Cloud TKE procedures

1. Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's intellectual property rights or other legally protectable rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, programs, or services, except those expressly designated by IBM, are the user's responsibility.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Commercial Relations, IBM Corporation, Purchase, NY 10577.

Contents

1. Notices ... 2
2. Introduction ... 6
  2.1 Changes ... 6
    2.1.1 Version 1.0 ... 6
3. General concepts and considerations ... 7
  3.1 Hyper Protect Crypto Services ... 7
    3.1.1 Crypto units ... 7
    3.1.2 Hyper Protect Crypto Services master key ... 7
    3.1.3 Hyper Protect Crypto Services administrators ... 8
  3.2 IBM Cloud TKE ... 8
  3.3 Dual control ... 8
  3.4 Split knowledge ... 8
  3.5 Separation of duties ... 9
  3.6 Redundancy ... 9
  3.7 Simplicity ... 9
  3.8 Security Organization ... 9
  3.9 Ceremonies ... 9
  3.10 Education ... 9
  3.11 Handling Hyper Protect Crypto Services Master Key parts ... 10
  3.12 Administrator smart cards and PINs ... 10
  3.13 CA smart cards and PINs ... 10
  3.14 Documenting the inventory ... 11
  3.15 Collection of evidence ... 11
4. Planning ... 12
  4.1 Define the security organization ... 12
    4.1.1 Organizational Roles ... 12
    4.1.2 Documenting the security organization ... 14
  4.2 Planning for smart cards ... 14
    4.2.1 Documenting smart card usage ... 16
5. Procedures for Hyper Protect Crypto Services crypto unit management ... 18
  5.1 Service instance initialization using smartcards ... 19
    5.1.1 Purpose ... 19
    5.1.2 Participants ... 19
    5.1.3 Prerequisites ... 19

5.1.4 Evidence to be collected........20
5.1.5 Procedure steps........20
5.2 Restore Hyper Protect Crypto Services crypto units using smartcards........26
5.2.1 Purpose........26
5.2.2 Participants........26
5.2.3 Prerequisites........27
5.2.4 Evidence to be collected........27
5.2.5 Procedure steps........28
5.3 Add Hyper Protect Crypto Services administrator using smartcards........31
5.3.1 Purpose........31
5.3.2 Participants........31
5.3.3 Prerequisites........31
5.3.4 Evidence to be collected........32
5.3.5 Procedure steps........32
5.4 Remove Hyper Protect Crypto Services administrator using smartcards........36
5.4.1 Purpose........36
5.4.2 Participants........36
5.4.3 Prerequisites........36
5.4.4 Evidence to be collected........37
5.4.5 Procedure steps........37
5.5 Rotate Hyper Protect Crypto Services master key using smart cards........40
5.5.1 Purpose........40
5.5.2 Participants........40
5.5.3 Prerequisites........40
5.5.4 Evidence to be collected........41
5.5.5 Procedure steps........42
5.6 Freeze Hyper Protect Crypto Services instance using smart cards........45
5.6.1 Purpose........45
5.6.2 Participants........45
5.6.3 Prerequisites........45
5.6.4 Evidence to be collected........45
5.6.5 Procedure steps........46
5.7 Reload Hyper Protect Crypto Services master key using smart cards........49
5.7.1 Purpose........49
5.7.2 Participants........49
5.7.3 Prerequisites........49

5.7.4 Evidence to be collected 50
5.7.5 Procedure steps 50
6. Appendix 53
Hyper Protect Crypto Services Security Organization overview 54

2. Introduction

The purpose of this document is to provide a template with procedures for the secure initialization and management of IBM Cloud Hyper Protect Crypto Services Enterprise PKCS#11 Hardware Security Modules using Cloud TKE. The document is intended as a template that should be tailored to fit the requirements of your organisation.

The management of Hyper Protect Crypto Services may be subject to internal or external audits – for example, the setup and procedures for initialization and management of Hyper Protect Crypto Services must be documented, and evidence must be collected during execution of the procedures.

Several decisions must be taken by your Hyper Protect Crypto Services management team to establish a secure setup and making it operational for a production environment. Most of these decisions should be taken up front and incorporated into this document.

