Intralinks Customer Managed Keys

Technical Overview

Version 2.0
October 2014

About This Document

Purpose

This document provides an overview of the technical collateral and other information to help set customer expectations and understanding of this capability.

Intended Audience

Intended audience for this document is technical or compliance audience within large enterprise customers of the Intralinks service.

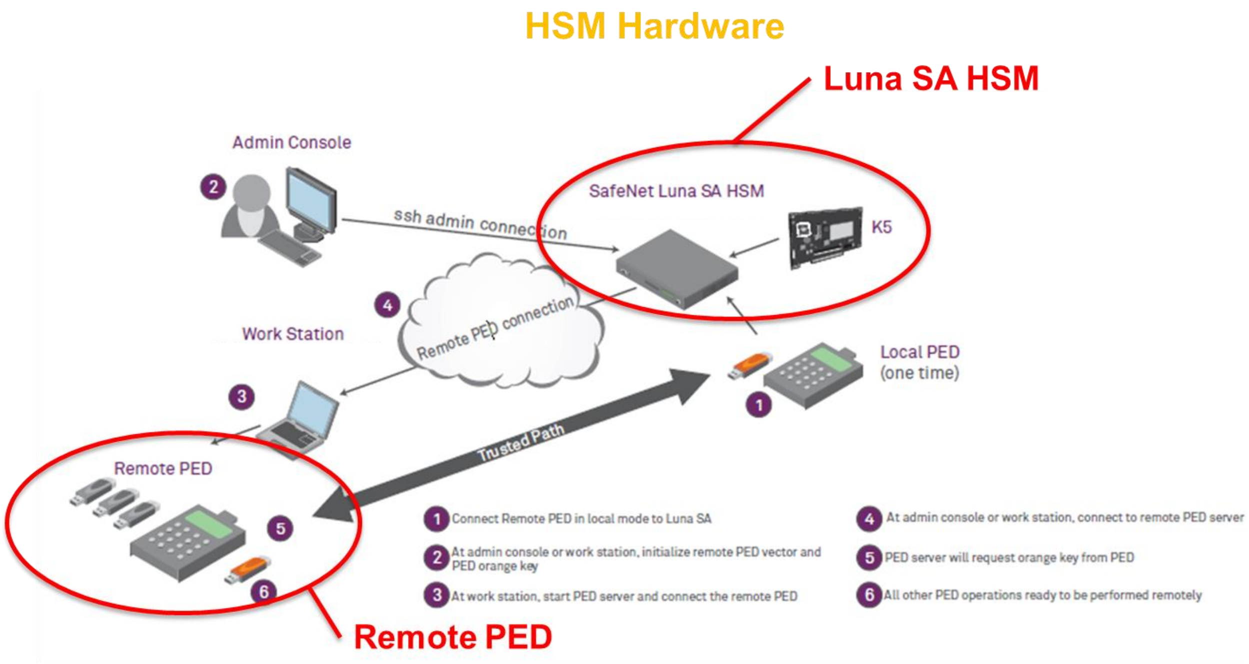
What is CMK?

CMK

Customer Managed Keys (CMK) is a combined hardware/software solution that provides customers control over their own master encryption keys, where they can generate, rotate and deactivate keys according to their own policies and procedures.

CMK Hardware Components

The hardware components of the CMK service are shown and described below.



