

PROTOCOLO ■■■
PROVINCIAL DE CIBERSEGURIDAD

Estándar de Autenticación de Tokens

03
CAPÍTULO



Estándar de Autenticación de Tokens

1.0 Propósito y Beneficios

El propósito de este estándar es enumerar los tokens de autenticación apropiados que se pueden usar con sistemas desarrollados u operados que requieren acceso autenticado según el Nivel de garantía del autenticador (AAL). Este documento también proporciona los requisitos para la gestión de esos dispositivos de autenticación.

2.0 Alcance

Esta norma se aplica a la autenticación de cuentas que acceden a sistemas de tecnología de la información con el fin de realizar actividades administrativas gubernamentales de forma electrónica.

3.0 Declaración de información

3.1 NIVELES DE GARANTÍA Y TIPOS DE TOKENS REQUERIDOS

El Nivel de Garantía del Autenticador (AAL) de un sistema determina el grado de certeza requerido al autenticar a un usuario. La siguiente tabla describe el nivel de confianza asociado con cada AAL. Estos niveles de garantía son consistentes con los establecidos por NIST¹.

¹ Descrito en la publicación especial del NIST 800-63-3: Pautas de identidad digital

Nivel de garantía del autenticador (AAL)	
AAL1	AAL1 proporciona cierta seguridad de que el usuario controla un “autenticador” vinculado a la cuenta gubernamental. AAL1 requiere autenticación de factor único (por ejemplo, contraseña) o de múltiples factores (por ejemplo, contraseña + token) utilizando los métodos de autenticación disponibles. Una autenticación exitosa requiere que la persona que inicia sesión demuestre la posesión y/o el control del autenticador, a través de un protocolo de autenticación seguro como se define en el Estándar de encriptación.
AAL2	AAL2 proporciona una alta confianza en que el usuario controla los autenticadores vinculados a la cuenta gubernamental. Se requiere prueba de posesión y control de dos factores de autenticación distintos (multifactor) a través de protocolos de autenticación seguros. Se requieren técnicas criptográficas aprobadas, tal como se define en el Estándar de cifrado en AAL2 y superiores.
AAL3	AAL3 proporciona una confianza muy alta en que el usuario controla los autenticadores vinculados a la cuenta gubernamental. La autenticación en AAL3 se basa en la prueba de posesión de una clave mediante un protocolo criptográfico. La autenticación AAL3 debe utilizar un autenticador criptográfico basado en hardware y un autenticador que proporcione resistencia a la suplantación del verificador; el mismo dispositivo puede cumplir ambos requisitos. Para autenticarse en AAL3, los usuarios deben demostrar la posesión y el control de dos factores de autenticación distintos a través de protocolos de autenticación seguros. Se requieren técnicas criptográficas aprobadas.

La Cartera Administrativa debe identificar el nivel de aseguramiento apropiado para cada sistema. Cada nivel de seguridad requiere diferentes tokens de autenticación que incorporan uno o más factores de autenticación (es decir, algo que usted sabe, algo que tiene y algo que es). Los niveles de garantía del autenticador (AAL) 1 y 2 requieren autenticación de un solo factor. AAL 3 requiere autenticación multifactor.

Las reparticiones deben elegir los tipos de token apropiados para su nivel de seguridad de las Tablas 1 o 2. La Tabla 1 muestra el nivel de seguridad máximo que se puede lograr con un solo tipo de token.

Tabla 1: Opciones de un solo token

Tipos de tokens	AAL1	AAL2	AAL3
Token secreto memorizado	X		
Token de secretos de búsqueda (Look-Up Secrets)	X		
Token fuera de banda	X		
Dispositivo de contraseña de un solo uso	X		
Dispositivo criptográfico de factor único	X		
Dispositivo criptográfico de software multifactor		X	
Dispositivo de hardware de contraseña única de factor múltiple		X	
Dispositivo criptográfico de hardware multifactor			X

Las reparticiones pueden usar autenticación de múltiples tokens (es decir, una combinación de tokens) para mejorar el nivel general de seguridad como se muestra en la Tabla 2. Por ejemplo, AAL3 se puede lograr usando dos tokens clasificados en AAL2 que representan dos factores de autenticación diferentes (es decir, algo que sabes, algo que tienes y algo que eres).

