UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T X.832

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(04/95)

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

SEGURIDAD

TECNOLOGÍA DE LA INFORMACIÓN – INTERCONEXIÓN DE SISTEMAS ABIERTOS – SEGURIDAD GENÉRICA DE LAS CAPAS SUPERIORES: ESPECIFICACIÓN DEL PROTOCOLO DE ELEMENTO DE SERVICIO DE INTERCAMBIO DE SEGURIDAD

Recomendación UIT-T X.832

(Anteriormente «Recomendación del CCITT»)

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. En el UIT-T, que es la entidad que establece normas mundiales (Recomendaciones) sobre las telecomunicaciones, participan unos 179 países miembros, 84 empresas de explotación de telecomunicaciones, 145 organizaciones científicas e industriales y 38 organizaciones internacionales.

Las Recomendaciones las aprueban los Miembros del UIT-T de acuerdo con el procedimiento establecido en la Resolución N.° 1 de la CMNT (Helsinki, 1993). Adicionalmente, la Conferencia Mundial de Normalización de las Telecomunicaciones (CMNT), que se celebra cada cuatro años, aprueba las Recomendaciones que para ello se le sometan y establece el programa de estudios para el periodo siguiente.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI. El texto de la Recomendación UIT-T X.832 se aprobó el 10 de abril de 1995. Su texto se publica también, en forma idéntica, como Norma Internacional ISO/CEI 11586-3.

NOTA

En esta Recomendación, la expresión «Administración» se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

(Febrero de 1994)

ORGANIZACIÓN DE LAS RECOMENDACIONES DE LA SERIE X

Dominio	Recomendaciones
REDES PÚBLICAS DE DATOS	
Servicios y facilidades	X.1-X.19
Interfaces	X.20-X.49
Transmisión, señalización y conmutación	X.50-X.89
Aspectos de redes	X.90-X.149
Mantenimiento	X.150-X.179
Disposiciones administrativas	X.180-X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Modelo y notación	X.200-X.209
Definiciones de los servicios	X.210-X.219
Especificaciones de los protocolos en modo conexión	X.220-X.229
Especificaciones de los protocolos en modo sin conexión	X.230-X.239
Formularios para enunciados de conformidad de implementación de protocolo	X.240-X.259
Identificación de protocolos	X.260-X.269
Protocolos de seguridad	X.270-X.279
Objetos gestionados de capa	X.280-X.289
Pruebas de conformidad	X.290-X.299
INTERFUNCIONAMIENTO ENTRE REDES	
Generalidades	X.300-X.349
Sistemas móviles de transmisión de datos	X.350-X.369
Gestión	X.370-X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400-X.499
DIRECTORIO	X.500-X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	
Gestión de redes	X.600-X.649
Denominación, direccionamiento y registro	X.650-X.679
Notación de sintaxis abstracta uno	X.680-X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700-X.799
SEGURIDAD	X.800-X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Cometimiento, concurrencia y recuperación	X.850-X.859
Tratamiento de transacciones	X.860-X.879
Operaciones a distancia	X.880-X.899
TRATAMIENTO ABIERTO DISTRIBUIDO	X.900-X.999

ÍNDICE

Sumario

Esta Recomendación | Norma Internacional pertenece a una serie de recomendaciones que proporcionan un conjunto de facilidades para ayudar a la construcción de los protocolos de capas superiores de OSI que sustentan la prestación de servicios de seguridad. En la presente Recomendación | Norma Internacional se define el protocolo proporcionado por el elemento de servicio de intercambio de seguridad (SESE). El SESE es un elemento de servicio de aplicación (ASE) que facilita la comunicación de la información de seguridad para sustentar la prestación de servicios de seguridad dentro de la capa de aplicación de OSI.

