IBM Cloud Hyper Protect Crypto Services Key Ceremony

Using Key Part Files and the TKE CLI

Version 1.0

Author: Sandeep Batta (sbatta@us.ibm.com)

Document History

Revision History

Date of this revision: Jun 28th, 2023	Date of next revision: TBD

Revision Number	Date	Summary of Changes	Changes by
V 1.0	June 28, 2023	Adopted from Doc owned by Stacey Donahue, Joachim Schaefer; Review comments and editing, removed and modified several formalities	Sandeep Batta, Timo Kussmaul

1. Introduction

1.1 Purpose of this document

This document details a key ceremony for Hyper Protect Crypto Services (HPCS) using key part files and the TKE CLI.

1.2Referenced Documents

The following documents are referenced in this document.

Reference Information	Location
HPCS Key Ceremony Documentation	https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm

2. Performance Actors

ALL persons defined in the roles below must attend the key ceremony.

Role-ID	Role Name	Role Description
KCD	Key Ceremony Director	▪ Manage the Key Ceremony process. ▪ Schedule a date and time for procedure performance. ▪ Check that each required attendee has organized their bring-in items/information. ▪ Organize build location access for each required attendee. ▪ Prepare the workstation that is used to run the TKE CLI and make sure the KCD or another person can log into the workstation with the required rights to install the IBM Cloud CLI, the TKE plugin and set up the other prerequisites.
KCA	Key Ceremony Auditor	▪ Ensure that the actions in the document are followed by all actors and that the success/failure of these tasks is suitably recorded.
ADMIN	Crypto Unit Administrator	▪ Carry out the documented steps as described. ▪ Create administrator password and enter as required. ▪ You can create up to 8 different crypto unit administrators per HPCS instance.
MKPO	Master Key Part Owner	▪ Create and own one part of the master key. ▪ Create the password that protects the master key part. ▪ Create two or three master key parts.

Notes

- These are functional roles
- Participants of the key ceremony can assume multiple roles, if appropriate and conformant to your requirements. For example:
  - KCD and KCA roles can be the same individual
  - An ADMIN can also act as an MKPO
- All roles need to attend the key ceremony, and they need to be able to access the workstation (either physically or over a screen sharing session).

Fill in the following table:

Role-ID	Name	Email / Phone#
KCD		
KCA		
ADMIN-1		
ADMIN-2		
ADMIN-3		
…		
ADMIN-n		

MKPO-1		
MKPO-2		
MKPO-3		

3. Prerequisites

- Identify an IBM Cloud account where the HPCS instance will be created.
- Make sure that all participants have reviewed the key ceremony process described at "HPCS Initialization with Key Part files"

Assign roles to all participants. Make sure that all participants have reviewed the requirements for the role being performed.

- Make sure that the KCD has a "TKE Laptop / Workstation / VM" that has been set up with the following configurations:
  - ibmcloud cli is installed
  - **The TKE CLI plugin** is installed with the command:
    `ibmcloud plugin install tke`
  - The CLOUDTKEFILES directory is created and the CLOUDTKEFILES environment variable is set:
    - `mkdir /<home>/cloudtkefiles-<environment>`
    - `export CLOUDTKEFILES=/<home>/cloudtkefiles-<environment>`
  - A working Internet / network connection to the IBM Cloud is available.
- Make sure that the KCD has identified a secure repository for storing and backing up the CLOUDTKEFILES directory.

After you meet and confirm the above conditions, you need to obtain a final approval from the KCD before you continue with the following procedure. The KCD will be responsible for pre-performance planning/coordination/checks.

The KCA must record all activities that should be available for future audit.

4. Procedure Performance

4.1 Ceremony Logistics

- The HPCS Key Ceremony will be executed in one sitting from start to finish.
- The ceremony can be recorded e.g. using Webex.
- The date for the key ceremony will be documented in the Example Procedure Track Record Form.
- On completion, the KCA must secure documentation of the key ceremony.

4.2 Actions Required

4.2.1. Actions Required if the Key Ceremony is Successful

Upon successful completion of the ceremony, all installation documents (containing any notes) and the Procedure Track Record forms from the actors in the ceremony (if used during the procedure) should be collected and stored securely, in case these forms will be required to audit the solution in the future.

After completing the key ceremony, the CLOUDTKEFILES directory contains the signature key files and the master key part files, as well as further files created during the procedure.

Potential future TKE operations need to be signed by a set of signature keys (depending on the defined quorum thresholds). This means a set of ADMINS needs to provide their signature keys and signature key passwords during potential future TKE operations.

