Sociedad Andaluza para el Desarrollo de las Telecomunicaciones
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

seguridad+ Y CONFIANZA DIGITAL | AndalucíaCERT CENTRO DE SEGURIDAD TIC

Informe de divulgación

Uso de autenticación multi-factor en sistemas y aplicaciones I

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-10025-161027*
Edición:	*0*
Categoría	*Uso Interno*
Fecha de elaboración:	*27/10/2016*
N° de Páginas	*1 de 21*

1 TABLA DE CONTENIDOS

2 OBJETO

El objeto de este documento es proporcionar las nociones básicas sobre los sistemas de autenticación multi-factor.

3 ALCANCE

Este documento va dirigido tanto al personal de la Junta de Andalucía, como al público en general. Pretende aportar información básica para que el lector pueda comprender en qué consisten los sistemas de autenticación multi-factor y cómo puede configurarlos en sus sistemas y aplicaciones.

4 INTRODUCCIÓN

Vivimos en un mundo globalizado e hiperconectado en el que cada persona tiene decenas de identidades digitales que debe proteger. En este escenario, el uso de la ya tradicional combinación usuario/contraseña para asegurar el acceso a los servicios no ofrece las garantías necesarias, como se empeñan en demostrarnos las noticias que a menudo copan los periódicos y los medios especializados.

El uso de un Factor de autenticación Múltiple añade una capa más de seguridad en la gestión de nuestras cuentas y nos ayuda a prevenir el robo de identidades de una forma simple y cómoda.

En los siguientes epígrafes de este informe se definirá el concepto de autenticación y se hablará sobre los servicios de gestión de identidades.

4.1 AAA (Authentication, Authorization and Accountig)

El acrónimo AAA se corresponde con las siglas de la expresión *Authentication, Authorization and Accounting*, es decir, autenticación, autorización y contabilidad. Esta expresión es usada con frecuencia en el ámbito de la seguridad de la información para referirse a las familias de protocolos que ofrecen los tres servicios citados.

La **autenticación** es el proceso por el que un cliente prueba su identidad frente a una entidad (normalmente una aplicación o sistema). La autenticación se consigue mediante la presentación de una propuesta de identidad, como por ejemplo un nombre de usuario, y la demostración de estar en posesión de las credenciales que permiten comprobarla, como por ejemplo mediante una contraseña.

Por **autorización** se entiende la concesión de privilegios específicos a una entidad o usuario basándose en su identidad (que ha debido ser previamente autenticada). El proceso de autorización suele depender de los privilegios que el usuario solicita, así como el estado actual del sistema o aplicación.

La **contabilidad** o contabilización se refiere al seguimiento del consumo de recursos de una determinada aplicación o sistema por parte de un usuario que previamente se ha autenticado y al que se le han asignado privilegios para poder usar dichos recursos. Esta información puede usarse posteriormente para administración, planificación, facturación, u otros propósitos.

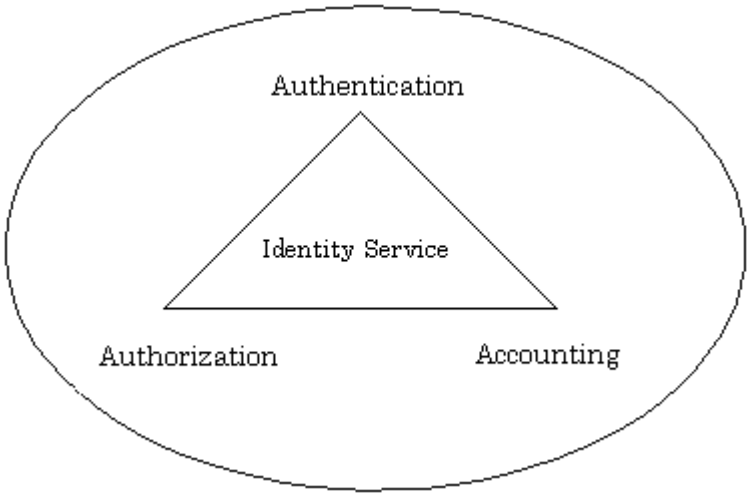

Figura 1. Servicio de identidad compuesto por la autenticación, la autorización y la contabilidad [3].

Hay que mencionar que en muchas ocasiones se añade otra A al acrónimo, convirtiéndose entonces en AAAA, para incluir el proceso de Auditoría (recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, utiliza eficientemente los recursos, cumple con las leyes y regulaciones establecidas, etc.).

4.2 Tipos de sistemas de autenticación

Así pues, la autenticación no es más que uno de los elementos presentes en un servicio de gestión de identidades y consiste en verificar la identidad de un usuario. Esto es, asegurarse de que alguien es quién dice ser.

A la hora de realizar este proceso existen diversas alternativas. A continuación se mencionan algunas de ellas:

- **Contraseñas**: Consiste en proporcionar, como prueba de su identidad, un secreto que sólo el usuario conoce. Suponen el método más ampliamente usado, pero también uno de los más vulnerables (pueden ser fáciles de adivinar, es necesario escribirlas en un área visible mientras otras personas pueden observar, son susceptibles de ser obtenidas por técnicas de sniffing o ingeniería social...).

- **One-Time Password (OTP)**: Consiste en una contraseña de un sólo uso. De esta forma se evita el problema de reusar las mismas contraseñas, aportando más robustez al sistema. Generalmente el usuario cuenta con un listado o libreta de contraseñas y sólo una de ellas será válida en un instante de tiempo dado.

- **Criptografía de clave pública**: La criptografía asimétrica (o de clave pública) hace uso de complejas funciones matemáticas para generar un par de claves pública y privada con los que establecer un canal de comunicaciones seguro. En el contexto del proceso de autenticación se puede usar un certificado digital emitido por un tercero de confianza.