Introducción

Esta Recomendación | Norma Internacional pertenece a una serie de Recomendaciones | Normas Internacionales, que colectivamente proporcionan un conjunto de facilidades para sustentar la prestación de servicios de seguridad en protocolos de capa de aplicación. Las Partes son las siguientes:

- Parte 1: Sinopsis, modelos y notación
- Parte 2: Definición de servicio del elemento de servicio de intercambio de seguridad
- Parte 3: Especificación del protocolo del elemento de servicio de intercambio de seguridad
- Parte 4: Especificación de la sintaxis de transferencia de protección
- Parte 5: Formulario PICS del elemento de servicio de intercambio de seguridad
- Parte 6: Formulario PICS de la sintaxis de transferencia de protección

Esta Recomendación | Norma Internacional constituye la Parte 3 de esta serie.

NORMA INTERNACIONAL

RECOMENDACIÓN UIT-T

TECNOLOGÍA DE LA INFORMACIÓN – INTERCONEXIÓN DE SISTEMAS ABIERTOS – SEGURIDAD GENÉRICA DE LAS CAPAS SUPERIORES: ESPECIFICACIÓN DEL PROTOCOLO DE ELEMENTO DE SERVICIO DE INTERCAMBIO DE SEGURIDAD

1 Alcance

1.1 Esta serie de Recomendaciones | Normas Internacionales define un conjunto de facilidades genéricas destinadas a facilitar la prestación de servicios de seguridad en los protocolos de capa de aplicación, que comprenden:

a) un conjunto de herramientas de notación que permitan la especificación de requisitos de protección selectiva de los campos en una especificación de sintaxis abstracta, y la especificación de intercambios de seguridad y transformaciones de seguridad;

b) una definición de servicio, especificación de protocolo y formulario PICS para un elemento de servicio de aplicación (ASE) que permita la prestación de servicios de seguridad dentro de la capa de aplicación de OSI;

c) una especificación y formulario PICS para una sintaxis de transferencia de seguridad, asociada con soporte de la capa de presentación para servicios de seguridad en la capa de aplicación.

1.2 Esta Recomendación | Norma Internacional define el protocolo proporcionado por el elemento de servicio de intercambio de seguridad (SESE), que es un elemento de servicio de aplicación que permite la comunicación de información de seguridad para sustentar la prestación de servicios de seguridad dentro de la capa de aplicación.

2 Referencias normativas

Las siguientes Recomendaciones y Normas Internacionales contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación | Norma Internacional. Al efectuar esta publicación estaban en vigor las ediciones indicadas. Todas las Recomendaciones y Normas Internacionales son objeto de revisiones, por lo que se preconiza que los participantes en acuerdos basados en la presente Recomendación | Norma Internacional investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y Normas citadas a continuación. Los miembros de la CEI y de la ISO mantienen registros de las Normas Internacionales actualmente vigentes. La Oficina de Normalización de las Telecomunicaciones de la UIT mantiene una lista de las Recomendaciones UIT-T actualmente vigentes.

2.1 Recomendaciones | Normas Internacionales idénticas

– Recomendación UIT-T X.207 (1993) | ISO/CEI 9545:1994, *Tecnología de la información – Interconexión de sistemas abiertos – Estructura de la capa de aplicación.*

– Recomendación UIT-T X.216 (1994) | ISO/CEI 8822:1994, *Tecnología de la información – Interconexión de sistemas abiertos – Definición del servicio de presentación.*

– Recomendación UIT-T X.217 (1995) | ISO/CEI 8649:...[1)], *Tecnología de la información – Interconexión de sistemas abiertos – Definición de servicio para el elemento de servicio de control de asociación.*

– Recomendación UIT-T X.226 (1994) | ISO/CEI 8823-1:1994, *Tecnología de la información – Interconexión de sistemas abiertos – Protocolo de presentación con conexión: Especificación del protocolo.*

– Recomendación UIT-T X.227 (1995) | ISO/CEI 8650-1:...[1)], *Tecnología de la información – Interconexión de sistemas abiertos – Protocolo con conexión para el elemento de servicio de control de asociación: Especificación del protocolo.*

---

1) Se publicará.

- Recomendación UIT-T X.680 (1994) | ISO/CEI 8824-1:1995, *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de la notación básica.*
- Recomendación UIT-T X.681 (1994) | ISO/CEI 8824-2:1995, *Tecnología de la información – Notación de sintaxis abstracta uno – Especificación de objetos de información.*
- Recomendación UIT-T X.682 (1994) | ISO/CEI 8824-3:1995, *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de constricciones.*
- Recomendación UIT-T X.683 (1994) | ISO/CEI 8824-4:1995, *Tecnología de la información – Notación de sintaxis abstracta uno: Parametrización de las especificaciones de la notación de sintaxis abstracta uno.*
- Recomendación UIT-T X.690 (1994) | ISO/CEI 8825-1:1995, *Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Especificación de las reglas de codificación básica, de las reglas de codificación canónica y de las reglas de codificación distinguida.*
- Recomendación UIT-T X.803 (1994) | ISO/CEI 10745:1995, *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de seguridad de las capas superiores.*

3 Definiciones

Se utilizan los siguientes términos definidos en la Rec. UIT-T X.803 | ISO/CEI 10745:

- intercambio de seguridad;
- elemento de intercambio de seguridad.

4 Abreviaturas

A los efectos de esta Recomendación | Norma Internacional se utilizan las siguientes abreviaturas:

ACSE	Elemento de servicio de control de asociación (*association control service element*)
APDU	Unidad de datos de protocolo de aplicación (*application-protocol-data-unit*)
ASE	Elemento de servicio de aplicación (*application-service-element*)
ASO	Objeto de servicio de aplicación (*application-service-object*)
OSI	Interconexión de sistemas abiertos (*open systems interconnection*)
PICS	Declaración de conformidad de implementación de protocolo (*protocol implementation conformance statement*)
SEPM	Máquina de protocolo de intercambio de seguridad (*security exchange protocol machine*)
SEI	Elemento de intercambio de seguridad (*security exchange item*)
SESE	Elemento de servicio de intercambio de seguridad (*security exchange service element*)

5 Visión general del protocolo

5.1 Prestación de servicios

El protocolo definido en esta Especificación presta los servicios definidos en la Rec. UIT-T X.831 | ISO/CEI 11586-2. Estos servicios son los siguientes:

SE-TRANSFERENCIA	No confirmado
SE-U-ABORTO	No confirmado
SE-P-ABORTO	Iniciado por el proveedor

5.2 Utilización de servicios subyacentes

El protocolo SESE define un conjunto de APDU, cada una de las cuales, puede corresponder con cualquier servicio de capa de presentación que transmite datos de usuario, o puede ser insertada o concatenada con cualquier otra PDU de aplicación, conforme a las reglas del contexto de ASO o del contexto de aplicación en vigor.

En la cláusula 8 se definen algunas correspondencias útiles con el servicio de presentación y el ACSE.

6 Elementos de procedimiento

6.1 APDU utilizadas

El protocolo SESE especifica las siguientes APDU:

APDU SE-TRANSFERENCIA (SETR)

APDU SE-U-ABORTO (SEAB)

APDU SE-P-ABORTO (SEPA)

6.2 Procedimiento de transferencia

Este procedimiento es utilizado por una SEPM solicitante para iniciar un intercambio de seguridad que requiere la transferencia de uno o más elementos de intercambio de seguridad. Es también utilizado por la SEPM solicitante o respondedora para transferir otros elementos de intercambio de seguridad iniciados por la SEPM solicitante.

Al recibir una primitiva de petición SE-TRANSFERENCIA, la SEPM retiene el identificador de intercambio de seguridad y genera una APDU SE-TRANSFERENCIA (SETR).

Al recibir una APDU SE-TRANSFERENCIA (SETR), la SEPM retiene el identificador de intercambio de seguridad y emite una primitiva de indicación SE-TRANSFERENCIA.

Si el intercambio de seguridad pertenece a la clase «alternada», y el intercambio no sigue las secuencias esperadas, el SEPM genera una APDU-SE-P-ABORTO (SEPA), y emite una indicación SE-P-ABORTO.

