Certifyz Enterprise Architecture Whitepaper

A Unified Automation Layer for Certificate Lifecycle Management

---

1. Executive Summary

The security and operational risks associated with manual or semi-automated TLS/SSL management are no longer acceptable for modern, high-velocity engineering teams. Certifyz provides a zero-downtime, zero-touch certificate lifecycle management platform that abstracts Certificate Authorities (CAs), automates DNS-01 validation, and strictly vaults all cryptographic material. This whitepaper details the underlying architecture, workflows, and deployment models that make Certifyz the modern standard for enterprise PKI management.

---

2. Core Architecture Principles

2.1 Agentless Engine

Unlike legacy PKI solutions, the Certifyz engine requires **zero agent installations** on your target infrastructure. It integrates natively with your existing cloud platforms via secure APIs, dramatically reducing the attack surface and eliminating maintenance overhead on compute nodes.

2.2 DNS-01 Standardization

HTTP-01 validation typically requires punching holes in firewalls or managing complex load balancer rules. Certifyz enforces **DNS-01 validation** by integrating directly with enterprise DNS providers. This allows certificates to be issued for internal, air-gapped, or highly restricted environments without ever exposing ports to the public internet.

2.3 Zero Plaintext Exposure

Traditional workflows often rely on engineers passing `.key` files over Slack, or storing them in generic CI/CD variables. Certifyz generates ephemeral keys securely, immediately mapping and injecting them directly into Enterprise Encrypted Vaults. Keys are protected by strict Identity and Access Management (IAM) policies from the millisecond they are generated.

---

3. The Automation Workflow

The Certifyz engine operates on a deterministic, highly resilient loop:

1. **Intelligent Domain & Expiry Monitoring:** The engine continuously audits all active domains against their true on-chain expiration dates, bypassing false-positives common in local calendar scripts.
2. **Automated ACME Challenge Execution:** 30 days prior to expiration, Certifyz automatically negotiates with the CA, provisions the necessary TXT records to your DNS provider, waits for global propagation, and confirms issuance.
3. **Vault Injection & Event Webhooks:** Upon successful issuance, the raw material is vaulted. Dependent systems are immediately notified via secure webhooks to seamlessly pull the new secret and reload their TLS contexts before the old certificate expires.

---

4. Multi-CA Abstraction Layer

A core vulnerability in modern infrastructure is "CA Lock-in". If a provider faces downtime or revokes its root certificates, enterprises face catastrophic outages.

Certifyz introduces a **Multi-CA Abstraction Layer**. Through a single unified interface, platform engineers can seamlessly pivot traffic and issuance between Let's Encrypt, ZeroSSL, or custom internal PKIs. This requires zero modifications to deployment scripts or Kubernetes operators—Certifyz normalizes the underlying ACME protocols for extreme resilience.

---

5. Enterprise Deployment Models

Compliance and data sovereignty require flexible isolation strategies. Certifyz offers two distinct architectures:

5.1 Shared Logical Isolation (Standard Enterprise)

Designed for standard enterprise teams. Projects are logically separated within our highly available control plane. Each tenant benefits from distinct project scopes, isolated database records, and dedicated external service accounts, ensuring strict cross-tenant data boundaries.

5.2 Dedicated Environments (Compliance-Grade)

For healthcare (HIPAA), government (FedRAMP), or heavily regulated financial institutions, Certifyz deploys a physical **Single-Tenant Air-Gapped Cluster**. The entire engine exists inside a dedicated, isolated cloud project utilizing exclusive compute and vaulting resources.

---

6. Conclusion

By removing humans from the cryptographic issuance loop and strictly enforcing cloud-native integration paradigms, Certifyz eliminates downtime incidents and eradicates manual toil. It is the definitive infrastructure safety net for the modern enterprise.

For sales inquiries or to book a live architectural review, please contact sales@certifyz.com.