>_ By: Mohamed Mohamed Elhelbawi

Built for Smarter AI Storage: Secure, Store & Feed AI Models

High-assurance, self-healing, and end-to-end encrypted distributed object storage engineered for enterprise and the public sector. Complete jurisdictional data sovereignty, client-held cryptographic custody, and **58.3% direct storage cost reduction** via hardware-accelerated Cauchy Reed-Solomon.

DATA_SOVEREIGNTY	STORAGE_SAVED	DURABILITY
100%	58.3%	11 Nines

Aarkam

The Problem

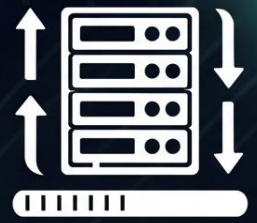
The Sovereignty & Compliance Dilemma

Strict Regulations

- KSA government agencies and vital enterprises must strictly comply with National Cybersecurity Authority (NCA) data residency regulations.

The Cloud Risk

- Public clouds (Azure, AWS, Google Cloud) introduce data **sovereighty concerns**, locking organizations into proprietary offshore storage platforms.



The On-Premise Headache

- Traditional on-premise storage is rigid, complex to scale, and lacks modern, **secure collaboration tools.**

The Core Issue: Organizatin for On-Premise critical Infrastructure compliance of on-premise and the agility of the cloud.

Aarkam

The Solution

Orchestrated Storage Infrastructure Ownership

Infrastructure Agnostic

Infrastructure Agnostic
We orchestrate the client's own physical, virtual, or edge storage drives. (We do not rent cloud space.)

Total Sovereignty

Total Sovereignty
Data never leaves the client's localized boundaries, fulfilling 100% unencilrrent residents of the KSA.

Enterprise Features

Enterprise Features
Modern web-based file management, collaborative and entry, lightning-fast preconting.

Military-Grade Security

Military-Grade Security
Fully isolated multi-tenant architecture with end-to-end envelope encryption.

Aarkam

SYSTEM BLUEPRINT

The Six-Engine Sovereign Architecture

Six independently deployable modules, client gateway, distributed data plane, persistence engine, erasure coding kernel, predictive telemetry sidecar, and unified operator CLI.

1. EDGE LAYER — Port :57776

Aarkam.IO & Gateway

Multi-tenant web portal, SigV4 S3 REST engine, DMZ rate limiter, and gradular RBAC orchestrator.

ASP.NET Core • SiqV4 • DMZ

2. CONTROL & DATA — Port :57777 / :57778

Rokka Distributed Plane

Raft MDN coordinator and per-host StorageNode deemon. Consistent hash ring placement with gRPC mTLS streaming.

Raft NDN • Consistent Hash Hing • gRPC

3. ENBDOCED STORAGE — Direct NVMe 1/O

Kdouja Engine

Embedded LSM-tree persistence with arena-allocated skip-list MemTables, WAL durability, and Direct I/O NVMe bypass.

LSM-Tree • Arena Skiplist • D_DIRECT

4. ERASURE CODING — AVX-512 SIMD

Ahmodi Math Kernel

Cauchy Reed-Solomon over GF(2⁸), 4-bit nibble table vectorization reaching 12.5 GB/s per core with 58% raw storage reduction.

SF(2*) • Cauchy-Solcomnon • AVX-512

simd

5. PREDICTIVE AT — Sidecar

Abodi Telemetry Sidecar

Observes physical drives via WMI/sysfs. Correlates SMART sectors and latency jitter to forecast failure and trigger proactive eviction.

SMART NL • Failure Runway • Hedged Reads

6. FLEET MANAGEMENT — or.EXD

Aarkam.AM (CLI Tool)

Unified claster management CLI. Manages Raft consensus, node evacuations, erasure coding benchmarks, rolling upgrades, and JSON automation.