1 Connect Remote PED in local mode to Luna SA

2 At admin console or work station, initialize remote PED vector and PED orange key

3 At work station, start PED server and connect the remote PED

4 At admin console or work station, connect to remote PED server

5 PED server will request orange key from PED

6 All other PED operations ready to be performed remotely

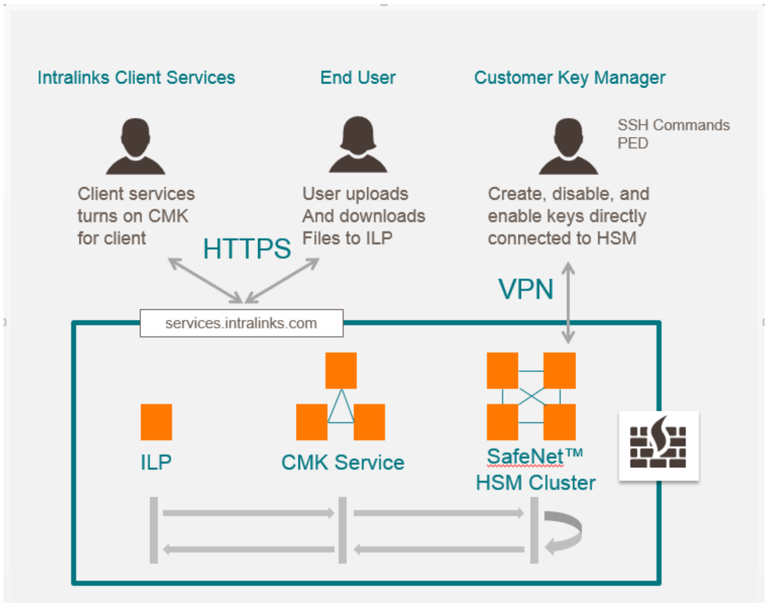
HSM

Hardware Security Module (HSM) is a specialized server that can be partitioned into multiple tenants where each tenant is assigned to a specific customer. Currently, Intralinks is using the SafeNet™ Luna 7000 SA HSM with remote PED access for this component of the service. These HSM devices are configured in a cluster of four HSM modules which provide redundancy and high availability.

PED and USB Keys

Pin Entry Device (PED) is a small specialized keypad used in conjunction with a USB key to authorize access to a specific HSM partition. A customer will use a PED and USB Key by connecting them to a specifically configured PC at their location in order to manage the HSM partition that has been assigned to them.

How does CMK work?


Intralinks Client Services
End User
Customer Key Manager
SSH Commands
PED
Client services turns on CMK for client
User uploads And downloads Files to ILP
Create, disable, and enable keys directly connected to HSM
HTTPS
VPN
services.intralinks.com
ILP
CMK Service
SafeNet™ HSM Cluster

Encryption / Decryption Processing

The CMK capability is embedding a new key encryption key (KEK) and an additional step in the encryption and decryption file storage and retrieval processing. This new step performs an extra level of encryption/decryption using the customer defined encryption key. Once this extra encryption step has been used to save a document, the file retrieval process must perform the corresponding step in the decryption process. If the customer key is unavailable for Intralinks to perform this corresponding decryption step, the documents are unusable.

Because this new step is integral to all file storage operations, once a customer defines their key and enables this functionality, any files that are stored in the customer's Intralinks repository will require the customer key to decrypt them and make them usable.

Customer Controlled HSM Partition

Once a customer has been setup and configured to access their assigned HSM partition as the partition owner, the customer has full control over the contents and usage of that partition. In addition to the partition owner, there is another type of user known as the "use" user. This "use" user is only able to perform encryption and decryption operations within a partition. This "use" user is unable to perform any of the partition management functions or view the encryption keys. The Intralinks application interacts with the HSM as a "use" user.

The following operations can be performed by the customer (i.e. partition owner) directly on the HSM device:

Change partition owner password – A customer changes the partition owner password so that only they are able to login as the partition owner. This is the first activity the customer will perform to ensure that only they can login as the partition owner going forward. The partition owner is the only user who is able to perform any of the other operations defined in this section. Please note that the password alone is not enough, they must also use the correct USB key (Orange) in order to access the partition.

Generate encryption key – A command can be run that automatically generates a 256 bit encryption key within the HSM device(s). The customer will be able to run a validate command to ensure each of the HSM devices was successful to generate the key.

Label encryption key – The customer can assign each encryption key a unique label. These labels are shared with the Intralinks service so that we know which key to use for the encryption/decryption processing.

Disable decryption processing for specific key label – The customer can disable a key such that it cannot be used by the "use" user for decryption. Once a key is disabled, the "use" user will be unable to decrypt any data that was encrypted with the now disabled key.

Delete encryption key for specific key label – For customers who rotate their keys, they will be able to permanently delete old keys once they are no longer needed. It is important that the key rotation process has completed fully before a customer deletes a key.

> **NOTE**: *If a customer deletes a key that is needed to decrypt data, that data will be permanently lost.*
>
> **NOTE**: The ability for a customer to rotate keys will not be supported in the first release. It will be supported in the next release.

Remote PED Access to HSM

In order to provide customers direct access to their HSM partition and control over the encryption processing, Intralinks will (through Professional and Client Services) configure a set number of PCs at the customer's location(s). These PCs will have specific software installed (SafeNet™ SSH Command Line Interface) and have network connectivity to the HSM devices.

