



INTERNATIONAL STANDARD ISO/IEC 9594-2:1998 TECHNICAL CORRIGENDUM 2

Published 2002-05-01

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОМИССИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

Information technology — Open Systems Interconnection — The Directory: Models

TECHNICAL CORRIGENDUM 2

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — L'annuaire: Les modèles

RECTIFICATIF TECHNIQUE 2

Technical Corrigendum 2 to International Standard ISO/IEC 9594-2:1998 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*.

Withdrawn

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information technology – Open Systems Interconnection –
The Directory: Models

TECHNICAL CORRIGENDUM 2

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

1) Defect reports covered by Draft Technical Corrigendum 3

(Covering resolutions to defect reports 229 and 230.)

1.1) 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.

Introduce the same changes in Annex P.

In 18.1.2:

Change the 4th paragraph to:

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

Delete the 5th paragraph (beginning "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:

- An administrative authority can create and sign the value, and the public key to verify the signature is known by off-line means.
- 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.
- 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.

Introduce the same changes to ASN.1 in Annex P.

Replace 18.1.3 with the following:

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
    aVHash      AVIHash     } }                  -- Hash value of protected attribute

```

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