6.3 Procedimiento de aborto iniciado por el usuario

Este procedimiento es utilizado por un usuario SESE para indicar al usuario SESE par y a la SEPM que se ha producido un error y que cualquier intercambio de seguridad en curso concluirá de manera anormal. Además, puede causar facultativamente la liberación anormal de la asociación ASO con la posible pérdida de información en tránsito. Es iniciado por una primitiva de petición SE-U-ABORTO.

Al recibir una primitiva de petición SE-U-ABORTO, la SEPM genera una APDU SE-ABORTO (SEAB).

Al recibir una APDU SE-ABORTO (SEAB), la SEPM emite una primitiva de indicación SE-U-ABORTO.

6.4 Procedimiento de aborto iniciado por el proveedor

Este procedimiento es utilizado por la SEPM para indicar a los usuarios SESE que se ha producido un error y que cualquier intercambio de seguridad en curso concluirá de manera anormal. Asimismo, puede causar facultativamente la liberación anormal de la asociación ASO con la posible pérdida de información en tránsito.

Al detectar un error, la SEPM emite una primitiva de indicación SE-P-ABORTO y genera una APDU SE-P-ABORTO (SEPA). Si la gravedad del error requiere la terminación de la asociación ASO, la APDU SEPA se pone en correspondencia con el servicio aborto de asociación de ASO. Al recibir una indicación aborto de asociación de ASO con APDU SEPA, la SEPM emite una indicación SE-P-ABORTO con el indicador de fatalidad fijado.

Una condición de error que genera SE-P-ABORTO tiene un *código de problema* asociado que puede ser indicado a ambos extremos. Los problemas así indicados están clasificados de la siguiente manera:

a) *Problema general* – No peculiar a ningún tipo de APDU particular.

b) *Problema de transferencia* – Problema resultante de la recepción de una APDU SE-TRANSFERENCIA.

c) *Problema de aborto* – Problema resultante de la recepción de una APDU SE-U-ABORTO.

Las condiciones de error particulares, así como los códigos de problemas asociados, se describen a continuación.

6.4.1 Problema general

– *APDU no válida* – La estructura y/o la codificación de la APDU no se conforma a las APDU SETR, SEAB o SEPA.

6.4.2 Problema de transferencia

a) *Identificador de invocación duplicado* – Se utiliza el mismo identificador de invocación para otra invocación de intercambio de seguridad activa.

b) *Intercambio de seguridad no reconocido* – El intercambio de seguridad identificado no es válido para este contexto de ASO.

c) *Elemento mal tipificado* – El tipo de SEI no se ajusta al de la definición de clase de objeto.

d) *Identificador de invocación inapropiado* – El identificador de invocación no figura dentro del conjunto especificado para este contexto de ASO.

e) *Error de secuencia alternada* – La SETR recibida no sigue la secuencia de la clase «alternada» del intercambio de seguridad.

6.4.3 Problema de aborto

a) *Identificador de invocación no reconocido* – El identificador de invocación no identifica una transferencia de intercambio de seguridad activa o recién completada.

b) *Aborto inesperado* – El intercambio de seguridad identificado no genera un aborto para *este* ítem de intercambio de seguridad.

c) *Error no reconocido* – El intercambio de seguridad identificado no genera este error.

d) *Error inesperado* – El intercambio de seguridad identificado no genera *este* error para este ítem de intercambio de seguridad.

e) *Parámetro de error mal tipificado* – El tipo de parámetro de error no se ajusta al de la definición de error.

7 Estructura y codificación de las APDU del SESE

El tipo de datos parametrizados de las APDU del SESE genéricas se especifica en 7.1 empleando la notación ASN.1 (véase la Rec. UIT-T X.683 | ISO/CEI 8824-4). El método de construcción de una sintaxis abstracta de SESE para sustentar un conjunto particular de intercambios de seguridad se describe en 7.2.

