Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1279

(09/2020)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad en el ciberespacio – Gestión de identidades

Marco de autenticación mejorada mediante telebiometría con mecanismos de detección antisuplantación

Recomendación UIT-T X.1279

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–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	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad (1)	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	**X.1250–X.1279**
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistemas de transporte inteligente (ITS)	X.1370–X.1379
Seguridad de tecnología de libro mayor distribuido	X.1400–X.1429
Seguridad de tecnología de libro mayor distribuido	X.1430–X.1449
Protocolos de seguridad (2)	X.1450–X.1459
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699
COMUNICACIÓN CUÁNTICA	
Terminologías	X.1700–X.1701
Generador de números aleatorio cuántico	X.1702–X.1709
Marco de seguridad QKDN	X.1710–X.1711
Diseño de seguridad para QKDN	X.1712–X.1719
Técnicas de seguridad para QKDN	X.1720–X.1729
SEGURIDAD DE LOS DATOS	
Seguridad de los macrodatos	X.1750–X.1759
SEGURIDAD DE 5G	X.1800–X.1819

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1279

Marco de autenticación mejorada mediante telebiometría con mecanismos de detección antisuplantación

Resumen

En la Recomendación UIT-T X.1279 se describe un marco arquitectónico de autenticación mejorada mediante telebiometría con mecanismos de detección antisuplantación. Además, se analizan las amenazas a las soluciones tradicionales de autenticación telebiométrica y se especifican el marco arquitectónico, los flujos del proceso de autenticación y las consideraciones en materia de seguridad pertinentes para la autenticación mejorada mediante telebiometría con mecanismos de detección antisuplantación.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T X.1279	03-09-2020	17	11.1002/1000/14261

Palabras clave

Detección antisuplantación, autenticación mejorada, telebiometría.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

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.

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.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Página

1 Alcance 1
2 Referencias 1
3 Definiciones 1
3.1 Términos definidos en otros documentos 1
3.2 Términos definidos en esta Recomendación 2
4 Abreviaturas y acrónimos 3
5 Convenios 3
6 Amenazas a la seguridad de la autenticación telebiométrica y contramedidas 3
6.1 Antecedentes 3
6.2 Métodos de autenticación de referencia 3
6.3 Amenazas a la seguridad 3
6.4 Contramedidas 4
7 Marco arquitectónico 4
7.1 Diagrama arquitectónico 4
7.2 Funciones del lado del cliente 5
7.3 Funcionalidades del lado del servidor 6
8 Flujos del proceso de autenticación 7
8.1 Tipos de mensajes 7
8.2 Flujos de procesos 8
9 Directrices de seguridad 11
9.1 Seguridad del cliente 11
9.2 Seguridad del servidor 11
9.3 Seguridad del almacenamiento 11
9.4 Seguridad de la comunicación 12
9.5 Otras consideraciones en materia de seguridad 12
Apéndice I – Casos e hipótesis de uso 13
I.1 Estudio relativo a un caso de uso de servicios de pago a través del teléfono móvil 13
I.2 Estudio relativo a un caso de uso de servicios de comercio electrónico 13
Apéndice II – Contraseña distante segura 14
Apéndice III – Ejemplos del modo en que un servidor ejecuta la ASD en el marco del reconocimiento facial 15
Bibliografía 16

Introducción

A menudo, la tecnología de autenticación telebiométrica se utiliza en ámbitos que requieren un elevado nivel de fiabilidad, entre ellos, la banca electrónica y los servicios de compras. Es necesario impulsar el desarrollo de un sistema de seguridad que pueda utilizarse preventivamente contra potenciales amenazas a la seguridad, con objeto de garantizar la seguridad de los datos telebiométricos.

En la presente Recomendación se analizan las amenazas a las soluciones tradicionales de autenticación telebiométrica y se propone un marco de autenticación mejorada mediante telebiometría con mecanismos de detección antisuplantación. La detección antisuplantación permite determinar si el usuario que envía la solicitud de autenticación telebiométrica es la persona activa titular de los datos biométricos, y puede combinarse con técnicas de verificación telebiométrica, para mejorar la seguridad y evitar falsificaciones biométricas. La funcionalidad de detección antisuplantación puede diseñarse de tal manera que mejore la seguridad y evite la fuga de datos biométricos.

Recomendación UIT-T X.1279

Marco de autenticación mejorada mediante telebiometría con mecanismos de detección antisuplantación

1 Alcance

En la presente Recomendación se describe un marco arquitectónico de autenticación mejorada mediante telebiometría con mecanismos de detección antisuplantación. Además, se analizan las amenazas a las soluciones tradicionales de autenticación telebiométrica y se especifican el marco arquitectónico, los flujos del proceso de autenticación y las consideraciones en materia de seguridad pertinentes para la autenticación mejorada mediante telebiometría con mecanismos de detección antisuplantación.

El marco arquitectónico especificado en la presente Recomendación puede utilizarse a título orientativo con miras al despliegue de soluciones mejoradas de autenticación telebiométrica que utilicen funcionalidades de detección antisuplantación.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

[UIT-T X.1086] Recomendación UIT-T X.1086 (2008), *Procedimientos de protección telebiométrica – Parte 1: Guía sobre las medidas técnicas y de gestión para la protección de la seguridad de los datos biométricos*.

[UIT-T X.1087] Recomendación UIT-T X.1087 (2016), *Contramedidas técnicas y operativas para las aplicaciones telebiométricas en dispositivos móviles*.

[ISO/CEI 24745] ISO/CEI 24745:2011, *Information technology – Security techniques – Biometric information protection*.

3 Definiciones

3.1 Términos definidos en otros documentos

En la presente Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 autenticación [b-ISO/CEI 2382-37]: Acción de probar o demostrar el origen o la veracidad de algo de forma irrefutable.

3.1.2 biométrico (adjetivo) [b-ISO/CEI 2382]: Perteneciente al ámbito de la biometría.

3.1.3 captura biométrica [b-ISO/CEI 2382-37]: Obtención y registro, en un formato recuperable, de una o varias señales de una o varias características biométricas directamente del individuo o individuos o de la representación o representaciones de dichas características.

3.1.4 característica biométrica [b-ISO/CEI 2382-37]: Característica biológica y conductual de un individuo, de la que pueden extraerse rasgos biométricos distintivos y repetibles a efectos del reconocimiento biométrico.

