UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T X.832

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(04/95)

RÉSEAUX DE COMMUNICATION DE DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS

SECURITÉ

TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DES SYSTÈMES OUVERTS – SÉCURITÉ GÉNÉRIQUE DES COUCHES SUPÉRIEURES: SPÉCIFICATION DU PROTOCOLE D'ÉLÉMENT DE SERVICE D'ÉCHANGE DE SÉCURITÉ

Recommandation UIT-T X.832

(Antérieurement «Recommandation du CCITT»)

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. Au sein de l'UIT-T, qui est l'entité qui établit les normes mondiales (Recommandations) sur les télécommunications, participent quelque 179 pays membres, 84 exploitations de télécommunications reconnues, 145 organisations scientifiques et industrielles et 38 organisations internationales.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution nº 1 de la Conférence mondiale de normalisation des télécommunications (CMNT), (Helsinki, 1993). De plus, la CMNT, qui se réunit tous les quatre ans, approuve les Recommandations qui lui sont soumises et établit le programme d'études pour la période suivante.

Dans certains secteurs de la technologie 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. Le texte de la Recommandation X.832 de l'UIT-T a été approuvé le 10 avril 1995. Son texte est publié, sous forme identique, comme Norme internationale ISO/CEI 11586-3.

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.

© UIT 1996

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.

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE COMMUNICATION DE DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS

(Février 1994)

ORGANISATION DES RECOMMANDATIONS DE LA SÉRIE X

Domaine	Recommandations
RÉSEAUX PUBLICS POUR DONNÉES	
Services et services complémentaires	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
Définition 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 de couche	X.280-X.289
Test de conformité	X.290-X.299
INTERFONCTIONNEMENT DES RÉSEAUX	
Considérations générales	X.300-X.349
Systèmes mobiles de transmission de données	X.350-X.369
Gestion	X.370-X.399
SYSTÈMES DE MESSAGERIE	X.400-X.499
ANNUAIRE	X.500-X.599
RÉSEAUTAGE OSI ET ASPECTS DES SYSTÈMES	
Réseautage	X.600-X.649
Dénomination, adressage et enregistrement	X.650-X.679
Notation de syntaxe abstraite numéro un (ASN.1)	X.680-X.699
GESTION OSI	X.700-X.799
SÉCURITÉ	X.800-X.849
APPLICATIONS OSI	
Engagement, concomitance et rétablissement	X.850-X.859
Traitement des transactions	X.860-X.879
Opérations distantes	X.880-X.899
TRAITEMENT OUVERT RÉPARTI	X.900-X.999

TABLE DES MATIÈRES

Page

1 Domaine d'application 1

2 Références normatives 1

2.1 Recommandations | Normes internationales identiques 1

3 Définitions 2

4 Abréviations 2

5 Aperçu général du protocole 2

5.1 Fourniture du service 2

5.2 Utilisation des services sous-jacents 2

6 Eléments de procédure 3

6.1 Unités APDU utilisées 3

6.2 Procédure de transfert 3

6.3 Procédure d'abandon lancée par l'utilisateur 3

6.4 Procédure d'abandon lancée par le fournisseur 3

7 Structure et codage des unités APDU SESE 4

7.1 Spécifications génériques de l'unité APDU 4

7.2 Construction de la syntaxe abstraite 6

8 Projection (mappage) sur les services sous-jacents 6

8.1 Considérations générales 6

8.2 Projection sur des services ACSE 7

9 Conformité 7

9.1 Déclaration 7

9.2 Conformité statique 7

9.3 Conformité dynamique 7

Annexe A – Tableaux des états de la machine SEPM 8

A.1 Considérations générales 8

A.2 Conventions 8

A.3 Tableaux 8

Annexe B – Définition du contexte d'application SESE de base 11

B.1 Nom de contexte d'application 11

B.2 Eléments du service application 11

B.3 Projections des unités APDU SESE 11

B.4 Contraintes de concaténation de valeur PDV 11

B.5 Contraintes d'intégration de valeur PDV 11

B.6 Contraintes de procédure 12

B.7 Contraintes de contexte de présentation 12

Résumé

La présente Recommandation | Norme internationale fait partie d'une série de Recommandations comprenant un ensemble de moyens destinés à la réalisation des protocoles des couches supérieures de l'OSI qui prennent en charge les services de sécurité. La présente Recommandation | Norme internationale spécifie le protocole fourni par l'élément de service d'échange de sécurité (SESE) qui est un élément de service d'application (ASE) facilitant la communication des informations nécessaires pour assurer les services de sécurité dans la couche Application de l'OSI.

