ITUPublications
Recomendaciones

Unión Internacional de Telecomunicaciones
Sector de la Normalización

Recomendación

UIT-T X.1280 (03/2024)

SERIE X: Redes de datos, comunicaciones de sistemas abiertos y seguridad

Seguridad en el ciberespacio – Gestión de identidades y autentificación

Marco para la autentificación de servidores fuera de banda mediante dispositivos móviles

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	X.1000-X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (I)	X.1100-X.1199
SEGURIDAD EN EL CIBERESPACIO	X.1200-X.1299
Ciberseguridad	X.1200-X.1229
Lucha contra el correo basura	X.1230-X.1249
Gestión de identidades y autentificación	**X.1250-X.1299**
APLICACIONES Y SERVICIOS CON SEGURIDAD (II)	X.1300-X.1499
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	X.1500-X.1599
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	X.1600-X.1699
COMUNICACIÓN CUÁNTICA	X.1700-X.1729
SEGURIDAD DE LOS DATOS	X.1750-X.1799
SEGURIDAD DE LAS TELECOMUNICACIONES MÓVILES INTERNACIONALES (IMT)	X.1800-X.1839
SEGURIDAD DEL METAVERSO Y DE LOS GEMELOS DIGITALES	X.2000-X.2199
SEGURIDAD DE LA CADENA DE SUMINISTRO DE SOFTWARE	X.2150-X.2199
SEGURIDAD DE LA INTELIGENCIA ARTIFICIAL / APRENDIZAJE AUTOMÁTICO	X.2200-X.2249

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

Recomendación UIT-T X.1280

Marco para la autentificación de servidores fuera de banda mediante dispositivos móviles

Resumen

En las normas de las tecnologías de autentificación, la resistencia a la suplantación del verificador se considera como un requisito del más alto nivel en lo que respecta a la garantía de autentificación. Sin embargo, las tecnologías de autentificación existentes se centran en la autentificación de los usuarios, y se produce en consecuencia una limitación pues no es posible verificar a los proveedores de servicio de manera explícita.

En la Recomendación UIT-T X.1280 se proporciona un marco para la autentificación de servidores fuera de banda mediante dispositivos móviles, lo que soluciona la vulnerabilidad frente a la suplantación del verificador y la limitación de la dependencia que tienen los autentificadores existentes de los terminales de usuario. Permite a un usuario proporcionar su información de autentificación de usuario después de verificar el proveedor de servicio, de manera explícita e independiente, en el proceso de autentificación de usuario desde cualquier terminal de usuario.

Historia[*]

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único
1.0	UIT-T X.1280	01-03-2024	17	11.1002/1000/15661

Palabras clave

Autentificación, autentificador, parte que confía, verificación, verificador, resistencia a la suplantación del verificador.

[*] Para acceder a la Recomendación, sírvase digitar el URL https://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación.

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 se pronuncia en lo que respecta a la existencia, validez o aplicabilidad de los derechos de propiedad intelectual reclamados, 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 patentes/derechos de autor de *software*, 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 las correspondientes bases de datos del UIT-T disponibles en el sitio web del UIT-T en http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1280

Marco para la autentificación de servidores fuera de banda mediante dispositivos móviles

1 Alcance

En esta Recomendación se proporciona un marco para la autentificación de servidores fuera de banda mediante dispositivos móviles, que incluye los siguientes aspectos:

- define el modelo y el procedimiento de autentificación de servidores fuera de banda;
- define criterios y directrices para la generación de la información de autentificación de servidores mediante dispositivos móviles;
- define las amenazas de seguridad y los requisitos de seguridad en el modelo de autentificación de servidores fuera de banda;
- describe casos de utilización del modelo de autentificación de servidores fuera de banda; y
- describe la relación con otras tecnologías de autentificación.

En esta Recomendación no se abordan cuestiones relacionadas con la autentificación de usuario, la reglamentación y los aspectos de privacidad.

2 Referencias

Las siguientes Recomendaciones UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. En el momento de la publicación, las ediciones indicadas eran válidas. 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 la edición más reciente de las Recomendaciones y las otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T vigentes. La referencia a un documento en esta Recomendación no le otorga, como documento autónomo, el rango de Recomendación.

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos.

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

3.1.1 autentificación [b-ISO/CEI 18014-2]: Acción de garantizar la identidad declarada por una entidad.

3.1.2 proveedor de servicios de credenciales (CSP) [b-UIT-T X.1254]: Actor de confianza, o fiable, que expide o gestiona credenciales.

3.1.3 parte que confía (RP) [b-UIT-T X.1254]: Actor que confía en el aserto o declaración de una identidad.

3.1.4 verificación [b-ISO/CEI 29115]: Proceso de verificación de la información comparando la información proporcionada con información corroborada previamente.

3.1.5 verificador [b-ISO/IEC 29115]: Actor que corrobora la información de identidad.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los términos siguientes:

3.2.1 autentificación de servidor: Proceso de verificación de la autenticidad del proveedor de servicios mediante la comparación de las informaciones de autentificación de servidor generadas por el verificador y por el autentificador del servidor fuera de banda de un usuario.

3.2.2 información de autentificación de servidor: Código de autentificación que se genera utilizando un algoritmo de contraseña de un solo uso (OTP) con prueba y respuesta en el verificador, y un autentificador de servidor fuera de banda de usuario.

3.2.3 autentificación de usuario fuera de banda: Proceso de verificación de la autenticidad de un usuario mediante otro canal de conmutación separado del canal de comunicación utilizado para iniciar una sesión o realizar una transacción.

3.2.4 autentificación de servidor fuera de banda: Proceso de verificación de la autenticidad de un servidor mediante otro canal de conmutación separado del canal de comunicación utilizado para iniciar una sesión o realizar una transacción.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

ATM Cajero automático (*automated teller machine*)

CSP Proveedor de servicio de credenciales (*credential service provider*)

CTAP Protocolo de cliente a autentificador (*client to authenticator protocol*)

DNS Sistema de nombres de dominio (*domain name system*)

FIDO Identidad rápida en línea (*fast identity online*)

IA Inteligencia artificial

ID Identificación

IdP Proveedor de identidad (*identity provider*)

IP Protocolo de Internet

OAuth Autentificación abierta (*open authentication*)

OTP Contraseña de un solo uso (*one-time password*)

PAM Módulos de autentificación conectables (*pluggable authentication modules*)

PIN Número de identificación personal (*personal identification number*)

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

RP Parte que confía (*relying party*)

SAML Lenguaje de marcación de asertos de seguridad (*security assertion markup language*)

SMS Servicio de mensajes cortos (*short message service*)

SSL Capa de zócalo seguro (*secure socket layer*)

QR Respuesta rápida (*quick response*)

U2F Universal de dos factores (*universal two factor*)

5 Convenciones

En esta Recomendación se aplican las siguientes formas verbales para la expresión de disposiciones:

a) "Deberá" indica un requisito.

b) "Debería" indica una recomendación.

c) "Podría" significa que se da permiso.

d) "Puede" indica una posibilidad o una capacidad.

6 Introducción

En las autentificaciones de usuario tradicionales, solo el servidor autentifica al usuario y el usuario es vulnerable a ciberataques como la suplantación de identidad o la redirección fraudulenta.

La autentificación de servidores basada en infraestructura de clave pública (PKI) es adecuada para el usuario cuando utiliza aplicaciones basadas en navegadores con barra de direcciones. La autentificación basada en PKI también se realiza independientemente del proceso de autentificación del usuario, lo que hace que el usuario sea fácilmente pasado por alto.

Esta Recomendación proporciona un marco para la autentificación de servidores fuera de banda mediante dispositivos móviles, diseñado para que el usuario autentifique primero el servidor y para hacer que el usuario participe en la autentificación de servidores de manera explícita, como parte del proceso de autentificación de usuario. En la autentificación de usuario, todos los procesos de autentificación de usuario pueden aplicarse conjuntamente.

La autentificación de servidores fuera de banda puede utilizarse con las aplicaciones basadas en navegador y muchos tipos de aplicaciones y sistemas operativos.

La autentificación de un servidor fuera de banda se realiza mediante la verificación por el usuario de la información de autentificación de servidor y, a continuación, la verificación de la información de autentificación del usuario por parte del servidor, proporcionando así la resistencia a la suplantación del verificador.