Tabla 2: Opciones de múltiples tokens

AL 2	AL 3	
<p>AAL 2 requiere que, una combinación de autenticadores de un solo factor incluya un autenticador secreto memorizado y un segundo factor basado en la posesión de alguna de las opciones de la siguiente lista:</p> <ul style="list-style-type: none"> • Secretos de búsqueda • Dispositivo fuera de banda • Dispositivo OTP de factor único • Software criptográfico de factor único • Dispositivo criptográfico de factor único 	<p>AAL 3 requiere el uso de una de las siguientes combinaciones de autenticadores:</p>	
	<p>1. Secreto memorizado</p>	<ul style="list-style-type: none"> • Dispositivo criptográfico de factor único
	<p>2. Dispositivo OTP multifactor (software y/o hardware)</p>	<ul style="list-style-type: none"> • Dispositivo criptográfico de factor único
	<p>3. Dispositivo OTP de factor único (solo hardware)</p>	<ul style="list-style-type: none"> • Autenticador de software criptográfico multifactor
<p>4. Dispositivo OTP de factor único (solo hardware)</p>	<ul style="list-style-type: none"> • Autenticador de software criptográfico de factor único • Secreto memorizado 	

3.2 TIPOS DE TOKENS DE AUTENTICACIÓN

3.2.1 Token secreto memorizado

Un token secreto memorizado “es algo que sabes”. Los tokens secretos memorizados suelen ser claves que combinan caracteres y números. Los ejemplos incluyen contraseñas, frases de contraseña y números de identificación personal (PIN).

Normalmente, se utiliza un token secreto memorizado por sí solo para AAL 1. En AAL 2 y 3 **requieren** autenticación multifactor. Cuando se utiliza un token secreto memorizado como uno de los factores en una solución de autenticación multifactor, se aplican los requisitos del token en la AAL asociada.

La siguiente tabla aborda los requisitos mínimos básicos relacionados con los tokens secretos memorizados. Otros cumplimientos de seguridad, pueden necesitar requisitos mínimos más estrictos. Se deben consultar los apartados de cumplimiento relevantes para abordar sistemas, aplicaciones, etc.

Tabla 3: Requisitos mínimos del token secreto memorizado

Categoría	Niveles de garantía		
	1	2 ²	3
Estándares de gestión de contraseñas			
Caducidad de la contraseña después de x días	731	183	Se requiere autenticación multifactor Este tipo de token solo se puede utilizar con autenticadores seleccionados en AAL 2 y 3. Consulte la Tabla 2 para obtener más información.
Sistema para proporcionar mensajes de caducidad de contraseña que comiencen al menos x días antes de la caducidad	14		
Reutilización de contraseña	Después de 24 contraseñas únicas		
Edad mínima de la contraseña	2 días		
Número máximo de inicios de sesión de gracia después del vencimiento, para permitir el cambio de contraseña	1		
Las contraseñas temporales se cambiaron inmediatamente en el primer inicio de sesión	Sí		
Estándares de composición de contraseñas³			
La contraseña no debe ser la misma que el ID de usuario.	Sí		Se requiere autenticación multifactor Este tipo de token solo se puede utilizar con autenticadores seleccionados en AAL 2 y 3. Consulte la Tabla 2 para obtener más información.
Longitud mínima	14		
Número máximo de caracteres repetidos	3		
Número mínimo de letras mayúsculas	1		
Número mínimo de letras minúsculas	1		
Número mínimo de letras	3		
Número mínimo de números	1		
Número mínimo de caracteres especiales	1		

2 Cuando se utiliza una solución multifactor para AAL2 y AAL3, según sea necesario, y uno de los factores es un secreto memorizado, se aplican los estándares AAL2.

3 Se reconoce que no todos los sistemas podrán hacer cumplir todos estos estándares. En esos casos, se puede solicitar una solicitud de excepción al Director de Seguridad de la Información (CISO).

3.2.2 Look-Up Secrets

Es un método utilizado para recuperar un acceso perdido. Un secreto de búsqueda es algo que tienes. Es un registro físico o electrónico que almacena un conjunto de datos privados que se comparten entre el usuario y el CSP. El autenticador se utiliza para buscar los datos privados apropiados necesarios para responder a un mensaje del verificador. Un ejemplo es el uso de preguntas y respuestas privadas (secretas) permitiendo acceder a la “clave de recuperación” en caso de que el autenticador se pierda, se olvide o no funcione correctamente.

Los secretos de búsqueda se utilizan comúnmente en AAL 1. En los casos de AAL 2 y 3 requieren autenticación multifactor. Cuando se combina con un secreto memorizado, se aplican las reglas de AAL 2.

