



# An Introduction to Crypto Command Center and HSM Provisioning for the Cloud

TECHNICAL WHITEPAPER

Crypto Command Center represents a revolution in provisioning cryptographic resources, and firmly plants the HSM and its associated key management and cryptographic functions in the evolving cloud and virtual world.

## Table of Contents

Introduction.....	2
Crypto Command Center Concepts .....	2
Provisioning System Components .....	3
Crypto Command Center .....	3
Crypto Command Center API .....	3
Crypto Command Center Client .....	3
Crypto Hypervisor Provisioning Detail .....	4
Create A Catalogue Item .....	4
Request A Service .....	4
What Does It Mean To Administrators? .....	5
What Does It Mean To Users? .....	6
Deployment Scenarios.....	6
Crypto-As-An It-Service (Caits) .....	6
Public Cloud .....	6
Private Cloud .....	7
What's Next.....	7

### Proprietary Notice:

This document contains proprietary information which shall not be reproduced or transferred to other documents and shall not be disclosed to others or used for manufacturing or any other purpose without prior written permission of SafeNet, Inc. SafeNet Proprietary and Confidential information is exempt from public disclosure under the Freedom of Information Act [5 USC 552 (b) (4)], the Arms Export Control Act [22 USC 2778 (e)], the Export Administration Act [50 USC APP. 2411 (c)] and the Trade Secrets Act [18 USC 1905].

## Introduction

Businesses and organizations of all types and sizes are embracing virtualization and cloud computing concepts to make more efficient use of their own IT infrastructure and to expand their IT capabilities, as required, by obtaining virtual computing resources from third-party providers. To realize maximum efficiency, all IT components should be manageable following the cloud computing model. With this in mind, SafeNet developed the world's first Crypto Hypervisor. The Crypto Hypervisor is the first solution that virtualizes hardware-based cryptographic modules into consumable, elastic, and isolated cryptographic resources for use by virtual applications in need of encryption. A fundamental component of the Crypto Hypervisor is the Crypto Command Center, which provides the capability to define, manage, and deploy cryptographic resources on an as-required basis.

## Crypto Command Center Provisioning Concepts

Before describing Crypto Command Center in detail, there are a number of concepts that must be introduced.

A crypto module is an entity that provides key management and cryptographic services. The crypto module can take multiple forms. As a physical device, it is known as a hardware security module (HSM). It could be in the form of a PCI Express expansion card plugged into the backplane of a server. This expansion card can be in the same server as the consumer of the cryptographic services or can be installed on a remote machine accessible on a network. Another physical manifestation is as a network-attached, securely-enclosed appliance. Inside this secure enclosure is a PCI Express expansion card that provides the cryptographic services.

A service provider is an organization that manages a pool of crypto modules to provide cryptographic and key management services to third-party consumers. The service provider and consumer might belong to separate sub-organizations within a larger company or organization, in which case we say that represents a private or enterprise cloud deployment. For many large organizations, this is the likely first step in “moving to the cloud” – one group within the company, for example, wants to reduce duplication and offer services to the rest of the company through a common set of devices. The two players might also be in completely separate commercial organizations, where the service provider is making its services available over the Internet to any subscriber and not just customers from within a larger group. This deployment scenario is known as public cloud.

SafeNet HSMs have the ability to segregate cryptographic capabilities into virtualized HSM subunits called partitions. A physical HSM consists of one or more partitions. A consumer of cryptographic services may want to use the entire physical HSM or at least ensure that no other consumer uses it. Alternatively, a consumer may be satisfied using a single partition while other consumers use other partitions on the same HSM.

Crypto Command Center manages crypto module (including HSM and partition) resources and their allocation to consumers. A resource may be physical (e.g., a specific PCI-e card) or virtual (i.e., the specific physical instance is not important). The mapping between a virtual module and a physical HSM or HSM partition is “cloudy”: the consumer does not generally know which physical HSM or partition has been allocated to provide the virtual HSM resource, and the virtual module could appear to behave like a physical HSM that is different from the one actually allocated (e.g., it could look like an appliance but in fact be based on the Luna stand-alone product, Luna PCI 5.x, with appliance components executing alongside the HSM).