Con la autentificación de servidores fuera de banda, los proveedores de servicio y los usuarios consiguen las ventajas siguientes:

1) Autentificación centrada en el usuario: en lugar de pedirle al usuario que recuerde e introduzca una compleja información de autentificación de usuario, el servidor presenta su información de autentificación para que el usuario autentifique el servidor. Los usuarios están libres de la carga de administrar las credenciales de usuario al cambiar su función de ingresar la información de autentificación de usuario a verificar la información de autentificación de servidor. La Figura 1 muestra la autentificación centrada en el usuario.

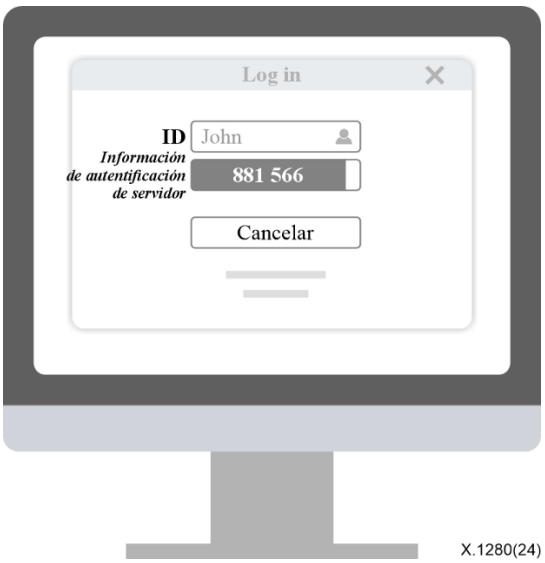

Figura 1 – Autentificación centrada en el usuario

2) Autentificación mutua: El usuario verifica la autenticidad del servidor con las informaciones de autentificación del servidor generadas por el servidor y por el autentificador de servidor fuera de banda, respectivamente. El servidor verifica la autenticidad del usuario con la información de autentificación del usuario enviada después de que el usuario ha confirmado que hay concordancia entre las dos informaciones de autentificación del servidor. La figura 2 muestra la autentificación mutua.

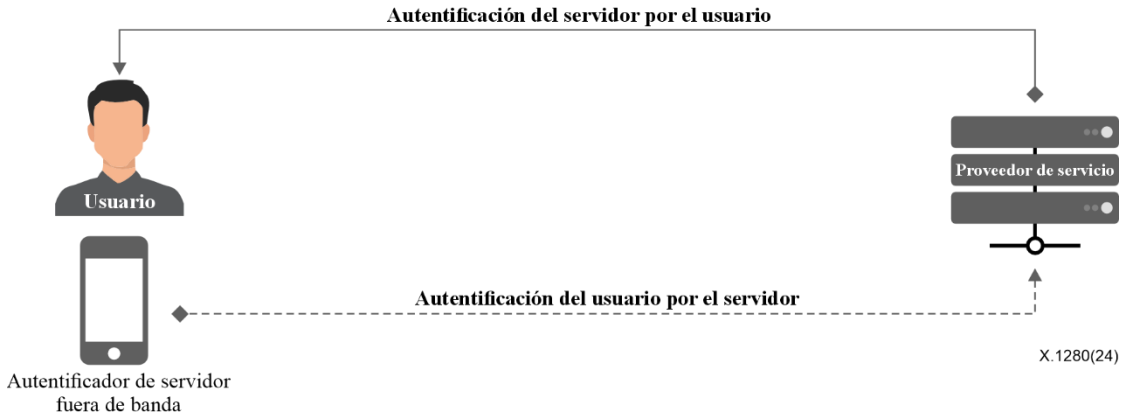

Figura 2 – Autentificación mutua

3) Autentificación unificada: Aunque se agreguen terminales de usuario adicionales, como computadoras, teléfonos inteligentes, cajeros automáticos (ATM) y altavoces de inteligencia artificial (IA), los métodos de autentificación se pueden unificar ya que los servidores presentan su información de autentificación de servidor al usuario en lugar de pedir al usuario que ingrese una variedad de informaciones de autentificación. La figura 3 muestra la autentificación unificada.

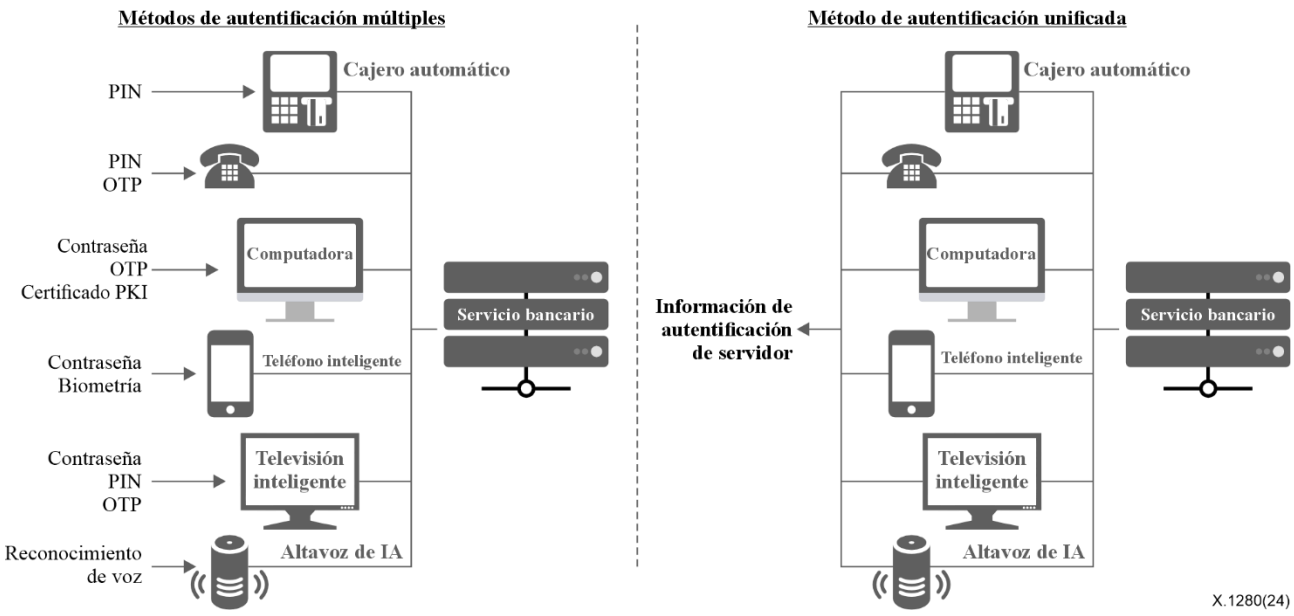

Figura 3 – Autentificación unificada (por ejemplo, servicio bancario)

7 Marco para la autentificación de servidores fuera de banda

En esta cláusula se definen las funciones y los componentes del modelo de autentificación para el marco de autentificación de servidores fuera de banda, que permite la autentificación mutua entre el usuario y el servidor. El flujo principal consiste en que el usuario verifique primero la información de autentificación del servidor y, a continuación, el servidor verifique la información de autentificación del usuario.

7.1 Funciones y componentes

En el Cuadro 1 se indican las funciones y los componentes del marco de autentificación de servidores fuera de banda.

Cuadro 1 – Funciones y componentes del modelo de autentificación de servidores fuera de banda

Nombre	Descripción
Verificador	Un verificador genera la información de autentificación de servidor en respuesta a la petición del usuario. La información se envía a la parte que confía para su presentación al usuario. Envía el desplazamiento (*offset*) de generación de la información de autentificación de servidor al autentificador de servidor fuera de banda para que éste genere la información de autentificación del servidor que se presenta al usuario.
Parte que confía	Una parte que confía presenta la información de autentificación del servidor generada y enviada por el verificador al usuario.
Usuario	Un usuario recibe servicios de partes que confían y verificadores.
Terminal de usuario	Un terminal de usuario muestra la información de autentificación de servidor a través de aplicaciones. Ejemplos de terminales de usuario son las computadoras, los teléfonos inteligentes, los cajeros automáticos y los altavoces de IA.
Autentificador de servidor fuera de banda	Un autentificador de servidor fuera de banda genera la información de autentificación del servidor utilizando el desplazamiento enviado por el verificador.

7.2 Información de autentificación de servidor

La información de autentificación de servidor es un código de varios dígitos utilizado cuando el usuario autentifica un servidor. Se generará cuando el usuario lo solicita utilizando la contraseña de un solo uso (OTP) con prueba y respuesta. Los valores dinámicos de las pruebas y una clave de verificación se utilizan para calcular y generar la información de autentificación de servidor. Los valores dinámicos de las pruebas y la clave de verificación se definen en la cláusula 8.