2.1 Changes

2.1.1 Version 1.0

- Initial version

3. General concepts and considerations

This chapter introduces some important concepts and considerations, which should be understood and addressed when defining the security organization and customizing the procedures used to manage Hyper Protect Crypto Services.

3.1 Hyper Protect Crypto Services

IBM Cloud® Hyper Protect Crypto Services is a dedicated key management service and Hardware Security Module (HSM) that provides you with the Keep Your Own Key capability for cloud data encryption. Built on FIPS 140-2 Level 4 certified hardware, Hyper Protect Crypto Services provides you with exclusive control of your encryption keys.

The followings are a few highlights of the Hyper Protect Crypto Services architecture:

- Applications connect to Hyper Protect Crypto Services through the PKCS #11 API or the GREP11 API.
- Dedicated keystore in Hyper Protect Crypto Services is provided to ensure data isolation and security. Privileged users are locked out for protection against abusive use of system administrator credentials or root user credentials.
- Secure Service Container (SSC) provides the enterprise level of security and impregnability that enterprise customers expect from IBM LinuxONE technology.
- FIPS 140-2 Level 4 compliant cloud HSM is enabled for highest physical protection of secrets.

More information can be found via Hyper Protect Crypto Services. (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-overview)

3.1.1 Crypto units

A crypto unit is an HSM and the corresponding software stack. This document will mostly use the term crypto unit because it's the term used in the administrative user interfaces, but for all practical purposes you can consider HSM and crypto unit as synonyms.

3.1.2 Hyper Protect Crypto Services master key

Hyper Protect Crypto Services uses a master key to protect the keystore. The keystore can only be used with Hyper Protect Crypto Services instances having the correct master key. Without the correct master key, it's not possible to recover the keys from the key store. The master key resides inside the crypto units, protected by the tamper resistant and tamper detecting hardware.

You must create and load your own master key into the crypto units associated with your Hyper Protect Crypto Services instance. The master key consists of two or more master key parts that are combined securely within the crypto units to provide the resulting master key. The people responsible for the master key parts are called key managers.

It is important that all crypto units associated with a specific Hyper Protect Crypto Services instance holds the same master key.

3.1.3 Hyper Protect Crypto Services administrators

Hyper Protect Crypto Services administrators are the people authorized to manage the Hyper Protect Crypto Services master key and access control system. The administrators use signature keys contained in password protected files or on PIN protected smart cards to sign updates to the Hyper Protect Crypto Services crypto units. Up to 8 administrators are supported.

The access control system can be configured to require two or more administrators to sign sensitive updates. This is called dual control and is implemented using a so-called signature threshold. The signature threshold specifies how many administrators must sign updates before they are executed.

3.2 IBM Cloud TKE

Hyper Protect Crypto Services instances are managed using an application called the Cloud TKE application.

The Cloud TKE application should be installed on a dedicated workstation which we will refer to as the TKE Workstation. The TKE workstation should be secured in a such a way that modification of the installed software and configuration by unauthorized people is prevented. Often, the TKE workstation is placed in a physically secured room or placed in a dedicated “safe”.

After moving the TKE workstation into production only personal having task in maintaining Hyper Protect Crypto Services should have access to the TKE workstation. The software, set up, and security on the TKE workstation should be the responsibility of security personnel only.

3.3 Dual control

Dual Control refers to a process where two or more persons or teams are required to execute sensitive functions or access sensitive material and equipment. It is a security measure intended to prevent compromise of security by a single individual.

In the context of cloud HSMs such as those used by Hyper Protect Crypto Services, dual control is useful to protect physical access to the devices used to manage the cloud HSMs, and to protect logical access to the functions used to manage cloud HSM configuration, access control and master keys.

Hyper Protect Crypto Services provides dual control using an M-out-of-N digital signature approach. This is implemented using a signature threshold. The signature threshold specifies how many (M) of the authorized administrators (N) that are required to execute updates. This approach allows for dual control as well as redundancy (if N>M).

In Hyper Protect Crypto Services, the functions covered by the dual control scheme are those used to manage Hyper Protect Crypto Services administrators and Hyper Protect Crypto Services access control, and those used to commit master keys to Hyper Protect Crypto Services.

