Sablier — BlackMesa Labs

Ningún dato cuya duración de confidencialidad supere la caducidad de los algoritmos que lo protegen.

2 hallazgos retenidos sobre el conjunto analizado. Fecha de caducidad empleada: 2035 — es el plazo reglamentario, no una predicción de ruptura criptográfica. Plazo verificado con sus fuentes el 30/09/2026.

Duración de confidencialidad de los datos, frente a la caducidad de los algoritmos



Cada barra es el tiempo durante el cual el dato debe seguir siendo confidencial. Pasa a rojo cuando un algoritmo recolectable lo protege más allá de la línea de caducidad; superar la línea sin ponerse en rojo significa que el dato dura mucho, pero lo protege una criptografía que aguantará.

Lo que el servidor negocia realmente

mesa.black

servicio	HTTPS
protocolo negociado	TLSv1.3
suite	TLS_AES_128_GCM_SHA256 (128 bits)
grupo negociado	X25519MLKEM768
firma del certificado	ecdsa-with-SHA384
clave del certificado	curva elíptica 256 bits
cadena	4 certificados
certificado válido hasta	12/01/2027
versiones aceptadas	TLSv1.3

Un handshake, no la lectura de un archivo: es la única forma de saber qué protege de verdad el tráfico, y puede contradecir lo que declara el repositorio.

VIGILAR 1

ECDSA sin declarar

Firma: no se puede recolectar. Migrar antes de 2030 por conformidad, sin urgencia de confidencialidad. Certificado de servidor. Su vida útil es corta: sustituirlo por una firma post-cuántica se hará en la renovación, sin migrar datos.

Aceptar este hallazgo: sablier accept 4d2a0227 --reason="…" --until=2027-05-20

¿La herramienta se equivoca? Abrir un aviso precargado

CONFORME 1

- tls://mesa.black:443:0

Lo que este informe no ha mirado

- la criptografía de sus servicios gestionados —base de datos, almacenamiento de objetos, terminación TLS en un intermediario— no aparece en ningún archivo de este repositorio
- lo que realmente se negocia en ejecución, para cualquier host no declarado en la sección de sonda
- las claves custodiadas en un HSM o en un proveedor

- la vida real de los datos: viene de su declaración, no del código; un dominio no declarado se calcula con una duración por defecto de 0 años
- El horizonte de explotación del sistema no está declarado: el cálculo supone que deja de escribir datos hoy. Es la lectura optimista: un servicio todavía en producción dentro de diez años producirá diez años más de datos que proteger. Añada `service_until` a la declaración.
- Caducidad empleada: 2035, según NIST IR 8547. Otro marco —institucional, defensa— da otra fecha: véase `regime` en la declaración.
- Las sumas de control (CRC32, Adler-32) solo se señalan junto a un token, un enlace o un secreto. Un dígito de control de Luhn o un módulo escritos a mano nunca: nada los distingue de un cálculo ordinario, y un código que acepta un número por su dígito de control no aparece aquí.
- Los archivos binarios (imágenes, fuentes, archivos comprimidos) se leen enteros hasta 8 MiB (8.388.608 bytes) — los más grandes no se leen en absoluto —, y solo en busca de tres señales verificables: un bloque de clave, bytes después del final de la imagen, una extensión que miente sobre el contenido. Un mensaje oculto en los bits de una imagen no se detecta aquí, y no se pretende lo contrario.
- Los archivos YAML de configuración se leen como texto, no se interpretan: un algoritmo definido por un parámetro, por un archivo importado o por una variable de entorno no se ve aquí.

Un inventario que no dice lo que no ha mirado no es un inventario.

Lo que buscó y no encontró

Cada línea es un resultado, no un silencio: un detector abrió esos archivos y no sacó nada de ellos. La cifra está ahí para que juzgue el alcance de la frase en lugar de creerla.