- **Huellas digitales**: Estrechamente relacionado con la criptografía de clave pública, consiste en generar una huella de un determinado recurso mediante el uso de una función de hash. Para comprobar la identidad del usuario, éste enviará tanto el hash como el propio recurso al que se le ha calculado la huella.

- **Pruebas de conocimiento cero**: Establece un método interactivo para que una de las partes pueda probar a otra su identidad sin revelar información secreta.

- **Autenticación biométrica**: Consiste en usar alguna característica propia de un usuario, y que sea única, para probar su identidad. La huella dactilar, el iris, reconocimiento facial...

- **Tarjetas o dispositivos de identificación**: Elementos físicos que permiten a su portador validar su identidad. Un ejemplo sería el tradicional DNI.

4.3 La importancia del proceso de autenticación

Garantizar que el proceso de verificación de la identidad de un usuario se ha realizado de forma correcta es vital en cualquier sistema de información. Más aún cuando, dependiendo del tipo de autenticación usada, es posible que exista la figura del "no repudio" respecto a las acciones posteriores que se realicen. Los usuarios deben estar seguros de que sus identidades digitales están a salvo.

No obstante, ¿las identidades digitales de los usuarios están realmente a salvo? La realidad demuestra que no es así. El sistema de autenticación más usado suele consistir en la dupla usuario/contraseña y rara vez se usan contraseñas seguras, ni se suele tener una contraseña diferente por cada servicio.

Además, las contantes brechas de seguridad que se producen provocan la filtración de gran cantidad de información (incluidas cuentas de usuario), lo que pone en riesgo no ya el sistema atacado, sino todos aquellos servicios en los que los usuarios usen la misma identidad digital. Algunos ejemplos serían los robos masivos de datos sufridos por Yahoo! [8], PlayStation Network [9] o el servicio iCloud de Apple [10].

Ante este escenario, todo mecanismo que ayude a fortalecer el proceso de autenticación de un usuario debe ser tenido en cuenta. Es ahí donde entran en juego los sistemas de autenticación multifactor. Es más, muchas normas y estándares internacionales comienzan a incluir el uso de un segundo factor de autenticación como un requisito más [11], de obligado cumplimiento.

5 DEFINICIÓN DE SISTEMA DE AUTENTICACIÓN MULTI-FACTOR

Un factor de autenticación múltiple (MFA por sus siglas en inglés) es una aproximación a la seguridad en el proceso de autenticación del usuario que requiere de la presentación de dos o más elementos de los siguientes tres elementos de autenticación: un factor de conocimiento (algo que sólo el usuario sabe), un factor de posesión (algo que sólo el usuario posee), y un factor inherente al usuario (algo que sólo el usuario es).

Tras la presentación de una combinación de estos factores el sistema debe validarlos y, si son correctos, proceder a autenticar al usuario.

5.1 Algo que sé, algo que soy y algo que tengo

Ahora bien, ¿en qué consiste realmente un factor de autenticación? Pues bien, tratamos de exponerlo de forma breve:

- **Algo que sólo el usuario sabe**: se trata de un secreto, como una contraseña o el PIN de una tarjeta de crédito.

- **Algo que sólo el usuario tiene**: algo que se posee, como una llave o, volviendo al ejemplo de la tarjeta de crédito, la propia tarjeta de plástico.

- **Algo que sólo el usuario es**: características que son únicas en cada usuario, como por ejemplo, la huella digital, el iris...

Hay que hacer notar que, en ocasiones, no está del todo claro a qué factor pertenece una determinada medida de autenticación (¿una firma manuscrita es algo que sé o algo que soy? ¿O ambas cosas?).