To reconstitute the master key (on this or another HPCS instance) via the TKE CLI, you need the master key part files as well as the master key part passwords.

The KCD therefore needs to make sure the CLOUDTKEFILES directory (including the signature key files and the master key part files) is stored and backed up to a secure repository.

The ADMINs and the MKPOs need to remember or securely keep the passwords for their key part files.

4.2.2. Actions Required in case of an issue with Key Ceremony

If there is an issue with part or the entire key ceremony, the comments recorded by the actors during the procedure, e.g. on the **Procedure Track Record forms,** you need to decide the next steps to either recover or regress the attempted installation.

5. Example Procedure Track Record Form

You can use the following example procedure track record form. To do so, the KCD can mandate and the KCA can verify that each person present at the procedure has their own printed copy of this document. Each person completes the form on this page **and notes within the body of the document any problems or deviations that occur during the procedure performance**. Make sure to give each note a unique reference number.

Name of the Procedure	HPCS key ceremony using key part files for the HPCS instance(s) …
Date of Procedure	
Name	
Role (in this procedure)	
Department	
Organization	
Email Address	
Phone number(s)	

COMPLETE THIS SECTION AT THE END OF THE PROCEDURE PERFORMANCE

I confirm that I have been present during performance of the procedure detailed above, from beginning to end.

Check one of the options below:

- ☐ The procedure was performed exactly as stated in this document, without any problems or deviations.
- ☐ The procedure was performed, but there were some problems or deviations. I have made a note within this document of each problem or deviation, and I have given each of my notes a unique reference number. The total number of notes that I have made is:

Check one of the options below:

- ☐ I am satisfied with the overall integrity of the procedure performance, even though I *may* have noted some problems or deviations. I confirm that the procedure was completed successfully.
- ☐ I am NOT satisfied with the procedure performance.

Signature	

6. Key Ceremony Process

The steps in this section must be performed by the **ADMIN.**

6.1 Log onto IBM Cloud UI

6.1.1. Create the HPCS Instance

- Log into the IBM Cloud UI with a the user ID of the account owner, or a user ID that has the permissions to create the HPCS instance.
- Follow the documentation to create an HPCS instance in the resource group and region of your choice with either the Standard or Unified Key Orchestrator plan.

6.1.2. Record HPCS Instance Details

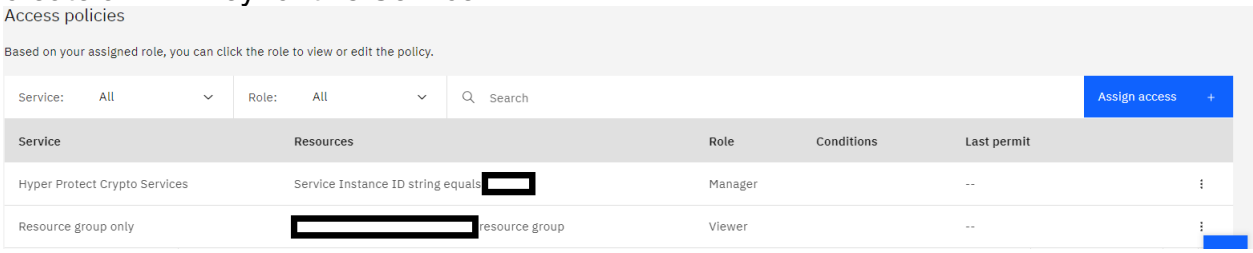
Name of HPCS Instance	
HPCS Instance-ID	
HPCS Region	
Resource Group	
Number of (Operational) Crypto Units	
Number of Failover Crypto Units (optional)	
Number of Recovery Units (optional)	

6.1.3. Create API Key for the IBM Cloud CLI

Option 1: You can create an API key for the currently logged in user, for example:

1. `Manage > Access (IAM)`
2. `API keys`
3. `Create`

Option 2: You can create a Service ID with at least the following access policies and create an API key for this Service ID.



Then download the API Key to a file and keep it for further use.

