SEMPER FORTIS SOLUTIONS

ENCRYPTION MANAGEMENT SERVICES UTILIZING FORNETIX™ KEY ORCHESTRATION™

Protect and Accelerate Your Enterprise—Unleash the Full Power of Encryption

Encryption can be a powerful cybersecurity instrument. But, unleashing the full power of encryption requires many encryption keys, which must be tracked and changed. Current cybersecurity products are not up to this task, impeding the effective implementation of encryption.

As part of a United States Air Force contract, Semper Fortis Solutions validated a new approach to key management based on the Key Management Interoperability Protocol (KMIP). Fornetix was established to mature the approach and Key Orchestration is the mature capability: it enables agile, dynamic key management which will work with existing encryption devices.

CENTRALLY MANAGE ALL OF YOUR KEYS

Key Orchestration centralizes the management of all keys and certificates and provides encryption policy enforcement at a granular level that is not delivered by traditional Key Management Systems (KMS). This reduces the attack surface in the event of a security breach and prohibits lateral movement.

Key Orchestration consists of four main components, which allow an organization to manage all encryption keys across all devices and servers throughout your enterprise—on premise, in the cloud, on IoT devices, at rest, or in motion.

1. The Key Orchestration Appliance (KOA) which comes in two models—KOA-1000 and KOA-2000—provides key management administration that is compliant with KMIP and which is configured to operate using the customer organization's policies for key management.

KOA-1000	KOA-2000
1U Rackmount System	2U Rackmount System
16GB DDR4 RAM	32GB DDR4 RAM
6 1GB RJ45/Copper Ports	6 1GB RJ45/Copper Ports
2 optional network upgrade slots*	6 optional network upgrade slots**
2-750w Hot-Swap Power Supplies	2-1000w Hot-Swap Power Supplies
Ability to Manage over 10M Keys	Ability to Manage over 100M Keys
FIPS 140-2 Compatible Secure Chassis	FIPS 140-2 Compatible Secure Chassis
	High-Availability Clustering Available

*4 x 1GB RJ45/Copper or 2 x 1GB Fiber Cards Available
*4 x 1GB RJ45/Copper, 2 x 10GB RJ45/Copper, 2 x 1GB Fiber, or 2 x 10GB Fiber Cards Available

2. The Key Orchestration Client is installed on a server or device and can push or pull keys generated by KOA or any other KMIP-compliant server.
3. The Key Orchestration Agent is used to manage keys on devices that are not compliant with KMIP and therefore the KOTM client cannot be installed.
4. The Key Orchestration API can be used to build custom applications or clients that can communicate with the KO Appliance.

Key Orchestration includes a standard capability to integrate Hardware Security Modules (HSMs) using PKCS#11; this provides for additional security and allows an organization to continue to use existing HSMs for storage of their cryptographic keys.

SIMPLIFY AND AUTOMATE WHILE MAXIMIZING SECURITY

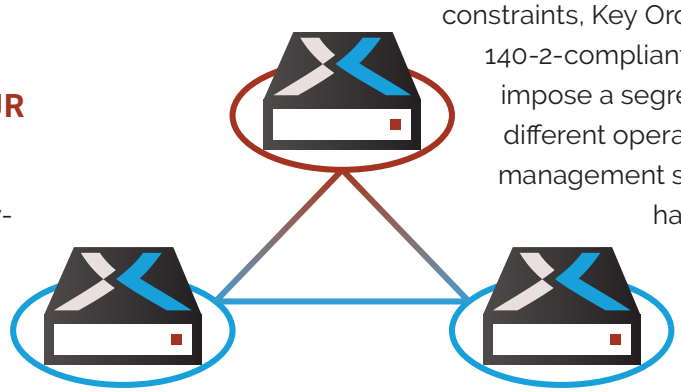
Key Orchestration is a policy-driven key management solution that automates and simplifies the entire key lifecycle. Rules based on an organization's key management policies are created in the KOTM Appliance: they define the rules around the who, what, when, where, and how of key lifecycle management. Compositions and Jobs are then created and scheduled in the KOTM Appliance: they are the catalysts for automating key generation, activation, rotation, and revocation.

Key Orchestration manages keys via hierarchies and groups so policies can be automatically applied to one or many devices. For example, if 50 web servers use the same key type, one policy dictating key type can be created for all 50 servers. If 5 of those web servers have a different maximum

key length, rather than having to use the smaller (and less secure) max length for all your web servers, one key length policy can be created for the 5 web servers and a separate one for the other 45.

SCALE TO THE SIZE OF YOUR ENTERPRISE

Key Orchestration is built on a fully-distributable, highly-scalable architecture that can support clustering, failovers, and backup/restore processes.



SECURE KEY MANAGEMENT

Key Orchestration enforces FIPS 140-2-compliant security constraints, Key Orchestration enforces FIPS 140-2-compliant security constraints, which impose a segregation of duties among the different operator roles or functions of a key management system so that operators only have access to those aspects of the key management process for which they have a functional responsibility.

SEMPER FORTIS SOLUTIONS, LLC

Semper Fortis Solutions (SFS) is a preferred reseller of Key Orchestration to the Federal Government.
SFS is focused on Cyber Security, Information Assurance, Key Management, Multiple Levels of Security (MLS), software-based Cross-Domain Solutions (CDS) and Advanced Analytics using Artificial Intelligence and Machine Learning.
SFS applies in-depth knowledge of our customers to focus on solving their really hard technical problems; e.g., dynamic key management and MLS by applying existing and emergent technology in new and integrated ways. The solutions we've identified include Key OrchestrationTM, software-based CDS, the application of a secure kernel hypervisor to achieve Multiple Independent Levels of Security and Safety (MILS) and analytic tools which permit rapid analysis and integration of concurrent data streams from several sensors.

Don't Just Manage Encryption—*Orchestrate* It!

SEMPER FORTIS SOLUTIONS

1602 Village Market Blvd, STE 210
Leesburg, VA 20175

(703) 544-5266