Si la información de autentificación generada por el servidor concuerda con la información de autentificación generada por el autentificador de servidor fuera de banda del usuario, queda verificada la autenticidad del servidor.

7.3 Modelo de autentificación

El flujo principal de la autentificación de servidores fuera de banda es que el usuario autentifica primero el servidor comparando las informaciones de autentificación generadas por el verificador y por el autentificador del servidor fuera de banda. Una vez que el usuario autentifica el servidor, el autentificador genera la información de autentificación de usuario y la envía al verificador. El verificador autentifica al usuario con la información de autentificación de usuario.

La Figura 4 muestra una visión general de la autentificación de servidores fuera de banda mediante dispositivos móviles.

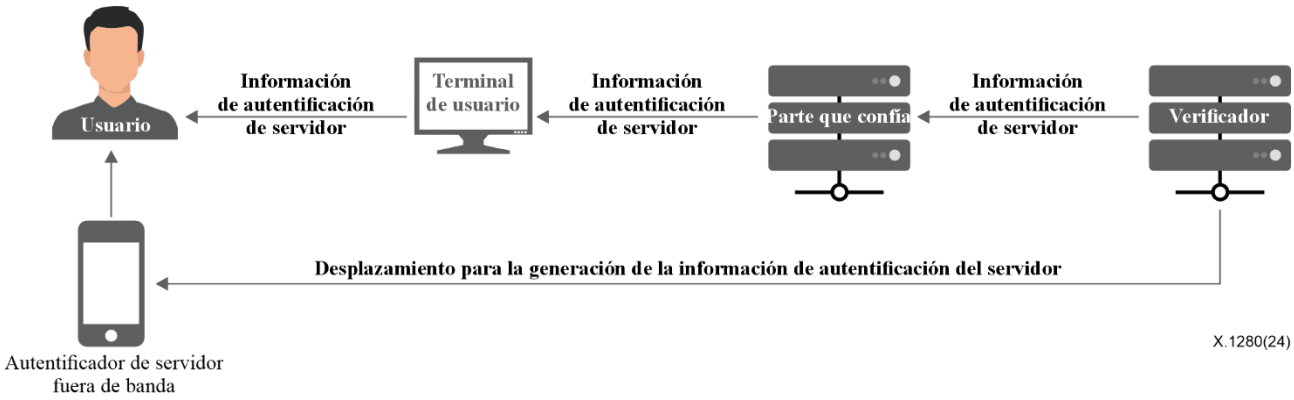

Figura 4 – Visión general de la autentificación de servidores fuera de banda mediante dispositivos móviles

Para iniciar la autentificación del servidor fuera de banda mediante dispositivos móviles, es necesario que el usuario escriba la ID de usuario en el terminal de usuario con una pantalla. Una vez que el usuario ha introducido la ID en el terminal de usuario, la parte que confía debe presentar al usuario, primero en el terminal de usuario, la información de autentificación del servidor generada por el verificador. A continuación, el usuario la compara con la información de autentificación generada por el autentificador del servidor fuera de banda del usuario.

8 Procedimientos para la autentificación de servidores fuera de banda

8.1 Instalación y registro del autentificador de servidor fuera de banda

En el paso de instalación y registro del autentificador de servidor fuera de banda, el usuario instala la aplicación de autentificación en el teléfono inteligente y la registra en el verificador.

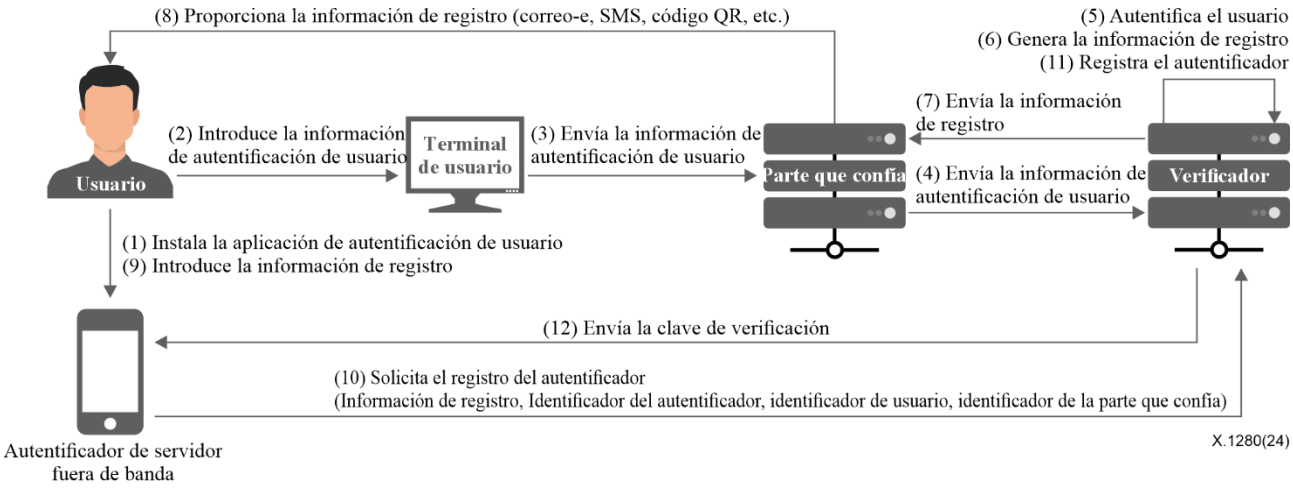

Figura 5 – Flujos de la instalación y el registro del autentificador de servidor fuera de banda

La Figura 5 identifica los datos necesarios en el paso de instalación y registro del autentificador de servidor fuera de banda y muestra los flujos. La explicación de los flujos es la siguiente:

1) El usuario instala la aplicación de autentificación de servidor fuera de banda en el teléfono inteligente.

2) El usuario introduce la información de autentificación de usuario a través del terminal de usuario para autentificarse como usuario legítimo mediante un método fiable, como un inicio de sesión, la verificación por correo electrónico o la identificación del teléfono móvil, de acuerdo con la política de la parte que confía.

3) La información de autentificación de usuario introducida en el terminal de usuario se envía a la parte que confía.

4) La parte que confía envía la información de autentificación de usuario al verificador.

5) El verificador autentifica el usuario.

6) El verificador genera la información de registro correspondiente al usuario autentificado.

7) El verificador envía la información de registro generada, incluidos el identificador de usuario de la parte que confía y el identificador de la parte que confía, a la parte que confía.

8) La parte que confía proporciona al usuario la información de registro utilizando métodos fiables, tales como correo electrónico, mensaje de texto, código de respuesta rápida (QR), etc.

9) El usuario introduce la información de registro del autentificador en el autentificador instalado en el teléfono inteligente.

10) El autentificador envía al verificador la información de registro, el identificador del autentificador, el identificador de usuario y el identificador de la parte que confía.

11) El verificador verifica la información de registro y registra al autentificador con el identificador de autentificador, el identificador de usuario y el identificador de la parte que confía.

12) Después de registrar el autentificador, el verificador envía la clave de verificación correspondiente al autentificador.

El proceso de registro del autentificador de servidor fuera de banda se proporcionará y realizará aplicando el protocolo de capa de zócalo seguro (SSL) utilizando certificados UIT-T X.509 para proteger la comunicación entre el autentificador y el verificador.

En el caso de que el autentificador de servidor fuera de banda no pueda utilizarse debido a una pérdida o un daño, el verificador puede permitir al usuario registrar más de un autentificador de servidor fuera de banda como autentificador de reserva.

