Inventory of algorithms and modules

Public version of the algorithms sheet: function, algorithm, use and scheme status, with the express declaration of absence of FIPS and Common Criteria validation.

How to read this document

This inventory reproduces the public version of the algorithms and modules sheet from the product dossier. The scheme status column states the position plainly: **no Abzu cryptographic module holds FIPS 140-3 validation or Common Criteria evaluation**. The algorithms used are current international standards, implemented with widely audited libraries. There is no proprietary cryptography and no in-house algorithm design; the only component implemented by the vendor is the secret-sharing scheme indicated in the table, which is a published and analysed algorithm.

Overall status: Available, except for the FIPS mode, which is declared as roadmap at the end of this document.

Inventory

Function	Algorithm or mechanism	Use in the product	Scheme status
Backup encryption in transit (stream)	AES-256-GCM	Backup encryption in the agent, in stream toward its destination	Algorithm approved under the reference international standards. Module not FIPS 140-3 validated. No Common Criteria evaluation
Hypervisor credential custody in the agent	AES-256-GCM	Encrypted credential store in the agent	Same as above
Signing of reports, minutes and documents	Ed25519	Digital signature in the console, in-process and without an external service	Standard algorithm (RFC 8032). Module not FIPS 140-3 validated; Ed25519 is admitted in FIPS 186-5, but module validation does not exist. No Common Criteria evaluation
Signing and verification of the recipe catalog and federation envelopes	Ed25519	Signing of the catalog and of the envelopes exchanged by the federation	Same as above

Function	Algorithm or mechanism	Use in the product	Scheme status
Custody secret sharing	Shamir over GF(256), with configurable quorum and weighted shares; codec with checksum	Key Custody Protocol. Shares are never stored: only metadata and fingerprint are retained	Standard mathematical scheme (Shamir, 1979). No scheme validation; the evidence is the protocol test suite and its exercise in a real ceremony
Share and recovery envelopes	Argon2id for derivation and AES-256-GCM for encryption	Protection of the custody protocol envelopes	Argon2id is the winner of the Password Hashing Competition and is recommended by RFC 9106. No FIPS validation: Argon2id is not a FIPS algorithm; in FIPS mode it would be replaced by PBKDF2
Agent–console transport and licensing	TLS with mutual authentication, X.509 certificates and signed heartbeat	Phone-home channel between each agent and the console	Standard protocols. Module not FIPS 140-3 validated
Backup repository immutability	S3-compatible object lock, in compliance mode (WORM)	Immutable retention of backup points in the repository	Standard industry mechanism; its certification depends on the site storage. It is a repository mechanism, not a product module
Fingerprints of printed ceremony codes and passwords	bcrypt with salt, as a one-way fingerprint	Custody of codes and credentials: only fingerprints reside in the database, never cleartext values	Standard practice
Optional sealing of shares to hardware	WebAuthn PRF extension and derived symmetric encryption	Optional sealing of a share to its custodian's authenticator	W3C WebAuthn standard; depends on the custodian's authenticator
Artifact and manifest integrity	SHA-256 and SHA-512	Fingerprints of artifacts, backup manifests and signed documents	Standard algorithms. Module not FIPS 140-3 validated

Perimeter delimitation

The product's cryptographic perimeter is deliberately narrow and comprises three areas: the backup package and the agent credential store; the console signing, custody and envelope services; and transport with mutual authentication.

Cryptographic agility

Status: Available

The architecture treats the algorithm as a parameter and is designed to replace primitives without redesign, with a fail-closed criterion. That agility is the basis both for the FIPS mode and for a future post-quantum transition.

FIPS mode

Status: Roadmap

The FIPS mode — incorporating a cryptographic provider with FIPS 140-3 validation in the components that encrypt and sign, with configuration-based switching and, in that mode, replacement of non-admitted mechanisms — is a declared plan, not an existing function. Its planned version in the dossier roadmap is v2.4.

Note on the official algorithm list

The classification of each algorithm against the official list of approved, deprecated and prohibited algorithms issued by the National Cryptographic Institute in its complementary instruments will be incorporated into this sheet when that list is published.