6.2 Log onto IBM Cloud CLI and list the crypto units

Run the following commands from the command line of the workstation:

```
ibmcloud login -g <resource-group> -r <region> --apikey <api-key>
ibmcloud tke cryptounits
```

Confirm the details of your HPCS instance and the corresponding crypto units are listed, for example:

```
SERVICE INSTANCE: 82c4f43a-cb5f-43f5-8d0f-bd855104879d
CRYPTO UNIT NUM   SELECTED   LOCATION
1                 false      [br-sao].[AZ2-sao2-qz1-sr1-rk107-a01].[02].[51]
2                 false      [br-sao].[AZ3-sao3-qz1-sr1-rk041-a01].[01].[29]

Note: all crypto units in a service instance must be configured the same.
Use 'ibmcloud tke cryptounit-compare' to check how crypto units are configured.
```

6.3 Follow the documented procedure

Official documentation: https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm

6.3.1. Select the crypto units to initialize

Run this command to select all crypto units of your HPCS instance.

```
ibmcloud tke cryptounit-add
```

Make sure that you have selected all operational and failover crypto units (if provisioned) of your HPCS instance and all crypto units are marked as selected:

```
SERVICE INSTANCE: 82c4f43a-cb5f-43f5-8d0f-bd855104879d
CRYPTO UNIT NUM   SELECTED   LOCATION
1                 true       [br-sao].[AZ2-sao2-qz1-sr1-rk107-a01].[02].[51]
2                 true       [br-sao].[AZ3-sao3-qz1-sr1-rk041-a01].[01].[29]

Note: all crypto units in a service instance must be configured the same.
Use 'ibmcloud tke cryptounit-compare' to check how crypto units are configured.
```

6.3.2. Create Signature Keys and select administrators

Run this command for every ADMIN:

```
ibmcloud tke sigkey-add
```

Each ADMIN will have to enter an administrator name and create and enter a password. Each ADMIN will also be responsible for keeping this password.
The command creates an administrator signature key file in the CLOUDTKEFILES directory, and this file will be protected by the entered password.

6.3.3. Create Crypto Unit Administrators

Run this command for every ADMIN to assign crypto unit administrators:

```
ibmcloud tke cryptounit-admin-add
```

The list of signature key files that were added in the previous step will be displayed. The ADMIN needs to select the number corresponding to the ADMIN's signature key and enter the corresponding signature key password.

6.3.4. Select signature keys

Run this command to select signature keys for signing subsequent operations:

```
ibmcloud tke sigkey-sel
```

The list of signature key files that were added in the previous step will be displayed.

Select the required set of signature keys. For example, assuming a quorum threshold (to be defined in the next step) is defined `n` out of `m`, you will need to select `n` signature keys.

The respective ADMINs need to enter the password for their signature keys.

6.3.5. Set the Quorum Threshold

Run this command to set the quorum threshold:

```
ibmcloud tke cryptounit-thrhld-set
```

- Enter values for the signature threshold and revocation signature threshold.
- The signature threshold controls how many signatures are required to execute subsequent and future administrative commands.
- The revocation signature threshold controls how many signatures are required to remove an administrator in future.
- The signature threshold values must be numbers between one and eight.

- The signature threshold and revocation signature threshold can be different.
- This selection constitutes a n out of m quorum for the signature threshold and the revocation threshold.
- n of the previously selected ADMINs need to enter their signature key passwords.

6.3.6. Create Master Key Parts (all MKPOs)

Make sure that each MKPO run this command once:

```
ibmcloud tke mk-add --random
```

- The MKPO (the person responsible for this master key part) enters a description for the key part and a password to protect the key part file.
- If the password is lost, the key part cannot be used.
- You need to create at least two master key parts and at maximum three master key parts.
- Each master key part should be owned by a different MKPO / person.
- The MKPO needs to be the only person who knows the password that is associated with the key part file.
- The master key part files are stored in the CLOUDTKEFILEs.
- The MKPO and the KCD need to make sure the master key part files are stored and are backed up in a secure way.

6.3.7. Load the Master Key

Load the master key with this command:

```
ibmcloud tke cryptounit-mk-load
```

- Select all master key parts to be loaded into the new master key register.
- This command will ask for the password of one of the previously seleted administrator signature key files (to be entered by the respective ADMIN), as well as the password for each selected master key part file (to be entered by the respective MKPO).

6.3.8. Commit the Master Key

Commit the master key with this command:

```
ibmcloud tke cryptounit-mk-commit
```

A set of ADMINs (their number depending on the defined signature quorum threshold) needs to enter their signature key passwords.

6.3.9. Activate the Master Key

Activate the master key with this command:

```
ibmcloud tke cryptounit-mk-setimm
```

- Confirm the warning message.
- One of the previously selected ADMINs needs to enter their signature key password.
- This completes the HPCS key ceremony for the HPCS initialization.
- Your HPCS instance is now fully initialized and functional.

End of document – HPCS Key Ceremony

The completion form should now be completed and handed to the auditor