

Recommendation X.501 | ISO/IEC 9594-2
Technical Corrigendum 2 to the 3rd edition

NOTE – This Technical Corrigendum covers the result of the ballot resolutions of Draft Technical Corrigenda 3, and 4.

Defect reports covered by Draft Technical Corrigendum 3
(Covering resolutions to defect reports 229 and 230)

This corrects the defects reported in defect reports 9594/229-230.

In 2.1:

Replace:

- ITU-T Recommendation X.525 (1997) | ISO/IEC 9594-8:1999, *Information technology – Open Systems Interconnection – The Directory: Replication.*

with:

- ITU-T Recommendation X.525 (1997) | ISO/IEC 9594-9:1998, *Information technology – Open Systems Interconnection – The Directory: Replication.*

In 17.4.3:

In the **attributeValueSecurityLabelContext** specification replace **SYNTAX** with **WITH SYNTAX**

Delete the **KeyIdentifier** type.

The same changes shall be done in Annex P

In 18.1.2:

Change the 4th paragraph to:

Digital signatures applied to the whole entry do not include operational, ~~or~~ collective attributes [or the **attributeIntegrityInfo** itself](#). Any attribute value contexts are included.

Delete the 5th paragraph (Additional control information ...).

*Change the **attributeIntegrityInfo** attribute definition and its supporting definitions to:*

```
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

Add the following text after the above ASN.1:

An **AttributeIntegrityInfo** value can be created in three different ways:

- a) An administrative authority can create and sign the value, and the public key to verify the signature is known by off-line means.
- b) The owner of the entry, i.e. the object represented by the entry, can create and sign the value. If the owner has several certificates, or expected to have that in the future, the certificate has to be identified by the CA issuing the certificate together with the certificate serial number.
- c) A third party may create and sign the value. The name of the signer, the name of the CA issuing the certificate and the certificate serial number is required.

If the scope is **wholeEntry**, all the applicable attributes shall be ordered as specified for a set-of type in 6.1 of ITU-T Rec. X.509 | ISO/IEC 9594-8. If scope is **selectedTypes**, the ordering shall be the same as the one given in the **SelectedTypes**.

NOTE – If a user does not retrieve all the complete attributes that are defined within the **Scope** data type, it will not be possible for the user to verify the integrity of the attributes.

Delete 18.1.2.1.

The changes to ASN.1 shall also be done in Annex P.

Replace 18.1.3 with:

18.1.3 Context for Protection of a Single Attribute Value

The following defines a context to hold a digital signature, along with associated control information, which provides integrity for a single attribute value. Any attribute value contexts are included in the integrity check, excluding the context used to hold signatures.

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

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

AVIMHash ::= 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 **contextList** shall be ordered as specified for a set-of type in 6.1 of ITU-T Rec. X.509 | ISO/IEC 9594-8.

Change the ASN.1 ASN.1 in Annex P as per above and delete **AVIAssertion** data type.

In annex B:

Delete **OPTIONALLY-SIGNED** import from **DirectoryAbstractService**

In annex C:

In the **application** component of **AttributeTypeInfo** replace **userApplication** with **userApplications**

In Annex D:

Add **directoryAbstractService** to the import from **UsefulDefinitions**

Add **SupportedAttributes** to the import from **InformationFramework**

Add:

Filter

FROM DirectoryAbstractService directoryAbstractService

In annex F:

Add **enhancedSecurity** to the import from **UsefulDefinitions**

Delete **OPTIONALLY-PROTECTED** and **DIRQOP** from the import from **EnhancedSecurity**. Add instead **OPTIONALLY-PROTECTED-SEQ**.

In annex P:

All the changes to annex P has been subsumed by the resolution of defect report 228

Defect reports covered by Draft Technical Corrigendum 4

(Covering resolutions to defect reports 228, 242, 255, 260, 261, 267 and 269)

This corrects the defects reported in defect report 9594/228.

Add at the beginning of 15.3 just before 15.3.1:

Warning – Subclause 15.3.1 and 15.3.2 are known to contain invalid specifications. These subclauses are therefore deprecated. A future edition will either remove the deprecated specifications or provide updated text.

The following specifications are provided to preserve the optionally signed capability provided by edition 2 of these Directory Specifications and to allow that capability to be extended to all operations and to errors:

OPTIONALLY-PROTECTED is a parameterized data type where the parameter is a data type whose values may, at the option of the generator, be accompanied by their digital signature. This capability is specified by means of the following type:

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

The **OPTIONALLY-PROTECTED-SEQ** is used instead of **OPTIONALLY-PROTECTED** when the protected data type is a sequence data type that is not tagged.

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

The **SIGNED** parameterized data type, which describes the form of the signed form of the information, is specified in ITU-T Rec. X.509 | ISO/IEC 9594-8.

Add at the beginning of 18.2 just before 18.2.1:

Warning – This subclause is known to contain invalid specifications. This subclause is therefore deprecated. A future edition will either remove the deprecated specifications or provide updated text.

In Annex A, add ASN.1 comment item as shown:

```
-- securityExchange          ID ::= {ds 32}  
  
-- directorySecurityExchanges ID ::= {module directorySecurityExchanges (29) 4}  
  
-- id-se                     ID ::= securityExchange
```

In clause 26, delete any occurrence of

DIRQOP.&...-QOP{@dirqop}

and change all occurrences of:

OPTIONALLY-PROTECTED

to:

OPTIONALLY-PROTECTED-SEQ

The same changes shall be made to Annex F.

Replace Annex P with:

Annex P

Enhanced security

(This annex forms an integral part of this Recommendation | International Standard)

This module is known to contain invalid specifications. Part of this module is therefore deprecated. The deprecated part is indicated by ASN.1 comment items. A future edition will either remove the deprecated specifications or provide updated specifications.

EnhancedSecurity { joint-iso-itu-t ds(5) modules(1) enhancedSecurity(28) 4 }

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) 4 }

**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 specification are know 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
--      DAPADDEENTRYARG-QOP             &dapAddEntryArg-QOP

```



```

--      DAPADDEENTRYRES-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 presen-- } ) )

```

```

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
    aVIMHash      AVIMHash } }           -- Hash value of protected attribute

AVIMHash ::= 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 know 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

```

This corrects the defects reported in defect report 9594/242.

Add size limit **SIZE (1..MAX)** to all optional **SET OF** and **SEQUENCE OF** constructs.

This corrects the defects reported in defect reports 9594/255.

In 12.7.2 and in Annex A, change in the **CONTENT-RULE** information object class from:

```

    &structuralClass          OBJECT-CLASS.&id    UNIQUE,
to:
    &structuralClass          OBJECT-CLASS    UNIQUE,

```

This corrects the defects reported in defect reports 9594/260.

Update the **AttributeTypeAndDistinguishedValue** as shown:

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

This corrects the defects reported in defect reports 9594/261.

Replace **CommonResults** with **CommonResultsSeq** in all ASN.1 constructs and in the import in Annex F.

In last paragraph of 26.5 (28.5 in addition 4) replace **CommonResults** with **CommonResultsSeq**.

This corrects the defects reported in defect reports 9594/267.

In NOTE 1 of 14.7.3, replace ITU-T Rec. X.680 | ISO/IEC 8824-1 with ITU-T Rec. X.682 | ISO/IEC 8824-3

Replace NOTE 1 in 14.7.10 with a copy of NOTE 1 in 14.7.3, but keep the last sentence.

In 25.2, swap Figure 19 and 20, but not the figure text.

In 22.2.1.2, make the **superiorKnowledge** attribute multi-valued and return to the old syntax (**AccessPoint**).

This corrects the defects reported in defect reports 9594/269.

In 12.5.2, item a), replace:

rule is applied to;

with:

...rule is applied to unless the matching rule specifies otherwise;

In 14.7.3 add **OPTIONAL** to the information component of **MatchingRuleDescription**