Although Crypto Command Center offers an enhanced ability to manage HSMs by abstracting the devices for the consumer, it does not abstract the access and control of the HSM usage from ownership by the consumer. Crypto Command Center allows for full control of the cryptographic usage of the HSM device to be owned by the consuming party. This control offers a clear separation between the provider and the consumer when using Crypto Command Center, something of significant advantage to both.

Crypto Command Center manages the set of devices available for use as subsets (pools) belonging to different user organizations. A user who wishes to obtain crypto module services must do so within the pool of devices allocated to his/her organization.

The service provider uses Crypto Command Center to publish the list of resources available for selection by the consumers. This takes the form of a catalogue, which can be browsed online, providing an organization's consumers with an easy-to-navigate and easy-to-use portal interface. Each catalogue item specifies the service(s) provided, the crypto module type, and parameters such as performance level, storage space, etc. Potential Crypto Command Center consumers will have a variety of use cases requiring HSM services. The requirements of these use cases are one way in which an HSM administrator might derive and identify the various resources to be offered in the catalogue. The service provider must maintain a device pool of suitable crypto modules to satisfy consumer requests as they arrive.

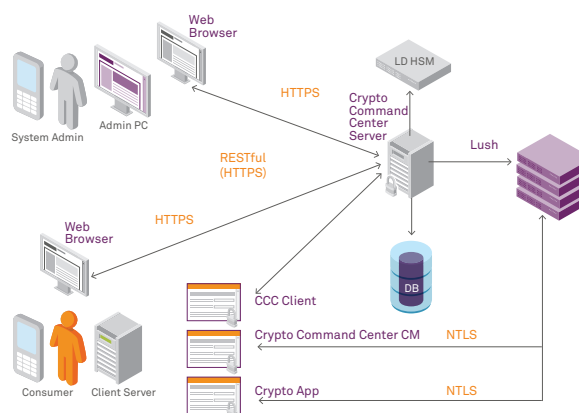
All of the core provisioning operations carried out using Crypto Command Center can also be incorporated into customer or partner software using the Crypto Command Center API. It is a stateless network transaction API that follows the REST architectural model. Thus, the Crypto Command Center functionality is available as a Web service via the GUI, or built into customer or partner software and tailored to meet their specific needs.

## Provisioning System Components

The Crypto Command Center provisioning system is based on three main components:

- Crypto Command Center
- Crypto Command Center API
- Crypto Command Center Client

Figure 1: Crypto Command Center Provisioning Components  
High Level Architecture



### Crypto Command Center

Crypto Command Center, as the GUI portal for HSM provisioning, acts as the primary interface for service provider administrators and consumers. Using the Crypto Command Center API, Crypto Command Center is able to perform all of the usual start-up administrative tasks while hiding from the consumer (and the administrator to a lesser degree) the complex, tedious steps that would normally be required to prepare the module for use.

### Crypto Command Center API

The Crypto Command Center API is a simple REST API that enables the administrator and the consumer to remotely perform the administrative actions needed to allocate a crypto module for use.

### Crypto Command Center Client

The Crypto Command Center Director Client uses the Crypto Command Center API to get and release HSMs via Crypto Command Center, as well as to get a catalogue of HSM services. It includes command-line utilities to accomplish these operations.

## Crypto Command Center Provisioning Detail

The best way to present the Crypto Command Center provisioning system and enable a discussion of its advantages is to consider the detailed sequence of steps necessary to administer the resources and make use of them. The description also puts particular focus on two simple but extremely common examples – the first being how to make a resource available as an administrator, and, the second, how to request a service as a consumer—to show the API calls invoked in performing those actions and, as previously noted, the clear separation of access and control for both roles.

