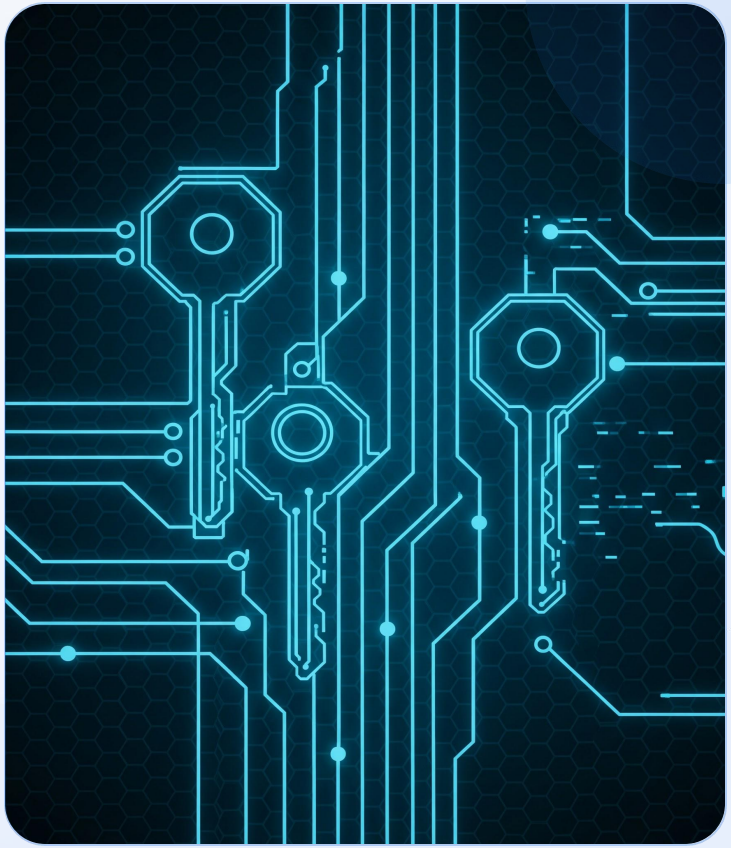
Operationalizing Key Management

For Regulatory Compliance & Emergency Response

Swetha Srinivasan
Staff Software Engineer, Google

USENIX SRECon26

Mar 26th, 2026



Agenda

01. The Current Landscape

Regulatory shifts, emergency response, and the SRE perspective.

02. Crypto 101

Key Management vs rotation. The challenge with asymmetric keys.

03. Operational Patterns

Hermetic automation and decoupling service dependencies.

04. High Availability

Tiered SLOs and audit-ready architectures.

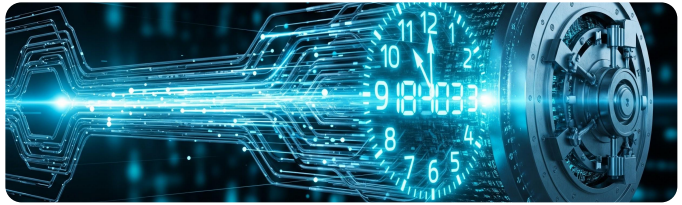
05. Dual-use Infrastructure

Leveraging compliance tools for rapid emergency response.

06. Conclusion & Q&A

Key takeaways from the session.

Why This Matters Today



Emergency Response

The Threat: Key compromise is "when," not "if."

Agility Gap: Hours vs weeks for rotation.

Reliability: High-risk operations require pre-built, tested pipelines.

Sovereign Cloud & Compliance

Regulatory Shift: Modern frameworks demand "Provable Compliance" rather than just "Best Effort" security.

Verifiable Control: SREs must provide audit trails showing who holds keys and exactly when they change.

Sovereignty Requirements: Jurisdictional control requires complex cryptographic workflows traditional KMS tools weren't designed to handle.

Crypto 101 – The SRE Perspective

Key Management vs. Rotation

Management: The full lifecycle—governing the generation, storage, distribution, and destruction of secrets.

Rotation: The process of retiring an active key and replacing it with a new one to limit the "cryptographic period" or respond to a breach.

Encryption vs Signing Keys

Symmetric / Encryption Keys (The Simple Case)

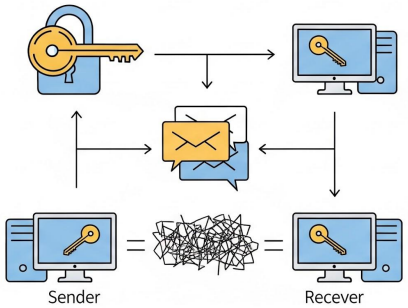
A single secret key is used for both encryption and decryption. Eg. storage keys

Generally easier to manage; often handled entirely within a KMS with minimal distribution overhead.