3.4 Split knowledge

In the context of Hyper Protect Crypto Services, Split Knowledge refers to the division of a master key into two or more parts, each part constantly kept under control by separate authorized individuals or teams, such that no individual will ever come to know or possess the value of the master key. These key parts must be combined to form the complete master key.

Hyper Protect Crypto Services implements split knowledge for master keys in such a way, that possession of a single master key part provides no information about the master key whatsoever. When master key parts are committed to the Hyper Protect Crypto Services they are combined to form the complete master key inside the Hyper Protect Crypto Services HSMs (using an XOR function).

3.5 Separation of duties

Separation of duties is a principle where critical functions are divided among different people to improve security.

An example is separation of Hyper Protect Crypto Services access control management from the management of the Hyper Protect Crypto Services master key components. Hyper Protect Crypto Services has no mechanisms to enforce this, so procedures are required to take care of this, if such a separation is desired.

3.6 Redundancy

It is always important to consider redundancy to prevent loss of data and/or disruption of operational capacity. With HSMs it's even more important. The main reason is that an HSM is designed to be tamper resistant and prevent any unauthorized or unintended access to or use of the HSM and the secrets kept within. With HSMs even a small mistake can have disastrous consequences.

Redundancy is needed at organizational level (people) and at physical level (devices, media)

3.7 Simplicity

Complexity is always a threat to security, operability, and ability for recovery. The more complex a system is, the greater the risk. Therefore, when there is a choice between two options, it is important to consider whether the more complex option offers enough benefits over the simpler option, before making the decision.

3.8 Security Organization

It is important to establish and document the Hyper Protect Crypto Services security organization, that is, the identities, roles, and responsibilities of the people involved in the management of the Hyper Protect Crypto Services crypto units. A proper security organization is the corner stone of the safe and secure management of Hyper Protect Crypto Services. No amount of technical measure can make up for a lacking or flawed security organization.

When planning the security organization, the principles of dual control, split knowledge, separation of duties and redundancy must be considered.

3.9 Ceremonies

It is standard practice to organize all management of HSMs (such as Hyper Protect Crypto Services crypto units) around so-called ceremonies. The purpose of this is to ensure that all management takes place in an orderly, controlled, and approved manner. The ceremonies are executed according to pre-defined procedures which defines the people required, the steps to be performed and the evidence to be collected.

3.10 Education

Team members (administrators, key managers, and supervisors) must know and understand the security concepts and procedures surrounding Hyper Protect Crypto Services and Cloud TKE. Lack of understanding constitutes a common risk for security exposures and loss of operational capacity.

3.11 Handling Hyper Protect Crypto Services Master Key parts

Key parts for the Hyper Protect Crypto Services Master Keys should be stored/archived in a way that nobody is able to obtain the value of the complete master key. Because of the need for key recovery at any time, for example in case of Hyper Protect Crypto Services crypto unit failure or replacement, more than one person should be able to install a master key part into Hyper Protect Crypto Services. The ability to get access to each key part must therefore be assigned to two or more individuals.

Key parts are generated on the TKE workstation and written to PIN protected smart cards or password protected files. Each key part should be written to at least two smart cards or files, in order to have one or more backups. When saving key parts, a naming syntax for the key parts should be established. For example:

Production MK KP1, 2021-07-31

for first part of a production master key created on July 31, 2021.

Each medium containing key parts should be marked with the type of the key parts (first, middle, last), date of generation and for which system this key part is generated (test/production/...).

The key verification patterns produced during generation and loading of key parts should be registered when journaling the key ceremonies. This is to make sure the proper key parts can be identified and reloaded later, for example in case of a recovery situation.

No individual should be able to copy or archive key material outside the authorized locations.

Each medium containing a key part can be put into a sealed envelope, so unauthorized attempts to get access to the key part can be identified. The envelope should identify the content of the envelope identical to the label of the medium containing the key part. The corresponding PIN or password should be put in an envelope as well to ensure the key part can always be recovered.

Keys not used anymore should be properly erased to avoid later improper use of the key. Thus, obsolete key parts should be deleted from all media where they are stored.

Notice: **Media and envelopes must be properly labelled. Avoid problems in uniquely identifying each envelope/key component. If a key is replaced and the old key components for some reason must remain in the safe – update the information to indicate the key is not in use.**

The way the key material is archived is subject to internal/external audits. The procedures to get access to the key material must be properly documented. A journal must also exist.

3.12 Administrator smart cards and PINs

The recommended way for Administrators to authenticate to Hyper Protect Crypto Services crypto units is by using PIN protected smart cards. If this option is chosen, the following must be considered.

For each administrator, an administrator signature key pair is generated and stored on a smart card protected by a 6-digit PIN. The public part of the key pair must be installed in the Hyper Protect Crypto Services crypto units.

Each administrator signature key pair must be copied to at least one other smart card – for backup purposes. The PINs on the other smart card(s) should be the same. The smart cards should be labelled with the name of the administrator and the date of creation.

3.13 CA smart cards and PINs

The smart card system used with Hyper Protect Crypto Services has a special CA smart card, which certifies (enrolls) all the other smart cards to create a secure zone. The smart cards can exchange key material with one another and with the Hyper Protect Crypto Services crypto units. All key material within the zone is encrypted by transport keys during exchange whenever outside tamper resistant hardware (smart cards and Hyper Protect Crypto Services crypto units).

The enrollment process is sensitive - only trusted smart cards should be enrolled into the secure zone. Therefore, the access to use the CA smart card is protected by dual control (two six-digit PIN's). Also, loss of the CA card can be critical because it may no longer be possible to enroll new smart cards into the secure zone as replacement for broken smart cards - ultimately that could mean loss of the access to key parts stored on smart cards.

The CA smart card should therefore be backed up on one or more other smart cards.

3.14 Documenting the inventory

It is important to create and maintain an inventory document to keep track of the whereabouts of sensitive material (media/smart cards with signature keys and master key parts).

3.15 Collection of evidence

When working with Cloud TKE it is important to collect and store various kinds of evidence.

This evidence is required for several purposes:

- To prove compliance with regulations and requirements
- To help reconstruct what happened in case of a security incident or similar
- To serve as reference when performing normal Hyper Protect Crypto Services crypto unit administration
- To serve as reference in recovery situations

Evidence to be collected during a Cloud TKE session includes, but is not limited to:

- Purpose of the session
- Identity and role of people involved
- Procedure steps completed and any deviations from the prescribed procedure
- Key verification patterns for master keys and administrator keys
- Sensitive material produced and/or used during the session

4. Planning

Before you use the procedures in this document to initialize and configure the crypto units in your Hyper Protect Crypto Services instance, you need to do some planning. You need to define and document your security organization, how the crypto units should be configured, and how the media containing Hyper Protect Crypto Services administrator keys and Hyper Protect Crypto Services master keys should be managed.

Without proper planning, the procedures used to configure and maintain the crypto units may be inefficient, or you may end up wasting time because required people or materials are missing during execution of procedures. Also, there is a higher risk of unintended security exposures.

In the appendix is a set of sheets you can use to document your organization and inventory of supporting material. The sheets are designed to support the procedures in this document and support a basic configuration. You can modify them and the procedures if needed, for example to support a simpler or more complex set up. However, you need to have some experience with Hyper Protect Crypto Services crypto units and Cloud TKE before doing that.

4.1 Define the security organization

You should define and document your Hyper Protect Crypto Services security organization. You can use the ***Hyper Protect Crypto Services Security Organization overview*** sheet to do that.

4.1.1 Organizational Roles

The roles of people in the security organization should be defined in such a way that the principles of dual control and split knowledge are enforced. This structure protects against a single individual compromising security. At the same time, the organization should include redundancy to ensure that no task depends on a single individual, in other words, every role should have at least two persons assigned to it. The ideal security organization requires more people than most companies can provide (for both economical and practical reasons). Therefore, compromises are usually needed.

