAREARG-QOP               &dapCompareArg-QOP
--      DAPCOMPARERES-QOP               &dapCompareRes-QOP
--      DAPLISTARG-QOP                  &dapListArg-QOP
--      DAPLISTRES-QOP                  &dapListRes-QOP
--      DAPSEARCHARG-QOP                &dapSearchArg-QOP
--      DAPSEARCHRES-QOP                &dapSearchRes-QOP
--      DAPABANDONARG-QOP               &dapAbandonArg-QOP
--      DAPABANDONRES-QOP               &dapAbandonRes-QOP
--      DAPADDENTRYARG-QOP              &dapAddEntryArg-QOP
```

```
--      DAPADDENTRYRES-QOP                      &dapAddEntryRes-QOP
--      DAPREMOVEENTRYARG-QOP                   &dapRemoveEntryArg-QOP
--      DAPREMOVEENTRYRES-QOP                   &dapRemoveEntryRes-QOP
--      DAPMODIFYENTRYARG-QOP                   &dapModifyEntryArg-QOP
--      DAPMODIFYENTRYRES-QOP                   &dapModifyEntryRes-QOP
--      DAPMODIFYDNARG-QOP                      &dapModifyDNArg-QOP
--      DAPMODIFYDNRES-QOP                      &dapModifyDNRes-QOP
--      DSPCHAINEDOP-QOP                        &dspChainedOp-QOP
--      DISPSHADOWAGREEINFO-QOP                 &dispShadowAgreeInfo-QOP
--      DISPCOORSHADOWARG-QOP                   &dispCoorShadowArg-QOP
--      DISPCOORSHADOWRES-QOP                   &dispCoorShadowRes-QOP
--      DISPUPDATESHADOWARG-QOP                 &dispUpdateShadowArg-QOP
--      DISPUPDATESHADOWRES-QOP                 &dispUpdateShadowRes-QOP
--      DISPREQUESTSHADOWUPDATEARG-QOP          &dispRequestShadowUpdateArg-QOP
--      DISPREQUESTSHADOWUPDATERES-QOP          &dispRequestShadowUpdateRes-QOP
--      DOPESTABLISHOPBINDARG-QOP               &dopEstablishOpBindArg-QOP
--      DOPESTABLISHOPBINDRES-QOP               &dopEstablishOpBindRes-QOP
--      DOPMODIFYOPBINDARG-QOP                  &dopModifyOpBindArg-QOP
--      DOPMODIFYOPBINDRES-QOP                  &dopModifyOpBindRes-QOP
--      DOPTERMINATEOPBINDARG-QOP               &dopTermOpBindArg-QOP
--      DOPTERMINATEOPBINDRES-QOP               &dopTermOpBindRes-QOP
-- }

attributeValueSecurityLabelContext CONTEXT ::= {
        WITH SYNTAX     SignedSecurityLabel     -- At most one security label context can be assigned to an
                                                -- attribute value
        ID              id-avc-attributeValueSecurityLabelContext }

SignedSecurityLabel  ::=  SIGNED {SEQUENCE  {
        attHash         HASH {AttributeTypeAndValue},
        issuer          Name            OPTIONAL,  -- name of labelling authority
        keyIdentifier   KeyIdentifier   OPTIONAL,
        securityLabel   SecurityLabel } }

SecurityLabel  ::=  SET {
        security-policy-identifier      SecurityPolicyIdentifier        OPTIONAL,
        security-classification         SecurityClassification          OPTIONAL,
        privacy-mark                    PrivacyMark                     OPTIONAL,
        security-categories             SecurityCategories              OPTIONAL }
                (ALL EXCEPT ( {-- none, at least one component shall be present -- } ) )

SecurityPolicyIdentifier  ::=  OBJECT IDENTIFIER

SecurityClassification ::= INTEGER {
        unmarked        (0),
        unclassified    (1),
        restricted      (2),
        confidential    (3),
        secret          (4),
        top-secret      (5) }

PrivacyMark  ::=  PrintableString (SIZE (1..ub-privacy-mark-length))

SecurityCategories ::= SET SIZE (1..MAX) OF SecurityCategory

clearance  ATTRIBUTE  ::=  {
        WITH SYNTAX     Clearance
        ID              id-at-clearance }

Clearance  ::=  SEQUENCE  {
        policyId                OBJECT IDENTIFIER,
        classList               ClassList                       DEFAULT {unclassified},
        securityCategories      SET SIZE (1..MAX) OF SecurityCategory   OPTIONAL }
```

