NORME INTERNATIONALE

ISO/CEI 11586-4

Première édition
1996-06-01

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Sécurité générique des couches supérieures: Spécification de la syntaxe de protection du transfert

Information technology — Open Systems Interconnection — Generic upper layers security: Protecting transfer syntax specification

Numéro de référence
ISO/CEI 11586-4:1996(F)

Sommaire

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment ensemble un système consacré à la normalisation internationale considérée comme un tout. Les organismes nationaux membres de l'ISO ou de la CEI participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des différents domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de la CEI collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales ou non gouvernementales, en liaison avec l'ISO et la CEI participent également aux travaux.

Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour approbation, avant leur acceptation comme Normes internationales. Les Normes internationales sont approuvées conformément aux procédures qui requièrent l'approbation de 75 % au moins des organismes nationaux votants.

La Norme internationale ISO/CEI 11586-4 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 21, *Interconnexion des systèmes ouverts, gestion des données et traitement distribué ouvert*, en collaboration avec l'UIT-T. Le texte identique est publié en tant que Recommandation UIT-T X.833.

L'ISO/CEI 11586 comprend les parties suivantes, présentées sous le titre général *Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Sécurité générique des couches supérieures*:

— *Partie 1: Présentation, modèles et notation*

— *Partie 2: Définition du service assuré par l'élément de service d'échange de sécurité (SESE)*

— *Partie 3: Spécification du protocole d'élément de service d'échange de sécurité (SESE)*

— *Partie 4: Spécification de la syntaxe de protection du transfert*

— *Partie 5: Formulaire de déclaration de conformité pour la mise en œuvre du protocole d'élément de service d'échange de sécurité (SESE)*

— *Partie 6: Formulaire de déclaration de conformité pour la mise en œuvre du protocole de syntaxe de protection du transfert*

Introduction

La présente Recommandation I Norme internationale appartient à une série de Recommandations I Normes internationales qui fournissent un ensemble de moyens destinés à la réalisation des protocoles des couches supérieures pour prendre en charge les services de sécurité. La structure de cette série est la suivante:

- Partie 1: aperçu général, modèles et notation
- Partie 2: définition du service «Elément de service d'échange de sécurité»
- Partie 3: spécification du protocole «Elément de service d'échange de sécurité»
- Partie 4: spécification de la syntaxe de protection du transfert
- Partie 5: formulaire PICS pour l'élément de service d'échange de sécurité
- Partie 6: formulaire PICS pour la syntaxe de protection du transfert

La présente Recommandation I Norme internationale constitue la Partie 4 de cette série.

NORME INTERNATIONALE

RECOMMANDATION UIT-T

TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DE SYSTÈMES OUVERTS (OSI) – SÉCURITÉ GÉNÉRIQUE DES COUCHES SUPÉRIEURES: SPÉCIFICATION DE LA SYNTAXE DE PROTECTION DU TRANSFERT

1 Domaine d'application

1.1 La présente série de Recommandations I Normes internationales définit une série de moyens génériques utilisés dans l'établissement de services de sécurité dans des applications de l'OSI. Elles comprennent:

a) une série d'outils de notation permettant de spécifier les besoins de protection sélective des champs dans une spécification de syntaxe abstraite et permettant la spécification d'échanges de sécurité et de transformations de sécurité;

b) une définition du service, la spécification du protocole et le formulaire PICS pour l'élément du service Application (ASE) qui contribueront à assurer les services de sécurité dans la couche Application de l'OSI;

c) une spécification et un formulaire PICS pour une syntaxe de protection du transfert, associés à la couche Présentation, pour les services de sécurité dans la couche Application.

1.2 La présente Recommandation I Norme internationale définit la syntaxe de protection du transfert utilisée en association avec la couche Présentation pour assurer des services de sécurité dans la couche Application.

2 Références normatives

Les Recommandations et Normes internationales suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Recommandation I Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute Recommandation et Norme internationale sont sujettes à révision, et les parties prenantes aux accords fondés sur la présente Recommandation I Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et Normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur. Le Bureau de la normalisation des télécommunications de l'UIT tient à jour une liste des Recommandations de l'UIT-T en vigueur.