- 6 archivo(s) PHP leído(s): ninguna llamada criptográfica.
- 401 archivo(s) leído(s): ninguna clave privada, ningún certificado, ningún almacén de claves en el árbol versionado.
- 112 archivo(s) binario(s) examinado(s): ninguno lleva un bloque de clave, bytes tras el final de la imagen, ni una extensión que mienta sobre su contenido.
- 2 archivo(s) de dependencias leído(s): ninguna biblioteca criptográfica del catálogo.
- 2 configuración(es) de servidor web leída(s): ningún cifrado ni versión de protocolo declarados.
- 7 script(s) y Dockerfile leído(s): ningún comando criptográfico.

Lo que hay que cambiar

1 lugar(es) por revisar, en 1 archivo(s). Las filas siguientes cuentan lugares, no semanas.

Algoritmo	Llamadas	Archivos	Dominios	Qué cambia eso
ECDSA	1	1	1	

La hoja de ruta europea cuenta el esfuerzo de migración entre los tres factores del riesgo cuántico. Esta herramienta lo cuenta en lugares, porque es lo que un repositorio sabe decir; no lo convierte en una duración. Ocho llamadas en un archivo detrás de una misma función son una tarde; ocho repartidas en seis servicios con un protocolo entre ellos son un trimestre, y nada en los archivos distingue ambos casos. Esa estimación es suya.

Qué hacer, y en qué orden

Un inventario que no concluye nada acaba archivado. Aquí está el arbitraje, y el orden importa tanto como la lista.

- Nada urgente, y eso también es un resultadoNingún dato de larga duración está expuesto a la recolección y nada está roto hoy. No hacer nada es aquí la decisión correcta: sustituir criptografía que aguanta cuesta tiempo, introduce riesgo y no mejora nada.
- Volver a poner este informe en el calendarioLa ventana se cierra sola: la fecha de caducidad no se mueve (2035), pero cada año que pasa acerca sus datos a esa línea. Un dominio conforme hoy con una duración de nueve años dejará de serlo el año que viene. Basta con repetir el análisis una vez al año, y comprobar de paso

que el plazo reglamentario no se ha movido.

Enviar el resumen por Threema

Abre Threema en un teléfono donde la aplicación esté instalada. En un ordenador el esquema no suele estar registrado y el navegador rechaza el enlace: copie el texto de abajo. No se envía nada a terceros.

¿Falso positivo?

Dos cosas distintas se llaman «falso positivo», y no van al mismo sitio.

1. La herramienta tiene razón, pero aquí se acepta el hallazgo. Es una decisión del proyecto: añada este bloque a su declaración. Está versionada, así que la revisión ocurre en la revisión de código. El motivo y la fecha de caducidad son obligatorios.

En línea de comandos: sablier accept <huella> --reason="…" --until=2027-05-20

2. La herramienta se equivoca. Es una regla que corregir, y su sitio es el repositorio de Sablier: github.com/mesa-black/sablier

La huella impresa junto a cada hallazgo lo identifica, y es lo que se cita en ambos casos. Se calcula a partir de la evidencia, no del número de línea: sobrevive a un desplazamiento del código y cambia el día en que la línea cambia de verdad.

Huella y firma

huella de los hallazgos	8ecb829ccc278ef7ab3138f56e07ee13319cbb72ce1dabbfc58ee7b4d6b670b5
firmado el	Ed25519 + ML-DSA-65 · 16/10/2026 22:20
clave pública	zEMKv+R/IT+XlaqW…
firma de la página	report.html.page.sig
fecha atestiguada	06/10/2026 21:58 UTC · Asseco Data Systems S.A.
anclaje Bitcoin	bloque 976238 · 17/11/2026 06:11 UTC

La huella cubre los hallazgos, no este archivo: dos renderizados del mismo inventario, en dos idiomas, dan el mismo valor.

Este informe lleva dos firmas: Ed25519, verificable en cualquier parte, y ML-DSA-65, que resiste a los algoritmos cuánticos conocidos. Ninguna sustituye a la otra: es la hibridación que pide la ANSSI, aplicada al propio documento.

Lo que el sellado de tiempo establece: la huella anterior existía en esa fecha, según un tercero sin interés alguno en estas conclusiones. Ninguna firma de este informe puede probarlo, porque la fecha que lleva sale del reloj de la máquina que firmó. Su límite: el token está firmado con RSA-4096, que este mismo informe clasifica como vulnerable al cuántico — es una prueba para un litigio en los próximos años, no para 2040.

