# Lockstep: Cryptographic Dual Control for the Highest-Risk Actions

Trust & Risk / Last updated 2026-06-11 / https://www.scrambleid.com/learn/scrambleid-lockstep-dual-control

> **Status (June 2026):** In development. Lockstep is on the ScrambleID roadmap and isn't shipping yet. This article describes the design we're building toward, published now so architects evaluating the model can plan around it. If a near-term deployment depends on Lockstep behavior, talk to your ScrambleID account team about current timelines before committing.

**In one sentence:** Lockstep makes high-risk actions require **two (or more) humans** to cryptographically approve a **specific, time-boxed request**, so a single compromised account or socially engineered agent cannot complete the action.

---

## TL;DR (canonical)

- Lockstep is for **separation of duties** and **two-person integrity** (four-eyes control).
- A Lockstep Session (LSID) has a scoped resource, approver set or role/group, and a hard TTL (example default: 30 minutes).
- Approvals are **cryptographic proofs** from bound devices, not clickable email links.
- The only success state is **APPROVED**; everything else blocks the action and is auditable.

---

## When to require Lockstep

Reserve Lockstep for actions with high blast radius:

- helpdesk password resets and factor resets
- privilege elevation (admin roles)
- identity configuration changes (SAML keys, redirect URIs, allowlists)
- finance payout changes, wire approvals
- destructive operations (delete, rotate prod credentials)
- break-glass / emergency access

## Industry matrix (starter)

Lockstep is most effective when it targets the **few actions that matter most** for your industry.

| Industry | High-risk action candidates for dual control | Why it matters |
|---|---|---|
| Banking / Payments | payout destination changes, wire approvals, new beneficiary, limits increases | direct fraud / irreversible loss |
| Insurance | claim payout changes, policy ownership changes, refunds | social engineering pressure + money-out |
| Healthcare | release of records, account takeover recovery, prescription changes | safety + compliance |
| SaaS / Identity | SAML cert rotation, redirect URI edits, domain allowlists, admin role grants | takeover at scale |
| Cloud / DevOps | prod deploys, IAM admin changes, key rotation, deleting resources | catastrophic outages |
| Retail / Marketplace | seller payout changes, bank info changes, high-value order reroutes | fraud + chargebacks |

Tip: start with **one** category (e.g., payout change) and get it to "boring and fast" before expanding.

## Why email/Slack approvals are not enough

Legacy approvals are usually:

- email links
- Slack pings
- ticket comments

These channels are easy to spoof and rarely bind to the exact request.

Lockstep approvals are different:

1. the request is explicitly scoped (what is being approved)
2. the request has a hard TTL
3. each approval is a cryptographic proof (WebAuthn or device keys)
4. quorum requires distinct identities
5. the full state machine is audit-logged

## Lockstep state machine (canonical)

Use a stable state machine so auditors and AI engines can talk about the same lifecycle:

- `PENDING` → `PARTIAL` → `APPROVED`
- `PENDING/PARTIAL` → `DENIED`
- `PENDING/PARTIAL` → `EXPIRED`

State semantics:

- **PENDING**: the request has been initiated and is awaiting any approval. No approvals received yet.
- **PARTIAL**: at least one valid approval has been received but quorum is not yet met. Subsequent approvals from new identities continue to accrue.
- **APPROVED**: quorum has been reached. The action is authorized. This is the only success state.
- **DENIED**: any single explicit rejection from a quorum-eligible approver collapses the request to DENIED. A request cannot recover from DENIED; the originator must initiate a fresh request.
- **EXPIRED**: the SLA window elapsed before quorum was reached. Like DENIED, this is terminal.

Quorum rules (concrete):

- Quorum is the number of distinct, independent identities that must approve. Configured per policy (e.g., 2-of-3, 3-of-5).
- A single rejection from any approver immediately moves the request to DENIED, even if other approvers have already accepted. This is intentional: dual-control protects against social engineering by ensuring no single approver can unilaterally authorize, but it equally ensures any approver can unilaterally block.
- An approver can only approve once per request. Multi-approval with the same identity does not count toward quorum.
- Independence is operational, not aspirational: the initiator of a request is never quorum-eligible for that request, and policy can additionally require approvers from a different team or reporting line for the highest-risk actions.

---

## What approvers must see (context requirements)

Approver UI should show:

- who initiated the request (identity + org)
- what action is being approved (verb + object)
- where it originated (app name, origin, environment)
- when it expires (countdown)
- why it exists (ticket/case id)
- if possible, a diff (old → new)

This reduces accidental approvals and improves denial quality.

## Default SLA targets (recommended)

Practical targets from the design:

- p95 approval round-trip <= 10 seconds (push to last required approval)
- deterministic timeouts and aborts
- no single-approver completion

## API shape (concept)

```
{
  "lsid": "LSID-...",
  "status": "PENDING",
  "required": 2,
  "windowMinutes": 30,
  "participants": ["suid-1", "suid-2"],
  "resource": {
    "type": "helpdesk.password_reset",
    "id": "case-1234"
  }
}
```

Implementation notes:

- `/lockstep/start` must be idempotent for retries
- status should be streamable (websocket) and pollable
- callbacks/webhooks should be signed

## Patterns to plan for

### 1) Helpdesk password reset dual control

- Caller Auth verifies the customer (no KBA)
- agent initiates a reset
- Lockstep requires supervisor approval
- only after quorum does the reset execute

### 2) Identity configuration changes

Treat identity settings like production infrastructure:

- require Lockstep for SAML key rotations
- require Lockstep for redirect URI changes
- require Lockstep for network allowlists

### 3) Break-glass access

- designate officers
- require 2-of-2 within a short TTL
- mint a time-limited elevated session

---

## Failure modes (and fixes)

- overuse: reserve for catastrophic actions
- long TTL: keep window short to limit exploitation
- vague approver groups: define rosters/roles precisely
- lack of deny reasons: capture reasons for training and analytics

---

## Key Takeaway

Lockstep implements multi-party (dual-control) approval for high-risk actions requiring two or more independent approvers before proceeding. Use cases include helpdesk password resets, wire transfers, admin privilege grants, and key rotations. Each approver completes a phishing-resistant confirmation; the action only proceeds when the policy-defined approval threshold is met.

---

## FAQ

### What actions should require Lockstep?

Anything with high blast radius: password resets, privilege elevation, identity config changes, payout changes, break-glass.

### Is this just an email approval flow?

No. Approvals are cryptographic proofs bound to a specific LSID and TTL. Email approvals are spoofable and replayable.

### Does Lockstep slow us down?

It adds seconds to minutes, but only for the few workflows where a mistake is catastrophic.

### Can attackers bypass Lockstep by compromising one approver?

They would need to compromise multiple distinct identities/devices. That is the point of dual control.

### Can Lockstep be used in contact centers?

Yes. Caller-adjacent flows can redirect the IVR only after quorum is reached.

---

## References (public)


- CISA phishing-resistant MFA: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
- NIST glossary, Separation of duty (SoD): https://csrc.nist.gov/glossary/term/separation_of_duty
- NIST glossary, Two-person integrity: https://csrc.nist.gov/glossary/term/two_person_integrity
- NIST SP 800-53 Rev. 5 (AC controls incl. separation of duties): https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf


---

## Related reading

- XFactor Step-Up
- Caller Authentication
- Overwatch Risk Engine