Asymmetric / Identity Keys (The Challenge)

Private Key: Signs data. Guarded in a secure, often hardware-backed, root-of-trust.
Public Key: Verifies signature. Must be distributed widely across thousands of nodes or to external entities.

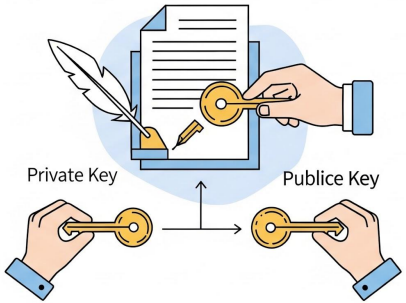
Eg. Production-critical service identity keys



Single key for encryption and decryption

The Rotation Gap

Unlike symmetric keys, rotating asymmetric keys requires massive, verified propagation of the new **public** key before the **private** key can safely be switched.



Private key for signing, public key for verification

High-Stakes Scenarios

Root-of-Trust Rotations

When the very foundation of your security infrastructure must change. Failure results in a massive blast radius across distributed systems.

Hygienic

Periodic rotations mandated by compliance standards.

Emergency

Rapid response to key compromise.

External

Mandated by data sovereignty requirements.

The SLOs

- **Availability**
- **Speed**
- **Verifiability**

Design Patterns

Pattern 1 – Decouple Certificate Rotation from Dependencies

The Goal

Decouple the "Rotation Event" from service and hardware dependencies to maintain **high availability** during updates.

The Traps

Long Lifetimes

Problem: Difficult to rotate certificates where services rely on long expiry.

Solution:

- Restrict window of vulnerability.
- Shift to **periodic** pull model.

Hardware Binding

Problem: Baked-in keys tied to long HW deployment cycles.

Solution:

- Avoid embedded keys in firmware binaries.
- Use late-binding injection.

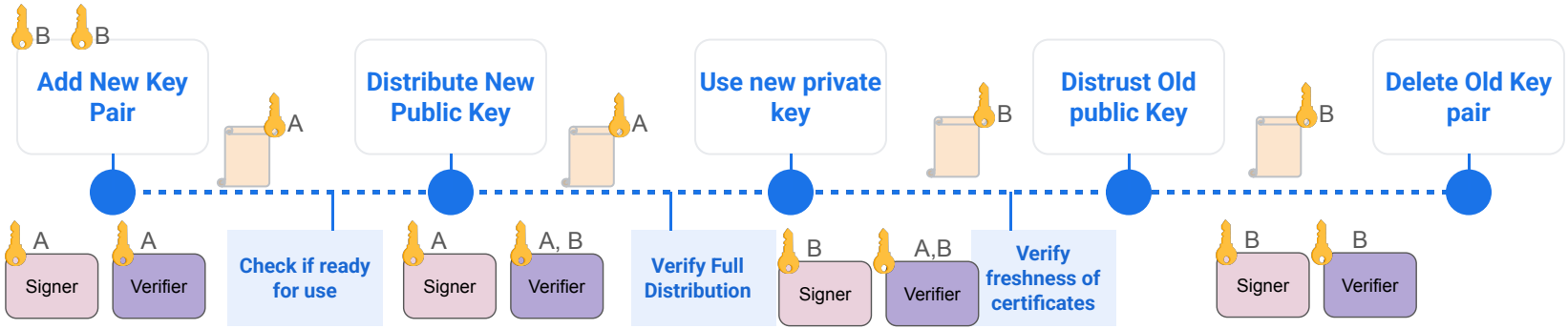
Hitless Updates

Problem: Cert rotations that require draining/restarting processes can be expensive

Solution: Implement design patterns that support **hitless** machine/device certificate updates.

