mini-kms

Owner:
Reviewer:
Contributors:
Date Generated: Wed Oct 01 2025

Executive Summary

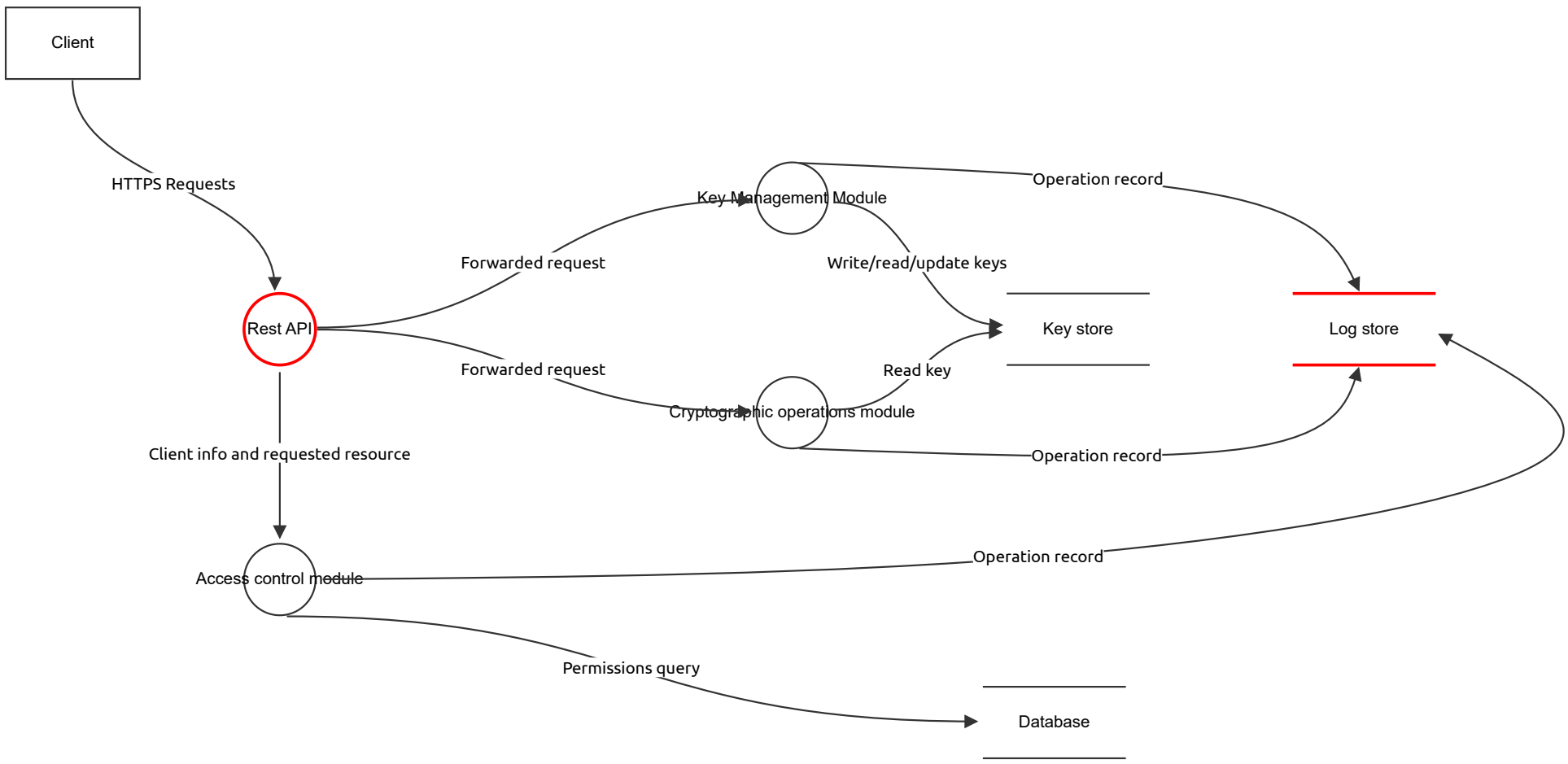
High level system description

Not provided

Summary

Total Threats	6
Total Mitigated	4
Total Open	2
Open / Critical Severity	0
Open / High Severity	2
Open / Medium Severity	0
Open / Low Severity	0

New STRIDE diagram



New STRIDE diagram

Rest API (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
16	The attacker overwhelms service with expensive cryptographic operations	Denial of service	High	Open	12	An attacker spams the Rest API with computationally expensive requests, exhausting server resources and making the service unavailable for legitimate users.	Implement rate limiting at the Rest API level.

Access control module (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
12	Attacker spoofs user idenity to access keys	Spoofing	High	Mitigated	10	An attacker obtains a user's JWT token and uses it to impersonate the legitimate user, allowing them to perform any operation as that user.	Strong authentication, secure token handling (short-lived JWTs), and mandatory TLS encryption. The Access control module is responsible for all token validation.

Key Management Module (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
17	User accesses another user's key	Elevation of privilege	Medium	Mitigated	5	A malicious authenticated user attempts to access or use a key they do not own by sending a request with a guessed keyId.	All data access logic within the Key Management Module (and other modules) must validate that the authenticated userId matches the owner userId of the requested key from the Key store.

Cryptographic operations module (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Client (Actor)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Key store (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
15	Attacker steals encrypted key material from the database	Information disclosure	High	Mitigated	10	An attacker gains read access to the Key store and exfiltrates all the stored, encrypted key material.	Envelope encryption ensures the data in the Key store is useless without the separate, securely stored Root Key.

Database (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Log store (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
13	Attacker modifies audit logs to hide malicious activity	Tampering	High	Open	12	An attacker with server access modifies or deletes entries in the Log store to remove evidence of their actions.	Shipping logs to a centralized, immutable storage. (Implemented) Restricted file permissions.
14	User denies performing a malicious action	Repudiation	Low	Mitigated	4	An authorized user performs a sensitive action and later claims they did not perform it.	Audit trails in the log store provide strong evidence linking users to their actions

HTTPS Requests (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Client info and requested resource (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Forwarded request (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Forwarded request (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Write/read/update keys (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Read key (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Operation record (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Operation record (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Operation record (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Permissions query (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations