DevOpsSchool

Course curriculum · November 2026

LEVEL 04 OF 04 · ADVANCED

Notary Advanced Training

Design signing PKI, key rotation and multi-cluster verification policy for an enterprise software supply chain.

LIVE ONLINE **Max 8-10 hours**	CORPORATE (DAY-WISE) **5 days · Days 1-5**	SELF-PACED VIDEO **1-year LMS access**
BATCH SIZE **Max 10 learners**	NEXT BATCHES **1st of every month · weekends: first Saturday**	CERTIFICATE **Verifiable certificate of completion**

Foundation	Essential	Intermediate	Advanced
1 day · Included	2 days · Included	3 days · Included	5 days · This curriculum

INSIDE THIS CURRICULUM

What you will achieve	Outcomes and level focus
Who should attend	Audience and prerequisites
Agenda	46 topics · Foundation to Advanced
Hands-on labs	4 labs
Formats and fees	Live, 1:1, self-paced, corporate
Trainer and reviews	Rajesh Kumar
Enrolment	Batches, payment, contacts

WHY DEVOPSSCHOOL

- Rated 4.6 on Google
- 1,500+ verifiable certificates issued in the public registry
- Trainer Rajesh Kumar: 20 years in industry
- Small batches: max 10 learners, every session recorded

Course page: www.devopsschool.com/courses/notary/notary-and-advance-training.html
Talk to us: WhatsApp +91 99057 40781 · +1 (469) 756-6329 · contact@DevOpsSchool.com · reply within 1 hour

OUTCOMES

What you will achieve

By the end of the Notary course path, you will be able to:

1

Sign and verify artifacts

Sign container images and other OCI artifacts with Notation and verify them with precise trust policies.

2

Enforce signatures at deploy

Block unsigned or untrusted images at Kubernetes admission using Ratify, Gatekeeper or Kyverno.

3

Run trustworthy signing PKI

Design certificate hierarchies, KMS-backed keys, timestamping and revocation for production signing.

WHAT THE ADVANCED LEVEL ADDS

Enterprise PKI, policy governance and hardening

Hands-on: Build an enterprise signed supply chain. Issue signing certificates from an internal CA, sign and timestamp release artifacts in CI and enforce verification across two clusters via GitOps.

WHO SHOULD ATTEND

- Experienced Notary practitioners responsible for quality, security and scale.
- Senior engineers, architects and leads who design and troubleshoot Notary solutions.
- Teams making Notary an organisation-wide standard.

BEFORE YOU START

- The Intermediate level, or equivalent hands-on experience.
- You can already: Sign with keys held in cloud KMS, enforce signatures at Kubernetes admission and attach SBOMs and scan results to images.
- Basic computer skills and a laptop with a stable internet connection for the live sessions and labs.
- This curriculum includes every earlier level, so it is complete on its own.

AGENDA · FOUNDATION TO ADVANCED

Notary Advanced Training agenda

46 topics. Each level builds on the one before it, so this curriculum lists every earlier level in full. Days are for corporate (day-wise) delivery; live online batches cover the same agenda in max 8-10 hours.

DAY 1 — Foundation: Supply chain trust and first Notation signature

Included from Foundation

1. Why sign artifacts: supply chain attacks, tampered images, integrity and provenance goals
2. Notary history: Notary v1 and TUF, Docker Content Trust and the move to the CNCF Notary Project
3. Core concepts: signatures, X.509 certificates, signing identities, trust stores and trust policies
4. OCI fundamentals: images, manifests, digests versus tags, OCI 1.1 artifacts and the referrers API
5. Notary Project components: Notation CLI, specifications, notation-go library, plugins and the Ratify verifier
6. Installing Notation: binary install, notation version and a local OCI registry such as Zot or Distribution
7. Test keys and certificates: notation cert generate-test, notation key list and where keys are stored
8. First signature: notation sign by digest, notation ls to list signatures and notation inspect
9. First verification: notation verify with a basic trust policy and a CA trust store
10. Signature envelopes: JWS and COSE formats and what a signature manifest contains
11. Notary Project and Sigstore Cosign compared: keys, keyless signing, ecosystem support and selection criteria

DAY 2 — Essential: Trust policies, registries and team signing workflow

Included from Essential

12. Trust policy in depth: registryScopes, verification levels strict, permissive, audit and skip, trustedIdentities
13. Trust store management: notation cert add, list and delete, ca, signingAuthority and tsa store types
14. Production certificates: chains from an internal CA, key usage requirements and certificate validity
15. Registry support: Azure Container Registry, Amazon ECR, Harbor and Zot, referrers API and tag fallback
16. Signing in CI: notation-action in GitHub Actions and Notation tasks in Azure Pipelines after the build step
17. Signing by digest: avoiding mutable tags, capturing pushed digests and passing them between pipeline jobs
18. Signature metadata: adding --user-metadata annotations and enforcing them during verification
19. Expiry and timestamping: --expiry, RFC 3161 timestamp authorities and verifying after certificate expiry
20. Docker Content Trust on Notary v1: DOCKER_CONTENT_TRUST, docker trust sign, inspect and delegations
21. Team workflow: who signs, separate development and release identities, signing gates on merge
22. Troubleshooting verification: scope mismatches, untrusted certificates, digest errors and --debug output

DAY 3 — Intermediate: KMS plugins, Kubernetes admission and automation

Included from Intermediate

23. Plugin architecture: how Notation plugins work and installing them with notation plugin install
24. Azure Key Vault plugin: signing with Key Vault certificates and managed identity access
25. AWS Signer plugin: signing profiles, profile revocation and the AWS Signer trust store
26. Other key stores: community plugins for HashiCorp Vault and HSM-backed signing options
27. Ratify on Kubernetes: installing Ratify with Gatekeeper, verifier and store configuration, constraints
28. Kyverno verification: verifyImages rules of type Notary with certificate attestors
29. Admission rollout: audit mode first, then deny unsigned images per namespace with documented exceptions
30. Signing more than images: notation blob sign for files, Helm charts and OCI artifacts pushed with ORAS