8.2 Petición de autentificación de servidor

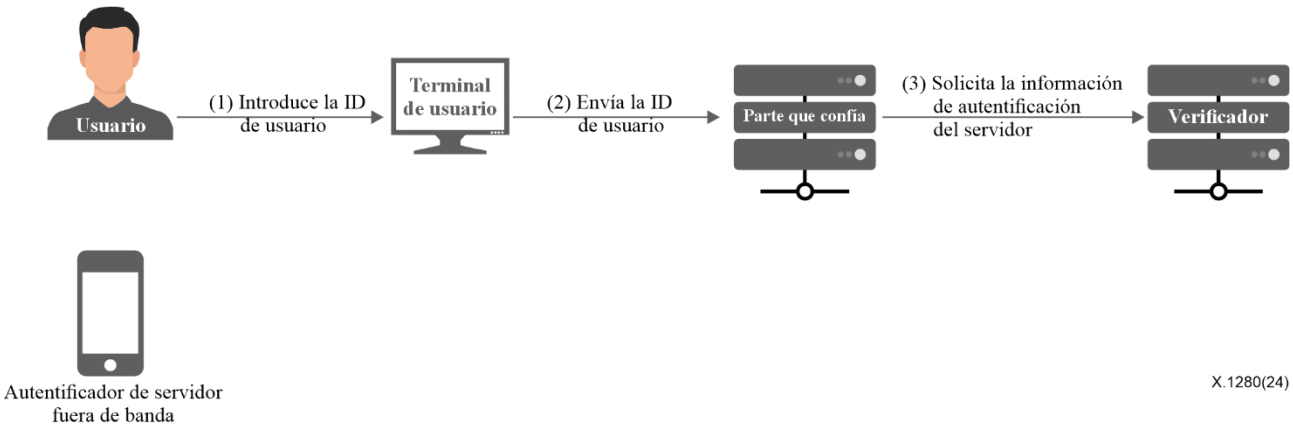

Figura 6 – Flujos de la petición de autentificación de servidor

La Figura 6 muestra los datos necesarios en el paso de petición de autentificación de servidor, así como los flujos. La explicación de los flujos es la siguiente:

1) El usuario en el terminal de usuario se conecta con la parte que confía e introduce su ID.
2) La ID de usuario introducida en el terminal de usuario se envía a la parte que confía.
3) La parte que confía solicita la información de autentificación de servidor al verificador.

8.3 Generación y presentación de la información de autentificación de servidor

En el paso de generación y presentación de la información de autentificación del servidor, el verificador genera la información de autentificación del servidor correspondiente a la ID de usuario una vez que ha recibido la petición de autentificación del servidor de la parte que confía. A continuación, el verificador envía la información de autentificación del servidor a la parte que confía para que la muestre en la pantalla del terminal de usuario. El verificador envía también el desplazamiento al autentificador de servidor fuera de banda del usuario. El autentificador utiliza el desplazamiento recibido para generar la información de autentificación del servidor y presenta la información de autentificación de servidor generada.

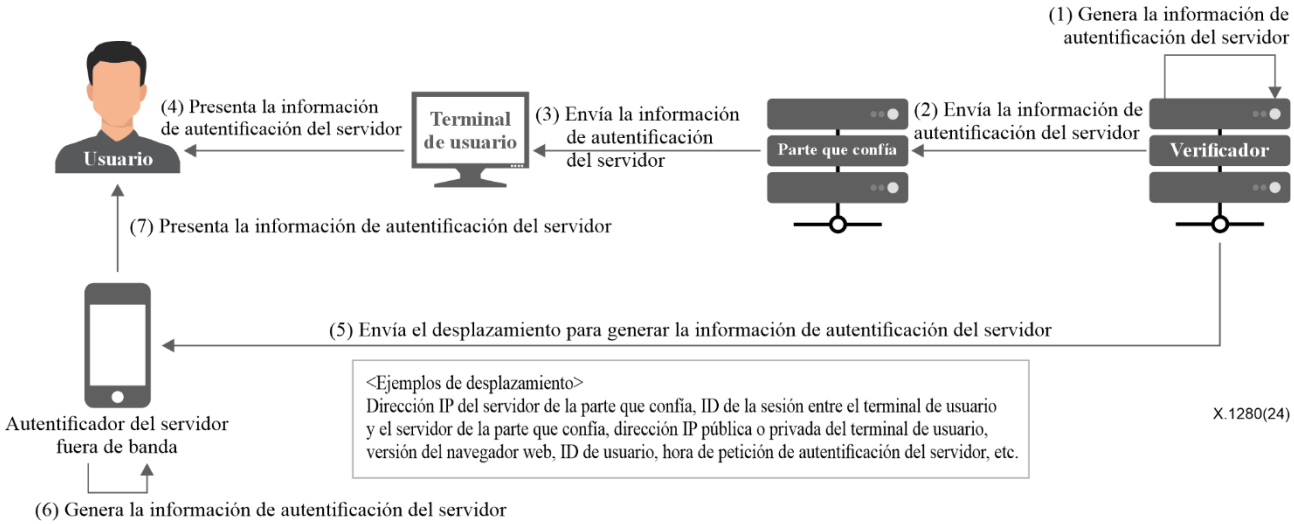

Figura 7 – Flujos de la generación y presentación de la información de autentificación de servidor

La Figura 7 muestra los datos requeridos en el paso de generación y presentación de la información de autentificación de servidor y muestra los flujos. La explicación de los flujos es la siguiente:

1) El verificador genera la información de autentificación de servidor una vez que recibe la petición de autentificación del servidor, incluyendo la ID de usuario y el desplazamiento por parte de la parte que confía. El verificador calcula y genera la información de autentificación de servidor con la clave de verificación, que tanto el verificador como el autentificador fuera de banda del usuario han recibido y almacenado durante el paso de instalación y registro del autentificador de servidor fuera de banda, así como el desplazamiento.
2) El verificador envía la información de autentificación de servidor generada a la parte que confía.
3) La parte que confía envía la información de autentificación del servidor recibida al terminal de usuario.
4) La parte que confía presenta la información de autentificación del servidor al usuario a través del terminal de usuario.
5) El verificador envía también el desplazamiento para generar la información de autentificación del servidor al autentificador de servidor fuera de banda del usuario.
6) El autentificador de servidor fuera de banda del usuario calcula y genera la información de autentificación del servidor con la clave de verificación, que tanto el verificador como el autentificador fuera de banda del usuario han recibido y almacenado durante el paso de instalación y registro del autentificador de servidor fuera de banda, así como el desplazamiento.
7) El autentificador de servidor fuera de banda presenta también al usuario la información de autentificación del servidor generada por él mismo.

El desplazamiento debe incluir la dirección de protocolo Internet (IP) del servidor de la parte que confía, la ID de la sesión entre el terminal de usuario y el servidor de la parte que confía, la dirección IP pública del terminal de usuario, la dirección IP privada del terminal de usuario, la versión del navegador web del terminal de usuario, la ID de usuario y la hora de petición de autentificación del servidor del usuario.

La información de autentificación de servidor debe calcularse y generarse utilizando la clave de verificación y el desplazamiento, y luego debe convertirse en un valor fácil de leer para los usuarios. El valor debe ser un número o una cadena de al menos 6 caracteres. El valor debe mostrarse en el

terminal de usuario y en el autentificador de servidor fuera de banda. Además, la información de autentificación de servidor debe tener un periodo de validez adecuado de acuerdo con el tipo de servicio en línea y debe mostrarse visualmente el tiempo restante de validez en varias formas dentro de la zona de visualización de la información de autentificación del servidor, como se muestra en la Figura 8.

Figura 8 – Ejemplo de presentación de la información de autentificación del servidor

En lugar de que el usuario compare la información de autentificación, la parte que confía puede mostrar un código QR, que incluye la información de autentificación del servidor para que el autentificador del servidor fuera de banda pueda leer y verificar el código. A continuación, el autentificador muestra una información comprensible al usuario para que pueda verificar si el servidor es auténtico.

8.4 Autentificación de servidores

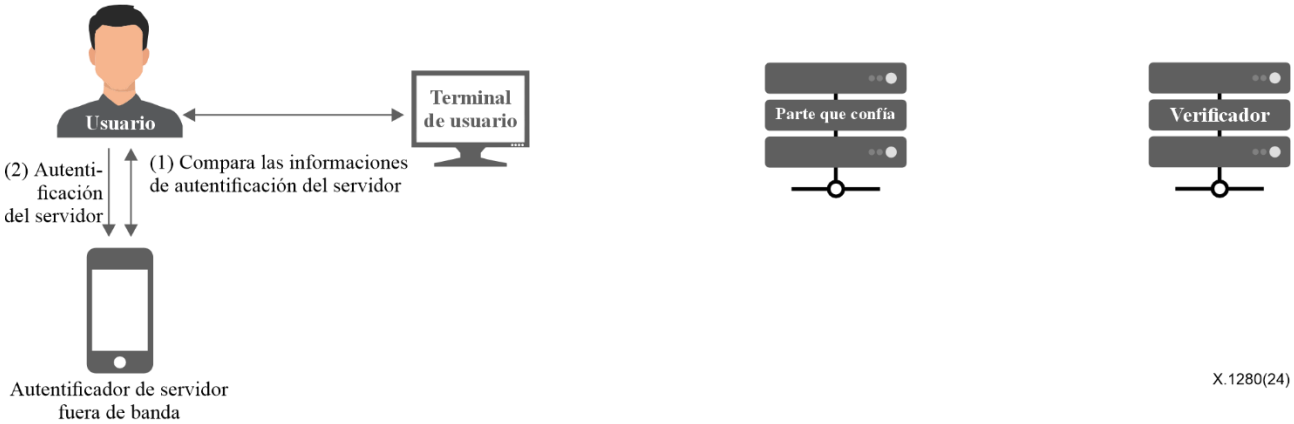

Figura 9 – Flujos de la autentificación de servidores

La Figura 9 muestra los datos requeridos en el paso de autentificación de servidores y muestra los flujos. La explicación de los flujos es la siguiente:

1) El usuario compara visualmente y verifica las informaciones de autentificación del servidor presentada en el terminal y en el autentificador de servidor fuera de banda.