Single Binary • POSTX Exit Codes • --watch

Aarkam

The Cryptographic & Storage Core

How Aarkam Works Under the Hood

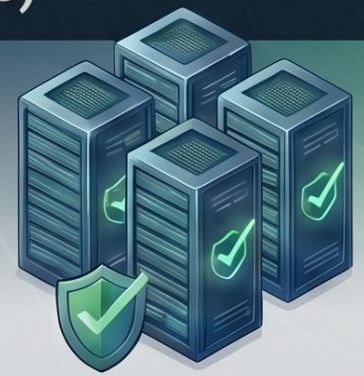
AarkamUI / API

Data Chunks

Cryptographic Operations

Kdouja (Storage Engine)

- Storage Node Management
- Heartbeat & Capacity
- Block-level Replication



Distributed, resilient storage management

Operations Core

CORE SERVICES

- Cryptographic Bos Coordination
- Secrets Management for Roites
- Capacity & Health Monitoring
- Distributed Cluster Governance

INTEGRATION APIs

- Aarkam Platform API
- KMS & PSCS#11 Interfaces
- Cloud Infrastructure Adapters

Rokka (Secrets Engine & KMS)

Centralized, sovereign Key Management System

- Envelope Key Wrapping for data
- Envelope Key Wrapping for secrets
- Master KEK / KMS Provider

KMS

Aarkam

How It Works

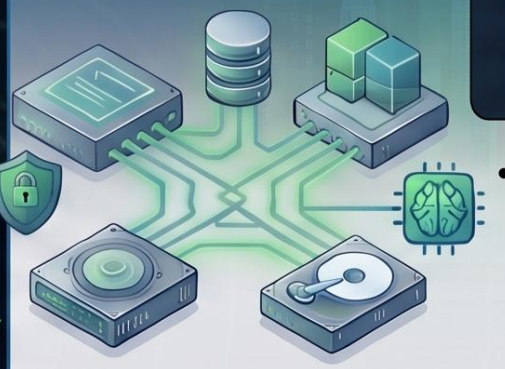
Decentralized Node Architecture (Abodi)

The Abodi is Node Agent Aarkam

installed on local hardware

- Scans, maps, and reports storage capacity automatically.

Smart Backing Matching



- Intelligent pairing of partitions to physical disk drives on Windows/Linux.

Central Control

- Centralized, web-based dashboard for managing permissions, tracking metrics, and secure file sharing.

Storage Directory Isolation

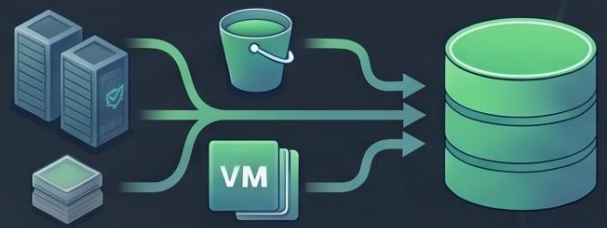
- Administrators manually designate folders as storage directories, protecting the OS from data write operations.

Aarkam

Aarkam Kdouja Engine

Resilient Distributed Storage Infrastructure

1. Unified Directory Layer



Aggregates mixed drives into one cohesive namespace.

Kdouja

Storage Node Management

2. Data Chunking & Replication

Splits files into secure block-level chunks for replication.

Heartbeat & Telemetry

Monitors real-time node health, routing away from failures.

Storage Node Management

4. Storage Protection

Enforces administrative directory-level mounts, protecting OS partitions.

Aarkam Kdouja is our proprietary data engine designed to orchestrate and manage storage across any infrastructure.

Aarkam

Aarkam Rokka Engine

Control Plane & Security Orchestration

1. Stateless Envelope Encryption

- ✓ Cryptographic Policy Enforcement
- ✓ Data Chunking & Tagging

Rokka

Coordinator Node

Rokka: Acts as the brain and security gatekeeper of the ecosystem, orchestrating the system's control plane.

2. Central Secrets Injection

- ✓ Non-persistent Node Credentials
- ✓ Dynamic Config Orchestration

3. Zero-Knowledge Architecture

Hosting cloud providers can't access data; keys wrapped & configs injected locally.

4. Auditability

Tamper-proof logging of every key access request; strict compliance.

Rokka is our proprietary control plane designed to orchestrate and manage security, key-custody, and audit logs across any infrastructure.