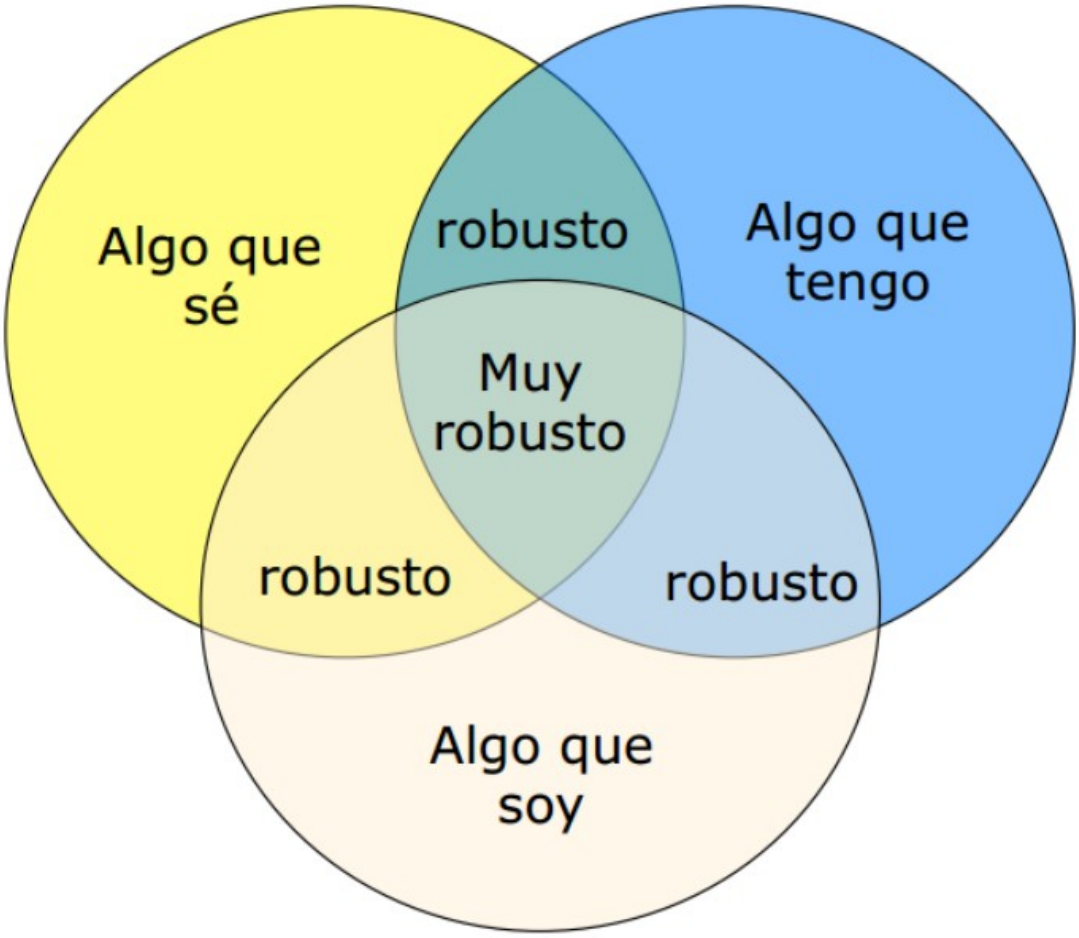

Figura 2. Diagrama de Venn que muestra la seguridad de un sistema de autenticación multifactor [12].

La fortaleza de estos sistemas queda bien definida por la anterior Figura, que muestra de forma gráfica cuán seguro es un sistema MFA mediante un diagrama de Venn.

De entre todos los posibles mecanismos de autenticación múltiple, el más usado es el segundo factor de autenticación, que implica el uso de dos de los factores anteriormente descritos. Se se suele conocer por el acrónimo 2FA (por sus siglas en ingles).

Por ejemplo, cuando una persona acude a un cajero automático a retirar dinero mediante el uso de una tarjeta de crédito, en realidad se está autenticando ante el banco con un mecanismo de 2FA, ya que combina algo que sólo el usuario tiene (una tarjeta de plástico personalizada), con algo que sólo el usuario sabe (el PIN de la tarjeta).

5.2 Autenticación fuerte vs. Autenticación multi-factor

Otro de los términos relacionados con la autenticación que a menudo es confundido con un mecanismo de MFA es el de "autenticación fuerte" (o *strong authentication* en inglés). Si bien este mecanismo supone una autenticación en varios pasos, éstos no deben mezclar necesariamente elementos de diferentes factores de autenticación.

5.3 Tipos de sistemas de autenticación multi-factor

Los métodos disponibles para establecer un sistema de autenticación múltiple pasan por una combinación de los ya expuestos en el epígrafe 4.2 de este documento, de forma que se consiga involucrar, al menos, a dos de los factores de autenticación expuestos.

Por ejemplo, un primer paso podría consistir en la presentación ante el sistema de los ya clásicos usuario/contraseña (algo que el usuario sabe), y continuar con un segundo paso que consista en introducir un código de un sólo uso que le haya llegado al usuario en forma de SMS a su teléfono móvil (algo que el usuario posee).

Como queda patente, la casuística es enorme, existiendo multitud de combinaciones para poder implementar un sistema de autenticación múltiple.

6 ESTADO DEL ARTE

En este epígrafe se pretende dar al lector una visión de las alternativas presentes en el mercado para implementar un sistema de autenticación múltiple. Nos centraremos en los sistemas 2FA (por ser los más extendidos) y dentro de éstos en los más usados.

6.1 Tokens físicos o por SMS

Supone la tenencia de un dispositivo físico que genere códigos de tipo OTP (One Time Password). Al tratarse de un dispositivo, se engloba dentro del factor de autenticación "algo que sólo el usuario tiene" y se debe combinar con algún otro factor de autenticación (generalmente algo que el usuario sabe, como una contraseña).

Figura 3. Token de seguridad de la firma RSA [15].

Dada la evolución de los tecnologías actuales, el dispositivo físico ha ido desapareciendo paulatinamente para dejar paso a sistemas que involucren, de una u otra forma, al teléfono móvil del usuario. Un ejemplo sería la recepción de códigos de verificación mediante el envío de mensajes SMS. Este último tipo de token suele ser uno de los sistemas más empleados por las entidades bancarias, si bien sus problemas de seguridad han llevado al NIST americano a desaconsejar su uso [16].

6.2 Google Authenticator

La evolución natural de los tokens físicos, pero sin el peligro de usar la red de telefonía móvil para enviar los códigos OTP, consiste en el uso de una app en el propio teléfono del usuario. Con este propósito surgió Google Authenticator.

Si bien en un principio fue desarrollado por el gigante de Mountain View para el uso en sus propias aplicaciones y servicios online, su app para smartphones es gratuita y el código fuente fue liberado, lo que permitió que haya sido implantado en multitud de aplicaciones y servicios (algunos de ellos que nada tienen que ver con el propio Google).

Su funcionamiento se basa en la generación de contraseñas de un sólo uso de tipo TOTP (*Time-based One-Time Password*), es decir, que para generar los códigos se usa una clave secreta precompartida y el instante de tiempo actual. La generación de dichos códigos debe realizarse tanto en el lado del servidor como en el lado del cliente y, posteriormente, comprobar que coinciden. Este mecanismo viene definido en el RFC 6238 del IETF y es uno de los más usados actualmente (en detrimento de sistemas HOTP). No sólo es empleado por la aplicación de Google, ya que otros fabricantes también hacen uso de este estándar.