Introduction

La présente Recommandation | Norme internationale appartient à d'une série de Recommandations | 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 | Norme internationale constitue la Partie 3 de cette série.

NORME INTERNATIONALE

RECOMMANDATION UIT-T

TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DES SYSTÈMES OUVERTS – SÉCURITÉ GÉNÉRIQUE DES COUCHES SUPÉRIEURES: SPÉCIFICATION DU PROTOCOLE D'ÉLÉMENT DE SERVICE D'ÉCHANGE DE SÉCURITÉ

1 Domaine d'application

1.1 La présente série de Recommandations | Normes internationales définit une série de moyens génériques utilisés dans l'établissement de services de sécurité dans des protocoles de couche Application. 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;

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

1.2 La présente Recommandation | Norme internationale spécifie le protocole fourni par l'élément de service d'échange de sécurité (SESE). Celui-ci est un élément ASE qui permet la communication d'informations de sécurité 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 | Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute Recommandation et Norme sont sujettes à révision, et les parties prenantes aux accords fondés sur la présente Recommandation | Norme internationale sont invites 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 | Normes internationales identiques

– Recommandation UIT-T X.207 (1993) | ISO/CEI 9545:1994, *Technologies de l'information – Interconnexion des systèmes ouverts – Structure de la Couche Application.*

– Recommandation UIT-T X.216 (1994) | ISO/CEI 8822:1994, *Technologies de l'information – Interconnexion des systèmes ouverts – Définition du service de Présentation.*

– Recommandation UIT-T X.217 (1995) | ISO/CEI 8649:...[1)], *Technologies de l'information – Interconnexion des systèmes ouverts – Définition de service applicable à l'élément de service de contrôle d'association.*

– Recommandation UIT-T X.226 (1994) | 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.227 (1995) | ISO/CEI 8650-1:...[1)], *Technologies de l'information – Interconnexion des systèmes ouverts – Protocole en mode connexion applicable à l'élément de service de contrôle d'association: Spécification du protocole.*

---

1) A publier.

- Recommandation UIT-T X.680 (1994) | 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) | 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) | ISO/CEI 8824-3:1995, *Technologies de l'information – Notation de syntaxe abstraite numéro un: Spécification des contraintes.*
- Recommandation UIT-T X.683 (1994) | 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: Spécification 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 de systèmes ouverts – Modèle de sécurité pour les couches supérieures.*

3 Définitions

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

- échange de sécurité;
- item d'échange de sécurité.

4 Abréviations

ACSE	Elément de service de contrôle d'association (*association control service element*)
APDU	Unité de données de protocole d'application (*application-protocol-data-unit*)
ASE	Elément de service d'application (*application-service-element*)
ASO	Objet de service d'applications (*application-service-object*)
OSI	Interconnexion des systèmes ouverts (*open systems interconnection*)
PICS	Déclaration de conformité d'une instance de protocole (*protocol implementation conformance statement*)
SEPM	Machine protocolaire d'échange de sécurité (*security exchange protocol machine*)
SEI	Item d'échange de sécurité (*security exchange item*)
SESE	Elément de service d'échange de sécurité (*security exchange service element*)

5 Aperçu du protocole

5.1 Fourniture du service

Le protocole spécifié dans la présente Spécification fournit les services définis dans la Rec. UIT-T X.831 | ISO/CEI 11586-2. Ces services sont les suivants:

SE-TRANSFER	Non confirmé – (transfert)
SE-U-ABORT	Non confirmé – (abandon par l'utilisateur)
SE-P-ABORT	Lancé par le fournisseur – (abandon par le fournisseur)

5.2 Utilisation des services sous-jacents

Ce protocole d'élément SESE définit une série d'unités APDU dont chacune a la capacité d'être individuellement projetée sur un service de couche Présentation acheminant des données d'utilisateur, d'être intégrée dans une autre unité PDU d'application ou d'être concaténée à celle-ci conformément aux règles du contexte ASO ou du contexte d'application en vigueur.

