

CIPHERA | Use Cases Summary

Cryptographic Trust Platform for Mission-Critical Systems

Value proposition. CIPHERA helps organizations establish, govern, and maintain cryptographic trust across connected and disconnected environments, while preparing for the transition from RSA/ECC to post-quantum cryptography (PQC).

Primary Use Cases

#	Use case	Description	Business value
1	DDIL cryptographic operations	Maintain locally authorized cryptographic functions and trust decisions during disconnected, degraded, intermittent, or limited connectivity.	Mission continuity when links are unavailable.
2	Post-quantum migration	Inventory and govern cryptographic algorithms; support planned transition to ML-KEM and ML-DSA and appropriate hybrid approaches.	Reduce long-term cryptographic transition risk.
3	Certificate authority lifecycle	Manage root/intermediate CAs, certificate issuance, renewal, revocation, and policy-controlled profiles.	Consistent enterprise trust administration.
4	Key lifecycle management	Generate, distribute, rotate, archive, revoke, and destroy keys according to approved policies and integrations.	Reduce key-management errors and exposure.
5	Device and workload identity	Provision certificates and cryptographic identities for terminals, satellites, services, devices, and users.	Authenticate distributed systems at scale.
6	Mission-specific trust policy	Apply tenant, mission, organization, and role-based authorization to cryptographic operations.	Enforce least privilege and separation of duties.
7	Disconnected trust recovery	Synchronize approved policy and lifecycle state after connectivity is restored, with conflict handling and auditability.	Controlled reconnection and reconciliation.
8	Certificate and key governance	Enforce approval workflows, cryptographic policies, certificate profiles, and lifecycle rules.	Lower operational and compliance risk.
9	Audit and compliance evidence	Record key ceremonies, administrative actions, approvals, failures, and cryptographic configuration changes.	Support security reviews and investigations.
10	Deployment flexibility	Deploy as customer-hosted infrastructure or managed multi-tenant service where suitable.	Adapt to sensitive and regulated environments.

Representative Operational Scenarios

Disconnected SATCOM mission. A remote terminal or deployed node loses reach-back connectivity. Locally provisioned trust materials and authorized policies allow supported cryptographic operations to continue until synchronization is possible.

Enterprise PQC transition. An organization inventories certificate and key usage, pilots PQC-capable profiles, and stages migration of applications and devices while maintaining compatibility with legacy systems.

Controlled key rotation. A security administrator initiates a scheduled rotation, requires multi-person approval for sensitive actions, and produces an auditable record of issuance and distribution.

Suggested MVP Priorities

1. Certificate authority and certificate-profile management
2. Core key lifecycle operations and secure policy enforcement
3. DDIL-capable local trust workflows with bounded offline authorization
4. RSA/ECC and initial PQC algorithm support with migration controls
5. Tenant administration, RBAC, audit trails, and operational dashboards

Product Roadmap and Differentiation

Initial focus: trusted cryptographic operations in DDIL environments and practical PQC migration. Later extensions: richer HSM/KMS integrations, device enrollment protocols, automated fleet-scale rotation, advanced ceremonies, and expanded compliance reporting.

Why CIPHERA: combines cryptographic lifecycle management, mission-aware policy, and offline resilience in one operational trust platform rather than treating PKI as a standalone certificate issuance service.

Target Markets

Defense and SATCOM programs; aerospace and satellite operations; critical infrastructure; telecommunications; industrial/edge IoT; and regulated enterprises undertaking PQC migration.

Scope note: This document describes product use cases and proposed capabilities. Feature availability, security assurances, algorithm validation, and offline operating limits must be verified against the deployed CIPHERA release.