3.1.5 datos biométricos [b-ISO/CEI 2382-37]: Muestra biométrica o suma de muestras biométricas en cualquier etapa de procesamiento, por ejemplo, referencias biométricas, sondas biométricas, rasgos biométricos o propiedades biométricas.

3.1.6 rasgo biométrico [b-ISO/CEI 2382-37]: Números o etiquetas extraídos de las muestras biométricas y utilizados para realizar comparaciones.

3.1.7 reconocimiento biométrico/biometría [b-ISO/CEI 2382-37]: Reconocimiento automático de individuos basado en sus características biológicas y conductuales.

3.1.8 base de datos de referencias biométricas [b-ISO/CEI 2382-37]: Base de datos de registros de datos de referencias biométricas.

3.1.9 plantilla biométrica [b-ISO/CEI 19784-1]: Conjunto de rasgos biométricos almacenados, que pueden compararse directamente con los rasgos biométricos de una muestra biométrica de reconocimiento.

3.1.10 verificación biométrica [b-ISO/CEI 2382-37]: Proceso de confirmación de una solicitud biométrica mediante comparación biométrica.

3.1.11 comparación (correspondencia) [b-ISO/CEI 19784-1]: Estimación, cálculo o medición de la similitud o disimilitud entre la muestra o muestras biométricas de reconocimiento y/o los rasgos biométricos y/o los modelos biométricos y la referencia o referencias biométricas.

3.1.12 decisión basada en la comparación [b-ISO/CEI 19784-1]: Determinación de si la muestra o muestras biométricas de reconocimiento y la referencia o referencias biométricas tienen el mismo origen biométrico, de acuerdo con un sistema de puntuación comparativa, una o varias políticas en materia de toma de decisiones con umbrales y, posiblemente, otras herramientas.

3.1.13 dispositivo móvil [b-ISO 18461]: Dispositivo informático portátil, que suele estar dotado de una pantalla de visualización táctil, un lápiz y/o un teclado, así como de conexión a Internet.

3.1.14 usuario [b-ISO/CEI 2382-37]: Toda persona u organización que interactúe de alguna manera con un sistema biométrico.

3.1.15 telebiometría [b-UIT-T X.1081]: Biometría aplicada a las telecomunicaciones.

3.2 Términos definidos en esta Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 detección antisuplantación: Proceso de detección y prevención de la suplantación de un sistema biométrico mediante acciones ilegítimas.

3.2.2 ofuscación: Acto deliberado de creación de un código fuente o un código de máquina difícil de interpretar para el ser humano. Esta técnica se basa en un conjunto de modificaciones, que cambian el funcionamiento aparente de un soporte lógico sin alterar sus resultados. Un soporte lógico ofuscado debería producir exactamente los mismos resultados que uno no ofuscado.

NOTA – La ofuscación es una técnica que suele utilizarse para encubrir el significado de algún tipo de soporte lógico reorganizando las operaciones; no obstante, también puede emplearse para añadir marcas de agua ligeras al código. En ambos casos, los algoritmos se basan en un conjunto de modificaciones, que cambian el funcionamiento aparente de un soporte lógico sin alterar sus resultados. Un soporte lógico ofuscado debería producir exactamente los mismos resultados que uno no ofuscado. [b-Disappearing Cryptography]

3.2.3 detección de calidad: Medida relativa a la idoneidad de una muestra biométrica para cumplir o aplicar una decisión basada en una comparación biométrica.

3.2.4 suplantación: Pretensión asumida por una entidad que afirma ser otra entidad diferente, mediante la presentación de una imagen grabada u otra muestra de datos biométricos, o una característica biométrica derivada artificialmente, a fin de hacerse pasar por un individuo.

NOTA – Definición adaptada de [b-UIT-T M.3016.0].

4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan las siguientes abreviaturas y acrónimos:

ASD detección antisuplantación (*anti-spoofing detection*)

PII información de identificación personal (*personally identifiable information*)

PKI infraestructura de clave pública (*public key infrastructure*)

SMS servicio de mensajes cortos (*short messaging service*)

SRP contraseña distante segura (*secure remote password*)

5 Convenios

Ninguno.

6 Amenazas a la seguridad de la autenticación telebiométrica y contramedidas

6.1 Antecedentes

A raíz de la aparición de los servicios de Internet, los mecanismos de autenticación basados en contraseñas tradicionales han dejado de satisfacer los requisitos en materia de experiencia de usuario y capacidades de seguridad. Actualmente, los mecanismos de autenticación telebiométrica se utilizan con mayor frecuencia por motivos de conveniencia y seguridad.

No obstante, los mecanismos de autenticación biométrica plantean problemas y riesgos. Por ejemplo, los atacantes pueden utilizar una fotografía, o una imagen generada por ordenador, o un rostro en la pantalla para la autenticación por reconocimiento facial, y los usuarios pueden utilizar una copia de una muestra telebiométrica (por ejemplo, huellas dactilares, iris o patrones de voz) para la autenticación telebiométrica.

6.2 Métodos de autenticación de referencia

A efectos de la autenticación telebiométrica en dispositivos móviles, existen dos métodos básicos de autenticación de referencia:

1) Método de autenticación local: los datos biométricos se almacenan en el dispositivo móvil y la verificación telebiométrica se realiza en el lado del dispositivo móvil. El resultado de la verificación telebiométrica se remite al lado del servidor.
2) Método de autenticación a distancia: los datos biométricos se almacenan en el servidor y la verificación telebiométrica se realiza en el lado del servidor.

Esta Recomendación se centra en el método de autenticación a distancia.

6.3 Amenazas a la seguridad

6.3.1 Amenazas a la seguridad en el lado del cliente

Cabe destacar las siguientes amenazas a la seguridad de la autenticación telebiométrica en el lado del cliente:

– El cliente es un agente falso o ha sido modificado con un código malicioso.
– Los atacantes tratan de alterar la disponibilidad e integridad del cliente.
– Los atacantes tratan de robar o modificar los datos biométricos capturados del cliente.
– Los atacantes pueden utilizar una fotografía, o una imagen generada por ordenador, o un rostro en la pantalla para la autenticación por reconocimiento facial.