L'article 8 définit quelques projections utiles sur le service de présentation et l'élément ACSE.

6 Eléments de procédure

6.1 Unités APDU utilisées

Le protocole SESE spécifie les unités APDU suivantes:

SE-TRANSFER (SETR)

SE-U-ABORT (SEAB)

SE-P-ABORT (SEPA)

6.2 Procédure de transfert

Cette procédure est utilisée par une machine SEPM demanderesse pour lancer un échange de sécurité nécessitant le transfert d'un ou de plusieurs items d'échange de sécurité. Elle est également utilisée soit par une machine SEPM appelante soit par une machine SEPM appelée pour transférer d'autres items d'échange de sécurité lancés par la machine SEPM appelante.

A la réception d'une primitive de demande SE-TRANSFER, la machine SEPM conserve l'identificateur d'échange de sécurité et produit une unité APDU SE-TRANSFER (SETR).

A la réception d'une unité APDU SE-TRANSFER (SETR), la machine SEPM conserve l'identificateur d'échange de sécurité et émet une primitive d'indication SE-TRANSFER.

Si l'échange de sécurité relève de la classe «à l'alternat» et que l'échange ne se déroule pas selon la séquence attendue, la SEPM génère une APDU SE-P-ABORT (SEPA) et émet une indication SE-P-ABORT.

6.3 Procédure d'abandon lancée par l'utilisateur

Cette procédure est utilisée par un utilisateur de l'élément SESE pour indiquer à l'utilisateur de SESE homologue et à la machine SEPM qu'une erreur s'est produite et qu'il y a lieu de terminer anormalement l'échange de sécurité en cours. De plus, elle peut facultativement entraîner la libération anormale de l'association ASO, avec la perte éventuelle d'informations en transit. Elle est lancée par une primitive de demande SE-U-ABORT.

A la réception d'une primitive de demande SE-U-ABORT, la machine SEPM produit une unité APDU SE-ABORT (SEAB).

A la réception d'une unité APDU SE-ABORT (SEAB), la machine SEPM émet une primitive d'indication SE-U-ABORT.

6.4 Procédure d'abandon lancée par le fournisseur

Cette procédure est utilisée par la machine SEPM pour indiquer aux utilisateurs de l'élément SESE qu'une erreur s'est produite et qu'il y a lieu de terminer anormalement l'échange de sécurité en cours. De plus, elle peut facultativement entraîner la libération anormale de l'association ASO, avec la perte éventuelle d'informations en transit.

A la détection d'une erreur, la machine SEPM émet une primitive d'indication SE-P-ABORT et produit une unité APDU SE-P-ABORT (SEPA). Si, en raison de la gravité de l'erreur, il est nécessaire de mettre fin à l'association ASO, l'unité APDU SEPA est projetée sur un service d'abandon Association ASO. A la réception de l'indication d'abandon Association ASO avec l'unité APDU SEPA, la machine SEPM émet une indication SE-P-ABORT dont l'indicateur de blocage est à 1.

Une situation d'erreur entraînant la production d'une SE-P-ABORT a un *code de problème* pouvant être signalé aux deux extrémités. Les difficultés ainsi signalées peuvent être:

a) *un problème d'ordre général:* ne se rapporte pas à un type d'unité APDU particulier;

b) *un problème de transfert:* difficulté résultant de la réception d'une unité APDU SE-TRANSFER;

c) *un problème d'abandon:* difficulté résultant de la réception d'une unité APDU SE-U-ABORT.

Les situations d'erreur particulières, ainsi que les codes de problèmes correspondants, sont décrits ci-après.

6.4.1 Problème d'ordre général

– *APDU non valide:* la structure et/ou le codage de l'APDU n'est pas conforme aux APDU SETR, SEAB ou SEPA.