2.1 Recommandations I Normes internationales identiques

- Recommandation UIT-T X.200 (1994) I ISO/CEI 7498-1:1994, *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de référence de base: Le modèle de référence de base.*
- Recommandation UIT-T X.216 (1994) I ISO/CEI 8822:1994, *Technologies de l'information – Interconnexion des systèmes ouverts – Définition du service de Présentation.*
- Recommandation UIT-T X.226 (1994) I ISO/CEI 8823-1:1994, *Technologies de l'information – Interconnexion des systèmes ouverts – Protocole de présentation en mode connexion: Spécification du protocole.*
- Recommandation UIT-T X.680 (1994) I ISO/CEI 8824-1:1995, *Technologies de l'information – Notation de syntaxe abstraite numéro un: Spécification de la notation de base.*
- Recommandation UIT-T X.681 (1994) I ISO/CEI 8824-2:1995, *Technologies de l'information – Notation de syntaxe abstraite numéro un: Spécification des objets informationnels.*
- Recommandation UIT-T X.682 (1994) I ISO/CEI 8824-3:1995, *Technologies de l'information – Notation de syntaxe abstraite numéro un: Spécification des contraintes.*
- Recommandation UIT-T X.683 (1994) I ISO/CEI 8824-4:1995, *Technologies de l'information – Notation de syntaxe abstraite numéro un: Paramétrage des spécifications de la notation de syntaxe abstraite numéro un.*

- Recommandation UIT-T X.690 (1994) | ISO/CEI 8825-1:1995, *Technologies de l'information – Règles de codage de la notation de syntaxe abstraite numéro un: Spécifications des règles de codage de base, des règles de codage canoniques et des règles de codage distinctives.*
- Recommandation UIT-T X.803 (1994) | ISO/CEI 10745:1995, *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de sécurité pour les couches supérieures.*
- Recommandation UIT-T X.830 (1995) | ISO/CEI 11586-1:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Sécurité générique des couches supérieures: Vue d'ensemble, modèles et notation.*

3 Définitions

3.1 La présente Recommandation | Norme internationale utilise le terme suivant défini dans la Rec. UIT-T X.200 | ISO/CEI 7498-1:

- syntaxe de transfert.

3.2 La présente Recommandation | Norme internationale utilise les termes suivants définis dans la Rec. UIT-T X.216 | ISO/CEI 8822:

- syntaxe abstraite;
- contexte de présentation;
- valeur de données de présentation.

3.3 La présente Recommandation | Norme internationale utilise les termes suivants définis dans la Rec. UIT-T X.803 | ISO/CEI 10745:

- association de sécurité;
- transformation de sécurité.

3.4 La présente Recommandation | Norme internationale utilise les termes suivants définis dans la Rec. UIT-T X.830 | ISO/CEI 11586-1:

- association de sécurité explicite (à contexte de présentation);
- association de sécurité explicite (à item simple);
- association de sécurité établie extérieurement;
- règles de codage initiales;
- contexte de protection de présentation;
- syntaxe de protection du transfert.

4 Abréviations

GULS	Sécurité générique des couches supérieures (*generic upper layers security*)
OSI	Interconnexion des systèmes ouverts (*open systems interconnection*)
PDU	Unité de données protocolaires (*protocol-data-unit*)
PDV	Valeur de données de présentation (*presentation data value*)
PICS	Déclaration de conformité d'une instance de protocole (*protocol implementation conformance statement*)

5 Aperçu général

Le principe de la syntaxe de protection du transfert a été introduit dans la Rec. UIT-T X.830 | ISO/CEI 11586-1. La présente Spécification définit une syntaxe de protection générique du transfert. Elle peut être utilisée, conjointement avec les définitions de transformation de sécurité particulières, pour produire des syntaxes particulières de protection du transfert, profilées de manière à satisfaire les besoins de protection d'une application donnée.

NOTE – La syntaxe de protection générique du transfert peut aussi être utilisée pour comprimer des données à des fins non liées à la sécurité, mais cela ne relève pas de la présente Spécification.

La syntaxe de protection générique du transfert est fondée sur un modèle de transformation de sécurité décrit dans la Rec. UIT-T X.830 | ISO/CEI 11586-1. Elle a pour but d'offrir un moyen standard de représentation, pour les besoins du transfert, des items d'information suivants:

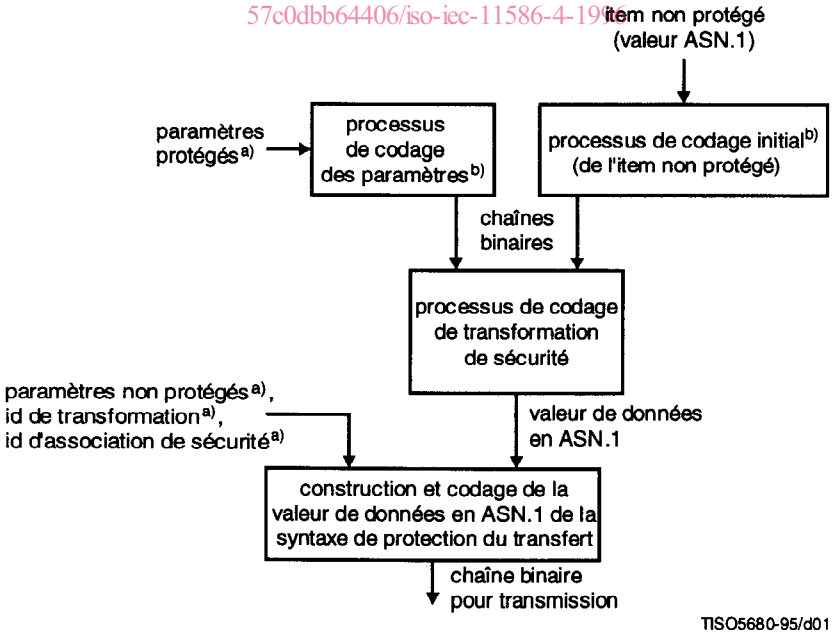
- l'item transformé résultant de l'application du processus de codage d'une transformation de sécurité à une représentation d'un item (non protégé) qu'il y a lieu de protéger;
- les paramètres statiques et dynamiques protégés d'une transformation de sécurité qui assurent la protection en étant traités dans le processus de codage de la transformation de sécurité (tout comme la représentation de l'item non protégé);
- les paramètres statiques et dynamiques non protégés d'une transformation de sécurité;
- la première valeur PDV d'un contexte de protection de présentation ou une valeur PDV envoyée hors d'un contexte de présentation:
  a) dans le cas d'une association de sécurité explicite, un identificateur de la transformation de sécurité; ou
  b) dans le cas d'une association de sécurité établie extérieurement, un identificateur de cette association de sécurité.

L'emploi d'une syntaxe de protection du transfert est négocié par le protocole de présentation ou annoncé dans une structure ASN.1 EXTERNAL ou EMBEDDED PDV. Elle peut être appliquée à toute syntaxe abstraite, qui peut être spécifiée en ASN.1 ou par d'autres moyens. Les identificateurs d'objet pour négocier ou annoncer des syntaxes de protection du transfert sont traités à l'article 9.

Une syntaxe de protection du transfert est une syntaxe de transfert sensible au contexte, c'est-à-dire que son état est conservé dans les codeurs et les décodeurs.

5.1 Modèle de syntaxe de protection de transfert

La Figure 1 illustre, de manière plus détaillée que dans la Rec. UIT-T X.830 | ISO/CEI 11586-1, les opérations associées à la syntaxe de protection du transfert au niveau d'un système de codage (les opérations correspondantes au niveau du système de décodage suivent naturellement).



a) le cas échéant.
b) ces deux processus de codage peuvent être combinés.

Figure 1 – Construction de la syntaxe de protection du transfert au niveau du système de codage

5.2 Règles de codage initiales

Le processus de codage initial (dans le système de codage) et le processus de décodage correspondant (dans le système de décodage) établissent une correspondance entre une syntaxe abstraite et une syntaxe non protégée. Les règles appliquées à ce processus sont connues en tant que règles de codage initiales.

NOTE – Dans le cas d'une syntaxe abstraite fondée sur l'ASN.1, cette mise en correspondance utilisera généralement une variante des règles de codage ASN.1.

Les règles de codage à valeur unique (telles que les règles de codage canoniques ou les règles de codage distinctives) devront être appliquées quand la transformation est une fonction de données qui peut également être envoyée séparément, surtout quand elle passe par un système relais.

Les règles de codage initiales pour une syntaxe de protection du transfert sont établies de la manière suivante:

a) si la transformation de sécurité en cours d'utilisation assure l'acheminement de l'identificateur d'une série spécifique de règles de codage sous forme d'un paramètre statique (protégé ou non), et si ce paramètre est présent dans le premier champ de valeur PDV applicable, ces règles de codage sont utilisées; à défaut

b) on utilise les règles de codage indiquées dans le champ &initialEncodingRules de la définition de la transformation de sécurité applicable.

5.3 Transformation de sécurité

Il y a deux manières de déterminer la transformation de sécurité à employer:

a) quand le transfert de la valeur PDV concerne une association de sécurité liée à un contexte de présentation ou liée à un item unique, l'identificateur de la transformation de sécurité est véhiculé dans la structure de la syntaxe de transfert, avec la première PDV de cette association de sécurité;

b) quand le transfert de la valeur PDV se rapporte à une association de sécurité établie extérieurement, l'identificateur de transformation de sécurité est un attribut de cette association de sécurité.