```
ClassList ::= BIT STRING {
        unmarked        (0),
        unclassified    (1),
        restricted      (2),
        confidential    (3),
        secret          (4),
        topSecret       (5) }

SecurityCategory ::= SEQUENCE {
        type    [0]   SECURITY-CATEGORY.&id ({SecurityCategoriesTable}),
        value   [1]   EXPLICIT SECURITY-CATEGORY.&Type ({SecurityCategoriesTable} {@type}) }

SECURITY-CATEGORY ::= TYPE-IDENTIFIER

SecurityCategoriesTable SECURITY-CATEGORY ::= { ... }

attributeIntegrityInfo ATTRIBUTE ::= {
        WITH SYNTAX                     AttributeIntegrityInfo
        ID                              id-at-attributeIntegrityInfo }

AttributeIntegrityInfo ::= SIGNED { SEQUENCE {
        scope           Scope,                  -- Identifies the attributes protected
        signer          Signer      OPTIONAL,   -- Authority or data originators name
        attribsHash     AttribsHash } }         -- Hash value of protected attributes

Signer ::= CHOICE {
        thisEntry   [0]   EXPLICIT ThisEntry,
        thirdParty  [1]   SpecificallyIdentified }

ThisEntry ::= CHOICE {
        onlyOne     NULL,
        specific    IssuerAndSerialNumber }

IssuerAndSerialNumber ::= SEQUENCE {
        issuer      Name,
        serial      CertificateSerialNumber }

SpecificallyIdentified ::= SEQUENCE {
        name        GeneralName,
        issuer      GeneralName                 OPTIONAL,
        serial      CertificateSerialNumber     OPTIONAL }
        ( WITH COMPONENTS { ..., issuer PRESENT, serial PRESENT } |
        ( WITH COMPONENTS { ..., issuer ABSENT, serial ABSENT } ) )

Scope ::= CHOICE {
        wholeEntry      [0]   NULL,             -- Signature protects all attribute values in this entry
        selectedTypes   [1]   SelectedTypes
                              -- Signature protects all attribute values of the selected attribute types
        }

SelectedTypes ::= SEQUENCE SIZE (1..MAX) OF AttributeType

AttribsHash ::= HASH { SEQUENCE SIZE (1..MAX) OF Attribute }
                -- Attribute type and values with associated context values for the selected Scope

attributeValueIntegrityInfoContext CONTEXT ::= {
        WITH SYNTAX     AttributeValueIntegrityInfo
        ID              id-avc-attributeValueIntegrityInfoContext }

AttributeValueIntegrityInfo ::= SIGNED { SEQUENCE {
        signer          Signer      OPTIONAL,   -- Authority or data originators name
        aVIHash         AVIHash } }             -- Hash value of protected attribute

AVIHash ::= HASH { AttributeTypeValueContexts }
                -- Attribute type and value with associated context values
```

```
AttributeTypeValueContexts ::= SEQUENCE {
        type                ATTRIBUTE.&id ({SupportedAttributes}),
        value               ATTRIBUTE.&Type ({SupportedAttributes}{@type}),
        contextList         SET SIZE (1..MAX) OF Context OPTIONAL }

-- The following out-commented ASN.1 specification are known to be erroneous and are therefore deprecated.

-- EncryptedAttributeSyntax {AttributeSyntax} ::= SEQUENCE {
--      keyInfo     SEQUENCE OF KeyIdOrProtectedKey,
--      encAlg      AlgorithmIdentifier,
--      encValue    ENCRYPTED { AttributeSyntax } }

-- KeyIdOrProtectedKey ::= SEQUENCE {
--      keyIdentifier       [0]     KeyIdentifier       OPTIONAL,
--      protectedKeys       [1]     ProtectedKey        OPTIONAL }
            -- At least one key identifier or protected key must be present

-- ProtectedKey ::= SEQUENCE {
--      authReaders         AuthReaders,--   -- if absent, use attribute in authorized reader entry
--      keyEncAlg           AlgorithmIdentifier  OPTIONAL, --   -- algorithm to encrypt encAttrKey
--      encAttKey           EncAttKey }
                                -- confidentiality key protected with authorized user's
                                -- protection mechanism

-- AuthReaders ::= SEQUENCE OF Name

-- EncAttKey ::= PROTECTED {SymmetricKey, keyProtection}

-- SymmetricKey ::= BIT STRING

-- keyProtection PROTECTION-MAPPING ::= {
--      SECURITY-TRANSFORMATION {genEncryption} }