– Los atacantes pueden utilizar una copia de los datos biométricos (por ejemplo, huellas dactilares, iris o patrones de voz) para la autenticación telebiométrica.

6.3.2 Amenazas a la seguridad en el lado del servidor

Cabe destacar las siguientes amenazas a la seguridad de la autenticación telebiométrica en el lado del servidor:

– Los atacantes pueden invadir el servidor, a fin de alterar su base de datos o su aplicación.

– Los datos biométricos capturados o los datos de las plantillas pueden ser sustituidos ilegalmente, o filtrados, como datos alterados o robados.

– Los datos biométricos capturados o los datos de las plantillas pueden ser alterados ilegalmente, en el momento de su transferencia.

– Se puede utilizar un programa de comparación ilegal.

6.3.3 Amenazas a la seguridad del canal de transmisión entre el cliente y el servidor

Cabe destacar las siguientes amenazas a la seguridad de la autenticación telebiométrica en el canal de transmisión entre el cliente y el servidor:

– Los atacantes pueden interceptar o modificar los mensajes entre el cliente y el servidor.

– Los datos biométricos pueden ser robados o modificados durante la transmisión del cliente al servidor.

6.4 Contramedidas

A fin de mitigar estas amenazas a la autenticación telebiométrica, suelen utilizarse técnicas de detección antisuplantación (ASD) y de verificación telebiométrica a efectos de autenticación.

La ASD debe aplicarse en un marco de autenticación telebiométrica. La funcionalidad de ASD puede utilizarse para determinar si el usuario que envía la solicitud de autenticación telebiométrica es la persona activa titular de los datos biométricos. Ello permite evitar que un usuario ilegal pueda utilizar datos biométricos falsos o copiados con miras a la autenticación telebiométrica.

La ASD puede combinarse con la verificación telebiométrica para mejorar la seguridad y evitar casos de falsificación biométrica. Por ejemplo, una aplicación móvil puede solicitar al usuario que asienta, mueva la cabeza, parpadee, abra la boca, etc., para comprobar que dicho usuario es la persona real que formuló la solicitud de autenticación.

En [UIT-T X.1086] y [UIT-T X.1087] se detallan amenazas a la seguridad y contramedidas adicionales.

7 Marco arquitectónico

7.1 Diagrama arquitectónico

La Figura 1 ilustra un diagrama arquitectónico de autenticación mejorada mediante telebiometría con mecanismos de ASD.

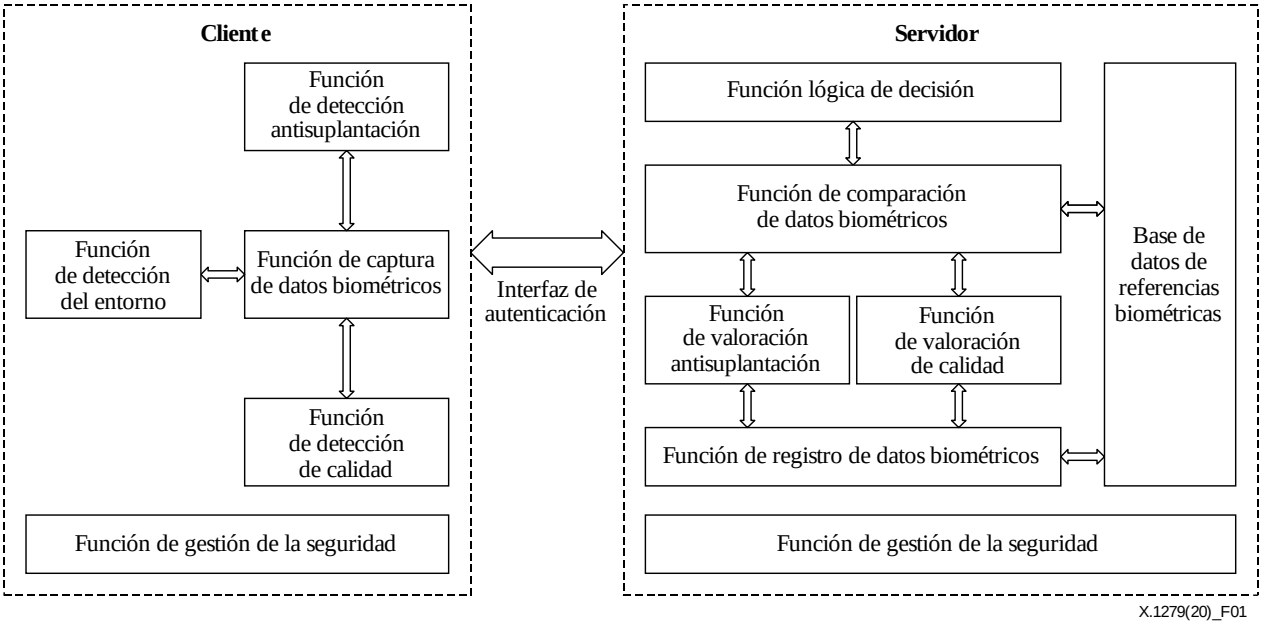

Figura 1 – Diagrama arquitectónico de autenticación mejorada mediante telebiometría con mecanismos de ASD

En las cláusulas 7.2 y 7.3 se detallan las funciones incluidas en este diagrama arquitectónico.

7.2 Funciones del lado del cliente

7.2.1 Función de detección del entorno

Esta función se utiliza para reconocer y detectar las características biométricas y las condiciones del entorno. En ese sentido, permite valorar si las características faciales satisfacen o no las condiciones de la recopilación, o si el entorno satisface o no las condiciones de la recopilación de datos.

7.2.2 Función de captura de datos biométricos

Esta función se utiliza para capturar los datos biométricos de los usuarios finales, enviarlos a una función de detección de calidad local y a una función de ASD para su procesamiento, y, a continuación, remitir los mismos datos biométricos al servidor a través de una interfaz de autenticación con miras a su autenticación a distancia.

7.2.3 Función de detección antisuplantación

Esta función se utiliza para detectar una serie de movimientos previstos conforme a las estrategias o políticas del servidor, como asentir, mover la cabeza, parpadear, abrir la boca, etc.