The standard procedures described in this document define the following general roles in the security organization:

- **CRYPTO UNIT ADMINISTRATOR 1 and 2:** Cooperates to issue smart cards, and to execute Hyper Protect Crypto Services crypto unit updates, such as access control updates, configuration changes and master key loading. Administrators use signature keys contained on PIN protected smart cards to authenticate to Hyper Protect Crypto Services crypto units.
- **MASTER KEY CUSTODIAN 1 and 2:** Manages first and last key part respectively for Hyper Protect Crypto Services master keys. Key parts are kept on PIN protected smart cards.
- **SUPERVISOR:** Directs ceremonies, records progress, records deviations, and collects evidence.

The roles can be assigned such that no individual has more than one role, or they can be combined in various ways such that individuals can have more than one role. The main reason for combining roles is to simplify procedures and reduce the number of people needed in the Hyper Protect Crypto Services security organization.

Below are some guidelines to consider when assigning the roles.

Dual control - *How many administrators will be required to execute dual controlled operations?*

An administrator able to execute sensitive Hyper Protect Crypto Services crypto unit updates on their own, can compromise security, for example by loading a known master key into the crypto units. Therefore, you should plan for dual control.

In Hyper Protect Crypto Services crypto units, all defined administrators have the same permissions. Dual control is enforced by configuring the crypto units to require two or more administrators to cooperate to execute updates. Even though these procedures define two different administrator roles (CRYPTO UNIT ADMINISTRATOR 1 and 2) they are effectively the same role from a Hyper Protect Crypto Services crypto unit point of view. However, to enforce dual control when issuing smart cards for use with the crypto units, the two PINs required to access the CA smart card must be controlled by different persons. The two administrator roles defined by these procedures (CRYPTO UNIT ADMINISTRATOR 1 and 2) provides that separation.

To implement dual control, you must require at least two administrators to cooperate to execute Hyper Protect Crypto Services crypto unit updates (for example, you must configure the crypto unit signature threshold and revocation threshold to a value of 2 or more) and split the PINs for the CA smart card between administrators using the CRYPTO UNIT ADMINISTRATOR 1 and 2 roles.

If you don't have a requirement for dual control, you can configure the crypto units to require only one administrator to execute updates (i.e., configure the crypto unit signature threshold and revocation threshold to 1) and combine the roles of CRYPTO UNIT ADMINISTRATOR 1 and 2 so all administrators have access to both CA smart card PINs. However, this circumvents the protection afforded by Hyper Protect Crypto Services crypto units and is strongly advised against!

Split knowledge – *How many key parts will be required to form the master key?*

No single individual should ever have access to a complete Hyper Protect Crypto Services master key. Therefore, master keys must be split in at least two components, and these components must be controlled by different people. The principle of split knowledge complements the physical protection provided by the Hyper Protect Crypto Services crypto units. Management of the Hyper Protect Crypto Services master keys requires at least as many people as the master key is split into.

To enforce split knowledge, the roles of MASTER KEY CUSTODIAN 1 and 2 must be assigned to different people.

If you want even stronger protection of the master key, you can split it in three or more parts. In that case you will need additional key manager roles (MASTER KEY CUSTODIAN 3, etc).

If you don't have a requirement for split knowledge, you can combine the roles of MASTER KEY CUSTODIAN 1 and 2. This means that a person assigned this combined role will be in control of the entire Hyper Protect Crypto Services master key and can load it into the crypto units of any Hyper Protect Crypto Services instance, even the crypto units of a personally controlled Hyper Protect Crypto Services instance. However, this circumvents the protection afforded by Hyper Protect Crypto Services and is strongly advised against!

Separation of duties – *will administrators also be key managers and/or supervisors?*

The standard roles above supports separation of duties as an extra layer of security. They do this by separating the responsibilities of administrators, key managers, and supervisors into the respective roles of ADMINISTRATOR, MASTER KEY CUSTODIAN and SUPERVISOR.

For most organizations, the roles can be combined such that CRYPTO UNIT ADMINISTRATOR 1 and MASTER KEY CUSTODIAN 1 are combined, and CRYPTO UNIT ADMINISTRATOR 2 and MASTER KEY CUSTODIAN 2 are combined.

The SUPERVISOR role can be combined with any of the other roles, but during actual ceremonies, it is recommended that people assuming the SUPERVISOR role does not assume any of their other roles.