6.4.2 Problème de transfert

a) *identificateur d'invocation double:* le même identificateur d'invocation est utilisé pour une autre invocation d'échange de sécurité actif;

b) *échange de sécurité non reconnu:* l'échange de sécurité identifié n'est pas valable dans le contexte ASO en question;

c) *item de type erroné:* le type d'item SEI n'est pas conforme à celui de la définition de classe d'objet;

d) *identificateur d'invocation inapproprié:* l'identificateur d'invocation ne fait pas partie de l'ensemble spécifié pour le contexte ASO en question;

e) *erreur d'enchaînement à l'alternat:* la SETR reçue n'est pas conforme à l'enchaînement d'événements de la classe «à l'alternat» de l'échange de sécurité.

6.4.3 Problème d'abandon

a) *identificateur d'invocation non reconnu:* l'identificateur d'invocation ne reconnaît pas un transfert d'échange de sécurité actif ou venant de se terminer;

b) *abandon imprévu:* l'échange de sécurité identifié ne donne pas lieu à un abandon pour l'élément d'échange de sécurité en question;

c) *erreur non reconnue:* l'échange de sécurité identifié ne produit pas cette erreur;

d) *erreur imprévue:* l'échange de sécurité identifié ne produit pas cette erreur pour l'élément d'échange de sécurité en question;

e) *paramètre d'erreur de type erroné:* le type de paramètre d'erreur n'est pas conforme à celui de la définition de l'erreur.

7 Structure et codage des unités APDU SESE

Le type de données paramétré des APDU SESE génériques est spécifié au 7.1 en ASN.1 (Rec. UIT-T X.683 | ISO/CEI 8824-4). La méthode de construction d'une syntaxe abstraite SESE de prise en charge d'un ensemble particulier d'échanges de sécurité est décrite au 7.2.