2) El usuario autentifica el servidor seleccionando una aprobación en el autentificador fuera de banda del usuario.

8.5 Autentificación de usuario y prestación de servicio

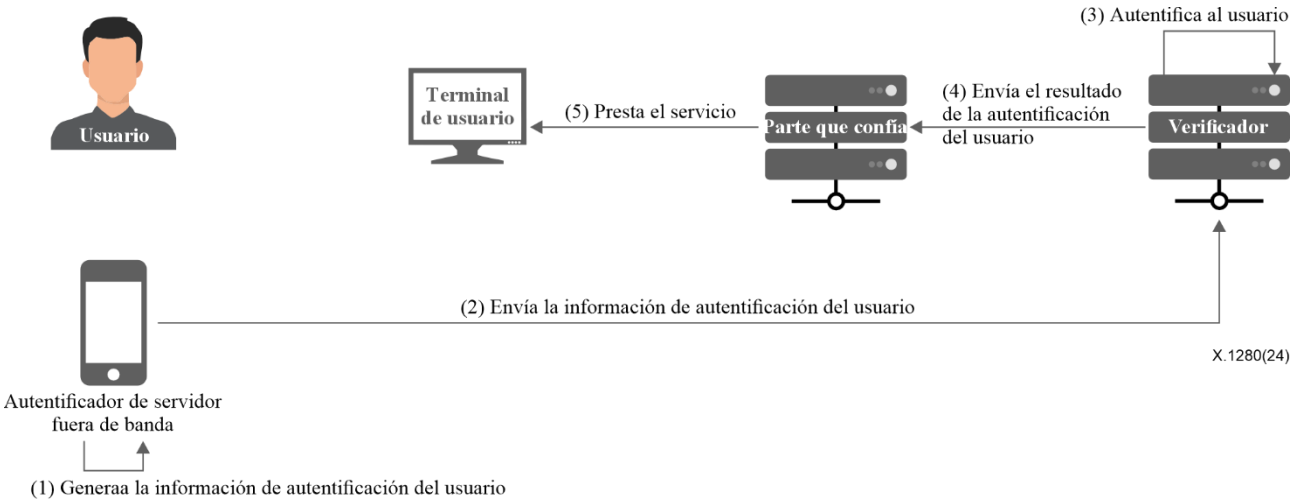

Figura 10 – Flujos de la autentificación de usuario y prestación de servicio

La Figura 10 muestra los datos requeridos en el paso de autentificación de usuario y prestación de servicio y muestra los flujos. La explicación de los flujos es la siguiente:

1) Cuando el usuario autentifica el servidor en el autentificador de servidor fuera de banda del usuario, el autentificador genera la información dinámica de autentificación del usuario, como una contraseña de un solo uso. Para confirmar que la utilización legítima por el usuario del autentificador, el usuario puede tener que identificarse utilizando información biométrica como la cara y las huellas dactilares o el número de identificación personal (PIN) del usuario en el teléfono inteligente.
2) El autentificador del servidor fuera de banda del usuario envía la información de autentificación del usuario al verificador.
3) El verificador autentifica al usuario verificando la información de autentificación de usuario recibida.
4) El verificador envía el resultado de la autentificación del usuario a la parte que confía.
5) La parte que confía presta el servicio de acuerdo con el resultado de la autentificación de usuario recibido del verificador.

En lugar de una información de autentificación de usuarios dinámica, se puede utilizar la autentificación de usuario basada en PKI fuerte, como una PKI y una identidad rápida en línea (FIDO). El valor de la prueba requerida en la autentificación de usuario basada en PKI puede recibirse conjuntamente en el paso de generación y presentación de la información de autentificación de servidor, o el desplazamiento recibido puede usarse como el valor de la prueba.

9 Amenazas de seguridad y requisitos de seguridad

9.1 Amenazas de seguridad

En esta cláusula se identifican las posibles amenazas para la seguridad que puede plantear el modelo de autentificación de servidores fuera de banda.

9.1.1 Proveedor de servicio en línea fraudulento

Un atacante hace que un usuario acceda a un proveedor de servicio en línea fraudulento e induce al usuario a introducir su contraseña para robársela, en lugar de utilizar el autentificador de servidor fuera de banda.

9.1.2 No se puede utilizar el autentificador de servidor fuera de banda

Si un usuario no puede utilizar su autentificador de servidor fuera de banda debido a la pérdida o avería del autentificador, es posible que el usuario no pueda acceder al servicio en línea porque puede haber olvidado la contraseña de usuario en vigor o es posible que no pueda utilizar otro método de autentificación.

9.1.3 Utilización no autorizada del autentificador de servidor fuera de banda

Un atacante puede utilizar el autentificador de servidor fuera de banda de un usuario, por ejemplo, robándolo.

9.1.4 Ataques remotos al autentificador de servidor fuera de banda

Un atacante puede realizar una autentificación a distancia instalando un software malicioso en el teléfono inteligente en el que está instalado el autentificador de servidor fuera de banda del usuario.

9.1.5 Petición de autentificación de servidor falsa

Cuando un usuario utiliza un servicio en línea que proporciona autentificación de servidores fuera de banda, en el momento en que intenta la autentificación de un servidor mediante la comparación y verificación de las informaciones de autentificación de servidor, un atacante puede enviar una petición de autentificación de servidor falsa al autentificador fuera de banda del usuario introduciendo la ID de usuario en un terminal diferente para inducir al usuario a realizar una autentificación incorrecta.

9.2 Requisitos de seguridad

En esta cláusula se describen los requisitos de seguridad en respuesta a las posibles amenazas a la seguridad que puede plantear el modelo de autentificación de servidores fuera de banda. En el Apéndice I se describe la relación entre cada amenaza a la seguridad y los requisitos de seguridad.

9.2.1 Restricción de la autentificación mediante contraseña de usuario

Para evitar que los usuarios registren un autentificador de servidor fuera de banda utilizando una contraseña de usuario robada o que se haya filtrado, puede restringirse el método de autentificación mediante contraseña de usuario y permitirse sólo la autentificación de usuario a través del autentificador de servidor fuera de banda.

9.2.2 Métodos complementarios para liberar un autentificador de servidor fuera de banda y restablecer la contraseña del usuario

Deben proporcionarse métodos complementarios para liberar un autentificador de servidor fuera de banda registrado y restablecer la contraseña de usuario mediante una autentificación de usuario independiente, como una verificación de identidad, una verificación de correo electrónico o preguntas de seguridad.

9.2.3 Métodos de autentificación adicionales dentro del autentificador de servidor fuera de banda

Al autentificar el servidor mediante el autentificador, puede utilizarse un método de autentificación adicional para verificar que el usuario es legítimo, como un PIN o una autentificación biométrica a través del teléfono inteligente en el que está instalado el autentificador de servidor fuera de banda.

9.2.4 Control de peticiones simultaneas de autentificación de servidores

Una vez que el autentificador de servidor fuera de banda muestre la información de autentificación de un servidor, deben bloquearse las nuevas peticiones de autentificación de servidores o ponerse en cola hasta que el usuario complete la autentificación del servidor.

Anexo A

Procedimiento complementario para la autentificación de servidores fuera de banda

(Este anexo forma parte integrante de la presente Recomendación.)

A.1 Renovación automática de la contraseña de usuario

En el paso de renovación automática de la contraseña de usuario, después de que la parte que confía presta un servicio al usuario mediante la autentificación de un servidor fuera de banda, el proveedor de servicio en línea renueva automáticamente la contraseña de la cuenta de usuario. Los proveedores de servicio en línea pueden mantener el concepto de contraseñas de usuario para minimizar los cambios en las estructuras y las funciones de datos existentes, al tiempo que refuerzan la seguridad de las contraseñas de usuario.

