Key Custody Protocol

Public commitments of the protocol: configurable quorum, separation of duties, mandatory access key, encrypted envelopes, cooldown, custody watchdog and recovery only by quorum.

What the protocol protects

Status: Available

The Key Custody Protocol governs the product's critical operations — version signing, licence activation and recovery — through a quorum ceremony. No single person, on their own, can execute those operations or reconstruct a protected key.

This document records only the protocol's public commitments. The complete design is provided under confidentiality in an evaluation session, as stated in the confidentiality document of this library.

Public commitments

Quorum through Shamir secret sharing

The protected key is split using the Shamir secret-sharing scheme over GF(256), with a **configurable quorum** and the option of weighted shares. Shares are never stored in the system: only their metadata and fingerprint are retained. The reconstructed key exists only during the ceremony and for the authorised act.

Separation of duties

The ceremony applies separation of duties: whoever requests an operation is not whoever contributes the shares that authorise it. The requester and contributor functions are disjoint by design.

Mandatory access key for every participant

Every participation in a ceremony requires the participant's **WebAuthn access key** (passkey). Without it, operation is not possible. Optionally, a share may be sealed to its custodian's authenticator hardware.

Encrypted envelopes

Shares and recovery envelopes are protected with **Argon2id** derivation and **AES-256-GCM** encryption. Printed codes involved in the ceremony reside in the system only as salted one-way fingerprints; their cleartext values exist in no database.

Ceremony recorded in the log

Each ceremony is recorded in the log, with its participants and its outcome, and its minutes are digitally signed within the platform.

Cooldown period on recovery

Every recovery is subject to a **cooldown period** and to notice to all custodians before it completes. During that period the recovery can be stopped. The existence of this mechanism is public; its operational parameters are not disclosed.

Custodian protection mechanisms

The protocol incorporates custodian protection mechanisms. Their detail forms part of the design provided under confidentiality in an evaluation session.

Document forensic marking

Printed custody documents incorporate a **forensic mark** whose purpose is to attribute leaks of custody documents. Its existence and purpose are public; its format is not disclosed.

Custody watchdog

There is a **custody watchdog** whose function is to detect loss or degradation of custodies and to alert on it. Its existence and function are public; its operational parameters are not disclosed.

Without quorum there is no recovery

Without quorum, the key is not recovered, by design and without back doors, including the vendor's. This is not an operational limitation: it is the central property of the protocol.

The two forms

Form	Custody
Government	The vendor **retains no share** of institutional keys. Recovery is possible only by quorum of the institution's own custodians.
Commercial	The vendor retains a **weighted recovery share**, which on its own reconstructs nothing: recovery still requires quorum with the custodians.

The vendor's own exercise

As evidence of exercise — not as a parameter of any client installation — the vendor exercises this protocol over its own version-signing key with a **2 of 3** quorum, with a real ceremony executed and recorded. The quorum of each installation is defined by that installation.