7.1 Spécifications génériques de l'unité APDU

La spécification suivante de l'unité APDU paramétrée est compatible avec la définition des syntaxes abstraites d'éléments SESE adaptés, prenant en charge tout type d'échange de sécurité défini dans le cadre de spécification de la Partie 1 de la présente Recommandation | Norme internationale. Dans ce qui suit, le paramètre ValidSE identifie l'ensemble de security exchange pris en charge. Le paramètre InvocationIdSet définit les valeurs disponibles pour identifier les invocations d'échange de sécurité distinctes qui peuvent être simultanément actives, et pouvant être utilisées dans des réponses ultérieures pour mettre en corrélation les indications d'erreur avec les invocations d'échange de sécurité actives. Si une telle corrélation n'est pas requise dans certaines réalisations (les différentes invocations d'échange de sécurité ne se chevauchent jamais, par exemple), il y a lieu de mettre InvocationIdSet à la valeur NoInvocationId.

```
SeseAPDUs {joint-iso-ccitt genericULS(20) modules(1) seseAPDUs(6) }
DEFINITIONS AUTOMATIC TAGS::=
BEGIN

-- EXPORTE TOUT --

IMPORTS

        notation
            FROM ObjectIdentifiers {joint-iso-ccitt genericULS (20)
                modules (1) objectIdentifiers (0) }
        dirAuthenticationTwoWay
            FROM GulsSecurityExchanges {joint-iso-ccitt genericULS (20)
                modules (1) gulsSecurityExchanges (2) }
        SECURITY-EXCHANGE {}, SE-ERROR {}
            FROM NOTATION notation;
```

```
SESEapdus {SECURITY-EXCHANGE:ValidSEs, InvocationId:InvocationIdSet }::=

        CHOICE {
            se-transfer         SETransfer {{ValidSEs},{InvocationIdSet}},
            se-u-abort          SEUAbort {{ValidSEs},{InvocationIdSet}},
            se-p-abort          SEPAbort {{ValidSEs},{InvocationIdSet}}
            }

SETransfer {SECURITY-EXCHANGE:ValidSEs, InvocationId:InvocationIdSet }::=
SEQUENCE {
        seIdentifier        SECURITY-EXCHANGE.&sE-Identifier ( {ValidSEs}),
                            -- Identifie un des échanges de sécurité
                            -- pris en charge par cette syntaxe abstraite SESE
        itemIdentifier      SECURITY-EXCHANGE.&SE-Items.&itemId
                            ( {ValidSEs}{@seIdentifier}),
                            -- Identifie un des éléments de l'échange de sécurité
                            -- désigné par "seIdentifier"
        seItem              SECURITY-EXCHANGE.&SE-Items.&ItemType
                            ({ValidSEs}{@seIdentifier, @itemIdentifier}),
        invocationId        InvocationId (InvocationIdSet)
                            (CONSTRAINED BY {-- Doit être identique à l'identificateur
                            -- "invocationID" d'un échange de sécurité actif
                            -- si le fanion de départ n'a pas la valeur TRUE --})
                            DEFAULT noInvocationId,
        startFlag           BOOLEAN DEFAULT FALSE,
                            -- Ce champ n'est positionné que lors du transfert
                            -- du premier élément de l'échange de sécurité.
        endFlag             BOOLEAN DEFAULT FALSE
                            -- Ce champ est positionné lors du transfert
                            -- du dernier élément d'un échange de sécurité. Il est
                            -- nécessaire pour la prise en charge des mécanismes impliquant
                            -- n échanges, lorsque n n'est pas connu a priori -- }

SEUAbort {SECURITY-EXCHANGE:ValidSEs, InvocationId:InvocationIdSet }::=
SEQUENCE {
        invocationId        InvocationId (InvocationIdSet)
                            (CONSTRAINED BY {-- Doit être identique à l'identificateur
                            --  "invocationId" d'un échange de sécurité actif
                            --  ou venant de se terminer --})
                            DEFAULT noInvocationId,
        itemIdentifier      SECURITY-EXCHANGE.&SE-Items.&itemId
                            ( {ValidSEs.&SE-Items}) OPTIONAL,
                            --  Ce composant ne figure
                            --  que lorsque l'ABORT est générée
                            --  suite à la réception d'une APDU SETransfer.
        errors              SEQUENCE OF SEerror {{ValidSEs}}    OPTIONAL
                            --  nécessaire pour traiter les codes d'erreur multiples -- }

SEPAbort {SECURITY-EXCHANGE:ValidSEs, InvocationId:InvocationIdSet }::=
SEQUENCE {
        invocationId        InvocationId (InvocationIdSet) OPTIONAL,
        itemIdentifier      SECURITY-EXCHANGE.&SE-Items.&itemId
                            ( {ValidSEs.&SE-Items}) OPTIONAL,
                            --  Ce composant ne figure que lorsque
                            --  l'ABORT est générée
                            --  suite à la réception d'une APDU SETransfer.
        problemCode         ProblemCode }

InvocationId ::= CHOICE {
        present             INTEGER,
        absent              NULL }

noInvocationId InvocationId ::= absent:NULL

NoInvocationId InvocationId ::= {noInvocationId}
```

```
SEerror {SECURITY-EXCHANGE:ValidSEs }::= SEQUENCE {
        errorCode       SE-ERROR.&errorCode
                        ({Errors{{ValidSEs}}}) OPTIONAL,
        errorParameter  SE-ERROR.&ParameterType
                        ({Errors{{ValidSEs}}}{@errorCode}) OPTIONAL}

Errors{SECURITY-EXCHANGE:ValidSEs} SE-ERROR ::= {ValidSEs.&SE-Items.&Errors}

ProblemCode ::= CHOICE {
        general         GeneralProblem,
        transfer        TransferProblem,
        abort           AbortProblem }

GeneralProblem ::= ENUMERATED {
        invalidAPDU (0) }

TransferProblem ::= ENUMERATED {
        duplicateInvocationId (0),
        unrecognizedSecurityExchange (1),
        mistypedItem (2),
        inappropriateInvocationId (3),
        alternatingSequenceError (4) }

AbortProblem ::= ENUMERATED {
        unrecognizedInvocationId (0),
        abortUnexpected (1),
        unrecognizedError (2),
        unexpectedError (3),
        mistypedErrorParameter (4) }

END
```

7.2 Construction de la syntaxe abstraite

La syntaxe abstraite d'un SESE prenant en charge un ensemble donné d'échanges de sécurité est spécifiée à l'aide de la classe d'objets informationnels ABSTRACT-SYNTAX définie à l'Annexe B de la Rec. UIT-T X.681 | ISO/CEI 8824-2.