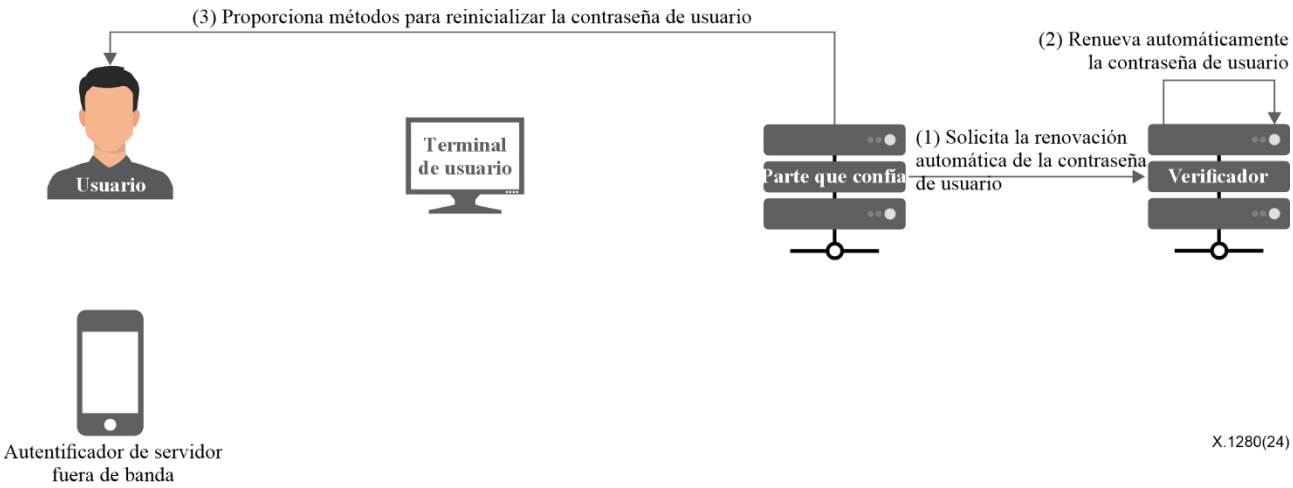

Figura A.1 – Flujos de la renovación automática de la contraseña de usuario

La Figura A.1 muestra los datos necesarios en el paso de la renovación automática de la contraseña de usuario y muestra los flujos. Estos flujos suponen que el verificador realiza la renovación automática de la contraseña de usuario, y que pueden realizarla la parte que confía o el verificador. La explicación de los flujos es la siguiente:

1) Después de que la parte que confía presta servicio al usuario con la autentificación de un servidor fuera de banda, se envía al verificador una petición de renovación de la contraseña de usuario para dicho usuario.

2) El verificador cambia la contraseña de usuario a un valor generado aleatoriamente con una regla compleja.

3) En caso de que sea imposible utilizar el autentificador de servidor fuera de banda registrado por el usuario en caso de pérdida, etc., la parte que confía proporciona un método para liberar el autentificador y reinicializar la contraseña de usuario mediante una autentificación de usuario independiente, de modo que el usuario pueda utilizar el servicio con la contraseña de usuario restablecida.

El usuario puede administrar su contraseña de usuario sin tener que cambiarla regularmente por sí mismo y permanece a salvo de las fugas de contraseñas.

Apéndice I

Relación entre los requisitos de seguridad y las amenazas

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

En este apéndice se define en el Cuadro I.1 la relación entre las posibles amenazas a la seguridad que puede plantear el modelo de autentificación de servidores fuera de banda y los requisitos de seguridad.

Cuadro I.1 – Relación entre los requisitos de seguridad y las amenazas

Requisitos de seguridad	**Amenazas a la seguridad**				
	Servicio en línea fraudulento	**No se puede utilizar el autentificador de servidor fuera de banda**	**Utilización no autorizada del autentificador de servidor fuera de banda**	**Ataques remotos al autentificador de servidor fuera de banda**	**Petición de autentificación de servidor falsa**
Restricción de la autenticación mediante contraseña de usuario	o	-	-	-	-
Métodos complementarios de autentificación	-	o	-	-	-
Métodos adicionales de autentificación de usuario	-	-	o	o	-
Control de peticiones simultáneas de autentificación de servidor	-	-	-	-	o

Apéndice II

Casos de utilización del modelo de autentificación de servidores fuera de banda

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

II.1 Sitios web y aplicaciones

Los sitios web, las aplicaciones web y diferentes aplicaciones que no utilizan un explorador web pueden solucionar las limitaciones de la autentificación de servidores basada en PKI aplicando el modelo de autentificación de servidores fuera de banda.

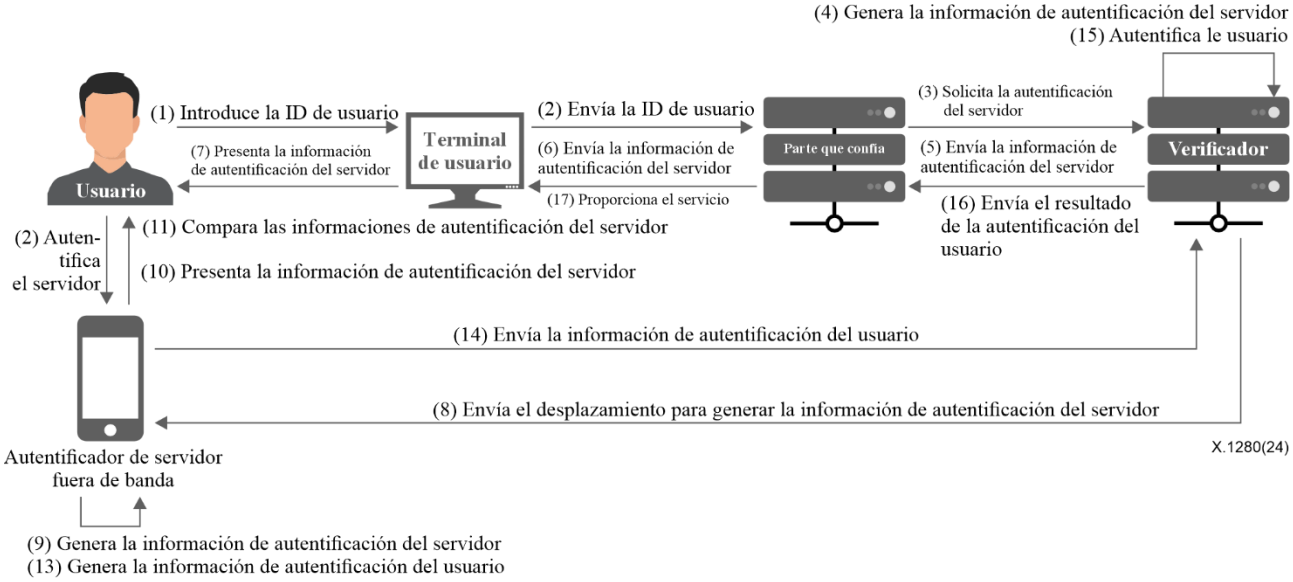

Figura II.1 – Flujos de la autentificación de servidores fuera de banda para sitios web y aplicaciones

En la Figura II.1 se muestran los flujos de la autentificación de servidores fuera de banda para sitios web y aplicaciones.

Incluso en el caso de los sitios web corporativos y de las aplicaciones web que utilizan un sistema de nombres de dominio (DNS) privado, que no pueden obtener un certificado PKI a través de una autoridad de certificación, y las aplicaciones basadas en direcciones IP, así como las aplicaciones que no utilizan un navegador web, el usuario puede realizar una autentificación de manera segura después de una verificación previa clara de los proveedores de servicios en línea.

II.2 Proveedores de identidad

Los proveedores de identidad (IDP) que ofrecen servicios OAuth 2.0 y SAML (lenguaje de marcación de aserción de seguridad) pueden aplicar el modelo de autentificación de servidores fuera de banda para garantizar la seguridad de las cuentas de usuario en todos los servicios en línea conectados a ellos.