Podemos resumir el funcionamiento de este sistema de segundo factor de autenticación en la siguiente Figura:

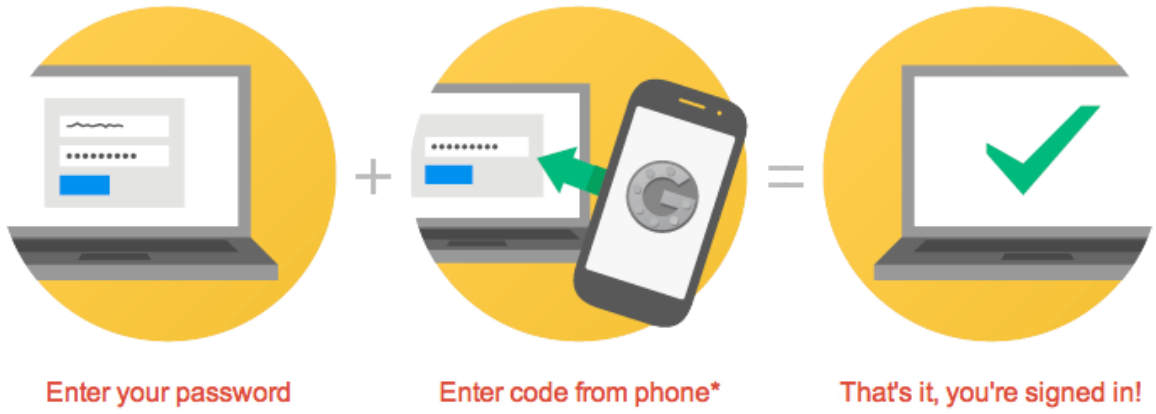

Figura 4. Funcionamiento del sistema 2FA basado en Google Authenticator [19].

Esto es, una vez proporcionado un factor de autenticación basado en conocimiento, como es el clásico usuario/contraseña, el usuario debe proporcionar el código que le indica la app Google Authenticator de su teléfono móvil.

Para ello, obviamente, el usuario ha debido configurar previamente Google Authenticator en el servicio o aplicación en el que lo desea usar. Esto es, se ha debido generar una clave secreta que será compartida por dicho servicio o aplicación y por la app Google Authenticator del teléfono móvil del usuario. Este esquema puede verse en la siguiente Figura:

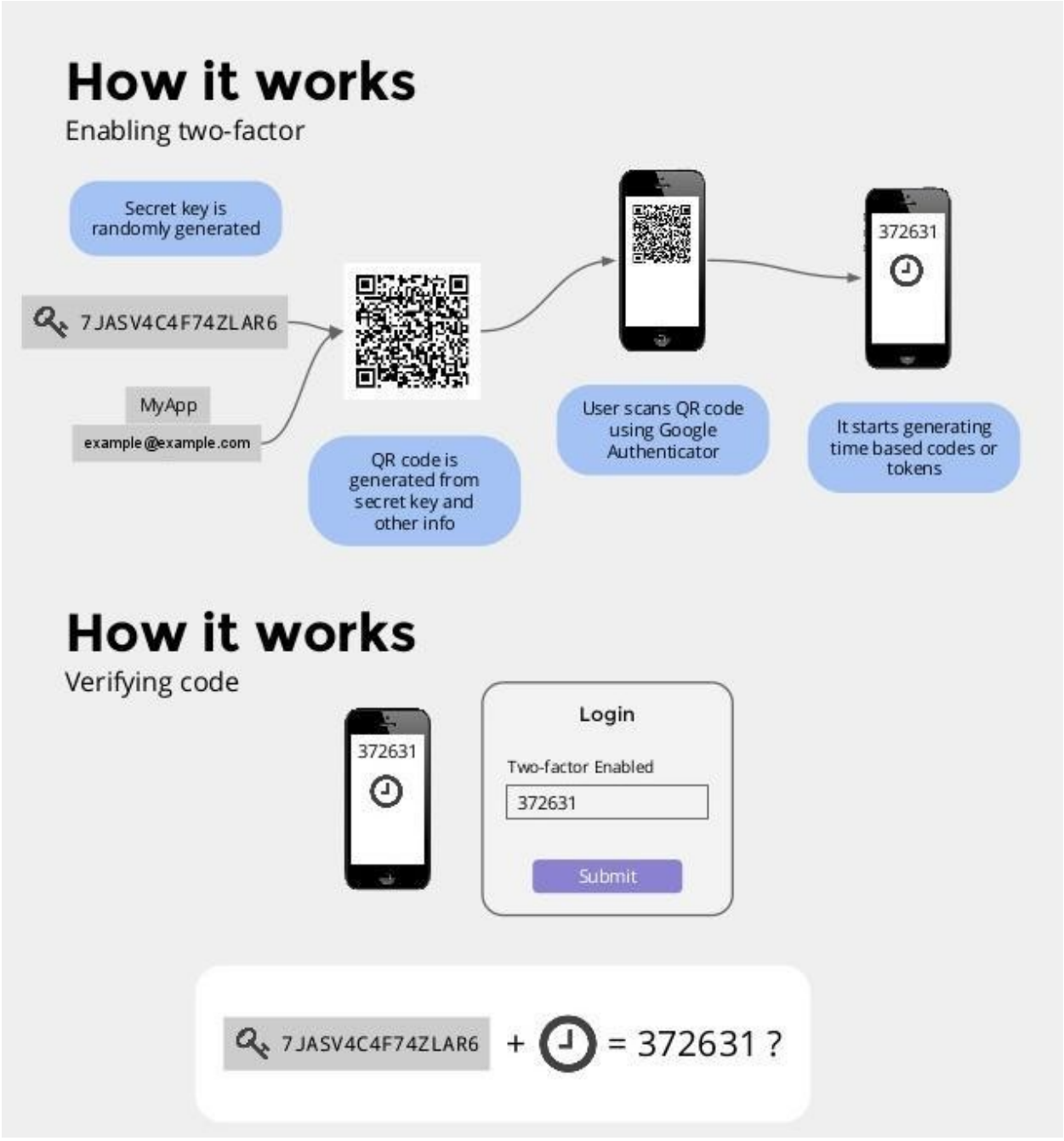

Figura 5. Configuración y uso de un 2FA en Google Authenticator [20].