A titre d'exemple, pour spécifier une syntaxe abstraite SESE assurant deux des échanges de sécurité définis dans les Annexes D et F de la Partie 1 de la présente Spécification, pour une réalisation qui ne nécessite pas d'identificateurs d'invocation, on utilisera la notation suivante:

```
AccCtl-Authent-Abstract-Syntax
ABSTRACT-SYNTAX ::=
    { SESEapdus {
        { boundAccessControlCert | dirAuthenticationTwoWay },
        NoInvocationId }
    IDENTIFIED BY {..Abstract Syntax Object Identifier..}
```

8 Mappage sur les services sous-jacents

8.1 Considérations générales

Le protocole SESE définit une série d'unités APDU dont chacune a la capacité d'être projetée sur un service de couche Présentation qui achemine des données d'utilisateur ou qui peut être intégrée dans une autre unité APDU ou concaténée à celle-ci, selon les règles du contexte ASO ou du contexte d'application en vigueur.

Sauf spécification contraire dans la définition du contexte ASO (ou du contexte d'application), un échange SEAB dont l'indicateur de blocage est à 1, ou un échange SEPA dont la gravité de l'erreur nécessite de terminer anormalement l'association, est projeté sur le service A-ABORT, alors qu'un échange SETR est projeté sur un service P-DATA.

Si l'élément SESE fait partie d'une spécification de contexte d'application, l'introduction d'une unité fonctionnelle ACSE-Authentication dans ce contexte d'application n'est ni requise ni exclue.

L'élément SESE n'utilise pas directement d'autres éléments ASE, mais indirectement via une fonction de contrôle (comme défini dans la structure de la couche Application). Quelques exemples de projections utiles pouvant être spécifiées sont présentés ci-dessous.

8.2 Mappage sur des services ACSE

8.2.1 Mappage d'échange SE-TRANSFER sur A-ASSOCIATE

Quand le premier des deux transferts d'un échange de sécurité peut survenir conjointement avec l'établissement d'association, une unité APDU SE-TRANSFER peut être projetée sur le champ de valeur d'authentification ou le champ d'information d'utilisateur d'une demande/indication A-ASSOCIATE.

Quand une unité APDU SE-TRANSFER est donnée en réponse à une unité APDU SE-TRANSFER acheminée sur une demande/indication A-ASSOCIATE, l'ancienne unité APDU SE-TRANSFER peut être projetée sur le champ de la valeur d'authentification ou sur le champ de l'information d'utilisateur de la réponse/confirmation A-ASSOCIATE.

Lorsqu'une APDU SE-TRANSFER est mise en correspondance avec le champ «valeur d'authentification» d'une primitive A-Associate, l'option EXTERNAL doit être utilisée et le champ «nom du mécanisme d'authentification» ne doit pas être utilisé.

8.2.2 Mappage d'échanges SE-TRANSFER additionnels

Quand l'échange de sécurité qui survient conjointement avec l'établissement de l'association nécessite le transfert d'un ou de plusieurs items d'échange de sécurité, le troisième transfert (SE-TRANSFER) et le suivant doivent être projetés sur P-DATA. Dans ce cas, le contexte d'application est susceptible d'avoir une règle qui stipule que même si l'association a été établie avec succès après les deux premiers transferts, elle ne doit pas être utilisée par d'autres éléments ASE à moins que l'échange de sécurité n'ait abouti.

9 Conformité

Un système réputé conforme aux procédures de mise en œuvre spécifiées dans la présente Recommandation | Norme internationale satisfera aux prescriptions des 9.1 à 9.3.

9.1 Déclaration

Les éléments suivants seront déclarés par le responsable de la mise en œuvre:

a) la série d'échanges de sécurité qui est fournie;

b) pour chaque échange de sécurité qui est prévu, si le système a la capacité de lancer un échange de sécurité et/ou de répondre à un échange de sécurité lancé par l'autre extrémité;

c) la gamme des identificateurs d'invocation pouvant être simultanément produits ou actifs;

d) si le système peut prendre en charge la classe d'échanges de sécurité «à l'alternat» et/ou la classe «libre».