Aunque se pueden utilizar muchos métodos a efectos de la ASD, la detección de vida resulta mucho más adecuada para la autenticación telebiométrica en dispositivos móviles. Los protocolos de desafío-respuesta pueden utilizarse como instrumentos para determinar si la presentación de un sujeto posee alguna de las propiedades de un ser vivo previstas en el repertorio del subsistema de captura de datos biométricos. Por ejemplo, se espera que el iris de un individuo vivo responda a alteraciones de la iluminación con luz visible (desafío) mediante cambios en el tamaño de la pupila (respuesta esperada de un ser vivo).

La detección de vida puede llevarse a cabo en los siguientes pasos, que son similares a los incluidos en los procesos de reconocimiento biométrico:

– capturar datos en bruto para la ASD de un sujeto utilizando el subsistema de captura de datos biométricos;

– extraer rasgos de los datos de ASD;

– comparar los rasgos de ASD con los criterios.

7.2.4 Función de detección de calidad

Esta función se utiliza para valorar a título preliminar la calidad de los datos biométricos, con arreglo a las estrategias o políticas del servidor. La función de detección de calidad evalúa la calidad de los datos biométricos recopilados y extrae las características biométricas. Esta función suele combinarse con las funciones de ASD y de captura de datos biométricos, para obtener los mejores datos biométricos a afectos de la modelización y valoración de estos últimos.

7.2.5 Función de gestión de la seguridad

La función de gestión de la seguridad en el lado del cliente se utiliza para gestionar las credenciales, el entorno de confianza, etc.

7.3 Funcionalidades del lado del servidor

7.3.1 Función de registro de datos biométricos

Esta función se utiliza para gestionar el registro de datos biométricos. Los datos biométricos de este registro pueden obtenerse de un cliente, de un lote importado directamente o de otros canales, como una base de datos de identidad nacional. A tal efecto, puede utilizarse una plantilla de registro de datos biométricos.

7.3.2 Función de valoración antisuplantación

Esta función se utiliza para valorar si los datos biométricos son falsos o copiados. En este caso, el servidor procede a una valoración antisuplantación exhaustiva, basándose en los resultados de la detección preliminar del lado del cliente y en las estrategias y políticas del servidor.

El servidor puede indicar al cliente que realice los movimientos previstos conforme a las estrategias o políticas del servidor, como asentir, mover la cabeza, parpadear, abrir la boca, etc. El servidor recibe del cliente una serie de datos biométricos característicos extraídos y utiliza su referencia biométrica y su estrategia predefinida para valorar si la presentación del sujeto posee alguna de las propiedades de un ser vivo.

7.3.3 Función de valoración de calidad

Esta función se utiliza para valorar la calidad de los datos biométricos a partir de los resultados de la detección preliminar del lado del cliente y de las estrategias y políticas del servidor. La función de valoración de calidad permite evaluar la calidad de los datos biométricos recibidos. Si la calidad no alcanza el umbral establecido, el servidor rechaza los datos biométricos recibidos y solicita al cliente que vuelva a capturarlos. Si la calidad alcanza el umbral establecido, los datos biométricos se remiten a la función de comparación de datos biométricos para que los compare.

La capacidad de captura de datos biométricos puede variar en función del tipo de dispositivo. Además, la calidad de los datos biométricos también puede ser mejor en unos dispositivos que en otros. El servidor puede solicitar al usuario que utilice varios dispositivos para capturar los datos biométricos, a fin de mejorar la calidad. Si la referencia biométrica se capturase con diferentes tipos de dispositivos, el servidor debería almacenar y utilizar las diferentes referencias biométricas para los diferentes tipos de dispositivos.

7.3.4 Función de comparación de datos biométricos

Esta función se utiliza para realizar comparaciones y verificaciones entre los rasgos biométricos extraídos de un cliente y los de las referencias biométricas almacenadas en el lado del servidor. Las referencias biométricas almacenadas en una base de datos de referencias biométricas se generan a partir del proceso de registro de datos biométricos.

7.3.5 Función de lógica de decisión

Esta función comprende estructuras lógicas de decisión que permiten llevar a cabo diferentes procesos de autenticación y enviar al cliente las instrucciones correspondientes para ejecutar los distintos procesos de autenticación. Las decisiones se toman de acuerdo con los datos existentes en materia de gestión de riesgos, incluida la información relativa al *software* y al *hardware* del dispositivo móvil y al perfil del usuario. Por ejemplo, si, con arreglo al análisis de los datos, el usuario final se considera de alto riesgo, esta función puede solicitar al cliente que ejecute la ASD, además de la captura y comparación biométricas básicas.

7.3.6 Base de datos de referencias biométricas

La base de datos de referencias biométricas se utiliza para almacenar datos biométricos, datos en materia de gestión de riesgos, nombres de usuario, identidades, etc.

7.3.7 Función de gestión de la seguridad

Esta función se utiliza para garantizar la seguridad en la ejecución de las funcionalidades del servidor y en el almacenamiento de la base de datos de referencias biométricas, con objeto de evitar la manipulación o el robo de los datos biométricos o de las plantillas.

8 Flujos del proceso de autenticación

8.1 Tipos de mensajes

La pila de protocolo de autenticación telebiométrica en dispositivos móviles comprende un mínimo de tres tipos de mensajes para diferentes etapas:

– registro: un servidor inscribe la información de registro de un usuario y el tipo de autenticación correspondiente, conforme a lo negociado por el usuario y el servidor;

– autenticación: un servidor compara los datos biométricos recibidos con una referencia biométrica registrada;

– cancelación de registro: un usuario cancela su registro en un servidor. El servidor elimina los datos de registro del usuario.

NOTA – La presente Recomendación se centra en la verificación a distancia. En este caso, el cliente registra una referencia biométrica en el servidor. Una vez recibida la solicitud de verificación, el servidor compara los datos biométricos recibidos con la referencia biométrica registrada.