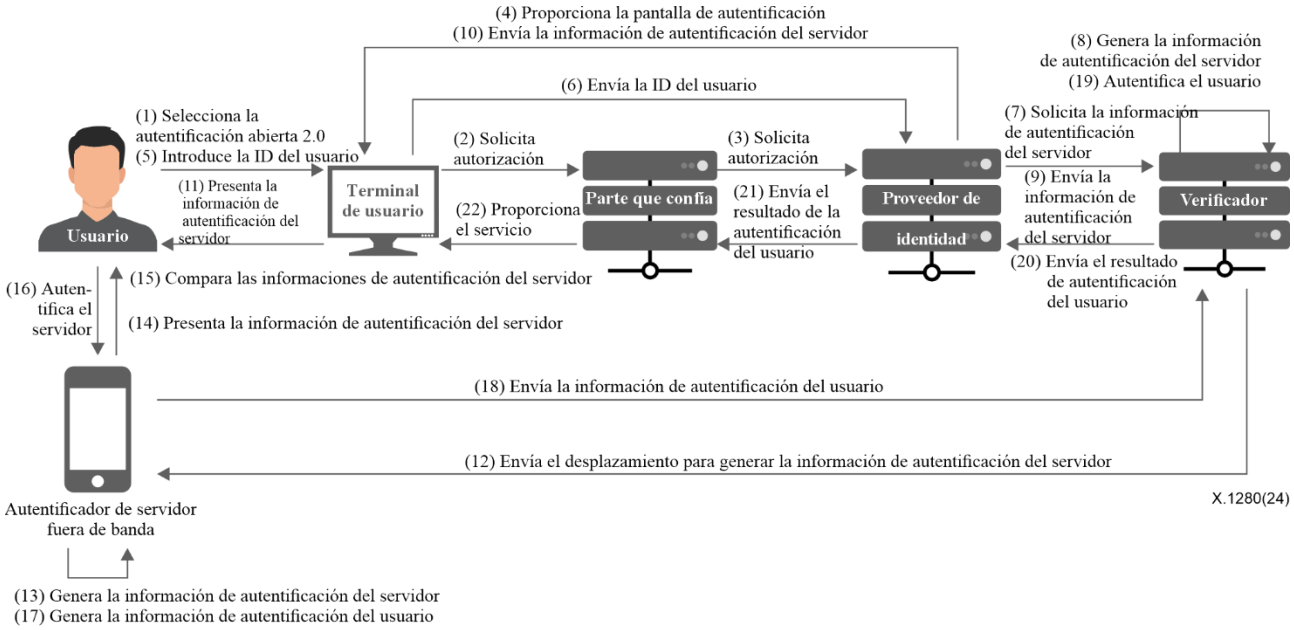

Figura II.2 – Flujos de la autentificación de servidores fuera de banda para los IDP

En la Figura II.2 se muestran los flujos de la autentificación de servidores fuera de banda para los IDP.

Si la información de autentificación del usuario del proveedor de ID se filtra debido a un ciberataque mediante suplantación de la pantalla de autentificación del IDP, las cuentas de usuario de todos los proveedores de servicios registrados por dicho usuario podrían estar en peligro. Los IDP pueden protegerse de la suplantación de identidad y el redireccionamiento fraudulento agregando una autentificación de servidores fuera de banda.

II.3 Sistemas operativos

Los sistemas operativos basados en Windows y Linux pueden aplicar el modelo de autentificación de servidores fuera de banda para reforzar la seguridad de la cuenta local del sistema operativo.

Para aplicar el modelo de autentificación al sistema operativo basado en Windows, es necesario instalar y configurar un cliente de un proveedor de credenciales externo que pueda controlar las credenciales del sistema operativo.

Para aplicar el modelo de autentificación a los sistemas operativos basados en Linux, es necesario instalar y configurar módulos de autentificación conectables (PAM).

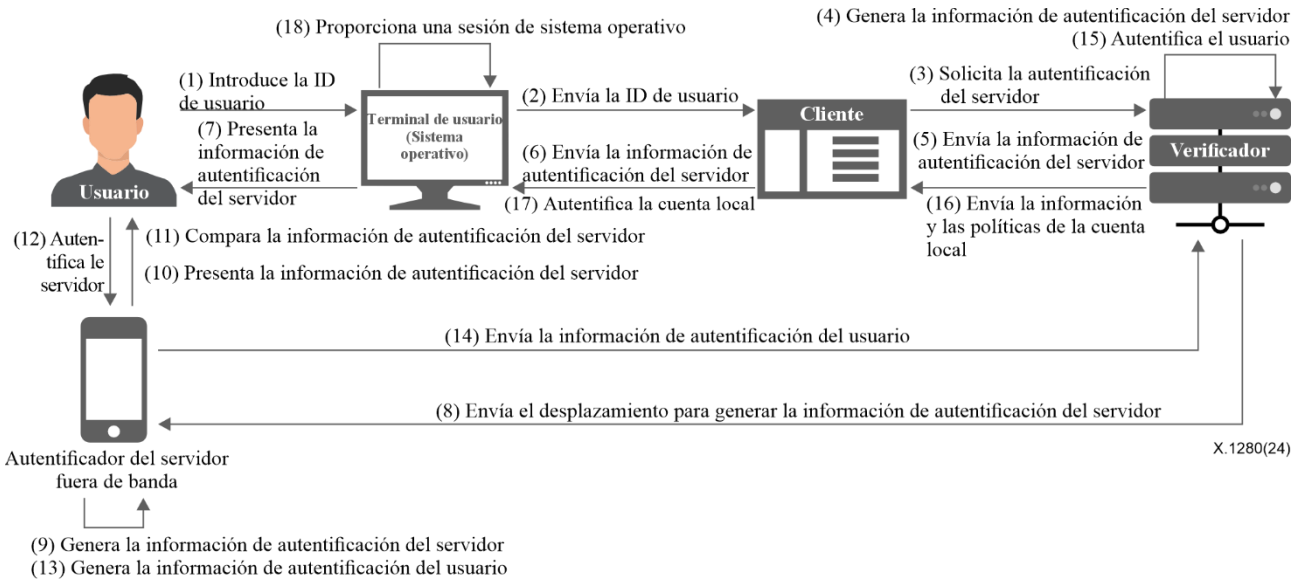

Figura II.3 – Flujos de la autentificación de servidores fuera de banda para sistemas operativos

La Figura II.3 muestra los flujos de la autentificación de servidores fuera de banda para sistemas operativos.

Los usuarios pueden verificar de manera clara que el sistema operativo al que intentan acceder es correcto, y es posible evitar los incidentes provocados por escribir la información de acceso en un papel o compartirla con otros usuarios, aunque el sistema operativo se esté ejecutando en la nube.

Además, si se aplica la renovación automática de la contraseña de usuario, un paso adicional en el procedimiento de autentificación de servidores fuera de banda, se pueden administrar de manera más fácil y segura las políticas de cambio de contraseña para las cuentas locales.

Después de introducir la ID de usuario, el usuario puede utilizar el sistema operativo después de verificar la información de autentificación del servidor que se muestra en la pantalla de inicio de la sesión del sistema operativo y en el autentificador del servidor fuera de banda. El usuario no necesita escribir una contraseña de usuario ni utilizar un archivo de clave para acceder a los sistemas operativos.

Además, si se aplica al cliente la renovación automática de la contraseña de usuario, un paso adicional en el procedimiento de autentificación del servidor fuera de banda, se puede administrar de manera más fácil y segura la cuenta del sistema operativo cambiando automáticamente la contraseña de la cuenta local del sistema operativo.

Apéndice III

Relación con otras tecnologías de autentificación

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

Las tecnologías de autentificación son unas tecnologías fundamentales que mantienen la confianza entre los usuarios y los proveedores de servicios en línea en la era digital. Se han desarrollado diversas tecnologías de autentificación, como OTP, FIDO y la autentificación de envío forzado móvil, que se han utilizado ampliamente, teniendo en cuenta que la autentificación sea segura, rentable y práctica. Así pues, se han establecido distintos niveles de garantía de autentificación para las nuevas tecnologías de autentificación en [b-UIT-T X.1254], [b-ISO/CEI 29115] y [b-NIST SP 800-63-3].

A medida que se han mejorado y normalizado las tecnologías de autentificación, existe una mayor demanda de resistencia frente a la suplantación del verificador y de la autenticidad del usuario. Las tecnologías de autentificación que cumplen con el requisito se clasifican con el nivel más alto.

Sin embargo, dado que las tecnologías de autentificación existentes sólo autentifican a los usuarios, existen limitaciones para proporcionar únicamente la información de autentificación de usuario a los proveedores de servicio sin que los usuarios los verifiquen explícitamente para evitar la suplantación del verificador.

Las tecnologías de autentificación de usuario existentes pueden dividirse principalmente en las autentificaciones dentro de banda, que proporcionan la información de autentificación a través del canal de comunicación primario entre los servidores del proveedor de servicio y los usuarios, y las autentificaciones fuera de banda que proporcionan la información de autentificación a través de un canal de comunicación separado.