The first thing the administrator must do is **register** devices for use. Each device is registered, specifying its attributes such as performance level, security policy settings, and storage capability. Once devices have been registered, they must be **allocated to pools** and each pool must be **associated with an organization**.

The administrator can then create a catalogue of services for each organization and begin to populate the catalogue with requestable items.

### Create a Catalogue Item

To create a catalogue item, the administrator must provide a name and description (to assist the user in selecting appropriate services), as well as specifying the service type (e.g., HSM or HSM Group), the member type (e.g., SA partition), and the capabilities of that resource. The API is invoked as follows:

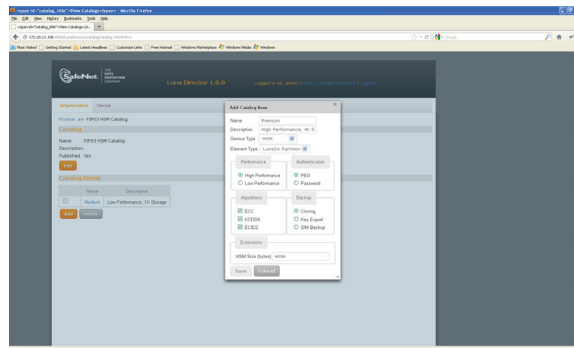
URL:/admin/organization/{orgId}/catalog/{catId}/item Method: POST

Item name

Item description

Link to resource type (e.g. SA partition)

Capabilities (subset of resource type capabilities)



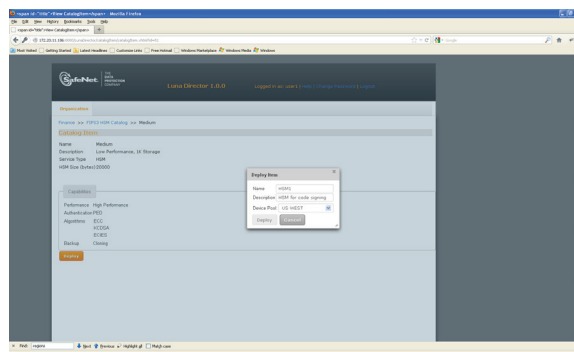
### Request a Service

A consumer can request to deploy a service by selecting the appropriate item from the catalogue. The API is invoked as follows:

URL:/usr/organization/{orgId}/catalog/{catId}/item/1/action/deploy Method: POST

Pool id

Extensions (partition size)



## **The Importance of Protecting Cryptographic Keys**

*“As the use of encryption grows and various solutions are deployed, key management becomes exponentially critical and complex. Mismanagement of keys can expose an organization to unnecessary risks.”*

*-Gartner*

The consumer can now **initialize** the service (establish passwords, PED keys, etc.) to make it ready for use by his/her applications. When the service is no longer required, the consumer can **release** the service.

For consumers, all of the steps required to request and initialize a service for operation can be done remotely, including full use of Remote PED, from the comfort of their workstations. Getting access to crypto module resources, putting them into service and retiring them when no longer needed could not be simpler.

## **How Does Crypto Command Center Provide Role Separation?**

Crypto Command Center creates a clear separation between the consumers/users of HSM resources and administrators. With Crypto Command Center in place, users have no access to the administrative interface of the HSM – the user is presented with a set of abstracted HSM services from which he/she can choose. Having chosen a service to deploy, the user then has the ability, through the Crypto Command Center user interface and the client-side utility Crypto Command Center CM, to initialize it and make it ready for use.

Conversely, administrators have access, through the Crypto Command Center administrator page, to the HSM administrative functions in order to initialize and configure new HSMs to be deployed in pools, but once a user has initialized a service, the administrator has no access to the user’s keys and crypto functionality.

This role separation is based on the PKCS #11 Security Officer and User roles but goes beyond PKCS #11 by separating the administrative and user interfaces to ensure that one individual cannot easily assume both roles (as is normally the case with PKCS #11).

The Crypto Command Center software uses an attached G5 HSM to securely manage the various credentials needed for access to Crypto Command Center and from Crypto Command Center to the installed HSMs. This enables Crypto Command Center to access administrative functions on the HSMs in order to, for example, initialize an HSM and create an empty partition.