Aarkam

The Hybrid Scale Architecture

Ultimate Deployment Flexibility

1. Private On-Premise Clouds

Deploy Aarkam & Rokka KMS fully inside client's air-gapped physical data centers.

Aarkam Kdouja & Rokka KMS
(Unified Data & Security Logic)

Powered by pairing Aarkam Kdouja & Rokka

Central Rokka Vault

2. Compliance-Ready Public Clouds

Use standard public cloud machines for storage, while keeping all encryption **keys strictly** inside client's own **physical Rokka KMS** in KSA.

Deploy Aarkam & Rokka KMS fully inside client's air-gapped physical data centers.

Sovereign Edge Storage

Deploy edge nodes on local sites (factories, ships, regional offices) securely by a central **Rokka** vault.

Deployment capabilities traditional clouds cannot replicate.

Aarkam

International Standards & Frameworks

Global Assurance

ISO/IEC 27001:2022 — ISMS

Information Security Management

ISMS

Comprehensive implementation of Annex A security controls, covering cryptographic policy, access control enforcement, multi-tenant physical isolation, and incident management workflows.

- ✓ Annex A.8: Technological Controls
- ✓ Annex A.5: Information Security Policies

NIST SP 800-53 Rev. 5 — High Baseline

Security and Privacy Controls

NIST control

Architected to fulfill NIST High-Impact baseline controls for federal and global enterprise infrastructure, including AC (Access Control), SC (System and Communications Protection), and SI (System Integrity).

- ✓ SC-13: Cryptographic Protection
- ✓ AC-3: Access Enforcement (SigV4)

SOC 2 Type II

AICPA
Trust Services Criteria

Security

Availability

Confidentiality

Telemetry Stream
with non-repudiation symbol

Independently auditable controls validating operational effectiveness across the Security, Availability, and Confidentiality pillars. Continuous automated access confideiation. Continuus automated telemetry ensures non-repudiation.

- ✓ CC6.1 - CC6.8: Logical Access Controls
- ✓ A1.2: Environmental Availability & Failover

Aarkam

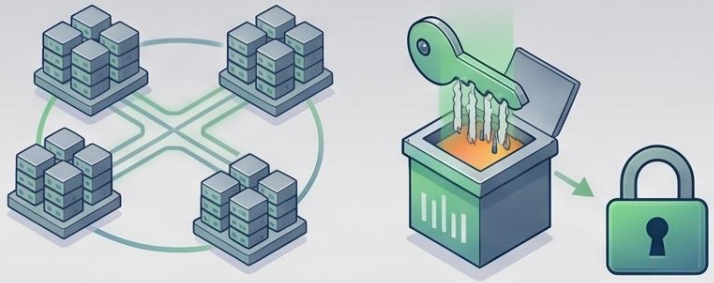
European Union Regulations & Directives

EU Mandates

Strict European privacy rights, critical infrastructure network defenses, and financial sector operational resilience.

EU GDPR — Articles 25 & 32

Data Protection by Design

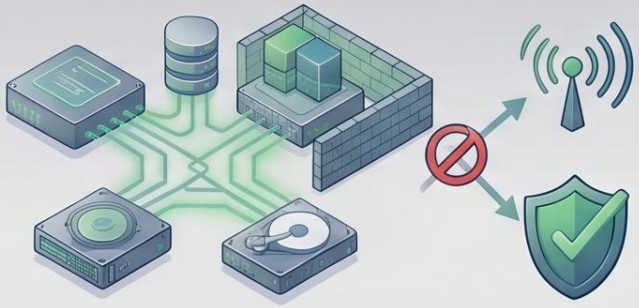


Default client-side encryption ensures personal data is safeguarded against unauthorized processing. Dedicated cryptographic key shredding satisfies the Article 17 Right to Erasure mathematically.