In order to access their HSM partition from one of these PCs, the customer will plug the PED into the USB drive on the PC and then plug the USB Key into the PED. Once this is done, they will be able to log into their partition and perform the various operations described in the preceding sections

What is the Value of CMK?

Ultimate Control in Customers' Hands

Companies who put their data in the hands of service providers need assurances that they are the ultimate owners of the data. By giving them the ability to shut off access to their data, companies gain a level of control that ensures they still control the data.

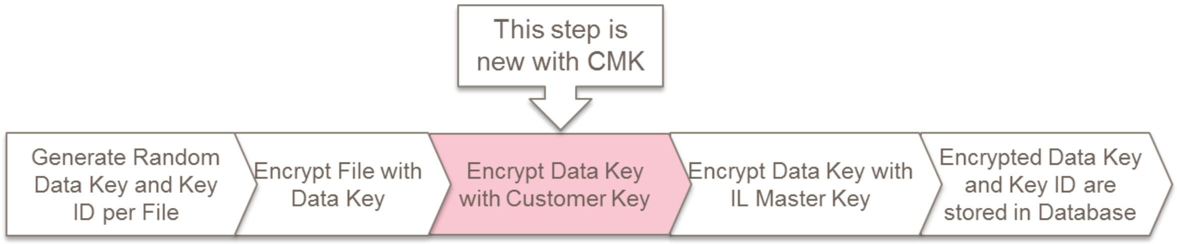
Regional Data Storage Alternative

A business case can also be made that by holding the encryption keys themselves, customers may have another option worth considering when defining their compliance with data sovereignty laws.

Increased Security Breach Protection

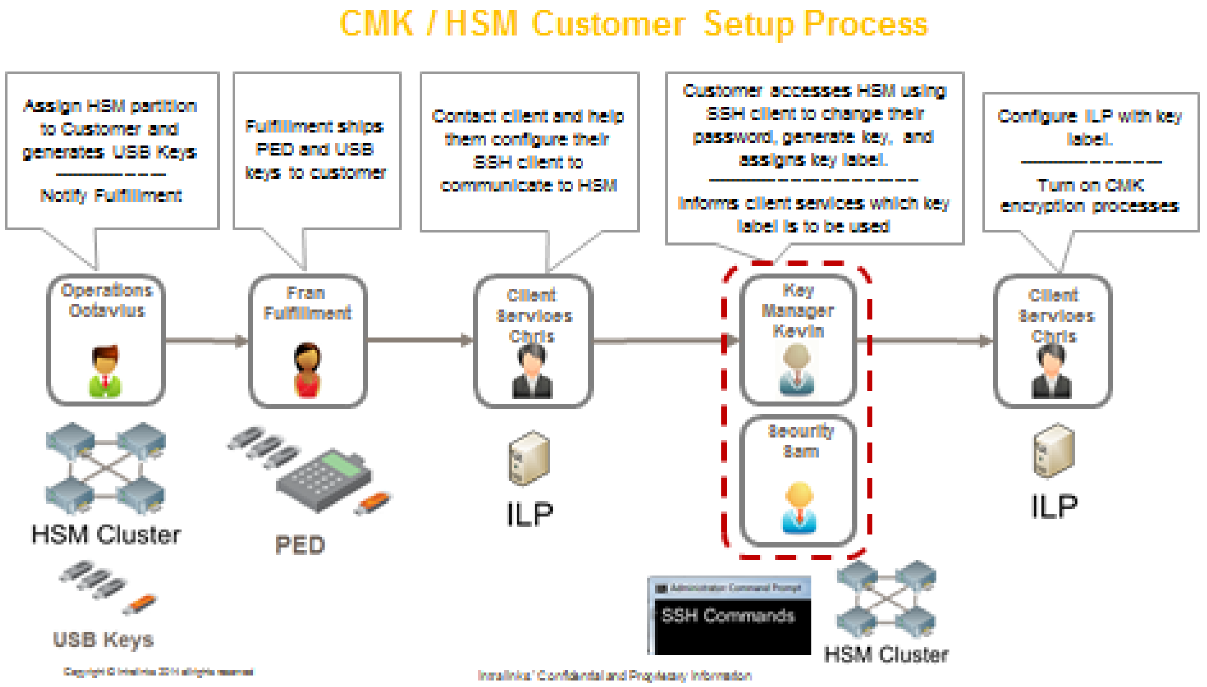
The unique process Intralinks has implemented where we encrypt the customer's data keys with our own master key in addition to the customer managed key, means that even if there is a breach at the customer's end, the files are still safe because the process requires both the customer's key as well as the Intralinks master key. The diagram below shows how files are encrypted and all the keys involved in the process.