Les règles d'une transformation de sécurité indiquent comment une chaîne binaire de données d'utilisateur et une série de valeurs de paramètre protégées doivent être projetées sur une valeur ASN.1 pour les besoins du transfert.

5.4 Structure syntaxique

Une syntaxe de protection de transfert définit la structure de données utilisée pour acheminer le résultat d'un processus d'un codage d'une transformation de sécurité ainsi que les paramètres et identificateurs non protégés de la transformation de sécurité ou de l'association de sécurité (selon le cas). La structure de données transférée varie d'un cas à l'autre:

a) c'est la première PDV selon le contexte de présentation de protection d'une association de sécurité liée à un contexte de présentation, ou l'unique PDV d'une association de sécurité liée à un item unique;

b) dans le cas d'une association de sécurité établie extérieurement, elle est la première valeur PDV du contexte de protection de présentation ou une valeur PDV protégée envoyée hors d'un contexte de présentation;

c) dans un contexte de protection de présentation, c'est une valeur PDV subséquente.

6 Structures de données pour une syntaxe de protection du transfert

La série de structures de données utilisées par une syntaxe de protection de transfert est définie par un type ASN.1 SyntaxStructure dans le module ASN.1 ci-après. Le type SyntaxStructure est paramétré par l'ensemble d'objet ValidST, qui est un ensemble d'objets SECURITY-TRANSFORMATION. Quand une valeur est fournie pour ValidST, avec les spécifications de transformation de sécurité correspondantes, le type SyntaxStructure devient une spécification de syntaxe complète pour une syntaxe de protection de transfert spécifique.

```
GenericProtectingTransferSyntax {joint-iso-ccitt genericULS (20)
        modules (1) genericProtectingTransferSyntax (7) }
DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS
        SyntaxStructure {};
```

```
IMPORTS
        notation
            FROM ObjectIdentifiers {joint-iso-ccitt
            genericULS (20) modules (1) objectIdentifiers (0) }
        SECURITY-TRANSFORMATION, ExternalSAID
            FROM Notation notation;

SyntaxStructure {SECURITY-TRANSFORMATION: ValidSTs}::= CHOICE
{
        firstPdvExplicit      FirstPdvExplicit {{ValidSTs}},
        -- A utiliser sur la première PDV d'un contexte de protection de
        -- présentation ou, dans le cas d'une association de sécurité explicite,
        -- sur une PDV protégée envoyée hors du contexte de présentation.
        firstPdvExternal      FirstPdvExternal {{ValidSTs}},
        -- A utiliser sur la première PDV d'un contexte de protection de présentation ou,
        -- dans le cas d'une association de sécurité établie extérieurement,
        -- sur une PDV protégée envoyée hors du contexte de présentation.
        subsequentPdv         SubsequentPdv {{ValidSTs}}
        -- A utiliser sur une PDV subséquente dans un contexte
        -- de protection de présentation.
}
FirstPdvExplicit {SECURITY-TRANSFORMATION: ValidSTs}::= SEQUENCE
{
        transformationId  SECURITY-TRANSFORMATION.&sT-Identifier
                ({ValidSTs}),
        staticUnprotParm
            SECURITY-TRANSFORMATION.&StaticUnprotectedParm
                ({ValidSTs}{@transformationId})
                OPTIONAL,
        dynamicUnprotParm
            SECURITY-TRANSFORMATION.&DynamicUnprotectedParm
                ({ValidSTs}{@transformationId})
                OPTIONAL,
        xformedData  SECURITY-TRANSFORMATION.&XformedDataType
                ({ValidSTs}{@transformationId})
}
FirstPdvExternal {SECURITY-TRANSFORMATION: ValidSTs}::= SEQUENCE
{
        externalSAID          ExternalSAID,
        dynamicUnprotParm
            SECURITY-TRANSFORMATION.&DynamicUnprotectedParm
                ({ValidSTs}) OPTIONAL,
            -- Le membre réel de ValidSTs est celui
            -- que dénote externalSAID
        xformedData  SECURITY-TRANSFORMATION.&XformedDataType
                ({ValidSTs})
            -- Le membre réel de ValidSTs est celui
            -- que dénote externalSAID
}
SubsequentPdv {SECURITY-TRANSFORMATION: ValidSTs}::= SEQUENCE
{
        dynamicUnprotParm
            SECURITY-TRANSFORMATION.&DynamicUnprotectedParm
                ({ValidSTs}) OPTIONAL,
        xformedData  SECURITY-TRANSFORMATION.&XformedDataType
                ({ValidSTs})
            -- Le membre réel ValidSTs est dénoté
            -- par le contexte de présentation
}
END
```