7.1 Especificación de APDU genérica

La siguiente especificación de APDU parametrizada sustenta la definición de sintaxis abstractas para SESE particulares que admiten cualquier conjunto de intercambios de seguridad definidos que utilizan el marco de especificación indicado en la Parte 1 de esta Recomendación | Norma Internacional. A continuación, el parámetro ValidSEs (elementos de seguridad válidos) identifica el conjunto de intercambios de seguridad sustentado. El parámetro InvocationIdSet (conjunto de Id de invocación) define los valores disponibles para identificar distintas invocaciones de intercambio de seguridad que pueden ser activadas simultáneamente, y para utilizar en la correlación de respuestas subsiguientes e indicaciones de error con las invocaciones de intercambio de seguridad activas. Si en alguna implementación no es necesaria tal correlación (por ejemplo, las invocaciones de intercambio de seguridad diferentes nunca se superponen), el parámetro InvocationIdSet se debe poner al valor fijado NoInvocationId (ningún Id de invocación).

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

-- EXPORTS ALL --

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}),
                            -- This identifies one of the security-
                            -- exchanges supported by the particular SESE
                            -- abstract syntax
        itemIdentifier      SECURITY-EXCHANGE.&SE-Items.&itemId
                            ( {ValidSEs}{@seIdentifier}),
                            -- This identifies one of the security-
                            -- exchange-items of the security exchange
                            -- indicated by "seIdentifier"
        seItem              SECURITY-EXCHANGE.&SE-Items.&ItemType
                            ({ValidSEs}{@seIdentifier, @itemIdentifier}),
        invocationId        InvocationId (InvocationIdSet)
                            (CONSTRAINED BY {-- Must be the same as the
                            -- invocationId on an active security exchange
                            -- if start flag is not true --})
                            DEFAULT noInvocationId,
        startFlag           BOOLEAN DEFAULT FALSE,
                            -- This field is set only as the first security-
                            -- exchange-item of a security-exchange is
                            -- transferred.
        endFlag             BOOLEAN DEFAULT FALSE
                            -- This field is set as the last security-exchange-
                            -- item of a security-exchange is transferred. It is
                            -- needed to accommodate those mechanisms requiring
                            -- n exchanges, where n is not known a priori -- }

SEUAbort {SECURITY-EXCHANGE:ValidSEs, InvocationId:InvocationIdSet }::=
SEQUENCE {
        invocationId        InvocationId (InvocationIdSet)
                            (CONSTRAINED BY {-- Must be the same as the
                            --  invocationId on an active or just-completed
                            --  security exchange --})
                            DEFAULT noInvocationId,
        itemIdentifier      SECURITY-EXCHANGE.&SE-Items.&itemId
                            ( {ValidSEs.&SE-Items}) OPTIONAL,
                            --  This component will only be present
                            --  when the Abort is generated subsequent
                            --  to receipt of a SETransfer APDU.
        errors              SEQUENCE OF SEerror {{ValidSEs}}    OPTIONAL
                            --  needed to handle multiple error codes -- }

SEPAbort {SECURITY-EXCHANGE:ValidSEs, InvocationId:InvocationIdSet }::=
SEQUENCE {
        invocationId        InvocationId (InvocationIdSet) OPTIONAL,
        itemIdentifier      SECURITY-EXCHANGE.&SE-Items.&itemId
                            ( {ValidSEs.&SE-Items}) OPTIONAL,
                            --  This component will only be present
                            --  when the Abort is generated subsequent
                            --  to receipt of a SETransfer APDU.
        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 Construcción de sintaxis abstracta

Se especifica una sintaxis abstracta para un SESE que sustenta un conjunto determinado de intercambios de seguridad utilizando la clase de objeto información SINTAXIS ABSTRACTA (ABSTRACT-SYNTAX) definido en la Rec. UIT-T X.681 | ISO/CEI 8824-2, Anexo B.

Por ejemplo, para especificar una sintaxis abstracta SESE que sustenta dos de los intercambios de seguridad definidos en los Anexos D y F de la Parte 1 de esta Especificación, para una implementación que no requiere identificadores de invocación, se debe utilizar la siguiente notación:

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

8 Correspondencia con servicios subyacentes

8.1 Generalidades

El protocolo SESE define un conjunto de APDU, que pueden corresponder con cualquier servicio de capa de presentación que transmite datos de usuario, o que pueden ser insertadas o concatenadas con cualquier otra APDU, conforme a las reglas del contexto de ASO o del contexto de aplicación en vigor.

