UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.501

Corrigendum 2
(02/2001)

SÉRIE X: RÉSEAUX DE DONNÉES ET
COMMUNICATION ENTRE SYSTÈMES OUVERTS

Annuaire

Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: les modèles

Corrigendum technique 2

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

(Antérieurement Recommandation du CCITT)

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS

RÉSEAUX PUBLICS DE DONNÉES	
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	
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 des couches	X.280–X.289
Tests de conformité	X.290–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	
Généralités	X.300–X.349
Systèmes de transmission de données par satellite	X.350–X.369
Réseaux à protocole Internet	X.370–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	**X.500–X.599**
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	
Réseautage	X.600–X.629
Efficacité	X.630–X.639
Qualité de service	X.640–X.649
Dénomination, adressage et enregistrement	X.650–X.679
Notation de syntaxe abstraite numéro un (ASN.1)	X.680–X.699
GESTION OSI	
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 et fonctions ODMA	X.730–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	
Engagement, concomitance et rétablissement	X.850–X.859
Traitement transactionnel	X.860–X.879
Opérations distantes	X.880–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999

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

NORME INTERNATIONALE ISO/CEI 9594-2
RECOMMANDATION UIT-T X.501

Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: les modèles

CORRIGENDUM TECHNIQUE 2

Source

Le Corrigendum 2 de la Recommandation X.501 (1997) de l'UIT-T, élaboré par la Commission d'études 7 (2001-2004) de l'UIT-T, a été approuvé le 2 février 2001. Un texte identique est publié comme Corrigendum technique 2 de la Norme Internationale ISO/CEI 9594-2.

AVANT-PROPOS

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

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

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

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

NOTE

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

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

© UIT 2002

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.

TABLE DES MATIÈRES

Page

NORME INTERNATIONALE
RECOMMANDATION UIT-T

Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: les modèles

CORRIGENDUM TECHNIQUE 2

NOTE – Le présent corrigendum technique couvre le résultat des résolutions de vote concernant les projets de Corrigendum technique 3 et 4.

1) Relevés de défauts couverts par le projet de Corrigendum technique 3

(Couvrant les résolutions relatives aux relevés de défauts 229 et 230.)

1.1) Ce qui suit rectifie les défauts figurant dans les relevés de défauts 9594/229-230

Au 2.1:

(Modification non applicable à la version française)

Au 17.4.3:

Dans la spécification du contexte **attributeValueSecurityLabelContext**, *remplacer* **SYNTAX** *par* **WITH SYNTAX**.

Supprimer le type **KeyIdentifier**.

Il convient d'apporter les mêmes modifications dans l'Annexe P.

Au 18.1.2:

Modifier comme suite le 4e alinéa:

Les signatures numériques appliquées à l'entrée complète ne comprennent pas les attributs opérationnels, les attributs collectifs ou la définition **attributeIntegrityInfo** proprement dite. Tous les contextes de valeur d'attribut sont inclus.

Supprimer le 5e alinéa ("Des informations de contrôle additionnelles ...").

Modifier comme suit la définition de l'attribut **attributeIntegrityInfo** *et ses définitions corrélatives*:

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

AttributeIntegrityInfo  ::=  SIGNED { SEQUENCE  {
        scope               Scope,                          -- Identifie les attributs protégés
        signer              Signer      OPTIONAL,           -- Nom de l'autorité ou des émetteurs des données
        attribsHash         AttribsHash } }                 -- Valeur de hachage des attributs protégés

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,          -- La signature protège toutes les valeurs d'attribut
                                             -- dans cette entrée
        selectedTypes   [1]   SelectedTypes
                              -- La signature protège toutes les valeurs d'attribut des types
                              -- d'attribut sélectionnés
        }