8.2 Flujos de procesos

8.2.1 Flujos del proceso de registro

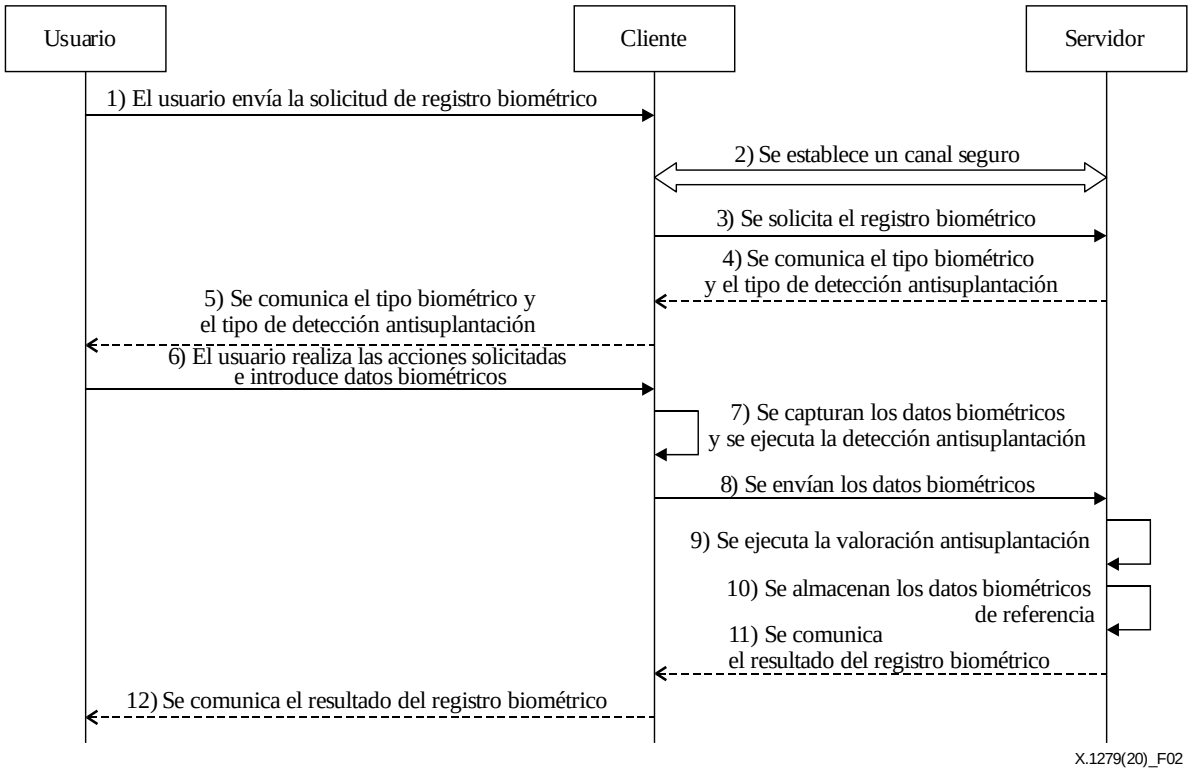

Figura 2 – Flujos del proceso de registro

La Figura 2 ilustra los flujos del proceso de registro, los cuales se detallan a continuación.

Condición previa: el usuario se autentica de forma satisfactoria ante el servidor, a través de mecanismos de autenticación tales como identificadores/contraseñas de cuenta de usuario y códigos de verificación del servicio de mensajes cortos (SMS).

1) El usuario utiliza el identificador/contraseña de la cuenta para iniciar la sesión y envía la solicitud de registro biométrico al cliente.
2) El cliente establece un canal seguro con el servidor para proteger la sesión y la transmisión de datos, por ejemplo, aplicando el protocolo de contraseña distante segura (SRP).
3) El cliente envía al servidor la solicitud de registro biométrico, junto con el identificador de la cuenta de usuario y los datos en materia de gestión de riesgos.
4) En el lado del servidor, la función de lógica de decisión remite al cliente el tipo biométrico y el tipo de ASD correctos, de acuerdo con un análisis de los datos de gestión de riesgos y la lógica comercial.
5) El cliente solicita al usuario que realice una serie de acciones determinadas para capturar datos biométricos.
6) El usuario realiza las acciones solicitadas e introduce los datos biométricos del cliente.
7) En el lado del cliente, la función de captura de datos biométricos captura los datos biométricos correspondientes y la función ASD detecta los movimientos previstos del usuario.
8) El cliente extrae los rasgos biométricos y se los envía al servidor en calidad de referencia biométrica a través del canal seguro establecido.

9) El servidor vincula los datos biométricos con el identificador de la cuenta de usuario y ejecuta la ASD.

10) El servidor almacena la referencia biométrica recibida en la base de datos de referencias biométricas.

11) El servidor comunica el resultado del registro biométrico al cliente.

12) El cliente informa al usuario del resultado del registro biométrico.