9.2 Conformité statique

Le système:

a) doit agir en tant qu'appelant et/ou appelé pour un ou plusieurs échanges de sécurité;

b) doit prendre en charge (au minimum) le codage qui résulte de l'application des règles de codage ASN.1 de base à l'ASN.1 spécifiée dans l'article 7 pour les besoins d'échange d'unités SESE APDU.

9.3 Conformité dynamique

Le système suivra toutes les procédures spécifiées à l'article 6.

Annexe A

Tableaux des états de la machine SEPM

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

A.1 Considérations générales

La présente annexe définit la machine protocole d'échange de sécurité (SEPM) en termes d'un tableau des états. Celui-ci fait apparaître une relation interne entre l'état d'une machine SEPM, les événements entrants qui surviennent dans le protocole, les actions entreprises et l'état résultant de la machine SEPM.

Ce tableau des états ne constitue pas une définition formelle de la machine en question. Il a été ajouté dans le but de donner une spécification plus précise des éléments de procédure définis à l'article 6. Comme la présente annexe et l'article 6 ont la même préséance, toute contradiction entre les deux doit être traitée comme une erreur de la spécification.

La présente annexe contient les tableaux suivants:

1) le Tableau 1 spécifie le nom abrégé, l'origine et le nom de chaque événement entrant. Les origines sont:
   a) l'utilisateur du service SEPM (utilisateur SE);
   b) la machine SEPM homologue (homologue SE),
2) le Tableau 2 spécifie le nom abrégé, l'objectif et le nom de chaque événement sortant. Les objectifs sont:
   a) l'utilisateur du service SEPM (utilisateur SE);
   b) la machine SEPM homologue (homologue SE),
3) le Tableau 3 contient les prédicats à utiliser,
4) le Tableau 4 contient le nom abrégé et la description de chaque état,
5) le Tableau 5 est le tableau des états SEPM établi avec les abréviations des tableaux qui précèdent.

A.2 Conventions

L'intersection d'un événement entrant (une rangée du tableau des états) et d'un état (une colonne du tableau des états) forme une cellule.

Dans le tableau des états, une cellule vierge représente la combinaison d'un événement entrant et d'un état qui n'est pas défini pour la machine SEPM.

Une cellule non vierge représente un événement entrant et un état qui est défini pour la machine SEPM. Une telle cellule contiendrait une liste d'actions à entreprendre (obligatoirement et/ou conditionnellement).

A.3 Tableaux

Tableau 1 – Liste des événements entrants

Nom abrégé	Origine	Nom
SE-TRANSFER req	utilisateur SE	primitive de demande SE-TRANSFER
SETR	homologue SE	APDU SE-TRANSFER
SE-U-ABORT req	utilisateur SE	primitive de demande SE-U-ABORT
SEAB	homologue SE	APDU SE-U-ABORT
SEPA	homologue SE	APDU SE-P-ABORT
invalid APDU	homologue SE	APDU non valide

Tableau 2 – Liste des événements sortants

Nom abrégé	Objectif	Nom
SE-TRANSFER ind	utilisateur SE	primitive d'ind. SE-TRANSFER
SETR	homologue SE	APDU SE-TRANSFER
SE-U-ABORT ind	utilisateur SE	primitive d'ind. SE-U-ABORT
SEAB	homologue SE	APDU SE-U-ABORT
SEPA	homologue SE	APDU SE-P-ABORT
SE-P-ABORT ind	utilisateur SE	primitive d'ind. SE-P-ABORT

Tableau 3 – Prédicats

Code	Signification
p1	endFlag = Vrai
p2	Problème de transfert détecté
p3	Problème d'abandon détecté

Tableau 4 – Etats SEPM

Nom abrégé	Description
STA0	Etat de repos
STA1	Etat d'échange

Tableau 5 – Tableau des états SEPM

	STA0 Etat de repos	STA1 Etat d'échange
SE-TRANSFER req	p1 SETR STA0 ^p1 SETR STA1	p1 SETR STA0 ^p1 SETR STA1
SETR	p2 SE-P-ABORT ind SEPA STA0 ^p2&p1 SE-TRANSFER ind STA0 ^p2&^p1 SE-TRANSFER ind STA1	p2 SE-P-ABORT ind SEPA STA0 ^p2&p1 SE-TRANSFER ind STA0 ^p2&^p1 SE-TRANSFER ind STA1
SE-U-ABORT req		SEAB STA0
SEAB		p3 SE-P-ABORT ind SEPA STA0 ^p3 SE-U-ABORT ind STA0
SEPA	SE-P-ABORT ind STA0	SE-P-ABORT ind STA0
APDU non valide	SE-P-ABORT ind SEPA STA0	SE-P-ABORT ind SEPA STA0
NOTE – Tous les cas non repris dans le Tableau 5 sont traités par la machine SEPM comme des questions locales.		

Annexe B

Définition du contexte d'application SESE de base

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

La présente annexe définit un contexte d'application contenant uniquement les éléments ACSE et SESE. C'est un contexte d'application jugé utile dans la mise au point d'applications de serveur de sécurité.

B.1 Nom de contexte d'application

{ joint-iso-itu-t genericULS (20) application-contexts (7) basic (1) }

B.2 Eléments du service application

Eléments ACSE et SESE.

B.3 Projections des unités APDU SESE

a) Les unités APDU SE-U-ABORT et SE-P-ABORT entraînent toujours la fin anormale de l'association d'application sous-jacente et seront donc toujours projetées sur le paramètre d'information d'utilisateur d'une primitive de service A-ABORT.

b) Dans le cas d'un échange de sécurité unidirectionnel, le demandeur projettera l'unité APDU SE-TRANSFER sur le paramètre d'information de l'utilisateur de la primitive de service de demande A-ASSOCIATE. L'appelé:

- enverra une unité de réponse APDU A-ASSOCIATE avec le résultat «refusé (provisoirement)», indiquant l'aboutissement de la réussite de l'échange sans nécessité d'établir une association; ou
- en cas d'erreur, interrompra l'association avec une unité APDU SE-U-ABORT ou SE-P-ABORT décrite ci-dessus (au 3.1). On notera qu'une collision de procédure de service A-ABORT n'est pas possible étant donné que dans ce scénario, le demandeur n'émet pas de A-ABORT.

c) Dans tous les autres cas, le demandeur projettera l'unité APDU SE-TRANSFER sur le paramètre d'information d'utilisateur de la primitive de service de demande A-ASSOCIATE. Le demandé:

- enverra une unité de réponse APDU A-ASSOCIATE dont le champ d'information d'utilisateur est vide (si le demandeur doit envoyer l'item SEI suivant) ou (plus généralement) contenant une unité APDU SE-TRANSFER et le résultat «accepté»; ou
- en cas d'erreur, appliquera la même procédure qu'au 3.2 b) ci-dessus.

Les deux unités APDU SE-TRANSFER sont projetées sur P-DATA; on notera que l'élément SESE est le seul utilisateur du service P-DATA.

Les erreurs sont signalées au moyen des unités APDU SE-U-ABORT et SE-P-ABORT comme indiqué au 3.1 ci-dessus. On notera que certains échanges de sécurité permettront aux items SEI d'être envoyés de manière asynchrone (autrement dit sans obligation de respecter une alternance stricte). Dans un tel cas pourrait se produire une collision de procédure de service A-ABORT, et dès lors, les unités APDU SE-U-ABORT ou SE-P-ABORT ne seraient pas remises aux entités homologues. Néanmoins, les deux entités sont informées que l'association a été libérée.

B.4 Contraintes de concaténation de valeur PDV

Ne s'appliquent pas; l'élément SESE est le seul utilisateur du service P-DATA.

B.5 Contraintes d'intégration de valeur PDV

Etant donné que l'élément SESE est le seul utilisateur du service P-DATA, les seules valeurs PDV intégrées dans les APDU SESE sont celles qui résultent de l'utilisation du type paramétré PROTECTED.

B.6 Contraintes de procédure

Aucune, exception faite des contraintes de procédure ACSE.

B.7 Contraintes de contexte de présentation

Aucune.

NOTE – Il pourrait être indiqué de restreindre le contexte de ces unités APDU SESE aux règles de codage de base (BER) afin de simplifier le travail du créateur du logiciel. On peut bien entendu utiliser n'importe quel contexte dans la valeur EMBEDDED PDV produite par le type PROTECTED.