Encryption Process when Uploading a Document


This step is new with CMK
Generate Random Data Key and Key ID per File
Encrypt File with Data Key
Encrypt Data Key with Customer Key
Encrypt Data Key with IL Master Key
Encrypted Data Key and Key ID are stored in Database

CMK Setup and Fulfillment Process

The following diagram provides a high level view of the fulfillment and initial setup process for a customer who purchases CMK:


CMK / HSM Customer Setup Process
Assign HSM partition to Customer and generates USB Keys
Notify Fulfillment
Fulfillment ships PED and USB keys to customer
Contact client and help them configure their SSH client to communicate to HSM
Customer accesses HSM using SSH client to change their password, generate key, and assigns key label.
Informs client services which key label is to be used
Configure ILP with key label.
Turn on CMK encryption processes
Operations Octavius
Fran Fulfillment
Client Services Chris
Key Manager Kevin
Security Sam
Client Services Chris
HSM Cluster
USB Keys
PED
ILP
SSH Commands
HSM Cluster
ILP
Copyright © Intralinks 2014 all rights reserved
Intralinks' Confidential and Proprietary Information

Customer Orders CMK

Customers who order CMK will need to indicate how many slots they want to reserve for use. Based on the amount of slots reserved, the initial one-time charge will vary.

Assign Partition to Customer

The first step in the process once the order is placed is for Intralinks Operations to configure a partition and generate the USB keys for a customer. As the partition is assigned to a customer, USB Keys will be generated that are specific to that partition.

By default there will be five Orange keys and five Black keys created for each customer partition.

Provide PED and USB Keys to Customer

Once the partition has been configured and USB keys created, the keys along with the PED will be shipped to the customer along with instructions for how to use them.

Professional Services Configure Customer PCs with SSH Client Software

Professional/Client services will help a customer configure up to 5 PCs that can be used to connect to their HSM partition. The minimum PC requirements and network connectivity will be covered in the technical details section of this document.

Client Services Configure ILP

Once the customer has connected to their HSM partition, changed their password, and generated an encryption key; they can contact Client Services to have them associate the appropriate key label with the appropriate ILP Organization IDs. A customer can associate as many Organization IDs as needed to cover the portion of their organization that is covered by the contract (basically covering all exchanges they own.)

The customer is not required to include every organization ID that represents their company, but it is likely they will want to do so. Additional organization IDs can be added later as more are created within ILP. Also, in the next release we will allow for additional keys to be assigned to business groups and exchanges directly.

Activate CMK Service

When the organization IDs have been properly associated with the customer key label, Client Services will “turn on” the service. This kicks off a job that processes all data keys associated with the documents in that client’s organization. The processing includes decrypting and re-encrypting the data keys such that the customer’s key is required for future decryptions of the data key.

This process is expected to take tens of minutes and once complete, Client Services will contact the customer to let them know the process is complete and that they are now in control of the encryption process. During the time this processing is occurring, the customer’s existing files will continue to be available for download and new files are permitted to be uploaded without an interruption in service.

Technical Details

CMK Encryption Level

All encryption using the customer key is done within the HSM device. At no time do the keys leave the device. The specific encryption used is:

- AES 256 bit
- Mode of operation is cipher-block chaining (CBC)

Customer System Requirements (Network)

In order for the client's PC to connect to the Intralinks hosted HSM, the following installation and configuration must be accomplished:

- Installation of the Luna SDK client software
- The Firewall or any other anti-virus utilities on system should be configured to allow c:\program files\safeNet\LunaClient\*.exe processes to run
- The firewall should be configured to allow communication through ports 22, 1792 and 1503
- .Net framework 3.5 is required on 2012 windows platforms
- Windows Random Number Generator service must be running

Any PC the client plans on using to connect to the HSM from their location will need to have the above configuration and connectivity.

Customer System Requirements (PC)

The operating system requirements for any PC that will be used to connect to the HSM are described in the following table:

OS	Driver	App
Windows Server 2003 Standard / Enterprise	32/64 bit	32/64 bit
Windows Server 2008 R2	64 bit	64 bit
Windows 7+	32/64 bit	32/64 bit