SEALING · KEY AND SECRET MANAGEMENT

REVIEWIT SEAL security sheet

REVIEWIT SEAL keeps the technical credentials our customers entrust to us, signs on their behalf and seals the audit trail every day. This sheet answers the usual questions of security officers, and also states what we do not guarantee.

VERSION
1.0 · November 2026

SCOPE
REVIEWIT SAS · REVIEWIT SEAL module, all regions

DISTRIBUTION
Public

CONTENTS

01 At a glance
02 Design principles
03 Cryptography and key management
04 Access control and isolation
05 Traceability and evidence
06 Revocation and continuity
07 What we do not guarantee
08 Further reading

PURPOSE

To collect access data, REVIEWIT holds technical access to its customers' environments: application secrets, tokens, service accounts, certificates. REVIEWIT SEAL protects them, performs the signatures that depend on them and seals the audit trail. This sheet describes the design of the module; only the commitments of the contract and of the data processing agreement are binding.

HOW TO READ

In service: operating at the date of publication. **Planned**: on REVIEWIT's roadmap, with no date committed.

SECTION 01 At a glance

THE CISO'S QUESTION	SHORT ANSWER
Where are our technical credentials stored?	Encrypted in our repository under a master key dedicated to your organisation, kept in a key management service it never leaves. Encryption binds the value to its holder: an envelope presented for another holder does not open.
Are our keys separate from other customers' keys?	Yes: one master key per customer, never shared. The keys that run the platform belong to a separate hierarchy.
Can we bring our own key?	For signing, yes: you can import your own connection private key into the SEAL vault, which signs with it and never exports it. Encryption under a key you hold or import is planned.
Can your administrators read our secrets?	No. No function, administrative or otherwise, can list or read the value of a secret.
How do we know who accessed what?	Every access and every refusal is recorded in an audit trail whose integrity does not depend on SEAL; the evidence is written before any value is released.
What happens if we revoke an access?	Invalidation within the platform takes effect within 60 seconds at most; revocation at the source system is triggered as well, where that system allows it.
Are keys renewed?	Yes: automatic yearly rotation of each subscription's master key, yearly rotation of each customer's keys in the vault, a fixed expiry and an alert for the SEAL signing key.

SECTION 02 Design principles

PRINCIPLE	WHAT IT MEANS
Key service abstraction	No application component calls the key management service directly: a change of provider or key model does not affect how secrets are handled.
The key service never sees secrets	It only operates on keys, with no access to any secret value or business data.
Proven context, never declared	That a process belongs to your organisation is established by a signed execution context bound to a real object, never by a parameter supplied by the caller.
Access by identity	Platform components authenticate to each other with certificate identities, renewed automatically and revocable; no static password authenticates the platform itself.
Least capability	Signing keys are never exportable: they are used only operation by operation, inside the vault. Each component is authorised only for the secret classes its function needs, for listed purposes and for the duration of the current process.
Evidence before disclosure	Evidence of an access is written before the value is released; if the evidence cannot be written, the access does not take place.

Bounded revocability	Revocation times are quantified; the scopes we cannot guarantee are stated rather than promised (section 07).
Customer containment	An incident affecting a master key or an execution context has no effect beyond the organisation concerned; no component holds a standing right over the master keys of several customers.

