NORME INTERNATIONALE ISO/CEI 9594-2:1998
RECTIFICATIF TECHNIQUE 2

Publié 2002-05-01

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

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

RECTIFICATIF TECHNIQUE 2

Information technology — Open Systems Interconnection — The Directory: Models

TECHNICAL CORRIGENDUM 2

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Le Rectificatif technique 2 à la Norme internationale ISO/CEI 9594-2:1998 a été élaboré par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 6, *Téléinformatique*.

ISO/IEC 9594-2:1998/Cor 2:2002
https://standards.iteh.ai/catalog/standards/sist/6aa4a5b6-6a38-4988-9fd5-43d97ce5a6cd/iso-iec-9594-2-1998-cor-2-2002

ICS 35.100.70 **Réf. nº ISO/CEI 9594-2:1998/Cor.2:2002(F)**

© ISO/CEI 2002 – Tous droits réservés

Imprimé en Suisse

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 9594-2:1998/Cor 2:2002
https://standards.iteh.ai/catalog/standards/sist/6aa4a5b6-6a38-4988-9fd3-43d97ce5a6cd/iso-iec-9594-2-1998-cor-2-2002

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:

iTeh STANDARD PREVIEW
(standards.iteh.ai)

(Modification non applicable à la version française)

Au 17.4.3:

ISO/IEC 9594-2:1998/Cor 2:2002
https://standards.iteh.ai/catalog/standards/sist/6aa4a5b6-6a38-4988-9f13-43d97ce5a6cd/iso-iec-9594-2-1998-cor-2-2002

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:

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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;

ISO/IEC 9594-2:1998/Cor 2:2002
https://standards.iteh.ai/catalog/standards/sist/faa4a5b6-6a38-4b88-9fd3-42d97ca5a6cd/iso-iec-9594-2-1998-cor-2-2002

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
```

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Dans l'Annexe F:

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

ISO/IEC 9594-2:1998/Cor 2:2002
https://standards.iteh.ai/catalog/standards/sist/6aa4a5b6-6a38-4988-9fd3-
4b197cafc6ab/iso-iec-9594-2-1998-cor-2-2002

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Apporter les mêmes modifications à l'Annexe F.

ISO/IEC 9594-2:1998/Cor 2:2002
https://standards.iteh.ai/catalog/standards/sist/6aa4a5b6-6a38-4988-9fd3-43d97ce5a6cd/iso-iec-9594-2-1998-cor-2-2002

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.
```

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 9594-2:1998/Cor 2:2002
https://standards.iteh.ai/catalog/standards/sist/6aa4a5b6-6a38-4988-9fd3-43d97ce5a6cd/iso-iec-9594-2-1998-cor-2-2002

```
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"
```

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 9594-2:1998/Cor 2:2002
https://standards.iteh.ai/catalog/standards/sist/6ad4a5b6-6a38-4988-9fd3-43d97ce5a6cd/iso-iec-9594-2-1998-cor-2-2002

```
-- 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
```

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 9594-2:1998/Cor 2:2002
https://standards.iteh.ai/catalog/standards/sist/...
43d97ce5a6cd/iso-iec-9594-2-1998-cor-2-2002