Salvo especificación en contrario en la definición del contexto de ASO (o contexto de aplicación), una SEAB con un indicador de fatalidad fijado, o una SEPA con una gravedad de error que requiere la terminación anormal de la asociación, corresponden con el servicio A-ABORTO, mientras que una SETR corresponde con el servicio P-DATOS.

Si el SESE está incluido en una especificación de contexto de aplicación, no se requiere ni excluye la inclusión de la unidad funcional de autenticación de ACSE en este contexto de aplicación.

El SESE no utiliza otros ASE directamente, sino sólo indirectamente a través de una función de control (como se indica en la estructura de la capa de aplicación). No obstante, a continuación se indican algunos ejemplos de correspondencias útiles que pueden ser especificadas.

8.2 Correspondencia con los servicios ACSE

8.2.1 Correspondencia de SE-TRANSFERENCIA con A-ASOCIACIÓN

Cuando se va a producir la primera o las dos primeras transferencias de un intercambio de seguridad junto con el establecimiento de la asociación, una APDU SE-TRANSFERENCIA puede corresponder con el campo valor de autenticación o con el campo información de usuario de una primitiva de petición/indicación A-ASOCIACIÓN.

Cuando se emite una APDU SE-TRANSFERENCIA en respuesta a la APDU SE-TRANSFERENCIA transmitida en la primitiva de petición/indicación A-ASOCIACIÓN, la primera APDU SE-TRANSFERENCIA puede corresponder con el campo valor de autenticación o con el campo información de usuario de una primitiva de respuesta/confirmación A-ASOCIACIÓN.

Cuando una APDU SE-TRANSFERENCIA se hace corresponder con el campo valor de autenticación de una A-ASOCIACIÓN, debe utilizarse la opción EXTERNA y no debe utilizarse el campo nombre de mecanismo de autenticación.

8.2.2 Correspondencia de SE-TRANSFERENCIA adicionales

Cuando el intercambio de seguridad que se produce junto con el establecimiento de la asociación requiere la transferencia de más de dos elementos de intercambio de seguridad, la tercera transferencia (SE-TRANSFERENCIA) y siguientes pueden poder corresponder con P-DATOS. En este caso, es probable que el contexto de aplicación posea una regla que estipula que, aunque la asociación se haya establecido satisfactoriamente después de las primeras dos transferencias, no ha de ser utilizada por otros ASE hasta que el intercambio de seguridad se haya completado satisfactoriamente.

9 Conformidad

Un sistema que alega ejecutar los procedimientos especificados en esta Recomendación | Norma Internacional debe satisfacer los requisitos establecidos en las cláusulas 9.1 a 9.3.

9.1 Requisitos de la declaración

El implementador debe declarar lo siguiente:

a) el conjunto de intercambios de seguridad suministrado;

b) para cada intercambio de seguridad suministrado, si el sistema es capaz de iniciar el intercambio de seguridad y/o responder al intercambio de seguridad iniciado en el otro extremo;

c) la gama de identificadores de invocación que pueden ser generados/activados simultáneamente;

d) si el sistema puede sustentar la clase de intercambio de seguridad «alternada» y/o «arbitraria».

9.2 Requisitos estáticos

El sistema deberá:

a) actuar en el cometido de iniciador y/o respondedor de uno o más intercambios de seguridad;

b) sustentar (como mínimo) la codificación resultante de la aplicación de las reglas de codificación ASN.1 básicas a la ASN.1 especificada en la cláusula 7 con el objeto de intercambiar las APDU de SESE.

9.3 Requisitos dinámicos

El sistema aplicará todos los procedimientos especificados en la cláusula 6.