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

AttribsHash ::= HASH { SEQUENCE SIZE (1..MAX) OF Attribute }
                -- Type et valeurs d'attribut avec valeurs de contexte associées pour le domaine sélectionné
```

Ajouter ce qui suit après l'ASN.1 ci-dessus:

Une valeur **AttributeIntegrityInfo** peut être créée de trois façons différentes:

a) une autorité administrative peut créer et signer la valeur. Dans ce cas, la clé publique permettant de vérifier la signature est connue par des moyens hors ligne;

b) le détenteur de l'entrée, c'est-à-dire l'objet représenté par celle-ci, peut créer et signer la valeur. Si le détenteur possède plusieurs certificats ou est censé en disposer ultérieurement, le certificat doit être identifié par l'autorité CA qui l'a émis ainsi que son numéro de série;

c) une tierce partie peut créer et signer la valeur. Le nom du signataire, le nom de l'autorité CA émettrice du certificat et le numéro de série de celui-ci sont requis.

Si le domaine de visibilité est **wholeEntry**, tous les attributs applicables doivent être ordonnés comme spécifié pour un type "ensemble-de" au § 6.1 de la Rec. UIT-T X.509 | ISO/CEI 9594-8. Si le domaine est **selectedTypes**, l'ordre doit être celui qui est indiqué dans l'objet **SelectedTypes**.

NOTE – Si un utilisateur n'extrait pas tous les attributs complets qui sont définis dans le type de données **Scope**, cet utilisateur ne pourra pas vérifier l'intégrité des attributs.

Supprimer le § 18.1.2.1.

Les modifications apportées à la notation ASN.1 doivent l'être également dans l'Annexe P.

Remplacer le § 18.1.3 par ce qui suit:

18.1.3 Contexte de protection d'une valeur d'attribut unique

La notation suivante définit un contexte qui détient, conjointement avec les informations de contrôle associées, une signature numérique qui assure l'intégrité d'une valeur d'attribut unique. Sont inclus dans le contrôle d'intégrité tous les contextes de valeur d'attribut, à l'exclusion du contexte utilisé pour contenir les signatures.

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

AttributeValueIntegrityInfo  ::=  SIGNED { SEQUENCE {
        signer          Signer      OPTIONAL,      -- Nom de l'autorité ou des émetteurs des données
        aVIHash         AVIHash } }                -- Valeur de hachage de l'attribut protégé
```

```
AVIHash  ::=  HASH { AttributeTypeValueContexts }
                -- Type et valeurs d'attribut avec les valeurs de contexte associées

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

La liste **contextList** doit être ordonnée comme spécifié pour un type "ensemble-de" dans le § 6.1 de la Rec. UIT-T X.509 | ISO/CEI 9594-8.

Modifier la notation ASN.1 dans l'Annexe P comme indiqué ci-dessus et supprimer le type de données **AVIAssertion**.

Dans l'Annexe B:

Supprimer l'importation **OPTIONALLY-SIGNED** *en provenance de* **DirectoryAbstractService**.

Dans l'Annexe C:

Dans la composante **application** *de l'objet* **AttributeTypeInformation**, *remplacer* **userApplication** *par* **userApplications**.

Dans l'Annexe D:

Ajouter **directoryAbstractService** *à l'importation en provenance de* **UsefulDefinitions**.

Ajouter **SupportedAttributes** *à l'importation en provenance de* **InformationFramework**.

Ajouter:

```
Filter
      FROM DirectoryAbstractService directoryAbstractService
```

Dans l'Annexe F:

Ajouter **enhancedSecurity** *à l'importation en provenance* **UsefulDefinitions**

Supprimer **OPTIONALLY-PROTECTED** *et* **DIRQOP** *de l'importation en provenance* **EnhancedSecurity**. *Ajouter à la place* **OPTIONALLY-PROTECTED-SEQ**.

Dans l'Annexe P:

Toutes les modifications à l'Annexe P ont été incluses dans la résolution concernant le relevé de défauts 228.

2) Relevés de défauts couverts par le projet de Corrigendum technique 4

(Couvrant les résolutions relatives aux relevés de défauts 228, 242, 255, 260, 261, 267 et 269.)

2.1) Ce qui suit rectifie les défauts figurant dans le relevé de défauts 9594/228

Ajouter au début du § 15.3 juste avant le 15.3.1:

Avertissement – Les § 15.3.1 et 15.3.2 contiennent notoirement des spécifications invalides. Ces paragraphes sont donc à éviter. Une future édition supprimera ces spécifications à éviter ou fournira un texte mis à jour.

Les spécifications suivantes sont données afin de conserver la capacité de signature offerte dans l'édition 2 des présentes Spécifications d'annuaire et afin de permettre d'étendre cette capacité à toutes les opérations et aux erreurs.

OPTIONALLY-PROTECTED est un type de données paramétré dans lequel le paramètre et un type de données dont les valeurs peuvent, au choix de l'émetteur, être accompagnées de leur signature numérique. Cette capacité est spécifiée au moyen du type suivant:

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

Le type **OPTIONALLY-PROTECTED-SEQ** est utilisé à la place de **OPTIONALLY-PROTECTED** lorsque le type de données protégées est un type de données en séquence qui n'est pas étiqueté.

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

Le type de données paramétré **SIGNED**, qui décrit la forme signée des informations, est spécifié dans la Rec. UIT-T X.509 | ISO/CEI 9594-8.

Ajouter au début du § 18.2 juste avant le § 18.2.1:

Avertissement – Ce paragraphe contient notoirement des spécifications invalides. Il est donc à éviter. Une future édition supprimera ces spécifications à éviter ou fournira un texte mis à jour.

Dans l'Annexe A, ajouter un commentaire en notation ASN.1 comme indiqué:

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

Dans l'article 26, supprimer toute occurrence de:

DIRQOP.&…-QOP{@dirqop}

et remplacer toutes les occurrences de:

OPTIONALLY-PROTECTED

par:

OPTIONALLY-PROTECTED-SEQ

Apporter les mêmes modifications à l'Annexe F.

Remplacer l'Annexe P par ce qui suit:

Annexe P

Amélioration de la sécurité

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

Il est notoire que ce module contient des spécifications invalides. La partie de ce module qui est donc à éviter est indiquée par des commentaires en notation ASN.1. Une future édition supprimera les spécifications à éviter ou les remplacera par des spécifications mises à jour.

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

-- EXPORTER TOUT --

IMPORTS

-- de la Rec. UIT-T X.501 | ISO/CEI 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

-- de la Rec. UIT-T X.509 | ISO/CEI 9594-8

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

      GeneralName, KeyIdentifier
            FROM CertificateExtensions certificateExtensions

      ub-privacy-mark-length
            FROM UpperBounds upperBounds ;
-- de 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) };

-- Le mappage de protection "signé" et les transformations associées de type dirSignedTransformations,
-- importés de la spécification de sécurité générique des couches supérieures (Rec. UIT-T X.830 | ISO/CEI 11586-1)
-- produisent un codage identique au type de données identique qui est utilisé avec l'objet SIGNED qui est défini dans
-- la Rec. UIT-T X.509 | ISO/CEI 9594-8

-- Les trois déclarations ci-dessous sont données provisoirement afin de permettre la prise en charge
-- des opérations signées comme dans la 3e édition.
```