31. Supply chain evidence: SBOMs in SPDX or CycloneDX and vulnerability reports attached as OCI referrers
32. Revocation checking: OCSP and CRL handling during verification and responding to a compromised key
33. Promotion pipelines: build, scan with Trivy, sign, then copy with referrers using oras cp -r
34. Auditing: Gatekeeper audit results, Ratify logs and reporting unsigned workloads

DAYS 4-5 **Advanced: Enterprise PKI, policy governance and hardening** — **New at this level**

35. PKI design: root and intermediate CAs, leaf certificate lifetimes, HSM-backed keys and rotation plans
36. Key compromise response: revocation, re-signing images, trust policy updates and incident runbooks
37. Timestamping strategy: choosing a TSA and keeping signatures valid after certificates expire
38. Multi-tenant trust policies: per-team scopes, trusted identities by subject and separation of duties
39. Air-gapped environments: mirroring images with their signatures and maintaining offline trust stores
40. Geo-replicated registries: preserving signatures during promotion, import and replication
41. Migration from Notary v1: moving Docker Content Trust and TUF repositories to Notation signatures
42. Framework mapping: SLSA build levels, in-toto attestations and NIST SSDF practices
43. Policy at scale: Ratify, Gatekeeper and Kyverno policies rolled out to many clusters through GitOps
44. Resilience: verification caching, registry outages and fail-open versus fail-closed admission decisions
45. Compliance evidence: signed-workload reports and audit exports for SOC 2 and ISO 27001
46. Capstone: end-to-end signed supply chain from commit to cluster with KMS keys, TSA and admission enforcement

PRACTICE

Hands-on labs

You build these yourself during the course, guided by the trainer.

FOUNDATION

Sign and verify your first image

Push an image to a local registry, sign it by digest with a test certificate and verify it with a trust policy.

ESSENTIAL

Sign images in a CI pipeline

Build an image in GitHub Actions, sign it by digest with a CA-issued certificate and verify it with a strict trust policy before release.

INTERMEDIATE

Block unsigned images in Kubernetes

Sign images with a Key Vault or AWS Signer key, deploy Ratify with Gatekeeper and prove that unsigned or tampered images are rejected.

ADVANCED

Build an enterprise signed supply chain

Issue signing certificates from an internal CA, sign and timestamp release artifacts in CI and enforce verification across two clusters via GitOps.

HOW YOU CAN LEARN

Formats and fees

The same agenda in four formats. Fees are in Indian rupees as of November 2026; the course page shows them in your currency.

FORMAT	DURATION	WHAT YOU GET	FEE
Live & interactive (online)	Max 8-10 hours	Instructor-led public batch of max 10 learners with demos, labs, Q&A and assignment review. Weekday batches start on the 1st of every month, weekend batches on the first Saturday of every month.	**INR 34,999**
1:1 live training (online)	Max 8-10 hours, one-to-one	The same agenda, taught one-to-one by the trainer. Starts immediately, without waiting for the next batch; sessions planned around your working hours, at your pace.	**INR 99,999**
Self-paced video	1-year LMS access	All four Notary levels, plus 20+ more courses and 50+ tools, at your own pace.	**INR 833/month** billed yearly at INR 9,996
Corporate (day-wise)	5 days for this level	A private batch for your team, on demand. Foundation 1 day, Essential 2, Intermediate 3, Advanced 5 (cumulative).	**Quote on request**

ASSESSMENT AND CERTIFICATE

Your progress is checked through hands-on labs and assignments at every level. On completion you receive a DevOpsSchool certificate of completion with a unique credential ID that anyone can verify at devopsschool.com/certificates.

INCLUDED WITH EVERY LIVE BATCH

- Every live session is recorded and stays in your LMS for a year.
- Can't attend your batch? Move to next month's batch.
- Free demo class before you pay.
- Free 10-15 minute call with an advisor or the trainer to check the course fits you.

YOUR TRAINER

Learn from Rajesh Kumar

Principal Architect, trainer and mentor in DevOps, SRE, DevSecOps and platform engineering, with 20 years across 8+ software MNCs, including Staff DevOps/SRE Engineer for a leading Japanese mobile-payment platform and Principal DevOps Architect and Manager in Europe.

Profile: www.rajeshkumar.xyz · Videos: youtube.com/@TheDevOpsSchool

20 years in industry	**200+** corporate trainings
10,000+ engineers mentored	**70+** organisations coached

REVIEWS

What learners say

Rated 4.6 on Google · more reviews at devopsschool.com/testimonials and in our video testimonials.

> “Rajesh is very good trainer. Rajesh was able to resolve our queries and question effectively. We really liked the hands-on examples covered during this training program.”
>
> Indrayani, India

> “The training was very useful and interactive. Rajesh helped develop the confidence of all.”
>
> Abhinav Gupta, Pune

START YOUR NOTARY TRAINING

Join the next batch

Weekday batches start on the 1st of every month and weekend batches on the first Saturday of every month, with max 10 learners each. 1:1 training can start immediately; corporate batches run on demand. We reply within 1 hour.

Pay by UPI, credit and debit cards, net banking or PayPal. Before you pay, read our refund policy. All levels of this course: www.devopsschool.com/courses/notary/

ENROL OR RESERVE A SEAT
Notary Advanced Training

WHATSAPP · INDIA
+91 99057 40781

WHATSAPP · USA
+1 (469) 756-6329

EMAIL
contact@DevOpsSchool.com