6.3 Latch

Latch es un producto comercial de la empresa de seguridad española Eleven Paths (filial del grupo Telefónica).

Pese a que el concepto es el mismo, el uso de un factor de autenticación múltiple, se le da una vuelta de tuerca más a las tecnologías actuales, ya que no se trata exactamente de un sistema de generación de tokens mediante mecanismos TOTP como sus competidoras[1], sino que pretende trasladar al mundo digital el concepto de "pestillo de seguridad".

Esto es, pretende emular el tradicional pestillo de las puertas, de tal forma que, pese a que alguien tenga la llave que abre el cerrojo, si el pestillo está echado, no se pueda abrir la puerta. Y no sólo eso, sino que alertará a la persona que ha echado el pestillo de que alguien ha intentado entrar.

Para poder usar Latch debemos darnos de alta en la página que la empresa ha habilitado al efecto [20], tanto si vamos a usar el servicio como usuarios o como desarrolladores. Además, si nuestro rol es el de usuario es necesario descargar una app para nuestro terminal móvil.

Al igual que en Google Authenticator se requiere que el servicio online y la app para el terminal móvil compartan una clave, en Latch se requiere que un usuario realice un pareado de su cuenta con el servicio online que quiere proteger. El principio es el mismo, proporcionar un token a la aplicación web para que ésta dé al usuario de alta en el sistema Latch. Lo interesante llega tras haber pareado la cuenta, puesto que en ese instante simplemente tendremos un "pestillo virtual" que podremos deslizar para que cierre o abra los servicios online que tenemos asociados. Ya no será necesario enviar un token de autenticación cada vez que queramos ingresar en una aplicación web protegida.

Figura 6. Funcionamiento del sistema Latch desde el punto de vista del usuario [22].

1 Recientemente la app ha incorporado también la posibilidad de generar tokens TOTP.

Si con Latch no se envían tokens de autenticación entre el usuario y la aplicación o sistema, ¿cómo sabe dicha aplicación o sistema si debe validar o no al usuario? La respuesta a esta pregunta se halla en la siguiente Figura:

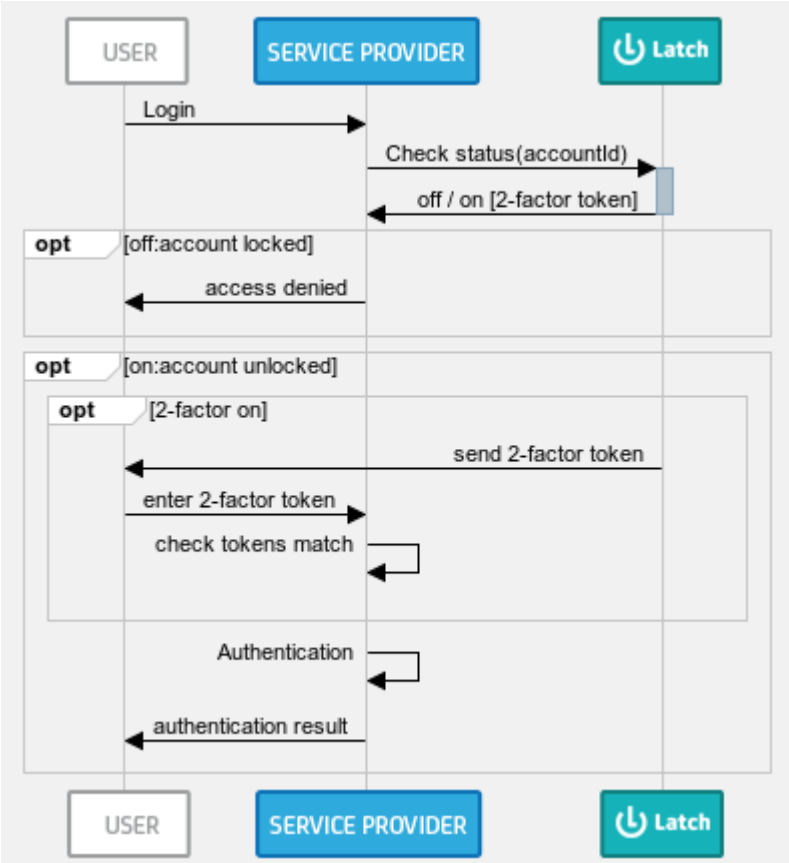

Figura 7. Diagrama de comprobación del estado de un usuario en Latch [23].

Como se puede observar, el primer paso consiste en una autenticación mediante un factor de conocimiento (login). Después se interroga al servidor de la empresa Eleven Paths para conocer si dicha cuenta tiene configurado el servicio y, en caso de ser así, si se le debe permitir el acceso o denegárselo. Dicha situación no es estática, ya que el propio usuario puede "echar o quitar el pestillo digital" en cualquier momento desde la app de su dispositivo móvil.

Como curiosidad acerca de la potencia del sistema, desde AndalucíaCERT no queremos dejar pasar la ocasión de mencionar el proyecto Lacth ARW [24] [25], que supone la creación de una nueva herramienta para prevenir los efectos del ransomware. Para ello se monitorizan las operaciones Entrada/Salida de un sistema Microsoft Windows para identificar si se producen sobre una carpeta protegida y si son de escritura o borrado. Obviamente, será Latch quien indicará si dichas operaciones están permitidas o no.