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

OPTIONALLY-PROTECTED-SEQ { Type } ::= CHOICE {
        unsigned        Type,
        signed    [0]   SIGNED { Type } }
-- La spécification ASN.1 ci-dessous, extraite pour citation sous forme de commentaire, est notoirement erronée et est
-- donc déconseillée.

-- genEncryptedTransform {KEY-INFORMATION: SupportedKIClasses } SECURITY-TRANSFORMATION ::=
--      {
--      IDENTIFIER                  { enhancedSecurity gen-encrypted(2) }
--      INITIAL-ENCODING-RULES      { joint-iso-itu-t asn1(1) ber(1) }
                                    -- Cette valeur par défaut pour les règles de codage initiales peut être
                                    -- neutralisée au moyen d'un paramètre statique protégé (initEncRules).
--      XFORMED-DATA-TYPE           SEQUENCE {
--              initEncRules        OBJECT IDENTIFIER DEFAULT { joint-iso-itu-t asn1(1) ber(1) },
--              encAlgorithm        AlgorithmIdentifier OPTIONAL, --  -- désigne le cryptage,
--              keyInformation      SEQUENCE {
--                  kiClass         KEY-INFORMATION.&kiClass ({SupportedKIClasses}),
--                  keyInfo         KEY-INFORMATION.&KiType ({SupportedKIClasses} {@kiClass})
--                                  } OPTIONAL,
                    -- Les informations clés peuvent avoir divers formats selon les membres pris en charge
                    -- de la classe d'objets informationnels KEY-INFORMATION (définie dans la
                    -- Rec. UIT-T X.830 | ISO/CEI 11586-1)
--              encData     BIT STRING ( CONSTRAINED BY {
                    -- la valeur encData doit être produite après
                    -- la procédure spécifiée au § 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,
                                -- Aucune classe DIRQOP n'est spécifiée pour l'opération
--          signed          PROTECTED {ToBeProtected, signed},
                                -- DIRQOP est de type "Signed"
--          protected       [APPLICATION 0]
--                              PROTECTED { ToBeProtected, generalProtection } }
                                -- DIRQOP est d'un type autre que " Signed"
```

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


-- DIRQOP  ::=  CLASS
-- Cette classe d'objets d'informations sert à définir la qualité de la protection
-- requise pendant toute l'opération d'annuaire.
-- La qualité de la protection peut être de type 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     -- Au plus un contexte d'étiquette de sécurité peut être
                                                -- affecté à une valeur d'attribut
        ID              id-avc-attributeValueSecurityLabelContext }

SignedSecurityLabel  ::=  SIGNED {SEQUENCE  {
        attHash         HASH {AttributeTypeAndValue},
        issuer          Name            OPTIONAL,  -- nom de l'autorité d'étiquetage
        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 ( {-- aucune exception, au moins un composant doit être présent -- } ) )

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,                  -- Identifie les attributs protégés
        signer          Signer      OPTIONAL,   -- Nom de l'autorité ou de l'émetteur des données
        attribsHash     AttribsHash } }         -- Valeur de hachage des attributs protégés

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,          -- La signature protège toutes les valeurs d'attribut dans cette entrée
        selectedTypes   [1]  SelectedTypes
                             -- La signature protège toutes les valeurs d'attribut des types d'attribut sélectionnés
        }

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

AttribsHash ::= HASH { SEQUENCE SIZE (1..MAX) OF Attribute }
                -- Type et valeurs d'attribut avec les valeurs de contexte associées pour le domaine
                -- d'application sélectionné

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

AttributeValueIntegrityInfo ::= SIGNED { SEQUENCE {
        signer          Signer      OPTIONAL,   -- Nom de l'autorité ou de l'émetteur des données
        aVIHash         AVIHash } }             -- Valeur de hachage de l'attribut protégé

AVIHash ::= HASH { AttributeTypeValueContexts }
                -- Type et valeur d'attribut avec les valeurs de contexte associées
```