8.2.2 Flujos del proceso de autenticación

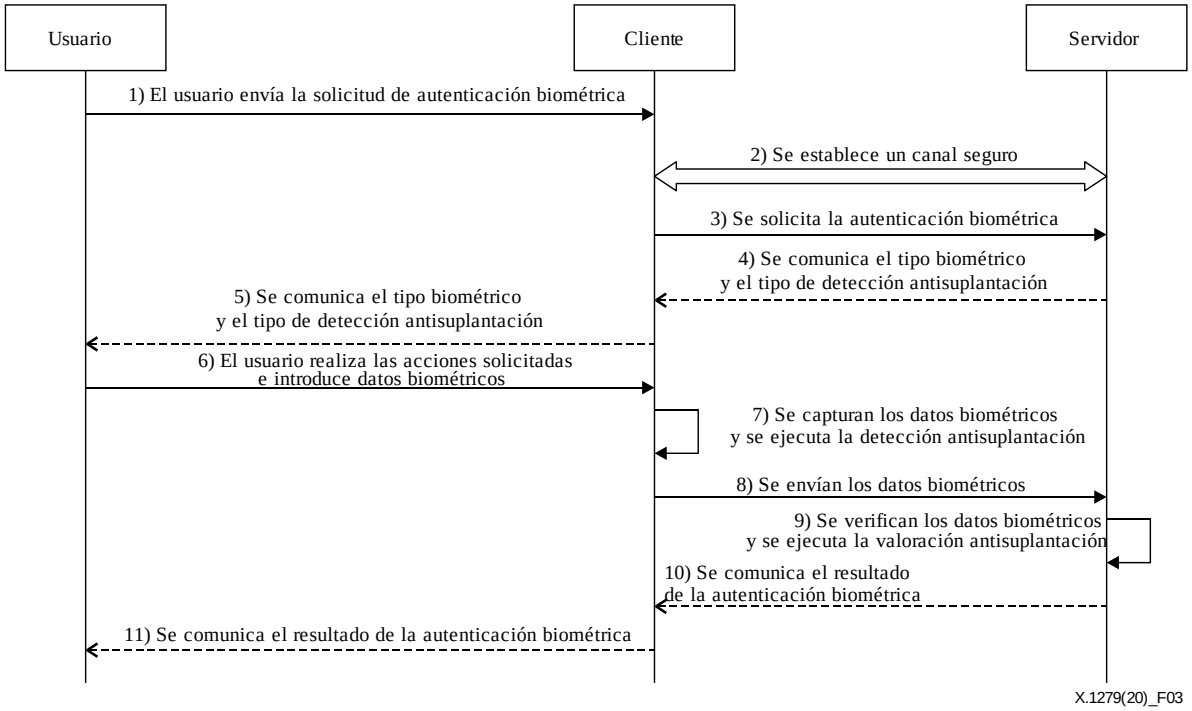

Figura 3 – Flujos del proceso de autenticación

La Figura 3 ilustra los flujos del proceso de autenticación, los cuales se detallan a continuación.

1) El usuario envía la solicitud de autenticación biométrica al cliente, junto con el identificador de la cuenta de usuario.

2) El cliente establece un canal seguro con el servidor para proteger la sesión y la transmisión de datos, por ejemplo, aplicando el protocolo de contraseña distante segura (SRP).

3) El cliente envía al servidor la solicitud de autenticación biométrica, junto con el identificador de la cuenta de usuario y los datos en materia de gestión de riesgos.

4) En el lado del servidor, la función de lógica de decisión remite al cliente el tipo biométrico y el tipo de ASD correctos, de acuerdo con un análisis de los datos de gestión de riesgos y la lógica comercial.

5) El cliente solicita al usuario que realice una serie de acciones determinadas para capturar datos biométricos.

6) El usuario realiza las acciones solicitadas e introduce los datos biométricos del cliente.

7) En el lado del cliente, la función de captura de datos biométricos captura los datos biométricos correspondientes y la función ASD detecta los movimientos previstos del usuario.

8) El cliente envía los datos de los rasgos biométricos extraídos al servidor a través del canal seguro establecido.

9) El servidor verifica los datos biométricos utilizando los rasgos biométricos extraídos y las referencias biométricas almacenadas, y ejecuta la función de ASD.

10) El servidor comunica el resultado de la autenticación biométrica al cliente.

11) El cliente informa al usuario del resultado de la autenticación biométrica.

8.2.3 Flujos del proceso de cancelación de registro

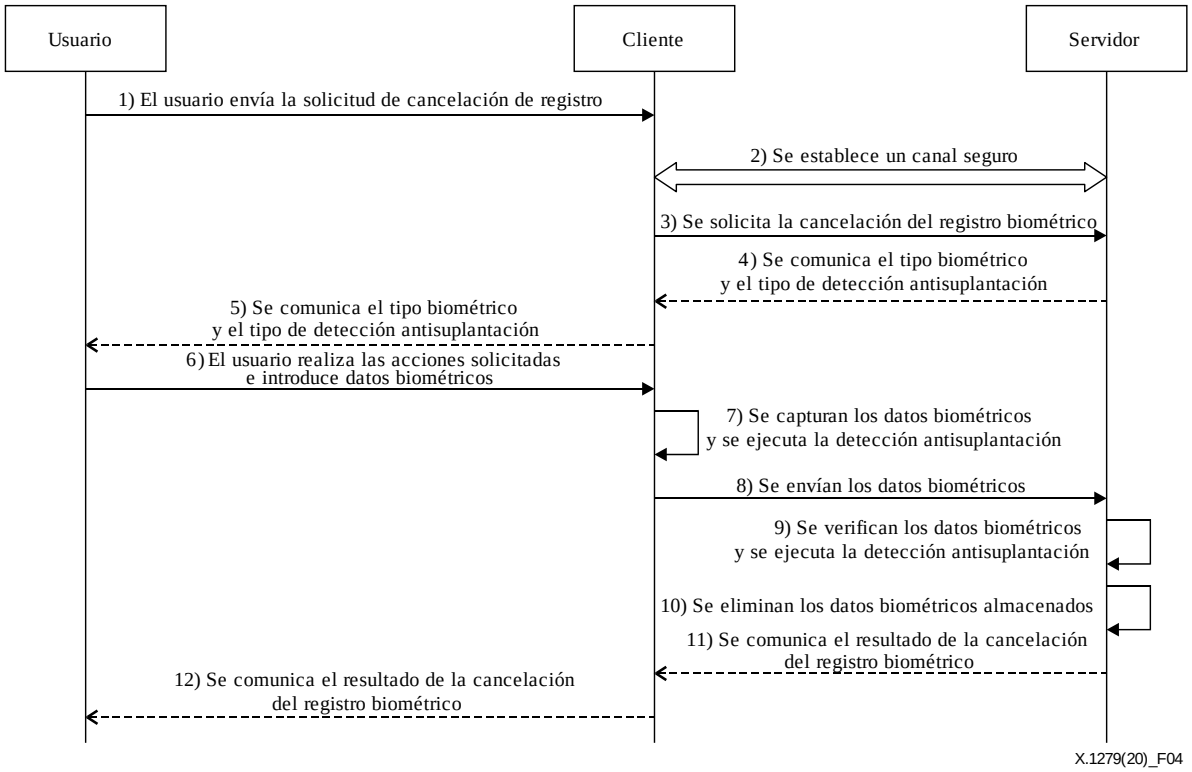

Figura 4 – Flujos del proceso de cancelación de registro

La Figura 4 ilustra los flujos del proceso de cancelación del registro, los cuales se detallan a continuación.

Condición previa: el usuario se autentica de forma satisfactoria ante el servidor, a través de mecanismos de autenticación tales como identificadores/contraseñas de cuenta de usuario y códigos de verificación SMS.

1) El usuario utiliza el identificador/contraseña de la cuenta para iniciar la sesión y envía la solicitud de cancelación del registro biométrico al cliente.

2) El cliente establece un canal seguro con el servidor para proteger la sesión y la transmisión de datos, por ejemplo, aplicando el protocolo SRP.