Requisitos del autenticador: los secretos de búsqueda deben tener al menos 4 caracteres y deben distribuirse a través de un canal seguro.

3.2.3 Token fuera de banda (OOB)

Los tokens OOB son algo que tienes. Son una combinación de un dispositivo físico (p. ej., teléfono celular, PDA, buscapersonas, línea fija) y un secreto que un verificador transmite al dispositivo a través de un canal de comunicaciones distinto para un uso único.

Un ejemplo de un token OOB sería un usuario que inicia sesión en un sitio web y recibe un mensaje de texto o una llamada telefónica en su teléfono celular (pre-registrado con el Proveedor de servicios de credenciales (CSP) durante la fase de registro) con un autenticador aleatorio que se presentará, como parte del protocolo de autenticación. El correo electrónico no se puede utilizar para transmitir el autenticador aleatorio para el dispositivo OOB.

Requisitos del autenticador: el usuario debe poseer y controlar el dispositivo y debe ser direccionable de forma única. El autenticador debe establecer un canal separado con el verificador para recuperar el secreto fuera de banda o la solicitud de autenticación. El canal secundario se considera fuera de banda (incluso si termina en el mismo dispositivo) si el dispositivo no filtra información de un canal al otro sin autorización del usuario.

El uso de la Red Telefónica Pública Conmutada (PSTN) está restringido a menos que el número de teléfono registrado previamente en uso esté asociado con un dispositivo físico específico. Cambiar el número de teléfono prerregistrado equivale a vincular un nuevo autenticador y debe seguir los requisitos aplicables. No se debe utilizar el protocolo de voz sobre Internet (VOIP) ni el correo electrónico para la autenticación OOB.

Requisitos del token: el usuario debe poseer y controlar el token, debe ser direccionable de forma única y debe admitir la comunicación a través de un canal/protocolo independiente del canal/protocolo principal para la autenticación electrónica.

Direccionable de forma única significa que el token puede ser direccionado mediante una característica única (por ejemplo, número de teléfono).

Al acceder a una aplicación a través de un dispositivo móvil y utilizar un teléfono virtual y un sistema de gestión de comunicaciones (es decir, Google Voice), ese dispositivo móvil no será viable como token OOB ya que no existe un canal/protocolo separado para la comunicación del autenticador aleatorio.

Una limitación con el uso de tokens OOB es que, si el dispositivo está infectado, incluso si la comunicación ocurre a través de un canal/protocolo separado, ambas formas de autenticación (acceso a la aplicación y recepción del token) se ven comprometidas y, por lo tanto, toda comunicación no es confiable.

Requisitos del verificador: el período de tiempo máximo que puede existir un token OOB es de 10 minutos y solo se puede usar una vez. El secreto generado por el verificador debe tener como mínimo 3 caracteres; sin embargo, cualquier secreto de autenticación que tenga menos de 8 caracteres debe limitar el número de intentos fallidos de autenticación a no más de 10.

3.2.4 Dispositivo criptográfico de factor único (SF)

Los dispositivos criptográficos SF son algo que tienes. Es un dispositivo de hardware que realiza operaciones criptográficas en la entrada proporcionada al dispositivo. No requiere un segundo factor. Generalmente es un mensaje firmado. Un ejemplo sería un certificado de Secure Socket Layer/Transport Layer Services (SSL/TLS).

Requisitos del autenticador: los módulos criptográficos utilizados deberán estar validados en FIPS 140-2, Nivel 1 o superior. También se aceptan productos validados según versiones posteriores de FIPS 140.

Requisitos del verificador: la entrada (por ejemplo, un nonce o desafío) para generar el token tiene al menos 8 caracteres (64 bits de entropía) y debe ser única durante la vida útil del autenticador o estadísticamente única utilizando un generador de bits aleatorios aprobado. La verificación debe utilizar criptografía aprobada.

3.2.5 Dispositivo de contraseña de un solo uso (OTP) de factor único (SF)

Los dispositivos SF OTP son algo que tienes. Es un dispositivo de hardware que admite la generación espontánea de OTP. Este dispositivo tiene un secreto incorporado que se utiliza como “semilla” (seed) para la generación de OTP y no requiere activación a través de un segundo factor. La autenticación se logra proporcionando una OTP aceptable y demostrando así la posesión y el control del dispositivo por parte del usuario. El dispositivo se utiliza cada vez que se requiere autenticación.

Los ejemplos incluyen tokens de llavero. Un usuario intenta iniciar sesión en un sitio web y proporciona un código generado por token u OTP.

Requisitos del autenticador: se debe utilizar un cifrado de bloque aprobado o una función hash para combinar una clave simétrica almacenada en el dispositivo con un nonce para generar una OTP. El nonce puede ser una fecha y hora o un contador generado en el dispositivo.

Requisitos del verificador: la OTP tendrá una vida útil limitada, con un máximo de 2 minutos. El módulo criptográfico que realiza las funciones de verificador deberá estar validado en FIPS 140-2 Nivel 1 o superior. También se aceptan productos validados según versiones posteriores de FIPS 140.

3.2.6 Token criptográfico de software multifactor (MF)

Un token criptográfico del software MF es algo que usted tiene y debe ser desbloqueado por algo que conoce o por algo que es.

Es una clave criptográfica que se almacena en un disco o en algún otro medio “soft” y debe desbloquearse mediante un segundo factor de autenticación independiente del factor de autenticación utilizado para acceder al disco u otro medio “soft”.

La autenticación se logra demostrando la posesión y control de la clave. El token depende en gran medida del protocolo criptográfico específico, pero generalmente es algún tipo de mensaje firmado.

Un ejemplo sería un certificado criptográfico privado que se desbloquea mediante una frase de contraseña independiente de la que desbloquea el dispositivo en el que está almacenado el certificado. El certificado implementado en la estación de trabajo del usuario (algo que usted tiene) en combinación con una frase de contraseña (algo que conoce) proporciona autenticación multifactor. La contraseña para acceder al dispositivo no puede desbloquear automáticamente el certificado.

Requisitos del autenticador: el módulo criptográfico deberá estar validado en FIPS 140-2 Nivel 1 o superior. También se aceptan productos validados según versiones posteriores de FIPS 140. Cada autenticación requerirá el ingreso de la contraseña u otros datos de activación y la copia no cifrada de la clave de autenticación se borrará después de cada autenticación.

Requisitos del verificador: la entrada del token generado por el verificador (por ejemplo, un nonce o desafío) tiene al menos 8 caracteres (64 bits de entropía).

3.2.7 Dispositivo de contraseña de un solo uso (OTP) multifactor (MF)

Un dispositivo MF OTP es algo que usted tiene y debe ser desbloqueado por algo que conoce o por algo que es.

Es un dispositivo de hardware que genera OTP para usar en la autenticación y que debe desbloquearse mediante un segundo factor de autenticación. El segundo factor de autenticación se puede lograr a través de un teclado de entrada integral, un lector biométrico integral (por ejemplo, de huellas dactilares) o una interfaz directa de computadora (por ejemplo, un puerto USB).

La OTP generalmente se muestra en el dispositivo y se ingresa manualmente en el verificador como contraseña, aunque también se permite la entrada electrónica directa desde el dispositivo a una computadora.

Un ejemplo sería un token de llavero en combinación con un PIN. Un usuario intenta iniciar sesión en un sitio web y proporciona un PIN definido por el usuario (establecido cuando se asignó el token) y un código generado por el token. La combinación del PIN y el código generado por el token se denomina contraseña.

Requisitos del autenticador: el módulo criptográfico debe validarse en FIPS 140-2 Nivel 2 o superior y el token en sí debe cumplir con la seguridad física en FIPS 140-2 Nivel 3 o superior. Esto significa que el token es a prueba de manipulaciones; no se puede abrir para realizar ingeniería inversa u obtener un valor inicial, etc. Los productos validados según versiones posteriores de FIPS 140 también son aceptables. Consulte el Estándar de encriptación para obtener información adicional.

La OTP debe generarse utilizando un cifrado de bloque aprobado o una función hash para combinar una clave simétrica almacenada en un dispositivo de hardware personal con un nonce para generar una OTP. El nonce puede ser una fecha y hora o un contador generado en el dispositivo. Cada autenticación requerirá la introducción de una contraseña u otros datos de activación a través de un mecanismo de entrada integrado.

Requisitos del verificador: la OTP tendrá una vida útil limitada, con un máximo de 2 minutos.

3.2.8 Dispositivo criptográfico multifactor (MF)

Un dispositivo criptográfico MF es algo que usted tiene y debe ser desbloqueado por algo que conoce o por algo que es.

Es un dispositivo de hardware que contiene una clave criptográfica protegida que debe desbloquearse mediante un segundo factor de autenticación.

La autenticación se logra demostrando la posesión del dispositivo y el control de la clave. El token depende en gran medida del protocolo y dispositivo criptográfico específicos, pero generalmente es algún tipo de mensaje firmado. Por ejemplo, en Transport Layer Services (TLS), hay un mensaje de "verificación de certificado". Un ejemplo sería una tarjeta de cajero automático.

Requisitos del autenticador: el módulo criptográfico deberá estar validado según FIPS 140-2, nivel 2 o superior; y el token en sí cumple con la seguridad física de FIPS 140-2 Nivel 3 o superior. Esto significa que el token es a prueba de manipulaciones; no se puede abrir para realizar ingeniería inversa u obtener un valor inicial, etc. Los productos validados según versiones posteriores de FIPS 140 también son aceptables.

Se requiere el ingreso de una contraseña, PIN o datos biométricos para activar la clave de autenticación. No se permite la exportación de claves de autenticación.

Requisitos del verificador: la entrada del token generado por el verificador (por ejemplo, un nonce o desafío) tiene al menos 8 caracteres (64 bits de entropía).

3.3 RENOVACIÓN / REEMISIÓN DE TOKENS

Todos los tokens deben caducar dentro de los dos (2) años posteriores a su emisión. Se debe proporcionar al usuario una notificación de advertencia sobre el vencimiento del token dentro de un mínimo de 14 días antes del vencimiento.

Una vez que el token haya caducado, su uso se desactivará y/o bloqueará automáticamente.

Algunos tipos de tokens admiten el proceso de renovación, mientras que otros admiten la reemisión. Dependiendo del nivel de garantía, el usuario deberá restablecer su identidad con el CSP si el token ha caducado o demostrar la posesión del token vigente antes de que se produzca la renovación o la reemisión.

4.0 Cumplimiento

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

5.0 Definiciones de términos clave

Término	Definición
Token de Secreto Memorizado	Hace referencia a "algo que sabes", por ejemplo una contraseña.

6.0 Historial de revisiones

Fecha	Descripción de Cambio	Crítico
06-06-2024	Draft final del documento	Alejandro Castro Pablo Zalazar

7.0 Documentos relacionados

Líneas guía de identidad digital NIST 800-63

Estándar de cifrado

8.0 Anexo

8.1 DISPOSITIVOS TOKEN RECOMENDADOS PARA UTILIZACIÓN CON SISTEMA GDE, VERSIÓN PROVINCIA 4

Dentro de la jurisdicción de la Provincia de Jujuy, el Sistema GDE ha sido desplegado en su *versión Provincia 4*. Por lo tanto, en relación con los dispositivos TOKEN, para firma digital, se recomienda lo de detallado a continuación:

Se debe adquirir un dispositivo criptográfico (token) que cumpla con el estándar FIPS 140-2 nivel 2 o superior, que soporte claves RSA de 2048 bits. Los mismos

deberán alinearse a lo recomendado en los estándares NIST (National Institute of Standards and Technology).

Además, deberá tratarse los dispositivos criptográficos del fabricante cuya marca, modelo, versión de hardware y firmware coincida con lo declarado en la correspondiente Certificación FIPS 140, limitando el no uso de dispositivos criptográficos del tipo OEM (Original Equipment Manufacturer).

Modelos Testeados tipo:

- **mToken Cryptoid:** mToken Cryptoid soporta aplicaciones basadas en los estándares de la industria CAPI y PKCS#11, como Windows smartcard logon, VPN (Cisco, Checkpoint, OpenVPN), Bit Locker, Internet Explorer, Mozilla Firefox, Google Chrome, etc.
- **EnterSafe ePass2003 X15:** ePass2003 utiliza los estándares de la industria como son el Microsoft MiniDriver, Microsoft Crypto API y el estándar PKCS#11. Adicionalmente soporta múltiples tipos de certificados y pares de llaves. Todas las aplicaciones compatibles con estos estándares pueden ser integradas con ePass2003.
- **SafeNet Etoken 5110:** Los SafeNet eToken 5110 (nueva versión del eToken PRO / 5100) son dispositivos criptográficos USB portables para la autenticación de usuarios basados en la misma tecnología de las tarjetas inteligentes. Esta tecnología de certificados (PKI), le permite generar y almacenar credenciales tales como claves privadas, contraseñas y certificados digitales, dentro del ambiente protegido del chip del token.