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

-- La spécification ASN.1 ci-dessous, extraite pour citation sous forme de commentaire, est notoirement erronée et est
-- donc déconseillée.

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

-- KeyIdOrProtectedKey ::= SEQUENCE {
--      keyIdentifier       [0]   KeyIdentifier     OPTIONAL,
--      protectedKeys       [1]   ProtectedKey      OPTIONAL }
            -- Au moins un identificateur de clé ou une clé protégée doit être présent

-- ProtectedKey ::= SEQUENCE {
--      authReaders     AuthReaders,--  -- s'il est absent, utiliser l'attribut de l'entrée du lecteur autorisé
--      keyEncAlg       AlgorithmIdentifier OPTIONAL, --  -- algorithme de chiffrement encAttrKey
--      encAttKey       EncAttKey }
                            -- clé de confidentialité protégée par le mécanisme de
                            -- protection de l'utilisateur autorisé

-- 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 }
-- Affectation des identificateurs d'objet --
-- attributs --
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}

-- règles de correspondance --
-- id-mr-readerAndKeyIDMatch                OBJECT IDENTIFIER   ::=   {id-mr 43}
.
-- contextes --
id-avc-attributeValueSecurityLabelContext   OBJECT IDENTIFIER   ::=   {id-avc 3}
id-avc-attributeValueIntegrityInfoContext   OBJECT IDENTIFIER   ::=   {id-avc 4}

END -- EnhancedSecurity
```

2.2) Correction des défauts signalés dans le relevé de défauts 9594/242

Ajouter une limite de taille **SIZE (1..MAX)** *à toutes les constructions facultatives* **SET OF** *et* **SEQUENCE OF**.

2.3) Correction des défauts signalés dans le relevé de défauts 9594/255

Au § 12.7.2 et dans l'Annexe A, remplacer la classe d'objets informationnels **CONTENT-RULE** *par la suivante*:

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

par:

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

2.4) Correction des défauts signalés dans le relevé de défauts 9594/260

Mettre à jour **AttributeTypeAndDistinguishedValue** *comme suit*:

```
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) Correction des défauts signalés dans le relevé de défauts 9594/261

Remplacer **CommonResults** *par* **CommonResultsSeq** *dans toutes les constructions ASN.1 et dans IMPORT (Annexe F).*

Au dernier alinéa du § 26.5 remplacer **CommonResults** *par* **CommonResultsSeq**.

2.6) Correction des défauts signalés dans le relevé de défauts 9594/267

Dans la Note 1 du § 14.7.3, remplacer "Rec. UIT-T X.680 | ISO/CEI 8824-1" *par* "Rec. UIT-T X.682 | ISO/CEI 8824 3".

Remplacer la Note 1 au § 14.7.10 en copiant la NOTE 1 du § 14.7.3, mais en gardant la dernière phrase.

Au § 25.2, intervertir les Figures 19 et 20, mais pas le texte des figures.

Au § 22.2.1.2, faire en sorte que l'attribut **superiorKnowledge** *ait plusieurs valeurs et revenir à l'ancienne syntaxe* (**AccessPoint**).

2.7) Correction des défauts signalés dans le relevé de défauts 9594/269

Au § 12.5.2, point a), remplacer:

... auquel la règle s'applique;

par:

... auquel la règle s'applique à moins que la règle de correspondance ne spécifie le contraire;

Au § 14.7.3, ajouter **OPTIONAL** *à la composante* **information** *de* **MatchingRuleDescription**.

SÉRIES DES RECOMMANDATIONS UIT-T

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

Genève, 2002