## **What Does It Mean to Administrators?**

The Crypto Command Center provisioning system brings with it a number of features of interest to system administrators. Some of the more important advantages include the following:

- It separates the physical deployment of crypto modules from their “logical” deployment. This allows the administrator to have complete control over the installation, initial configuration, and administrative maintenance operations without interfering with the use of crypto module resources by user applications. Deployments no longer need to be “big bang” system projects – they can now be incremental and respond to the real need at the time rather than an estimate whose accuracy is never understood until the system goes live (or has been in operation for some time).
- Administrators do not need to be aware of how the services of the crypto module are being used, and application owners do not need to be aware of the detailed configuration of the crypto module(s) providing the service.
- The Crypto Command Center provisioning model allows the organization providing the crypto module resources to centralize their expertise in one group, which is responsible for all aspects of installation and configuration of the crypto modules. This group can then focus on ensuring the best possible availability, policy, compliance, and security of the modules.
- Administrators can, by virtue of the catalogue items created, provide as simple or as sophisticated a set of services as the user organization(s) require. In cases where the users are not “crypto savvy,” for example, the administrator might choose only a few straightforward service choices. For user groups with crypto experience, on the other hand, the administrator might choose to open it up and provide a broad range of configuration options.

- Because the Crypto Command Center provisioning system uses the Crypto Command Center API at its core, administrators can feel confident in using the API themselves to integrate Crypto Command Center provisioning within a broader cloud provisioning system. The ability to use the API in this manner allows organizations to recognize the efficiencies associated with a consolidated provisioning environment.

### What Does It Mean to Users?

Users reap some obvious benefits – simplicity, flexibility, and scalability, as well as no changes to applications in order to take advantage of the new provisioning model.

Simplicity and flexibility have already been described. Scalability is also important in many cases since processing workloads only tends to increase over time and the ability to easily add more crypto resources as required can be essential to success.

An intangible benefit, associated with integrating the Crypto Command Center Provisioning system into a more general cloud provisioning system, is that consumers only need to understand and use one interface for all of the resources they need. Having one multi-purpose interface (whether Web- or client software-based), rather than several special-purpose interfaces, not only improves the user experience, it also reduces the opportunity for and likelihood of error.

### Deployment Scenarios

Some of the expected deployment scenarios were briefly mentioned earlier. With the background of Crypto Command Center provisioning features and its components, it is now possible to examine in more detail how it might be used in each of the deployment scenarios.

#### Crypto-as-an-IT-Service (CAITS)

In a crypto-as-an-IT-service (CAITS) deployment, a corporation owns, installs, and maintains a centrally managed pool of Luna HSMs, allocating resources to departments, divisions, or business units based on the specific needs of each. Consolidation/centralization of the HSMs is the usual business driver for this deployment scenario. Having the pool of HSMs centralized enables standardized security practices and operational efficiencies to be gained in the allocation of the resources. There is often a desire to centralize high-value resources like HSMs and, prior to the Crypto Command Center provisioning system, that normally meant having to centralize the management of everything to do with the HSMs and the way in which they are used (i.e., HSMs, application servers, and applications). With provisioning in place, the central HSM group can concentrate on managing the HSMs, while other groups can manage the servers and applications they require.

Resource allocation can follow a “push” model, where the provisioning tools are used by the central managers to provide the appropriate sets of resources to the individual user groups. Allocation can also be done on a “pull” basis where each user group selects the resources it requires based on the catalogue offerings created by the central managers. Thus, the HSM central managers are relieved of the responsibilities of day-to-day administration of the individual HSMs, as well as having the burden of server and application management lifted from them. This allows them to remain focused on providing up-to-date, highly secure crypto resources to the user groups within the company. Likewise user groups no longer need to know the details of HSM installation and setup, and can focus on using the cryptographic services within their application.