Anexo A

Tablas de estados de la SEPM

(Este anexo es parte integrante de esta Recomendación | Norma Internacional)

A.1 Generalidades

En este anexo se define la máquina de protocolo de intercambio de seguridad (SEPM) desde el punto de vista de una tabla de estados, que muestra la interrelación entre el estado de una SEPM, los eventos de entrada que se producen en el protocolo, las acciones ejecutadas, y el estado resultante de la SEPM.

La tabla de estados de la SEPM no constituye una definición formal de la SEPM. Se incluye para proporcionar una especificación más precisa de los elementos de procedimientos definidos en la cláusula 6. Este anexo y la cláusula 6 tienen igual precedencia. Cualquier conflicto debe ser tratado como un error de la especificación.

Este anexo contiene los siguientes cuadros:

1) Cuadro 1 – Especifica el nombre abreviado, fuente, y nombre de cada evento de entrada. Las fuentes son:
   a) el usuario del servicio SEPM (usuario SE);
   b) la SEPM par (par SE).
2) Cuadro 2 – Especifica el nombre abreviado, objetivo, y nombre de cada evento de salida. Los objetivos son:
   a) el usuario del servicio SEPM (usuario SE);
   b) la SEPM par (par SE).
3) Cuadro 3 – Especifica los predicados utilizados.
4) Cuadro 4 – Especifica el nombre abreviado y la descripción de cada estado.
5) Cuadro 5 – Especifica la tabla de estados SEPM utilizando las abreviaturas de las tablas anteriores.

A.2 Convenios

La intersección de un evento de entrada (una fila en la tabla de estados) y un estado (columna en la tabla de estados) forma una celda.

En la tabla de estados, una celda en blanco representa la combinación de un evento de entrada y un estado que no está definido para la SEPM.

Una celda que no está en blanco representa un evento de entrada y un estado que está definido para la SEPM. Dicha celda debe contener una lista de acciones (obligatorias y/o condicionales).

A.3 Tablas

Cuadro 1 – Lista de eventos de entrada

Nombre abreviado	Fuente	Nombre
pet. SE-TRANFERENCIA	usuario SE	primitiva pet. SE-TRANSFERENCIA
SETR	SE par	APDU SE-TRANSFERENCIA
pet. SE-U-ABORTO	usuario SE	primitiva pet. SE-U-ABORTO
SEAB	SE par	APDU SE-U-ABORTO
SEPA	SE par	APDU SE-P-ABORTO
APDU no válida	SE par	APDU no válida

Cuadro 2 – Lista de eventos de salida

Nombre abreviado	Objetivo	Nombre
ind. SE-TRANFERENCIA	usuario SE	primitiva ind. SE-TRANSFERENCIA
SETR	SE par	APDU SE-TRANSFERENCIA
ind. SE-U-ABORTO	usuario SE	primitiva ind. SE-U-ABORTO
SEAB	SE par	APDU SE-U-ABORTO
SEPA	SE par	APDU SE-P-ABORTO
ind. SE-P-ABORTO	usuario SE	primitiva ind. SE-P-ABORTO

Cuadro 3 – Predicados

Código	Significado
p1	endFlag=Verdadero
p2	Problema de transferencia detectado
p3	Problema de aborto detectado

Cuadro 4 – Estados de la SEPM

Nombre abreviado	Descripción
STA0	Estado de reposo
STA1	Estado de intercambio

Cuadro 5 – Tabla de estados de la SEPM

	STA0 Estado de reposo	STA1 Estado de intercambio
pet. SE-TRANSFERENCIA	p1 SETR STA0 ^p1 SETR STA1	p1 SETR STA0 ^p1 SETR STA1
SETR	p2 ind. SE-P-ABORTO SEPA STA0 ^p2&p1 ind. SE-TRANSFERENCIA STA0 ^p2&^p1 ind. SE-TRANSFERENCIA STA1	p2 ind. SE-P-ABORTO SEPA STA0 ^p2&p1 ind. SE-TRANSFERENCIA STA0 ^p2&^p1 ind. SE-TRANSFERENCIA STA1
pet. SE-U-ABORTO		SEAB STA0
SEAB		p3 ind. SE-P-ABORTO SEPA STA0 ^p3 ind. SE-U-ABORTO STA0
SEPA	ind. SE-P-ABORTO STA0	ind. SE-P-ABORTO STA0
APDU no válida	ind. SE-P-ABORTO SEPA STA0	ind. SE-P-ABORTO SEPA STA0
NOTA – Todos los casos que no figuran en el Cuadro 5 se tratan como un asunto local de la SEPM.		