SECTION 03 Cryptography and key management

REQUIREMENT	REVIEWIT ANSWER	STATUS
Encryption of credentials	Envelope encryption under the master key dedicated to your organisation. The organisation, holder and class of the secret are cryptographically bound to the envelope and checked at every decryption.	IN SERVICE
Separation per customer	One dedicated master key per customer, never pooled: compromising one customer scope gives access to no other.	IN SERVICE
Key managed by REVIEWIT	Standard model: a master key dedicated to your organisation, generated, kept and rotated by REVIEWIT.	IN SERVICE
Your key for signing	Import of your connection private key into the SEAL vault, which signs with it; the key is never exported.	IN SERVICE
Customer-held master key	Master key kept in your own key management service, whose use you delegate, revocable at any time.	PLANNED
Imported key material	Master key generated by you and imported into our key management service.	PLANNED
Rotation	Master key of each subscription: automatic yearly rotation. Each customer's keys in the vault: rotated every year. Phased rotation: a process already under way keeps access to the version it referenced during the overlap window, except in an emergency revocation.	IN SERVICE
Component identities	Internal certificate authority: identities renewed automatically before expiry, revocation list of callers.	IN SERVICE
End of life of a secret	Deletion removes the encrypted value from the active repository: it can no longer be released. It becomes complete when the backup copies expire.	IN SERVICE

SECTION 04 Access control and isolation

REQUIREMENT	REVIEWIT ANSWER	STATUS
Isolation between customers	Layered controls: signed execution context, authorisation policy per component type, purpose check at every read, cryptographic binding verified independently of application logic, cryptographic authority bounded to a single organisation by a temporary authorisation.	IN SERVICE

Administrator access	No listing or reading of values, administrators included. Sensitive operations under strengthened authentication and separation of roles, with four-eyes approval.	IN SERVICE
RITA assistant	Excluded by design from any access to secret values: no value can appear in a request, a trace or a tool result.	IN SERVICE
Configuration and logs	No secret value in environment variables, configuration files or logs.	IN SERVICE

SECTION 05 Traceability and evidence

REQUIREMENT	REVIEWIT ANSWER	STATUS
Access logging	Every access, refusal, rotation and revocation produces a timestamped event: calling identity, organisation, secret reference, operation, purpose, outcome. Never the value.	IN SERVICE
Independent integrity	The audit trail is signed and sequenced independently of SEAL: a compromise of SEAL cannot erase a trace after the fact.	IN SERVICE
Prior evidence	Written before the value is released, completed afterwards; an access without prior evidence is refused.	IN SERVICE
Daily seal	SEAL seals every chain of the audit trail every day. Its signing key carries an expiry, with an alert before its term.	IN SERVICE
Log of your secrets	Delivery to the customer of the log relating to its secrets, refusals included.	PLANNED

SECTION 06 Revocation and continuity

REQUIREMENT	REVIEWIT ANSWER	STATUS
Local revocation	Invalidation within the platform in 60 seconds at most, across all nodes.	IN SERVICE
Revocation at the source	Triggered at the issuing system where it allows it; the outcome is reported to you.	IN SERVICE
Key service unavailable	Processing for the organisation concerned is suspended in an orderly way and the customer is notified; no other organisation is affected.	IN SERVICE
Change of key provider	Re-wrapping of secrets under a new master key, without moving the values.	PLANNED

SECTION 07 What we do not guarantee

An unstated limit is an implied promise. We therefore state the following.

- Stopping the use of a value already passed to a running process is not instantaneous: it is bounded by a maximum usage time, communicated per secret class.
- Revocation at a third-party system depends on that system's capabilities: we trigger it and report the outcome to you, without being able to guarantee how long it takes.
- Credentials deposited before custody went into service are taken over under their organisation's master key, holder by holder; until then they are protected only by the databases' encryption at rest.
- We perform no cryptographic erasure: a deleted secret disappears from the active repository, its backup copies are erased when they expire, and we claim no enforceable deletion before that term.
- The private key you import for signing is never exported, including at the end of the contract: keep the original.
- Changing key provider and the customer-held or imported key models are not available today.

SECTION 08 Further reading

DOCUMENT	ACCESS
Key and Secret Management Annex: key models, responsibilities, revocation, deletion	Customers and prospects under a non-disclosure agreement
REVIEWIT security whitepaper	Public
Technical and organisational measures (Annex 1 of the DPA)	Customers · authenticated access

REVIEWIT SAS · Security: security@we-reviewit.com. Reviewed annually and after any major change to the module. The French version is authoritative.