Redundancy – *how many extra people are required in each role as backups?*

It is important to make sure having enough extra people in the various roles, such that operation is always possible even if a person is unavailable, no matter who. Preferably even if any two people are unavailable. The horror scenario is being unable to perform disaster recovery due to missing people.

With the roles proposed in this procedure document this implies that at least two people must be assigned to each of the roles CRYPTO UNIT ADMINISTRATOR 1, CRYPTO UNIT ADMINISTRATOR 2, MASTER KEY CUSTODIAN 1, MASTER KEY CUSTODIAN 2 and SUPERVISOR.

More information can be found via organizational roles. (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-manage-access#roles)

4.1.2 Documenting the security organization

The Hyper Protect Crypto Services Security Organization sheet has a role table with the above standard roles filled in. You can change these if you have specific requirements. If you do so, you may also have to adjust the procedures in this document to accommodate the changes. For each role, the table defines the following:

Organizational role name: name of the role, as it will be known throughout the procedures

Role description: brief description of the responsibilities assigned to the role

When you have decided upon the roles, you should appoint people to the roles. The people table on the Hyper Protect Crypto Services Security Organization sheet should be used for documentation. For each person the table holds the following information:

Full name: The name of the person

Organizational role(s): The roles (as per the role table) assigned to the person

4.2 Planning for smart cards

You can manage Hyper Protect Crypto Services using administrator signature keys and master key parts on either PIN protected smart cards or in password protected files. The procedures in this document assumes that you keep Hyper Protect Crypto Services administrator signature keys and Hyper Protect Crypto Services master key parts on smart cards.

If you chose to use smart cards, you need to decide how you will use the smart cards and how many smart cards you need. Below are some guidelines to help you do that. You can use the ***CA smart cards, Hyper Protect Crypto Services Administrator smart cards*** and ***Hyper Protect Crypto Services Master Key Part smart cards*** sheets to document your decisions.

To use smart cards to manage Hyper Protect Crypto Services, you must establish a smart card zone. The smart card zone is a collection of smart cards that can exchange information securely. It consists of a CA smart card and several EP11 smart cards. The CA smart card is required to initialize and enroll EP11 smart cards in the zone. The EP11 smart cards are the ones holding Hyper Protect Crypto Services administrator signature keys and Hyper Protect Crypto Services master key parts. Depending on their use, we refer to EP11 smart cards as either Hyper Protect Crypto Services Administrator smart cards or Hyper Protect Crypto Services Master Key Part smart cards.

To manage Hyper Protect Crypto Services using smart cards you need:

- A CA smart card.
- A Hyper Protect Crypto Services Administrator smart card for each Hyper Protect Crypto Services administrator signature key.
- A Hyper Protect Crypto Services Master Key Part smart card for each type of Hyper Protect Crypto Services master key part (1st, 2nd, etc.). You can have key parts for multiple master keys on a single smart card, but you should never have multiple key parts for the same master key on a single smart card.

- One or more backups of each smart card.

Assuming you have an organization with four Hyper Protect Crypto Services administrators, Hyper Protect Crypto Services master keys split in two parts, and you want one back up for every smart card, you need at least (1 CA smart card + 4 Hyper Protect Crypto Services Administrator smart cards + 2 Hyper Protect Crypto Services master key part smart cards) * 2 = 14 smart cards. In addition to this you should have some extra smart cards in spare, for example to replace broken smart cards.

To decide how you will use the smart cards and how many you need, consider the following questions:

Will Hyper Protect Crypto Services administrators use personal administrator smart cards or team administrator smart cards?

- **Personal smart cards:**
  Each administrator has a personal Hyper Protect Crypto Services administrator smart card.
- **Team smart cards:**
  Administrators are divided in teams. Each team has a shared Hyper Protect Crypto Services administrator smart card. The advantage of this is, that it is possible to require administrators managing the Hyper Protect Crypto Services crypto units to come from different teams. This protects against a single manager putting pressure on his subordinates to circumvent the protection provided by dual control. It also reduces the number of smart cards as all administrators on a team share the same smart card. A disadvantage is that system logs will not reflect the identity of the administrators, only of the teams.
  Redundancy is achieved by having multiple persons on each team.