Anexo B

Definición del contexto de aplicación SESE básico

(Este anexo es parte integrante de esta Recomendación | Norma Internacional)

Este anexo define un contexto de aplicación que sólo contiene el ACSE y el SESE. Este contexto de aplicación se considera útil para aplicaciones de servidores de seguridad.

B.1 Nombre de contexto de aplicación

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

B.2 Elementos de servicio de aplicación

ACSE y SESE.

B.3 Correspondencias de las APDU del SESE

a) Las APDU SE-U-ABORTO y SE-P-ABORTO siempre producirán la terminación anormal de la asociación de aplicación subyacente y por tanto siempre corresponderán con el parámetro información de usuario de una primitiva de servicio A-ABORTO.

b) Para un intercambio de seguridad unidireccional, el iniciador hará corresponder la APDU SE-TRANSFERENCIA con el parámetro información de usuario de la primitiva de servicio petición A-ASOCIACIÓN. El respondedor:

- enviará una APDU de respuesta A-ASOCIACIÓN con el resultado «rechazado (transitorio)» indicando la compleción satisfactoria del intercambio sin tener que establecer una asociación; o bien
- en caso de error, abortará la asociación con una APDU SE-U-ABORTO o SE-P-ABORTO como se describe en 3.1. Cabe señalar que no es posible una colisión de procedimientos del servicio A-ABORTO porque el iniciador no emitirá una primitiva A-ABORTO en este caso.

c) Para todos los otros casos, el iniciador hará corresponder la APDU SE-TRANSFERENCIA con el parámetro información de usuario de la primitiva de servicio petición A-ASOCIACIÓN. El respondedor:

- enviará una APDU de respuesta A-ASOCIACIÓN con el campo información de usuario sea vacío (si el iniciador va a enviar el SEI siguiente), o (más usualmente) con una APDU SE-TRANSFERENCIA, y un resultado de «aceptado»; o bien
- en caso de error, empleará el mismo procedimiento indicado en 3.2 b).

Las APDU SE-TRANSFERENCIA restantes se hacen corresponder con P-DATOS; cabe señalar que el SESE es el único usuario del servicio P-DATOS.

Los errores se indican utilizando las APDU SE-U-ABORTO y SE-P-ABORTO como se indica en 3.1. Se debe señalar que algunos intercambios de seguridad pueden permitir que los SEI sean enviados asíncronamente (es decir, sin forzar una secuencia de alternación estricta). En tal circunstancia, se podría producir una colisión de procedimientos del servicio A-ABORTO, en cuyo caso las APDU SE-U-ABORTO o SE-P-ABORTO no serían entregadas a las entidades pares. No obstante, se hace saber a ambas entidades que la asociación ha sido liberada.

B.4 Constricciones de concatenación de valor de datos de protocolo (PDV)

No es aplicable; el SESE es el único usuario del servicio P-DATOS.

B.5 Constricciones de inserción de valor de datos de protocolo (PDV)

Como SESE es el único usuario del servicio P-DATOS los únicos PDV insertados en las APDU SESE son los resultantes de la utilización del tipo parametrizado PROTEGIDO (PROTECTED).

B.6 Constricciones de procedimiento

Ninguna, excepto las constricciones de procedimiento de ACSE.

B.7 Constricciones del contexto de presentación

Ninguna.

NOTA – Sería razonable restringir el contexto para las APDU del SESE a la BER, para simplificar la tarea del diseñador de programas. Por supuesto, se puede utilizar cualquier contexto dentro del PDV insertado producido por el tipo PROTEGIDO.