Las tecnologías de autentificación dentro de banda son resistentes a la suplantación del verificador, pero no son convenientes y no son económicas. Las tecnologías de autentificación fuera de banda son convenientes y económicas, pero son vulnerables a la suplantación del verificador.

La Figura III.1 muestra los flujos de la información de autentificación para las autentificaciones dentro de banda y fuera de banda.

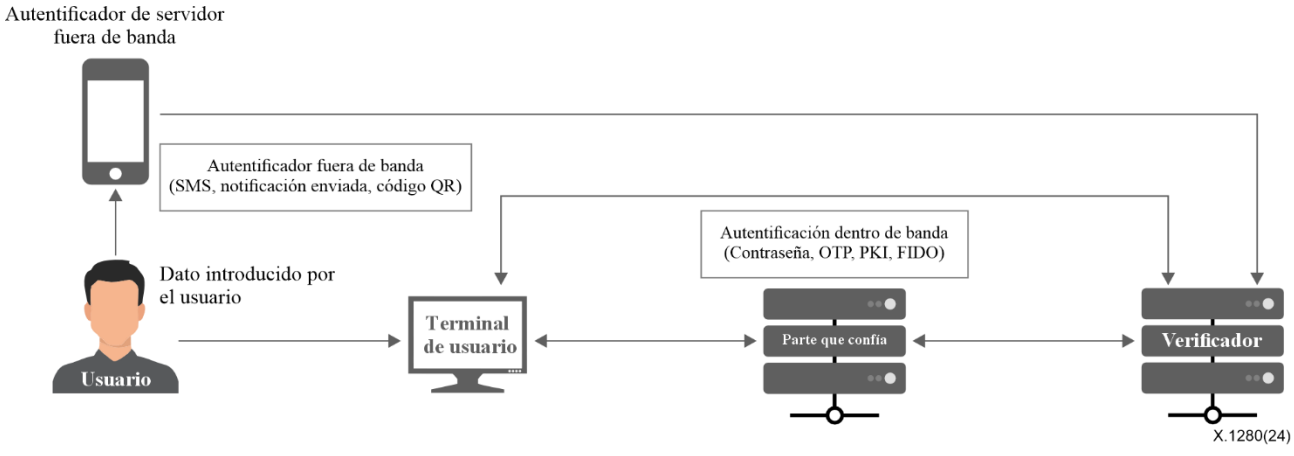

Figura III.1 – Flujos de la información de autentificación para las autentificaciones dentro y fuera de banda

La autentificación dentro de banda, como las tecnologías PKI, sólo proporciona de manera implícita la resistencia a la suplantación del verificador, ya que no proporciona de manera explícita al usuario un método para verificar el proveedor de servicio. Si se cambia un servidor o una aplicación, debe volver a identificar al usuario y volver a emitir el certificado en el terminal de usuario.

En particular, FIDO es una tecnología típica de autentificación dentro de banda porque el autentificador se comunica con el servidor de autentificación a través del terminal conectado en ese momento a la parte que confía, aunque el protocolo universal de dos factores (U2F) y el protocolo de cliente a autentificador (CTAP) den la sensación de un autentificador externo independiente del terminal. Por este motivo, si se utilizan dos o más terminales en casa o en el trabajo, el usuario tiene que volver a registrar el servicio en el autentificador FIDO de cada terminal. Además, incluso cuando se utiliza un autentificador CTAP, un autentificador externo de FIDO2, tiene que registrarse o reconectarse en cada terminal. En consecuencia, las tecnologías de autentificación dentro de banda basadas en PKI dependen del terminal, sin verificar los proveedores de servicio de manera explícita.

La autentificación fuera de banda, como las notificaciones enviadas (*push*) al móvil, es una tecnología de autentificación que verifica que el usuario posee un autentificador, pero que no necesita volver a identificar al usuario y volver a emitir el certificado, aunque se cambie un servidor o una aplicación. Sin embargo, si el usuario ya está conectado a un servidor fraudulento sin saber a dónde se ha conectado, no puede ofrecer resistencia a la suplantación del verificador, como se muestra en la Figura III.2.

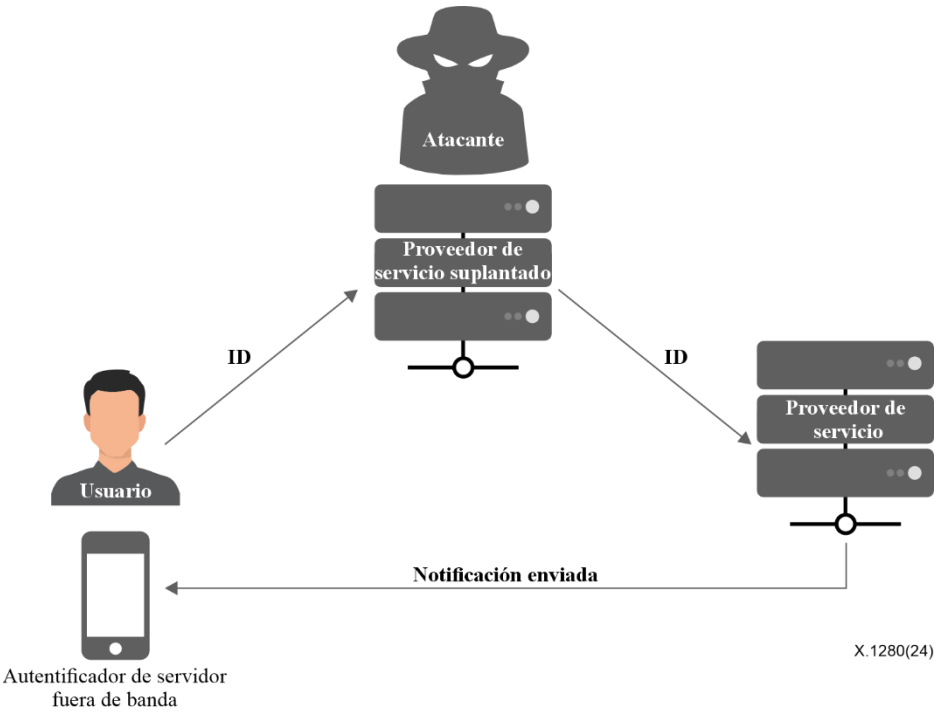

Figura III.2 – Vulnerabilidad de la autentificación de usuario fuera de banda frente a una suplantación de un proveedor de servicio

Independientemente de las tecnologías de autentificación de usuario, existe una tecnología de autentificación de los servidores web que puede utilizar un usuario para verificar el proveedor de servicio, al controlar el certificado UIT-T X.509 indicado con el símbolo de candado en el navegador, pero este control no está alineado con el proceso de autentificación de usuario, por lo que puede resultar difícil para los usuarios comprobar el certificado cada vez, y es posible que los usuarios que no estén familiarizados con la tecnología ni siquiera controlen el certificado. Por otro lado, es una solución vulnerable a los ataques de ingeniería social que utilicen nombres de dominio similares y no tiene la capacidad de verificar los servicios en línea que utilizan un servidor DNS privado, los servicios en línea basados en direcciones IP y los servicios en línea que no están basados en un navegador.

Por tanto, un marco para la autentificación de servidores fuera de banda puede ser necesario para poder solucionar la vulnerabilidad frente a la suplantación del verificador, que puede producirse cuando se utilizan tecnologías de autentificación de usuario fuera de banda, y la limitación de la dependencia del terminal que tienen los autentificadores y que proviene de la utilización de tecnologías de autentificación de usuario dentro de banda basadas en PKI.

Bibliografía

[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.1254] Recomendación UIT-T X.1254 (2020), *Marco de garantía de autentificación de entidad*.

[b-UIT-T X.1277] Recomendación UIT-T X.1277 (2018), *Marco de autentificación universal*.

[b-UIT-T X.1278] Recomendación UIT-T X.1278 (2018), *Protocolo de cliente a autentificador/marco universal de dos factores*.

[b-ISO/CEI 29115] ISO/CEI 29115:2013, *Tecnologías de la información – Técnicas de seguridad – Marco de garantía de la autentificación de entidades*.

[b-ISO/CEI 18014-2] ISO/CEI 18014-2:2021, *Seguridad de la información – Servicios de estampación de hora – Parte 2: Mecanismos que producen testigos independientes*.

[b-NIST SP 800-63-3] NIST SP 800-63-3: 2017, *Directrices sobre identidad digital*.

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

Publicado en Suiza
Ginebra, 2024