Inventario de algoritmos y módulos

Versión pública de la ficha de algoritmos: función, algoritmo, uso y estado frente a esquemas, con la declaración expresa de ausencia de validación FIPS y Common Criteria.

Regla de lectura

Este inventario reproduce la versión pública de la ficha de algoritmos y módulos del expediente. La columna de estado frente a esquemas declara la situación sin adornos: **ningún módulo criptográfico de Abzu posee validación FIPS 140-3 ni evaluación Common Criteria**. Los algoritmos empleados son los estándares internacionales vigentes, implementados con bibliotecas ampliamente auditadas. No existe criptografía propietaria ni algoritmos de diseño propio; el único componente implementado por el fabricante es el esquema de secreto compartido indicado en la tabla, que es un algoritmo publicado y analizado.

Estado general: Disponible, salvo la modalidad FIPS, que se declara como hoja de ruta al final de este documento.

Inventario

Función	Algoritmo o mecanismo	Uso en el producto	Estado frente a esquemas
Cifrado de respaldos en flujo	AES-256-GCM	Cifrado del respaldo en el agente, en flujo hacia su destino	Algoritmo aprobado por los estándares internacionales de referencia. Módulo no validado FIPS 140-3. Sin evaluación Common Criteria
Custodia de credenciales de hipervisores en el agente	AES-256-GCM	Almacén cifrado de credenciales en el agente	Igual que el anterior
Firma de informes, actas y documentos	Ed25519	Firma digital en la consola, en proceso y sin servicio externo	Algoritmo estándar (RFC 8032). Módulo no validado FIPS 140-3; Ed25519 está admitido en FIPS 186-5, pero la validación del módulo no existe. Sin evaluación Common Criteria
Firma y verificación del catálogo de	Ed25519	Firma del catálogo y de los sobres que	Igual que el anterior

Función	Algoritmo o mecanismo	Uso en el producto	Estado frente a esquemas
recetas y de sobres de federación		intercambia la federación	
Secreto compartido de custodia	Shamir sobre GF(256), con quórum configurable y fragmentos ponderados; códec con suma de verificación	Protocolo de Custodia de Llaves. Los fragmentos jamás se almacenan: solo se conservan metadatos y huella	Esquema matemático estándar (Shamir, 1979). Sin validación de esquema; la evidencia es la batería de pruebas del protocolo y su ejercicio en ceremonia real
Sobres de fragmentos y de recuperación	Argon2id para la derivación y AES-256-GCM para el cifrado	Protección de los sobres del protocolo de custodia	Argon2id es el ganador del concurso de derivación de contraseñas y está recomendado por RFC 9106. Sin validación FIPS: Argon2id no es un algoritmo FIPS; en la modalidad FIPS se sustituiría por PBKDF2
Transporte agente-consola y licenciamiento	TLS con autenticación mutua, certificados X.509 y latido firmado	Canal de llamada a casa entre cada agente y la consola	Protocolos estándar. Módulo no validado FIPS 140-3
Inmutabilidad de repositorios de respaldo	Bloqueo de objetos compatible con S3, en modo de cumplimiento (WORM)	Retención inmutable de los puntos de respaldo en el repositorio	Mecanismo estándar de la industria; su certificación depende del almacenamiento del sitio. Es un mecanismo del repositorio, no un módulo del producto
Huellas de códigos impresos de ceremonia y de contraseñas	bcrypt con sal, como huella unidireccional	Custodia de códigos y credenciales: en la base de datos solo residen huellas, nunca valores en claro	Práctica estándar
Sellado de fragmentos a hardware, opcional	Extensión PRF de WebAuthn y cifrado simétrico derivado	Sellado opcional de un fragmento al autenticador de su custodio	Estándar W3C WebAuthn; depende del autenticador del custodio
Integridad de artefactos y manifiestos	SHA-256 y SHA-512	Huellas de artefactos, manifiestos de respaldo y documentos firmados	Algoritmos estándar. Módulo no validado FIPS 140-3

Delimitación del perímetro

El perímetro criptográfico del producto es deliberadamente estrecho y comprende tres ámbitos: el paquete de respaldo y el almacén de credenciales del agente; los servicios de firma, custodia y sobres de la consola; y el transporte con autenticación mutua.

Agilidad criptográfica

Estado: Disponible

La arquitectura trata el algoritmo como un parámetro y está diseñada para sustituir primitivas sin rediseño, con criterio de no actuar ante la duda. Esa agilidad es la base tanto de la modalidad FIPS como de una futura transición post-cuántica.

Modalidad FIPS

Estado: Hoja de ruta

La modalidad FIPS —incorporar un proveedor criptográfico con validación FIPS 140-3 en los componentes que cifran y firman, con conmutación por configuración y sustitución, en ese modo, de los mecanismos no admitidos— es un plan declarado, no una función existente. Su versión prevista en la hoja de ruta del expediente es la v2.4.

Nota sobre la lista oficial de algoritmos

La clasificación de cada algoritmo contra la lista oficial de algoritmos aprobados, deprecados y prohibidos que emita el Instituto Criptográfico Nacional en sus instrumentos complementarios se incorporará a esta ficha cuando esa lista se publique.