3) El cliente envía al servidor la solicitud de cancelación del registro biométrico, junto con el identificador de la cuenta de usuario y los datos en materia de gestión de riesgos.

4) En el lado del servidor, la función de lógica de decisión remite al cliente el tipo biométrico y el tipo de ASD correctos, de acuerdo con un análisis de los datos de gestión de riesgos y la lógica comercial.

5) El cliente solicita al usuario que realice una serie de acciones determinadas para capturar datos biométricos.

6) El usuario realiza las acciones solicitadas e introduce los datos biométricos del cliente.

7) En el lado del cliente, la función de captura de datos biométricos captura los datos biométricos correspondientes y la función ASD detecta los movimientos previstos del usuario.

8) El cliente envía los datos de los rasgos biométricos extraídos al servidor a través del canal seguro establecido.

9) El servidor verifica los datos biométricos utilizando los rasgos biométricos extraídos y las referencias biométricas almacenadas, y ejecuta la función de ASD.

10 El servidor elimina la referencia biométrica del usuario de la base de datos de referencias biométricas.

11) El servidor comunica el resultado de la cancelación del registro biométrico al cliente.

12) El cliente informa al usuario del resultado de la cancelación del registro biométrico.

9 Directrices de seguridad

9.1 Seguridad del cliente

El sistema operativo del dispositivo móvil debería actualizarse de forma oportuna con la última versión segura.

El cliente debería identificarse, con miras a determinar su fuente.

El cliente debería gozar de protección contra modificaciones o actualizaciones no autorizadas.

La protección de códigos y datos debe mejorarse, con objeto de evitar procesos de ingeniería inversa en el lado del cliente, en especial de ofuscación.

La adquisición de datos en el lado del cliente debería realizarse en un entorno de confianza, para garantizar la confidencialidad e integridad de los datos recopilados.

9.2 Seguridad del servidor

Se debería aplicar una política estricta de control del acceso en el servidor, en el que cualquier operación debería ser autenticada y autorizada primero.

El servidor debería tener la capacidad de determinar la identidad del cliente.

La comunicación entre el servidor y el cliente debería protegerse contra ataques de reproducción, por ejemplo, mediante el uso de datos dinámicos en los mensajes, tales como mensajes aleatorios (nonce), desafíos o marcas de tiempo.

Deberían mantenerse registros de las operaciones efectuadas en el lado del servidor, cuya integridad cabría proteger.

9.3 Seguridad del almacenamiento

Los certificados y las claves privadas de la Recomendación UIT-T X.509 deberían almacenarse de forma segura y someterse a una estricta política de control de acceso.

Las claves privadas deberían almacenarse en calidad de texto cifrado y el algoritmo de cifrado debería alcanzar un alto nivel de seguridad para evitar la piratería.

Los datos biométricos almacenados en el servidor deberían cifrarse y el algoritmo de cifrado debería alcanzar un alto nivel de seguridad para evitar la piratería.

Los datos biométricos almacenados en el servidor deberían integrar un rasgo biométrico extraído, sin posibilidad de restauración a los datos originales.

Las demás consideraciones relacionadas con la seguridad del almacenamiento deberían conformarse a lo estipulado en la norma [ISO/CEI 24745].

9.4 Seguridad de la comunicación

Antes de que el cliente y el servidor puedan comunicarse, debería establecerse un canal seguro; por ejemplo, https es adecuado a efectos de la seguridad de la comunicación.

Debería proporcionarse un mecanismo de intercambio seguro de claves en el marco de la autenticación entre el cliente y el servidor; por ejemplo, el protocolo SRP puede utilizarse como mecanismo de intercambio seguro de claves.

Debería impedirse la intercepción de la clave utilizada para negociar el canal seguro; por ejemplo, el protocolo SRP puede utilizarse para negociar el canal seguro sin transporte de claves.

La información, en especial los datos biométricos procesados y el resultado del componente de decisión, debería codificarse antes de su transmisión, y su integridad debería verificarse mediante una función unidireccional, como una función hash o una infraestructura de clave pública (PKI), que prohíbe toda alteración de los datos durante la transmisión.

Los datos biométricos procesados deberían desensibilizarse y cifrarse antes de su transmisión, y la clave de cifrado debería variar en función del cliente. El servidor utiliza la clave de desencriptación coincidente para desencriptar la información.

Las demás consideraciones relacionadas con la seguridad de la comunicación deberían conformarse a lo estipulado en la norma [ISO/CEI 24745].

9.5 Otras consideraciones en materia de seguridad

Además de la seguridad del almacenamiento y de la comunicación, existen numerosos aspectos adicionales que es preciso tener en cuenta, entre ellos la seguridad del procesamiento, la protección de la información de identificación personal (PII), etc. Las demás consideraciones relacionadas con las técnicas de seguridad para la protección de la información biométrica deberían conformarse a lo estipulado en la norma [ISO/CEI 24745].

Apéndice I

Casos e hipótesis de uso

(Este Apéndice no forma parte integrante de la presente Recomendación.)

I.1 Estudio relativo a un caso de uso de servicios de pago a través del teléfono móvil

Alice es una usuaria que utiliza una aplicación llamada "mobile wallet" para realizar pagos a través del teléfono móvil. Este caso procede como sigue:

1) La primera vez que utiliza la aplicación "mobile wallet", Alice introduce su nombre de usuario y su contraseña para iniciar sesión. Por un lado, no quiere tener que introducir su contraseña cada vez que realice un pago y, por otro, tiene miedo de olvidarla, así que activa la opción de registro de pago con verificación facial en dicha aplicación.
2) La aplicación "mobile wallet" solicita a Alice que abra la aplicación de la cámara y asienta con la cabeza.
3) Alice recibe una notificación de "mobile wallet", según la cual el registro se ha llevado a cabo con éxito.
4) Alice pide una taza de café en la cafetería Starbucks y utiliza la aplicación "mobile wallet" para pagar. Alice abre la aplicación y se dispone a realizar el pago. La aplicación móvil le solicita que abra la aplicación de la cámara y asienta con la cabeza. Alice considera la experiencia bastante satisfactoria.
5) Alice recibe una notificación de la aplicación "mobile wallet", según la cual el pago se ha realizado con éxito.
6) Transcurrido un tiempo, Alice ya no quiere usar esa función y desactiva la opción correspondiente a ese método de pago.