-- confKeyInfo ATTRIBUTE ::= {
--      WITH SYNTAX                     ConfKeyInfo
--      EQUALITY MATCHING RULE          readerAndKeyIDMatch
--      ID                              id-at-confKeyInfo }

-- ConfKeyInfo ::= SEQUENCE {
--      keyIdentifier       KeyIdentifier,
--      protectedKey        ProtectedKey }

-- readerAndKeyIDMatch MATCHING-RULE ::= {
--      SYNTAX      ReaderAndKeyIDAssertion
--      ID          id-mr-readerAndKeyIDMatch }

-- ReaderAndKeyIDAssertion ::= SEQUENCE {
--      keyIdentifier       KeyIdentifier,
--      authReaders         AuthReaders OPTIONAL }
-- Object identifier assignments --
-- attributes --
id-at-clearance                                 OBJECT IDENTIFIER   ::=   {id-at 55}
-- id-at-defaultDirQop                          OBJECT IDENTIFIER   ::=   {id-at 56}
id-at-attributeIntegrityInfo                    OBJECT IDENTIFIER   ::=   {id-at 57}
-- id-at-confKeyInfo                            OBJECT IDENTIFIER   ::=   {id-at 60}

-- matching rules --
-- id-mr-readerAndKeyIDMatch                    OBJECT IDENTIFIER   ::=   {id-mr 43}

-- contexts--
id-avc-attributeValueSecurityLabelContext       OBJECT IDENTIFIER   ::=   {id-avc 3}
id-avc-attributeValueIntegrityInfoContext       OBJECT IDENTIFIER   ::=   {id-avc 4}

END -- EnhancedSecurity
```

2.2) Lo que sigue corrige defectos notificados en los informes de defectos 9594/242

Añadir el límite de tamaño **SIZE (1..MAX)** *en todos los* **SET OF** *opcionales y los constructivos* **SEQUENCE OF**.

2.3) Lo que sigue corrige defectos notificados en los informes de defectos 9594/255

En 12.7.2 y en el anexo A, cambiar en la clase de objeto de información **CONTENT-RULE** *de:*

```
&structuralClass                OBJECT-CLASS.&id    UNIQUE,
```

por:

```
&structuralClass                OBJECT-CLASS        UNIQUE,
```

2.4) Lo que sigue corrige defectos notificados en los informes de defectos 9594/260

Actualizar el **AttributeTypeAndDistinguishedValue** *como se muestra:*

```
AttributeTypeAndDistinguishedValue ::= SEQUENCE {
    type                        ATTRIBUTE.&id ({SupportedAttributes}),
    value                       ATTRIBUTE.&Type({SupportedAttributes}{@type}),
    primaryDistinguished        BOOLEAN DEFAULT TRUE,
    valuesWithContext           SET SIZE (1 .. MAX) OF SEQUENCE {
        distingAttrValue        [0]  ATTRIBUTE.&Type ({SupportedAttributes}{@type}) OPTIONAL,
        contextList                  SET SIZE (1 .. MAX) OF Context } OPTIONAL }
```

2.5) Lo que sigue corrige defectos notificados en los informes de defectos 9594/261

Sustituir **CommonResults** *por* **CommonResultsSeq** *en todos los constructivos ASN.1 y en la importación en el anexo F.*

En el último párrafo de 26.5 sustituir **CommonResults** *por* **CommonResultsSeq**.

2.6) Lo que sigue corrige defectos notificados en los informes de defectos 9594/267

En la nota 1 de 14.7.3, sustituir Rec. UIT-T X.680 | ISO/CEI 8824-1 *por* Rec. UIT-T X.682 | ISO/CEI 8824-3.

Sustituir la nota 1 de 14.7.10 por una copia de la nota 1 de 14.7.3, pero conservando la última frase.

En 25.2, intercambie las figuras 19 y 20, pero no el texto de las figuras.

En 22.2.1.2, convierta el atributo **superiorKnowledge** *a multivalores y retorne a la sintaxis antigua* (**AccessPoint**).

2.7) Lo que sigue corrige defectos notificados en los informes de defectos 9594/269

En 12.5.2, inciso a), sustituir:

... al que se aplica la regla;

por:

... al que se aplica la regla a menos que la regla correspondiente especifique otra cosa;

En 14.7.3 añadir **OPTIONAL** *al componente* **information** *de* **MatchingRuleDescription**.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedios
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: 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, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos y comunicación entre sistemas abiertos**
Serie Y	Infraestructura mundial de la información y aspectos del protocolo Internet
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Ginebra, 2002