SOLUTION BROCHURE

Meeting Morocco's Cloud Compliance and Cybersecurity Requirements

Law n°05-20 · Decree n°2-24-921 · Arrêté n°3-17-25
(Bulletin Officiel n°7432)

ENTRUST
SECURING A WORLD IN MOTION

Overview

Accelerate compliance and strengthen data sovereignty with customer-controlled encryption. Entrust enables telecom operators, cloud service providers, and regulated organizations in Morocco to keep exclusive control of encryption keys – while maintaining the governance, separation of duties, and audit evidence needed for today's cybersecurity and cloud requirements.

Regulatory Context

Morocco's cybersecurity and cloud framework – anchored in Law n°05-20 and detailed by Decree n°2-24-921 – sets clear expectations for protecting sensitive systems and data in the cloud. Arrêté n°3-17-25 defines the technical qualification requirements for cloud service providers. In practice, organizations are expected to demonstrate robust encryption, disciplined key management, separation of duties, and auditability to support regulator and customer confidence. Concerned companies are expected to be compliant by the end of 2026.

Regulatory Alignment

Regulatory Requirement	Entrust Capability
Keep customers in control of encryption keys	Customer-operated Entrust CSP Key Manager for key ownership and governance
Prevent cloud/provider access to customer keys	Hold Your Own Key (HYOK) architecture
Standardize governance across the key lifecycle	Centralized key lifecycle management, policy enforcement, and separation of duties
Reduce insider-risk for cryptographic keys	Optional Entrust nShield HSMs with non-exportable keys
Produce audit evidence for compliance	Audit-ready logs and reporting to support compliance evidence

Architecture Options for Customer Key Ownership (KMIP Vault Isolation)

To help meet Moroccan cloud compliance expectations – and common customer requirements for key ownership, tenant isolation, and auditability – Entrust CSP Key Manager can be deployed using several validated patterns. The options below reflect VMware KMIP constraints and highlight the operational and compliance tradeoffs to consider.

Option 1: Single shared appliance with multiple vaults (one vault per customer)

A single Entrust CSP Key Manager appliance hosts multiple KMIP vaults, with one vault per customer. Vault selection is performed using vault-specific certificates (rather than separate IP addresses or URLs).

Pros

- Lower infrastructure cost and fewer appliances to deploy and operate
- Supported by VMware: KMIP with certificate-based vault mapping
- Each vault can use its own identity provider (IdP), giving customers control over access

Cons

- Shared appliance boundary (vault-level separation rather than full infrastructure isolation)
- All vault data is stored in the same underlying object store, limiting clean backup/restore isolation per customer

Note: because vaults share the same appliance boundary and storage, this model may not satisfy strict isolation or per-customer backup/restore requirements. These constraints should be confirmed during requirements validation.

Option 2: Single appliance with one vault per customer (dedicated VMware resources per customer)

A single CSP Key Manager appliance provides one vault per customer, and each vault is used to protect dedicated VMware resources (for example, separate vSAN or vSphere resources per customer). This can align with VMware's unit-of-protection constraints while improving logical separation.

Pros

- Improved logical isolation compared to Option 1
- Avoids appliance sprawl while keeping vault-level separation technically supported
- Works within VMware's unit-of-protection model when infrastructure can be separated per tenant

Cons

- Still a shared appliance and shared object store (residual multi-tenant concerns)
- Requires separate vSAN/vSphere resources per customer, increasing VMware operational complexity
- Backup/restore isolation remains limited compared to dedicated appliances

Design consideration: this option assumes VMware infrastructure can be separated per customer (for example, dedicated vSAN/vSphere resources). Confirm feasibility and operating model early in the design.

Option 3: One appliance per customer (one vault per appliance)

Each customer receives a dedicated CSP Key Manager appliance with a single vault. This model provides clear separation across operational and compliance boundaries.

Pros

- Cleanest isolation model for regulated environments
- Full separation of keys, vaults, backups, and operations – simplifying compliance and audit discussions
- Aligns with customer-held key expectations and removes multi-tenant edge casesss

Cons

- Higher infrastructure cost
- More appliances to deploy and manage operationally

Recommendation (when strict isolation is required)

Where requirements call for strict key ownership and strong customer isolation, Option 3 (one appliance per customer) is typically the best fit. It delivers the clearest separation, simplifies backup/restore boundaries, and supports a straightforward compliance narrative aligned with VMware KMIP support.

Summary

Entrust helps Moroccan telecom operators and cloud service providers meet cloud compliance and cybersecurity expectations with customer-controlled encryption – so customers retain key ownership while you strengthen governance and auditability. The architecture is designed to scale across regulated customers and workloads and to support national cybersecurity and data-sovereignty objectives.

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit www.entrust.com.

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION