Cryptographic register

How Senua AI protects your data and its own software: every algorithm we use, how each measures up to the Australian Government's guidance (the Information Security Manual of September 2026, which approves RSA, ECDH, ECDSA, AES-128, SHA-256 and HMAC-SHA-256 only until 2030), and our path to quantum-safe cryptography. The engine and the products carry Senua AI's own implementation, with no third-party cryptography library, each primitive checked against public test vectors and an independent implementation.

The register

What it protects	Algorithm and parameters	ISM status	Planned move
Connections, key agreement	Hybrid X25519 + ML-KEM-768 offered first; X25519, ECDH P-256 (TLS 1.3)	ML-KEM-768 and P-256 approved until 2030; X25519 not listed	ML-KEM-1024 where both ends are Senua AI's
Connections, server authentication	ML-DSA-44, ML-DSA-65 and ML-DSA-87 certificates; RSA 2048 to 8192 (PKCS #1 v1.5, PSS), ECDSA P-256 and P-384, Ed25519; SHA-256, SHA-384, SHA-512; a shipped revocation denylist	ML-DSA-87 approved; RSA, ECDSA approved until 2030	ML-DSA certificates as authorities issue them
Connection traffic	AES-256-GCM offered first, with a SHA-384 handshake; AES-128-GCM, ChaCha20-Poly1305	AES-256 approved; AES-128 not beyond 2030	AES-256-GCM alone
Learned state at rest	AES-256-GCM, 256-bit keys, HKDF hierarchy; its keys sent to each system under ML-KEM-1024 (HPKE, HKDF-SHA-384); root key from AWS KMS, systemd credentials or an operator key	AES-256 and ML-KEM-1024 approved	Kept; records written before an upgrade keep their earlier keys
Product releases	ECDSA P-384 with SHA-384, key held in AWS KMS; verified by the installed system before unpacking	Approved until 2030	ML-DSA-87 added beside it
Engine software at rest	AES-256-GCM under a fresh 256-bit key per release (AWS KMS, sealed to the host); decrypted only into process memory	AES-256 approved	Kept
Passwords	PBKDF2-HMAC-SHA-256, 600,000 iterations, 16-byte salt, verified in a separate process	HMAC-SHA-256 approved until 2030	PBKDF2 on HMAC-SHA-512
Licences, engine-to-engine channels	Ed25519; X25519 with ChaCha20-Poly1305	Not listed	ML-DSA-87, ML-KEM-1024
Hashing, key derivation	SHA-256, SHA-384, SHA-512; SHA-3 and SHAKE; HMAC and HKDF on SHA-256 and SHA-384	Approved; SHA-256, HMAC-SHA-256 not beyond 2030	SHA-384, SHA-512 throughout
Sign-in codes	TOTP (HMAC-SHA-1, 30 s, 6 digits) for authenticator apps	SHA-1 not approved for new use	Compatibility only
Randomness, comparison	Operating-system random source, reads length-checked; constant-time compares for every secret and tag	Not applicable	Kept

Quantum-safe steps

Step	What changes	Date
Inventory and roadmap	Every use, its exposure and its move (ISM-2073)	Done
SHA-384, P-384, AES-256	The longer hash, curve and key ASD names	Done
SHA-3 and SHAKE	The base of ML-KEM and ML-DSA (FIPS 202)	Done
AES-256 for connections	TLS_AES_256_GCM_SHA384 offered first	Done
ML-KEM, hybrid	X25519 with ML-KEM-768 offered on every outbound connection (FIPS 203)	Done
AES-256 at rest	Learned state and engine software sealed with AES-256-GCM	Done
ML-KEM-1024 at rest	The keys that protect learned state, sent under ML-KEM-1024	Done
ML-DSA-87	Release, licence and update signatures (FIPS 204)	June 2027
ML-KEM-1024 links	Every link where both ends are Senua AI's	June 2027
No classical public key alone	Every key agreement and signature Senua AI controls	December 2027

Certificates issued by others, such as a cloud service's, move as their authorities issue ML-DSA certificates; Senua AI already verifies ML-DSA certificates.

How we measure up to Australian guidance

Who	What it asks	Where Senua AI stands
Australian Signals Directorate	A plan by the end of 2026, a start by 2028 and a finish by 2030	This register is our plan: started in October 2026, with everything Senua AI controls due by December 2027
ISM-1917	New cryptographic software supports ML-DSA-87, ML-KEM-1024, SHA-384, SHA-512 and AES-256 by 2030	SHA-384, SHA-512, AES-256 and ML-KEM-1024 in use now, ML-DSA-87 verified; our own ML-DSA-87 signatures due June 2027
ISM-2073	A post-quantum transition plan, developed, implemented and maintained	This register and its roadmap
CSIRO's method	Map every use of cryptography, then fix the most exposed first	We follow it
Independent assessment	An IRAP assessor judges compliance for a whole system, not a single product	We publish this register for assessors and customers to check

Hosted services

Senua AI's own hosted services on AWS hold keys in AWS Key Management Service (hardware security modules validated to FIPS 140-3) and encrypt stored data and volumes with AES-256. These are AWS's implementations, listed for completeness.

The full registry

The complete registry, every cryptographic use by service with key custody and lifetimes, what each connection negotiates and the roadmap step for each, is available to buyers and assessors under a non-disclosure agreement: sales@senuaai.com. This datasheet states the technology as shipped on its issue date and is reissued with each step.