6.4 Otros sistemas

Una vez detallado el funcionamiento de las opciones más relevantes del panorama actual en cuanto al uso de un mecanismo 2FA, se quiere recordar al lector la existencia de otras alternativas:

- FreeOTP: Solución para la generación de códigos OTP implementada por la empresa Red Hat. Su funcionamiento es similar a Google Authenticator.

- Authy: Usa un mecanismo similar a Google Authenticator para la generación de códigos TOTP, pero añade ciertas funciones de seguimiento y auditoría para las cuentas que usen el servicio.

- Touch ID de Apple: Los sistemas de autenticación biométrica se llevan empleando desde hace años, siendo el más común el lector de huellas dactilares. La compañía de la manzana simplemente ha añadido la electrónica necesaria a sus teléfonos inteligentes para lograr implementar esta funcionalidad.

- Autenticación basada en un certificado digital: No nos estamos refiriendo a que un servidor web presente un certificado digital al usuario para probar que es un sitio legítimo, sino a que sea un usuario el que presente un certificado digital a la aplicación o sistema contra el que se quiere autenticar.

- Yubikey: Se trata de dispositivo físico en forma de pendrive (o llave USB) fabricado por la empresa Yubico y que soporta el estándar *Universas 2nd Factor* (U2F) definido por la FIDO Alliance. Para que cumpla su cometido es necesario "pinchar" dicho dispositivo en el equipo desde el que nos estamos autenticando.

Figura 8. Llave USB Yubikey usada a modo de llavero.

6.5 Comparativa

A continuación se muestra una pequeña tabla que recoge, a modo de resumen, las principales características de los sistemas anteriormente mencionados:

	Tokens físicos/SMS	GAuthenticator	Latch	Biometría	PKI
Comercial/Gratuito	Comercial	Gratuito	Comercial	Comercial	Comercial/Gratuito[2]
¿Depende de un tercero de confianza?	No/Sí[3]	No	Sí	No	Sí
Uso muy extendido	Sí	Sí	No	No	No

Tabla 1. Comparativa con las principales soluciones de autenticación mencionadas.

7 RECOMENDACIONES DE SEGURIDAD SOBRE EL PROCESO DE AUTENTICACIÓN

Para concluir este informe divulgativo, desde AndalucíaCERT se realizan algunos comentarios y recomendaciones de seguridad al lector:

- El proceso de autenticación es de vital importancia, por lo que es necesario disponer de diversos métodos para verificar la identidad de los usuarios. Si alguno de dichos métodos involucra el uso de un esquema usuario/contraseña, es recomendable usar siempre contraseñas robustas y tener una diferente para cada aplicación o servicio. En este sentido será de gran utilidad el uso de gestores de contraseñas como LastPass, 1Password o KeePass.

- Por supuesto, el usuario deberá ser consciente de ante qué aplicación o sistema se está autenticando. Uno de los métodos más habituales para el robo de credenciales consiste en presentar una aplicación falsa al usuario para que éste proporcione sus datos, por lo que se insta al lector a realizar pequeñas comprobaciones de seguridad, como verificar la URL o el certificado del sitio web contra el que se autentica.

- Si el sistema o aplicación lo permiten, configurar siempre el uso de un segundo factor de autenticación. Cuál de ellos usar dependerá de los métodos ofertados y las preferencias personales de cada usuario.

2 Aunque la mayoría de las soluciones de PKI suponen la confianza en una autoridad de certificación externa que factura por sus servicios, también es posible que uno mismo se monte la suya, en cuyo caso no tendría coste.

3 Si el token es un dispositivo físico que acompaña al usuario, no se depende de un tercero. No obstante, en el caso de mensajes SMS recibidos en el smartphone, éstos deben ser generados y enviados por un tercero.

- Desde el punto de vista de los desarrolladores, nos gustaría recordar que la seguridad debe ser tenida en cuanta en todas las fases del desarrollo del proyecto, por lo que sería interesante plantearse ya desde el comienzo qué mecanismos de autenticación se ofertarán al usuario y contemplar el uso de un sistema de autenticación MFA.

8 GLOSARIO

2FA: Acrónimo de la expresión inglesa *Two-Factor Authentication*. Hace referencia al uso de un Segundo Factor de autenticación, esto es, utilizar de forma conjunta dos de los tres factores descritos en un sistema de autenticación multifactor.

AAA: Acrónimo de la expresión inglesa *Authentication, Authorization and Accounting*. Hace referencia a las familias de protocolos que ofrecen servicios de autenticación, autorización y contabilidad.

AAAA: Acrónimo de la expresión inglesa *Authentication, Authorization, Accounting and Audit*. Viene a ser lo mismo que el servicio de identidad ofertado por los protocolos AAA, pero añadiendo una fase de auditoría.

app: Contracción de *application* (aplicación en inglés). Suele hacer referencia a las aplicaciones especialmente diseñadas para teléfonos móviles.

autenticación: Proceso por el que un cliente prueba su identidad frente a una entidad (normalmente una aplicación o sistema).

certificado: Un certificado digital es un fichero informático generado por una entidad de servicios de certificación que asocia unos datos de identidad a una persona física, organismo o empresa, confirmando de esta manera su identidad digital en Internet.

código QR: Se trata de una imagen que almacena información en una matriz de puntos o en un código de barras bidimensional.

FA: Factor de autenticación. Los tres tipos existentes y en los que se basan los sistemas de autenticación son: algo que el usuario sabe, algo que el usuario tiene y algo que el usuario es.

FIDO Alliance: Acrónimo de *Fast Identify Online Alliance*. Se trata de un consorcio industrial creado en el año 2013 y que busca la interoperabilidad entre sistemas de autenticación fuerte.

GAuthenticator: Acrónimo de *Google Authenticator*. Software desarrollado por la empresa Google para implementar la autenticación basada en contraseñas de un sólo uso.

hash: Función resumen o *digest*. Hace uso de funciones matemáticas para generar un resumen o huella de tamaño fijo, de un recurso de tamaño arbitrario. Su bondad reside en que un mismo recurso siempre generará la misma huella y una pequeña modificación del mismo resultará en una huella completamente distinta. Además, las funciones hash no son reversibles, esto es, partiendo de una huella digital, nunca será posible obtener el recurso del que se ha obtenido dicha huella.

HOTP: Acrónimo de *HMAC-based One-Time Password*. Donde HMAC significa *Hash-based message authentication*. Contraseña de un sólo uso que consiste en la aplicación de una función de hash a una clave precompartida.

identidad: Conjunto de atributos que describen de forma unívoca a una persona en un contexto determinado.

IETF: Acrónimo de *Internet Engineering Task Force*. Organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet. Se encarga de regular las propuestas y los estándares de Internet.

Latch: Solución propietaria de la empresa ElevenPaths para implementar un mecanismo de 2FA.

market: Repositorio de aplicaciones para dispositivos móviles. Aunque existen diversos tipos, sólo se recomienda el uso de aquellos que sean oficiales, como Google Play y App Store.

MFA: Acrónimo de la expresión inglesa *Multi-Factor Authentication*. Un factor de autenticación múltiple consiste en una aproximación a la seguridad en el proceso de autenticación del usuario que requiere de la presentación de dos o más elementos de los siguientes tres elementos de autenticación: un factor de conocimiento (algo que sólo el usuario sabe), un factor de posesión (algo que sólo el usuario posee), y un factor inherente al usuario (algo que sólo el usuario es).

NIST: Acrónimo de la expresión *National Institute of Standards and Technology*. Es una agencia del Gobierno de USA cuya misión es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología.

OTP: Acrónimo de la expresión inglesa *One-Time Password*. Contraseña de un sólo uso, esto es, un secreto que sólo será válido en un instante de tiempo determinado, impidiendo que pueda ser reutilizado.

pendrive: Dispositivo de almacenamiento que incluye en su interior una memoria de tipo flash y una interfaz USB.

PIN: Acrónimo de la expresión inglesa *Personal Identification Number*. Contraseña que consiste únicamente en números, generalmente, de longitud corta.

PKI: Acrónimo de *Public Key Infraestructure*. Se trata de una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas (cifrado, firma digital, no repudio...).

RFC: Acrónimo de la expresión *Request For Comments*. Consiste en una serie de publicaciones del grupo de trabajo de Internet (IETF) que describen diversos aspectos del funcionamiento de Internet y otras redes de computadoras, como protocolos, procedimientos, etc. y comentarios e ideas sobre estos.

smartphone: Teléfono móvil inteligente o de última generación.

SMS: Acrónimo de la expresión inglesa *Short Message Service*. Sistema de mensajes de texto para teléfonos móviles.

sniffing: Proceso de capturar y analizar el tráfico de una red de comunicaciones.

TOTP: Acrónimo de la expresión *Time-based One-Time Password*. Contraseña de un sólo uso que usa una clave secreta precompartida y el instante de tiempo actual para generar los códigos de verificación.

Touch ID: Sistema de reconocimiento de huellas dactilares diseñado por la compañía Apple e incorporado en sus smartphones.

U2F: Acrónimo de la expresión inglesa *Universal 2nd Factor*. Se trata de un estándar de autenticación abierto que simplifica la implementación de un segundo factor de autenticación mediante el uso de dispositivos físicos de tipo USB o NFC..

USB: Acrónimo de la expresión inglesa *Universal Serial Bus*. Se trata de un estándar desarrollado en los años '90 y que define un protocolo de comunicaciones ampliamente extendido.

9 DOCUMENTACION DE REFERENCIA

[1] Editores de Wikipedia. <<*Protocolo AAA*>>. Wikipedia, la enciclopedia libre. Disponible en línea: https://es.wikipedia.org/wiki/Protocolo_AAA (Fecha de consulta, 27/10/2016).

[2] Editores de Wikipedia. <<*Auditoría informática*>>. Wikipedia, la enciclopedia libre. Disponible en línea: https://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica (Fecha de consulta, 03/11/2016).

[3] ネットワークエンジニアとして. <<*AAA (Authentication Authorization Accounting)*>>. Figura basada en la imagen con derechos de autor disponible en http://www.infraexpert.com/study/aaa.htm (Fecha de consulta, 03/11/2016).

[4] Personal del SANS Institute. <<*An Overview of Different Authentication Methods and Protocols*>>. SANS Institute. Disponible en línea: https://www.sans.org/reading-room/whitepapers/authentication/overview-authentication-methods-protocols-118 (Fecha de consulta, 04/11/2016).

[5] Editores de Wikipedia. <<*Prueba de conocimiento cero*>>. Wikipedia, la enciclopedia libre. Disponible en línea: https://es.wikipedia.org/wiki/Prueba_de_conocimiento_cero (Fecha de consulta, 04/11/2016).

[6] Editores de Wikipedia. <<*Diffie-Hellman*>>. Wikipedia, la enciclopedia libre. Disponible en línea: https://es.wikipedia.org/wiki/Diffie-Hellman (Fecha de consulta, 04/11/2016).

[7] Editores de Wikipedia. <<*Multi-factor authentication*>>. Wikipedia, la enciclopedia libre. Disponible en línea: https://en.wikipedia.org/wiki/Multi-factor_authentication (Fecha de consulta, 04/11/2016).