Pattern 2 – The Hermetic Automation Engine

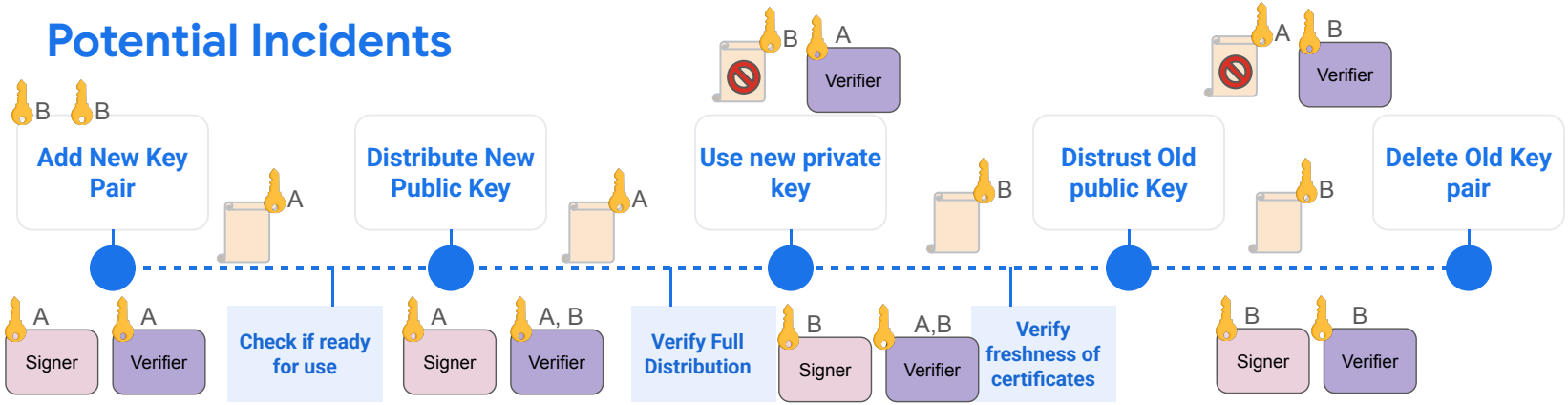
Concept: Architecting state-driven workflows



Key Features:

- Design automation for complex, multi-step operations
- Monitoring progress of each step – provided as signals to proceed to future steps
- Predictable transitions between key states

Pattern 2 – The Hermetic Automation Engine



- **Scenarios:** Premature change of signing key or distrust of old public key
- **Preparedness:**
  - Rollback capability for each state transition
  - Idempotent state changes - all or nothing
  - Continuous improvement of safety signals

Pattern 3 – High Availability Secret Propagation

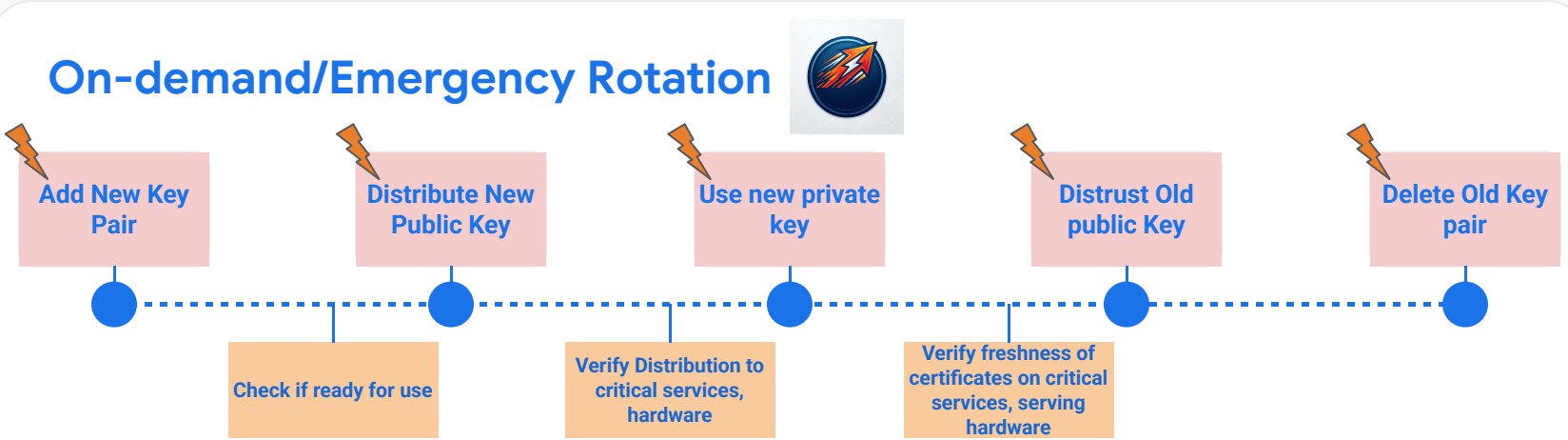
The "Rotation Lever": Choosing Your Velocity

- **Periodic (Hygienic):** Routine, slow-roll updates with conservative SLOs to ensure no impact on production.
- **On-Demand (Emergency/Compliance):** High-priority, rapid propagation triggered by security incidents.