#### Public Cloud

In a public cloud deployment, a service provider owns, installs, and maintains Luna HSMs for the purpose of renting cryptographic services in the general marketplace. A public cloud provider offers Luna HSMs for consumption in a way similar to how it offers customers access to virtual machines. The model used to offer and obtain HSM services may either parallel that used for VMs or incorporate HSMs into it, making cryptographic services simply an additional attribute when ordering up a VM. It is this latter model that we believe will prevail.

## What Do You Get with Crypto Command Center Package?

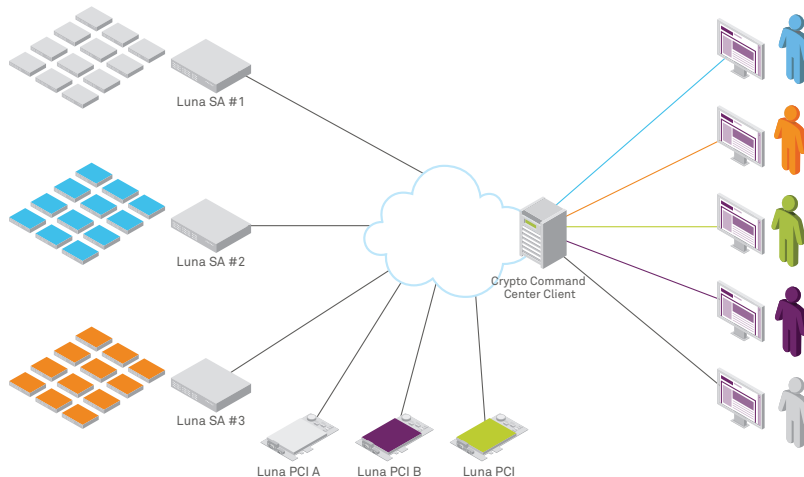
- G5 USB attached HSM
- **Crypto Command Center Server:** Web application responsible for allocating use of HSMs
- **Crypto Command Center Provisioning Client:** Command line tool to configure Luna Client access to HSMs allocated through Crypto Command Center
- **SDK:** API reference, programmer's guide and sample applications that demonstrate how to use the REST-API

## Private Cloud

A private cloud deployment is identical to a public cloud deployment but uses third-party software extended for the specific purposes of the organization or community deploying the cloud.

Two variants of a private cloud deployment may emerge. In the first deployment, the private cloud provider makes a client available to obtain virtual machines from the infrastructure and makes the Crypto Command Center Client available to request and release Luna HSMs. This variant deploys Crypto Command Center within the infrastructure. The advantage of this deployment is that it requires less integration but at the expense of a more disparate interface for the Crypto Administrator. Figure 2 shows an example of this variant deployment.

Figure 2:



The deployment option that is expected to be most popular stands up a third-party Cloud Director with Crypto Command Center provisioning functionality integrated into it. In this deployment, the Crypto Administrator has just one interface to request and release virtual machines and Luna HSMs.

## What's Next?

Crypto Command Center already represents a major step forward in making Luna HSMs cloud-friendly. It follows the same usage patterns as customers are accustomed to in deploying Virtual Machine services over the network. It provides administrators and managers with an easy-to-use interface with which to manage and offer HSM services. From the consumer perspective, it allows for easy adoption by user communities who might have previously been reluctant to adopt the technology. And, whether an organization fully embraces the cloud computing model or not, Crypto Command Center offers a modern, easy-to-understand GUI interface that brings real value to the consumer.

SafeNet understands, however, that there are still features required that will further enhance the usability of Luna HSMs in the cloud. SafeNet is committed to the ongoing effort to extend the Crypto Command Center and its ability to evolve with our customers, as their needs evolve...wherever that takes the HSM in the virtualized and cloudy world!

**Contact Us:** For all office locations and contact information, please visit [www.safenet-inc.com](http://www.safenet-inc.com)

**Follow Us:** [www.safenet-inc.com/connected](http://www.safenet-inc.com/connected)

©2013 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners. WP (EN)-02.19.13