[8] Bob Lord. <<*An Important Message About Yahoo User Security*>>. Yahoo! Disponible en línea: https://yahoo.tumblr.com/post/150781911849/an-important-message-about-yahoo-user-security (Fecha de consulta, 04/11/2016).

[9] Redactores de La Vanguardia. <<*Sony investiga el robo de datos de 77 millones de cuentas de PlayStation*>> Diario La Vanguardia, 2011. Disponible en línea: http://www.lavanguardia.com/internet/20110427/54146138829/sony-investiga-el-robo-de-datos-de-77-millones-de-cuentas-de-playstation.html (Fecha de consulta, 04/11/2016).

[10] Redactores de CincoDías. <<*El robo de fotos siembra dudas sobre la seguridad del iCloud*>>. Diario Cinco Días, 2014. Disponible en línea: http://cincodias.com/cincodias/2014/09/02/tecnologia/1409685127_337743.html (Fecha de consulta, 04/11/2016).

[11] Brian Kee. <<*PCI DSS Requirement 8.3: What is two-factor authentication, and when is it required?*>>. SecureWorks, 2013. Disponible en línea: https://www.secureworks.com/blog/general-pci-dss-two-factor-authentication (Fecha de consulta, 04/11/2016).

[12] Juan Manuel Vozmediano Torres. <<*Introducción a la seguridad e identificación digital. Módulo 1 del Máster en Seguridad de la Información y las Comunicaciones*>>. Figura extraída de la imagen con derechos de autor presente en el texto referenciado. Universidad de Sevilla, 2014.

[13] Editores de Wikipedia. <<*Strong authentication*>>. Wikipedia, la enciclopedia libre. Disponible en línea: https://en.wikipedia.org/wiki/Strong_authentication (Fecha de consulta, 04/11/2016).

[14] Paul A. Grassi, James L. Fenton, Elaine M. Newton y otros. <<*DRAFT NIST Special Publication 800-63B- Digital Authentication Guideline*>>. National Institute of Standars and Technology (NIST). Disponible en línea: https://pages.nist.gov/800-63-3/sp800-63b.html (Fecha de consulta 04/11/2016).

[15] Editores de Wikipedia. <<*Token de seguridad*>>. Wikipedia, la enciclopedia libre. Figura extraída de la imagen disponible en línea: https://es.wikipedia.org/wiki/Token_de_seguridad (Fecha de consulta, 04/11/2016).

[16] Bruce Schneier. <<*NIST is No Longer Recommending Two-Factor Authentication Using SMS*>>. Schneier on Security, 2016. Disponible en línea: https://www.schneier.com/blog/archives/2016/08/nist_is_no_long.html (Fecha de consulta, 04/11/2016).

[17] Trabajadores de Google. <<*Instalar Google Authenticator*>>. Ayuda de Cuentas de Google, 2016. Disponible en línea: https://support.google.com/accounts/answer/1066447?rd=1 (Fecha de consulta, 04/11/2016).

[18] D. M'Raihi, Verisign Inc., S. Machani, Diversinet Corp., M. Pei, Symantec, J Rydell y Portwise Inc. <<*RFC 6238. TOTP: Time-Based One-Time Password Algorithm*>> Internet Engineering Task Force (IETF). Disponible en línea: https://tools.ietf.org/html/rfc6238 (Fecha de consulta: 04/11/2016).

[19] Jeff Skinner. <<*Two-Factor Authentication via Google Authenticator*>>. Jeff's Skinner Box, 2015. Figura basada en la imagen con derechos de autor disponible en http://jeffskinnerbox.me/posts/2015/Nov/28/two-factor-authentication-via-google-authenticator/ (Fecha de consulta, 04/11/2016).

[20] Allan Denot. <<*Two factor authentication with Laravel and Google Authenticator*>>. SlideShare. Imagen con derechos de autor extraída de la presentación disponible en http://www.slideshare.net/allandenot/two-factor-authentication-with-laravel-and-google-authenticator (Fecha de consulta, 04/11/2016).

[21] Personal de Eleven Paths. <<*Latch. Sign up as a user*>>. Web Oficial de Latch, 2016. Disponible en línea: https://latch.elevenpaths.com/www/register (Fecha de consulta, 04/11/2016).

[22] Personal de Eleven Paths. <<*Cómo funciona*>>. Web oficial de Latch, 2016. Imagen con derechos de autor disponible en https://latch.elevenpaths.com/www/how.html (Fecha de consulta, 04/11/2016).

[23] Comunidad de Eleven Paths. <<*Latch Docs*>>. We oficial de Latch, 2016. Iamgen con derechos de autor disponible en https://community.elevenpaths.com/elevenpaths/category_sets/latch_119o0t (Fecha de consulta, 07/11/2016).

[24] Chema Alonso. <<*Latch ARW: Una nueva herramienta contra el Ransomware*>>. Latch Community Home, 2016. Disponible en línea: https://community.elevenpaths.com/elevenpaths/topics/latch-arw-una-nueva-herramienta-contra-el-ransomware (Fecha de consulta, 07/11/2016).

[25] Chema Alonso. <<*Latch ARW: Una nueva herramienta contra el Ransomware #Ransomware @elevenpaths #Latch*>>. Un informático en el lado del mal, 2016. Disponible en línea: http://www.elladodelmal.com/2016/10/latch-arw-una-nueva-herramienta-contra.html (Fecha de consulta, 07/11/2016).

[26] Aaron Woland. <<*Simply put: How does certificate-based authentication work?*>>. NetworkWorld, 2014. Disponible en línea: http://www.networkworld.com/article/2226498/infrastructure-management/simply-put-how-does-certificate-based-authentication-work.html (Fecha de consulta, 08/11/2016).