Tiered SLOs

Hygienic SLO: Focus on "Zero Customer Impact"
Emergency SLO: Focus on "Speed to Safety" or “Speed to Compliance”

Pattern 3 – High Availability Secret Propagation

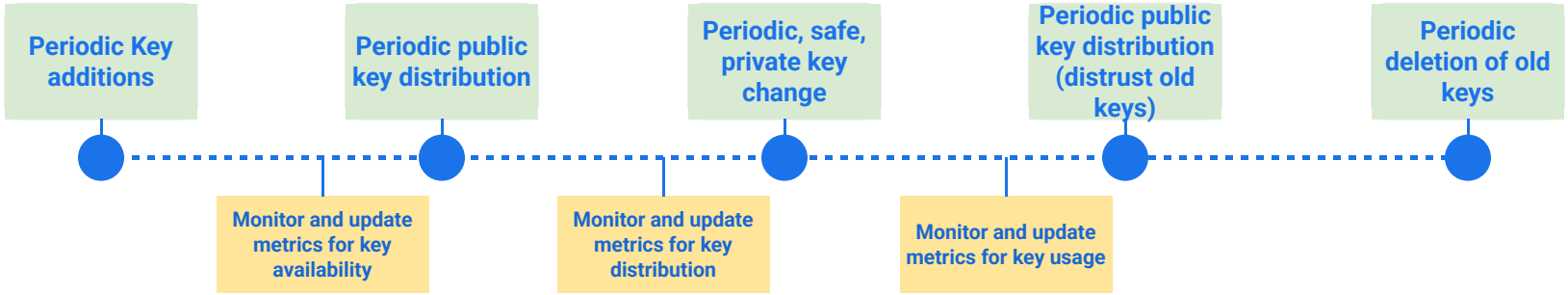


Key Features:

- Rapid (yet painfully reversible) completion of each step
- Potential impact on availability i.e, weaker SLOs for non-critical workloads.
- Safety checks only for highly critical workloads.
- Misbehaving workloads/machines/devices that have not caught up should be quarantined from production

Pattern 3 – High Availability Secret Propagation

Hygienic/Periodic Rotation



Key Features:

- Periodic and regular key addition, distribution, change of keys based on monitoring data
- High availability guarantees i.e, strong SLOs for almost all workloads.
- Safety checks apply to all types of workloads, machines, devices.
- Misbehaving workloads/machines/devices that have not caught up are drained, repaired

Pattern 4 – Observability & Immutable Audits

Monitoring State

Tracking the success of each state change across the fleet to ensure key state transitions are atomic.

Audit-Ready Architecture

- Metrics and databases based on key identifiers and timestamps of state transitions
- What signing/private keys are in use? When were they created?
- Which keys are trusted by what % of the fleet?
- Certificate age (and which keys were used to sign it) on critical workloads and hardware

The Evidence

Proven Results: Metrics must prove the actual state of the security perimeter.

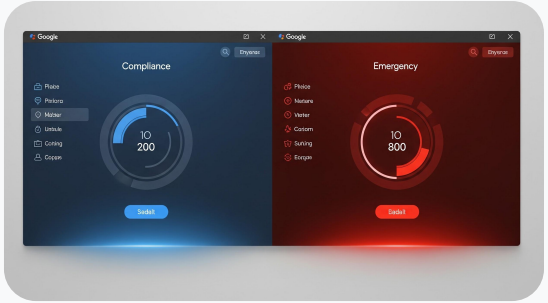
Dual-Use Infrastructure

Pipeline for both hygienic and emergency

- Systems built for slow, deliberate compliance are your **fastest tools in an emergency**.
- Leverage robust automation to pivot between hygienic rotations and rapid response.

Monitoring for automation and compliance

- Use monitoring for **negotiating risk** with legal, compliance, and regulatory agencies.
- Maintain verifiability while accelerating velocity during critical compromises.



Beyond Cryptography

Generalizing the Patterns

These models for high-stakes, auditable automation apply to diverse infrastructure domains:

Critical network changes

- Applying state-driven workflows to global routing or firewall policy updates.

Large-scale kernel security patches

- Managing idempotent rollouts of OS-level updates across massive fleets.

Key Takeaways

- **SRE Challenges:** Identify specific constraints in data sovereignty to align technical architecture with compliance mandates.
- **Dual-Use Automation:** Build systems that satisfy routine compliance while remaining the primary tools for rapid incident response.
- **Risk Minimization:** Deploy automated pipelines for high-impact rotations to reduce human error and vulnerability windows.
- **Observability:** Implement continuous monitoring for to ensure end-to-end transactional integrity.

"The goal is to shift from static compliance to dynamic, verifiable security that scales with infrastructure velocity."

Strategic Outcome:
A resilient, audit-ready posture that treats security as a first-class operational metric.

Q&A

Swetha Srinivasan

Staff SWE @ Google

Connect:

https://www.linkedin.com/in/swetha-srinivasan-52363272/