- ✓ Art. 25: Data Protection by Design & Default
- ✓ Art. 32: Security of Processing & Encryption

NIS2 Directive — Critical Infra

Critical Entity Cybersecurity

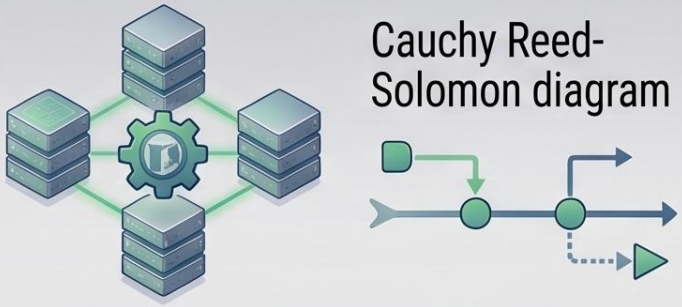


Mandated cybersecurity risk-management measures and supply chain security for essential entities. Air-gapped clusters operate with zero foreign remote remote telemetry dependencies.

- ✓ Supply Chain Isolation & Zero Telemetry
- ✓ Immediate Automated Incident Logging

DORA Framework — Financial Sector

Digital Operational Resilience



Ensures financial entities can withstand and recover from severe ICT disruptions. Cauchy Reed-Solomon erasure coding provides autonomous continuous operation during hardware failures.

- ✓ Multi-Node Consensus without SPOF
- ✓ Deterministic Disaster Recovery RTO < 5m

Kingdom of Saudi Arabia Sovereign Standards

KSA Sovereign · National Cybersecurity Authority (NCA) controls and SDAIA Personal Data Protection Law (PDPL).

NCA ECC-2:2024

Updated 2024

Essential Cybersecurity Controls

Strict alignment with the National Cybersecurity Authority's updated 2024 ECC baseline: end-to-end cryptographic defense, privileged identity governance, and continuous vulnerability telemetry.

- ✔ ECC §2-3: Cryptographic Protection
- ✔ ECC §2-8: Event Logging & Monitoring

CCC-2 & DCC-1

Cloud & Data Cybersecurity

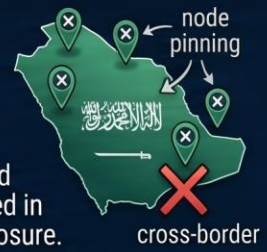
Compliance with Cloud Cybersecurity Controls (CCC-2:2024) and Data Cybersecurity Controls (DCC-1:2022). Guarantees tenant workload boundary isolation and verifiable air-gapped sovereign operations.

- ✔ CCC §1-2: Multi-Tenant Workload Segregation
- ✔ DCC §2-1: Data Classification & Protection

SDAIA PDPL

Law 2024

Personal Data Protection Law



100% sovereign in-jurisdiction storage node pinning ensures zero unauthorized cross-border egress. Master keys hosted in owned HSMs prevent external data exposure.

- ✔ Article 29: Cross-Border Transfer Restrictions
- ✔ Article 19: Confidentiality & Key Custody

HSM Cryptographic Custody & Air-Gapped Architecture

FIPS 140-3 Hardware Key Isolation · Complete Jurisdictional Autonomy

Client-Held Encryption Keys

Aarkam provides enterprise and sovereign sector operators with total cryptographic isolation. Data encryption keys (DEKs) are generated client-side and encrypted with key-encryption keys (KEKs) hosted strictly within customer-managed Hardware Security Modules (PKCS#11 / KMIP). Neither cloud vendors nor external operators ever have plaintext access.

Immutable WORM & Object Lock

Native support for S3 Object Lock in Compliance Mode enforces non-erasable, non-overwritable WORM (Write Once, Read Many) policies required for financial records, critical legal audit logs, and minimal registries.

Aarkam

The Market Opportunity

Tapping into KSA's Digital Transformation

Addressable Market:
Projected to exceed
$1.5 Billion

Enterprise IT & Cloud Storage Market

KSA Vision 2030:
Localizing digital infrastructure, scaling cybersecurity.