La fecha se comprueba sin esta herramienta, con el token depositado junto al informe:

Tres pasos en lugar de una línea, y cada uno repara una suposición falsa. La ruta del almacén de certificados no es la misma de un sistema a otro: el comando que se lee en todas partes, `-CAfile /etc/ssl/certs/ca-certificates.crt`, falla en Fedora, Rocky y openSUSE, donde ese archivo no existe. Y el testigo lleva su cadena completa, pero LibreSSL — el openssl que viene con macOS — no la lee y responde `unable to get local issuer certificate`: entregarla con `-untrusted` no cambia nada en los demás casos y resuelve ese. Verificado tal cual en Debian, Ubuntu, Alpine, Fedora, Rocky, openSUSE y en macOS con los dos openssl.

La misma huella se presentó a otras autoridades, en otras jurisdicciones. Cada una firmó su propio testigo sin saber nada de las demás, y cada una fija un límite independiente: la fecha defendible sin confiar en un solo operador es la más tardía de esta lista, así que falsificar la más antigua ya no basta para desligar este documento de una fecha.

- 08/10/2026 02:19 UTC, por GlobalSign nv-sa — testigo en report.html.2.tsr, verificable con la misma receta.
- 08/10/2026 02:19 UTC, por DigiCert — testigo en report.html.3.tsr, verificable con la misma receta.

Lo que el anclaje establece: la huella anterior existía a más tardar en ese bloque de la cadena Bitcoin, que miles de máquinas independientes conservan. No hay que creer a nadie: la prueba es una serie de operaciones

SHA-256 que lleva de la huella a la raíz de Merkle del bloque, verificada sin esta herramienta y sin ningún certificado. Sus límites: prueba cuándo, no quién — eso es tarea de la firma. Frente a un ordenador cuántico, la prueba misma solo contiene hashes (SHA-256, a veces RIPEMD-160), que el algoritmo de Grover debilita sin romper: no caduca como el RSA de los tokens; que la cadena Bitcoin conserve su consenso durante esa transición queda fuera de lo que la prueba puede decir.

Se verifica sin ninguna autoridad, con la prueba depositada junto al informe:

El cliente oficial (pip install opentimestamps-client) toma la cabecera del bloque de un nodo Bitcoin propio. sablier verify la toma de dos exploradores públicos que deben coincidir, y comprueba él mismo la prueba de trabajo de la cabecera en lugar de creerles; en una máquina sin red, la cabecera se pasa a mano con --block-header.

Esta fecha es anterior a la del informe (20/11/2026 09:46 UTC), y no es una incoherencia: los hallazgos no han cambiado desde entonces, así que se conservan tanto la firma como el testigo originales. Solo cambió la representación. La atestación más antigua es la que tiene valor: volver a firmar y a atestiguar en cada ejecución destruiría la anterioridad que establece, sin ganar ninguna información nueva.

Lo que la firma garantiza: la lista de lo que se encontró — cada algoritmo, el archivo donde se encontró, el veredicto que recibió. No depende de cómo está maquetada esta página ni del idioma en que está escrita: el mismo análisis se verifica en francés, inglés o español. La página tiene su propia firma, en el archivo report.html.page.sig depositado junto a ella. Esa se calcula sobre una huella del archivo — cambie un solo carácter y la huella cambia por completo —, así que si se modifica un solo carácter de esta página, un veredicto, una fecha, una coma, la verificación falla. Lo que ninguna de las dos puede impedir: quien tiene la clave de firma puede firmar otra página. Saber qué clave es la buena es el tema del párrafo siguiente. Un solo comando verifica las dos: sablier verify report.html.sig --declare=sablier.json

Lo que las firmas establecen: la lista y la página fueron firmadas por la clave que designa la declaración. Lo que ata esa clave a alguien no es esta página — es el historial del archivo que la declara, donde cualquier cambio de clave es un commit fechado que cualquiera puede leer.