

Drushtikosh

Custody with explicit authority.

Drushtikosh is a research-stage platform for examining who may use which organisational device, on which host, for which protected data and operation, and for how long. It separates policy decisions from minimum key release and records custody evidence.

THE DECISION

Encryption alone does not explain who authorised access, which context was checked or what happens when connectivity changes. A custody evaluation must make decision authority, key release, endpoint enforcement and evidence ownership explicit.

ARCHITECTURE / SELECTED BOUNDARIES

01	Decide	The Policy Authority evaluates principal, host, device, classification, operation and time before issuing a custody decision.
02	Release	A separate Key Authority process validates a short-lived, single-use, proof-bound ticket before releasing minimum Share B.
03	Use	Shares A and B meet transiently on the authorised lab path for a permitted operation on an encrypted data object. Neither share alone is the complete key.
04	Record	Custody records make selected changes or gaps detectable. The console observes without vault keys; exposed administrative actions route to the Policy Authority.

WHO SHOULD READ THIS

For custody owners, regulated operators, public institutions and security engineers evaluating device and data governance.

A focused evaluation brief, not a certification or production-readiness statement.

EVIDENCE & EVALUATION

What can be examined today.

Evidence reviewed 28 September 2026 / P11.1. Publication does not represent new testing. States are not a maturity score.

Implemented	The lab assembles custody context and contains classification-bounded offline-bundle and lease mechanics.
Tested	Selected lab paths exercise separated policy and key processes, proof-bound minimum release, transient reconstruction and change-detectable custody evidence.
Deployment-dependent	Live host and media enforcement, production isolation, hardware-rooted expiry and revocation or reconnect behaviour require target-environment verification.
Design proposal	Production HSM or KMS custody, TPM-backed expiry, write-once retention, database-role isolation and operational rollout remain future translation work.
Out of scope	MDM, DLP or encrypted-storage replacement, vendor integration, endpoint-protection claims and a combined deployment with Q-Kavach are not claimed.

BOUNDARY TO RETAIN

Single-machine research lab with software-sealed leases. Process separation is not hardware or administrative isolation from machine-level control. Offline revocation may remain unseen until reconnect or the remaining lease TTL. Live media enforcement, hardware-enforced expiry, certification, production deployment and a scoped pilot are not claimed. Post-quantum protection is not implemented.

A BOUNDED FIRST EVALUATION

- 01Which principal, host, device and operation facts must be bound to one custody decision?
- 02Can policy approval and minimum key release remain distinct in the intended environment?
- 03Is the remaining offline-revocation window acceptable, and how will expiry, reconnect and evidence be verified?

Discuss one custody decision. Define the host, hardware and enforcement boundary before translating the lab path into an operational evaluation.

Public dossier: astrasutra.in/work#drushtikosh
Read: Offline authorisation and the revocation gap
Read: Operator visibility and key authority