emudhra
Trust Delivered

Certificate Lifecycle Management
Capabilities Overview

1. Introduction

CertiNext is eMudhra's enterprise-grade Certificate Lifecycle Management (CLM) platform designed to provide centralized discovery, governance, issuance orchestration, deployment automation, and compliance visibility across hybrid, multi-cloud, on-premises, DevOps, and private PKI environments. This document provides a structured overview of CertiNext capabilities and maps them against commonly referenced evaluation dimensions for comprehensive CLM platforms, including:

- Multi-CA support
- Certificate type coverage
- Use case breadth
- Governance and lifecycle automation
- Infrastructure and ecosystem integrations

The objective is to present a clear and factual view of the platform's architecture, functional scope, and enterprise readiness.

2. Multi-CA Support

CertiNext enables centralized lifecycle management across multiple public and private Certificate Authorities (CAs) through a connector-based architecture.

Public CA Integrations

CertiNext supports integration with third-party public CAs, including:

- Digicert
- Sectigo
- GlobalSign

Additional public CAs via API and credential-based integration, enabling CA-agnostic lifecycle governance across heterogeneous environments. The connector framework is designed to be extensible, allowing additional CA integrations where required.

Private CA Integrations

For internal trust hierarchies, CertiNext integrates with:

- eMudhra emCA (private root CA)
- Microsoft ADCS

The emCA integration enables private root and intermediate CA hierarchy management. Private CA connectors are configurable within the platform and operate alongside public CA integrations in a unified lifecycle workflow.

CertiNext supports unified policy enforcement and reporting across both public and private CAs within a single management plane.

3. Certificate Type Coverage

CertiNext manages multiple certificate categories within enterprise environments, including:

- Web server (TLS/SSL) certificates
- Endpoint and device certificates
- Internal server certificates
- Load balancer certificates

- Kubernetes and container certificates
- Client authentication (mTLS) certificates
- S/MIME and document signing certificates (via CA integration)
- Private PKI certificates
- Code signing certificates (where supported through CA integration)

The platform is not limited to public TLS use cases but extends to internal infrastructure and device-level certificate governance.

4. Supported Enterprise Use Cases

CertiNext supports a range of operational and governance use cases, including:

- Automated web server certificate lifecycle management
- Private PKI lifecycle management
- Hybrid cloud certificate governance
- Kubernetes and DevOps certificate automation
- Network device certificate management
- Enterprise-wide certificate discovery and visibility
- Automated renewal and rotation aligned with shorter certificate validity periods
- mTLS and service identity management
- API gateway and load balancer certificate automation
- Short-lived certificate lifecycle management

The platform is structured to address both infrastructure teams and security governance teams.

5. Governance, Discovery & Lifecycle Automation

Governance and automation capabilities form a core component of CertiNext.

5.1 Enterprise Discovery Engine

CertiNext includes an IP-based discovery engine capable of:

- Single IP and IP range scanning
- Full port range scanning
- Custom port scanning
- Discovery across on-premises infrastructure
- Kubernetes and orchestration platforms
- Cloud-native discovery and visibility across AWS, with extensible architecture for Azure and GCP environments.
  Network devices such as firewalls and load balancers

During discovery, the platform extracts certificate metadata including issuer details, expiry information, root chain, and cryptographic algorithms.

5.2 Risk & Cryptographic Visibility

Discovery workflows also include validation checks such as:

- Expiry risk detection
- Outdated or weak algorithm identification
- Key strength validation
- Certificate vulnerability insights
- Centralized certificate-to-application mapping for ownership traceability
- Expiry trend analytics and reporting dashboards

This allows enterprises to assess cryptographic posture in addition to certificate inventory.

6. Lifecycle Workflow & Automation

CertiNext supports end-to-end lifecycle workflows including:

Discovery Request Approval Issuance Deployment Renewal Rotation Revocation Reporting

Key workflow capabilities include:

- Policy-driven and role-based provisioning workflows and configurable auto-renewal triggers
- Deployment scheduling (e.g., restricted deployment windows)
- Renewal notifications with configurable recipients and timing
- Certificate deletion and rediscovery
- Deployment rollback and retry functionality
- Zero-touch renewal capabilities, where supported by target systems
- Parallel deployment tracking across multiple endpoints

These automation features are designed to reduce operational overhead and help manage increasing certificate volumes.

7. Deployment Architecture

7.1 Remote Deployment Model

CertiNext supports remote deployment using secure protocol-based connectors and APIs, minimizing dependency on local agents, where supported by target systems.

This approach supports:

- Large-scale infrastructure deployment
- Hybrid environments
- Reduced dependency on endpoint agents

7.2 Agent-Based (Bot) Deployment

An agent-based model remains available for:

- Air-gapped environments
- Restricted access networks
- Environments requiring local execution

Both models operate within a unified lifecycle management framework.

8. Infrastructure & Ecosystem Integrations

CertiNext integrates with enterprise infrastructure components and protocols, including:

Infrastructure Components

- Kubernetes
- Web servers
- Load balancers (e.g., F5)
- Firewalls (e.g., Palo Alto)
- Network appliances
- API Gateways
- Web Application Firewalls (WAF)
- Reverse proxies

TCloud Platforms

- AWS
- Azure (in progress)
- GCP (in progress)

PKI & CA Systems

- eMudhra emCA
- Microsoft ADCS
- Sectigo
- GlobalSign

Protocol Support

- ACME (automated issuance where supported)
- SCEP (device enrolment use cases)
- EST/CMP (enterprise enrolment scenarios)
- REST-based APIs for Integration

These integrations enable interoperability across hybrid environments.

9. Private PKI & Crypto-Agility

CertiNext supports private trust hierarchies through emCA integration and provides flexibility for:

- Private root CA deployment
- Intermediate CA management
- Hybrid public-private trust models

The platform is designed to support crypto-agility strategies and can integrate with PQC-capable PKI infrastructures where underlying CA and HSM components support post-quantum algorithms.

10. Architectural Enhancements

Recent platform updates include:

- Backend re-architecture for improved processing efficiency
- Streamlined API endpoints
- Enhanced provisioning performance
- Enhanced user interface for operational efficiency and reporting customization
- Customizable reporting grids and export functionality
- Column-level filtering and configuration

These enhancements are designed to support enterprise-scale deployments and usability across global teams.

11. Operational Considerations

CertiNext includes operational features such as:

- Scheduled deployment windows
- Auto-rotation triggers
- Certificate revocation management
- Role-based access controls
- Reporting and audit visibility
- Legacy system compatibility considerations
- Role-based access control (RBAC) with segregation of duties
- Audit logging and exportable compliance reports
- Multi-tenant logical isolation (where deployed in shared environments)

These capabilities support operational continuity and lifecycle oversight.

12. Conclusion

CertiNext provides a structured approach to centralized, policy-driven certificate lifecycle management platform across public and private trust environments.

Through multi-CA support, discovery-driven governance, workflow automation, hybrid deployment models, and infrastructure integrations, the platform addresses the technical and operational requirements associated with managing increasing certificate volumes and reduced validity periods.