Target Audience

Government Ministries & Municipalities

Military & Defense Contractors

Banking & Financial Institutions

Oil, Gas, & Heavy Utilities (e.g., Aramco partners)

Aarkam

Business Model

High-Margin Software Licensing

Core Proposition:
we sell the **Aarkam management software.**

Block-level Replication
Distributed, resilient
storage management

Storage LIitation
Distributed, resilient
management

Summary:
- **Distributed, resilient** storage management
- 'vectorization" GF(2^8) text or somblean in Box 4
- Cauchy Reed-Solomon' GF(2^8) text in Box 4
- GF(2^8) and vectorization in Box 4

Envellope Key Wrapping for data
- GretorizationsGF(2^8)
- Port numbers

Envelope Key Wrapping for secrets
- Envelope Key depectism many, GF(2^8) and vectorization's looks
- Port numbers GF(2^8)
- Cauchy Reed-Solomon GF(2^8)

Master KEK / KMS Provider
- Keys provider assoitiated from vectorization" GF(2^8)
- AVX-512 and vectorization: Box 4

Aarkam

Product Traction

Built, Tested, and Validated

- **MVP 100% Complete:**
  Fully functional dashboard, node telemetry agent, backing drive mapping, and compliance restrictions built and ready.

- **Scalability Validated:**
  Heartbeat and capacity **telemetry successfully** tested across multi-TB physical enterprise enterprise setups.

Local Market Interest:

- Conducted initial discovery and validation interviews with 3 KSA government entities.

VERIFIED

SECURED

- Currently in discussion to finalize **2 corporate pilot agreements** for **on-premise deployment** in Q3.

Total effort: 2 years.
Project status: Active.

Aarkam

The Team

Domain Experts in Security & Scale

Cybersecurity DNA:

- Building military-grade encryption systems
- NCA compliance frameworks
- enterprise software systems

Led by professionals with deep domain expertise.

Proven Track Record:

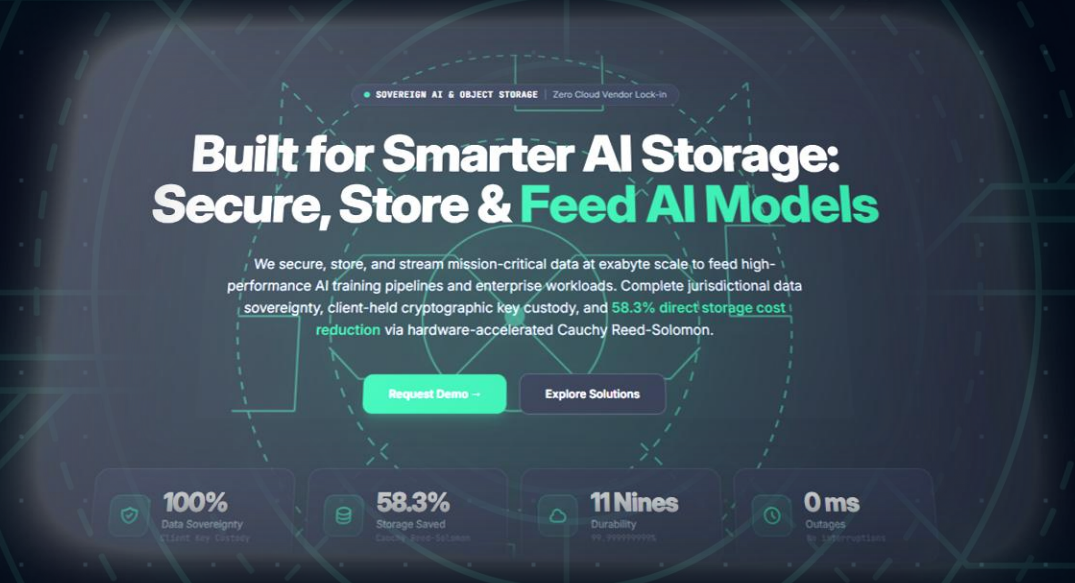
- High-availability database applications 99.99%
- resilient distributed software architectures
- suited for Saudi Arabia's regulatory landscape

Experience in designing tailored solutions.

Aarkam

Founded by **Mohamed Mohamed Elhelbawi**

Beta Version, NO Commercial registration



Thanks

Aarkam

https://aarkam.io/

Email: dr.m.elhelbawi@gmail.com

Phone: +966 595213497