I.2 Estudio relativo a un caso de uso de servicios de comercio electrónico

Bob es dueño de una tienda de ropa y quiere abrir una tienda *online* en una plataforma de comercio electrónico. Este caso procede como sigue:

1) La primera vez que utiliza la plataforma de comercio electrónico, Bob se registra y solicita abrir una nueva tienda. Bob determina su nombre de usuario y su contraseña en dicha plataforma desde una aplicación de comercio electrónico instalada en su dispositivo móvil.
2) La aplicación de comercio electrónico del dispositivo móvil de Bob le solicita que abra la aplicación de la cámara y realice una secuencia de acciones, por ejemplo, que abra la boca, mueva la cabeza, parpadee y asienta.
3) Bob recibe una notificación de la aplicación de comercio electrónico, según la cual el registro se ha llevado a cabo con éxito.
4) Transcurrido un tiempo, Bob quiere publicar algunas prendas de su tienda. La plataforma de comercio electrónico le pide que abra la aplicación de la cámara y realice una secuencia de acciones, por ejemplo, que mueva la cabeza, parpadee, abra la boca y asienta.
5) Bob recibe una notificación de la plataforma de comercio electrónico, según la cual se ha conectado con éxito.
6) Un tiempo después, Bob no quiere volver a utilizar esa función y desactiva la opción correspondiente a ese método de autenticación.

Apéndice II

Contraseña distante segura

(Este Apéndice no forma parte integrante de la presente Recomendación.)

Una contraseña distante segura (SRP) es un protocolo de autenticación de identidad e intercambio de claves basado en contraseñas. La ventaja de las SRP es que el texto sin cifrar de las claves no se transfiere en el proceso de autenticación; los usuarios sólo tienen que conservar las contraseñas. Además, el servidor no almacena las contraseñas de los usuarios, pero sí la información pertinente. Aun cuando el servidor cae en manos de un atacante, este último no puede hacerse pasar por un cliente legítimo (ya que no puede obtener la contraseña necesaria).

Los detalles del protocolo SRP pueden consultarse en [b-RFC 2945].

El protocolo SRP puede utilizarse para establecer canales seguros entre el cliente y el servidor en el marco de los procesos de registro biométrico, autenticación biométrica y cancelación del registro biométrico. El protocolo SRP puede utilizarse para negociar conexiones seguras utilizando una contraseña definida por el usuario y eliminando al mismo tiempo los problemas de seguridad que suelen asociarse a las contraseñas reutilizables. El protocolo SRP también puede utilizarse para realizar un intercambio seguro de claves en el proceso de autenticación, lo que permite habilitar capas de seguridad (protección de la privacidad y/o la integridad) durante la sesión.

Apéndice III

Ejemplos del modo en que un servidor ejecuta la ASD en el marco del reconocimiento facial

(Este Apéndice no forma parte integrante de la presente Recomendación.)

Entre los ejemplos del modo en que un servidor ejecuta la ASD en el marco del reconocimiento facial figuran, entre otros, los siguientes:

1) Siguiendo ciertos consejos o instrucciones del servidor, el usuario puede realizar una acción específica, que el servidor detecta a partir de la imagen facial.
2) El servidor debería tener la capacidad de detectar el ángulo de la cara y de la cámara, así como el cuerpo del individuo vivo mediante el cambio del ángulo facial en el marco de este proceso.
3) El servidor debería tener la capacidad de detectar la continuidad de la acción facial y evitar tanto el juego de diapositivas como el cambio de personas en el marco de este proceso.
4) El servidor debería tener la capacidad de detectar la repetición de vídeos de acción facial.
5) El servidor debería tener la capacidad de prevenir ataques basados en imágenes faciales.
6) El servidor debería tener la capacidad de detectar el uso de modelos faciales en 3D, producidos mediante tecnología gráfica por ordenador.

Bibliografía

[b-UIT-T M.3016.0] Recomendación UIT-T M.3016.0 (2005), *Seguridad en el plano de gestión: Visión general*.

[b-UIT-T X.509] Recomendación UIT-T X.509 (2019), *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos*.

[b-UIT-T X.1081] Recomendación UIT-T X.1081 (2011), *El modelo telebiométrico multimodal – Marco para la especificación de los aspectos de la telebiometría relativos a protección y seguridad*.

[b-UIT-T X.1085] Recomendación UIT-T X.1085 (2016) | ISO/IEC 17922:2017, *Tecnología de la información – Técnicas de seguridad – Marco de autentificación telebiométrica mediante un módulo de seguridad de hardware biométrico*.

[b-UIT-T X.1089] Recomendación UIT-T X.1089 (2008), *Infraestructura de autenticación telebiométrica*.

[b-UIT-T X.1252] Recomendación UIT-T X.1252 (2010), *Términos y definiciones sobre gestión de identidad de referencia*.

[b-UIT-T X.1254] Recomendación UIT-T X.1254 (2012), *Marco de garantía de autentificación de entidad*.

[b-ISO 18461] ISO 18461:2016, *International museum statistics*.

[b- ISO/CEI 19784-1] ISO/CEI 19784-1:2018, *Information technology –Biometric application programming interface – Part 1: BioAPI specification*.

[b-ISO/CEI 19792] ISO/CEI 19792:2009, *Security evaluation of biometrics*.

[b-ISO/CEI 19989] ISO/CEI 19989, *Evaluation of presentation attack detection for biometrics*.

[b-ISO/CEI 2382] ISO/CEI 2382:2015, *Information technology – Vocabulary*.

[b-ISO/CEI 2382-37] ISO/CEI 2382-37:2017, *Information technology – Vocabulary – Part 37: Biometrics*.

[b-ISO/CEI 24761] ISO/CEI 24761:2009, *Information technology – Security techniques – Authentication context for biometrics*.

[b-ISO/CEI 30107] ISO/CEI 30107:2017, *Information technology – Biometric presentation attack detection*.

[b-ISO/CEI 30125] ISO/CEI 30125:2016, *Biometrics – Biometrics used with mobile devices*.

[b-RFC 2945] RFC 2945, *The SRP Authentication and Key Exchange System*.

[b-Disappearing Cryptography] Disappearing Cryptography (tercera edición), 2009, páginas 355-364.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2021