How many backups will there be for each smart card?

There should be at least one back up for each primary smart card. This applies to all smart cards (CA smart cards, Hyper Protect Crypto Services Administrator smart cards and Hyper Protect Crypto Services Master Key Part smart cards). Having more than one backup for each smart card makes it possible to store a backup together with the primary smart card and one or more backups in a different geographical location.

Who will take responsibility of which smart cards and PINs?

Based on the organization defined in the previous chapter and the decisions taken in this chapter, you should decide who will take responsibility of the different smart cards and corresponding PINs.

Where and how will smart cards be stored when not in use?

Smart cards containing Hyper Protect Crypto Services master key parts should be stored securely, accessible only to members of the team responsible for the relevant type of master key part (1st, 2nd, etc.), for example in safes.

CA smart cards and Hyper Protect Crypto Services Administrator smart cards should also be stored securely, accessible only to the relevant administrators, for example in safes.

At least one set of backup smart cards should be stored in a different geographical location.

Where will PINs for smart cards be stored?

Since smart cards are not used often, the PINs used to access the smart cards may be forgotten. One option is to store the PINs in safes, another is to store them in electronic form.

Whatever is chosen, it is important to make sure the PINs are only available to the relevant administrators and/or key managers.

Special consideration is required for the two PINs protecting the CA smart card. Under normal circumstances they should be stored separately.

Will smart cards and PINs be stored in sealed envelopes?

A common way to enable detection of unauthorized access to smart cards and PINs is to keep these in sealed envelopes when not in use.

Zone description

The zone description is written to all smart cards in the smart card zone. You should choose something informative, for example something that characterizes the Hyper Protect Crypto Services instance(s) managed with the smart cards.

More information can be found via following links:

- Smart Card: (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-instance-mode#understand-smart-card)
- Security: (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialization-security-policy)
- FAQ: (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-faq-provisioning-operations#faq-smart-card-setup)

4.2.1 Documenting smart card usage

Information about the decisions taken should be documented in the following sheets:

CA Smart cards sheet:

- Zone description
- The Hyper Protect Crypto Services instance(s) where these smart cards are going to be used
- Administrators of PIN 1
- Administrators of PIN 2
- Storage location

Hyper Protect Crypto Services Administrator smart cards

- Zone description
- The Hyper Protect Crypto Services instance(s) where these smart cards are going to be used
- Administrator or team
- Storage location

Hyper Protect Crypto Services Master Key Part smart cards

- Zone description
- The Hyper Protect Crypto Services instance(s) where these smart cards are going to be used

- Key manager team
- Storage location

The remaining information (Zone ID, Card IDs, Subject key IDs, master key verification patterns and AES-VPs for master key parts) is generated and documented as part of the actual procedures used to initialize and manage the crypto units of the Hyper Protect Crypto Services instance(s).

5. Procedures for Hyper Protect Crypto Services crypto unit management

This chapter contains example procedures required to initialize and manage IBM Cloud Hyper Protect Crypto Services Enterprise PKCS#11 Hardware Security Modules (in the following referred to as Hyper Protect Crypto Services crypto units).

The procedures refer to people in the following roles:

- **CRYPTO UNIT ADMINISTRATOR 1 and 2:** Executes Hyper Protect Crypto Services crypto unit updates, such as access control updates, configuration changes and master key loading. Administrators use signature keys contained on PIN protected smart cards to authenticate themselves to Hyper Protect Crypto Services.
- **MASTER KEY CUSTODIAN 1 and 2:** Manages key parts for Hyper Protect Crypto Services master keys. Key parts are kept on PIN protected smart cards.
- **SUPERVISOR:** Directs ceremonies, records progress, records deviations, and collects evidence.

The procedures are targeted a basic setup. You can modify them if needed, for example to support a simpler or more complex set up. However, you need to have some experience with Hyper Protect Crypto Services and Cloud TKE before doing that.

The procedures are based on the following assumptions and decisions:

- Hyper Protect Crypto Services administrator signature keys and Hyper Protect Crypto Services master key parts are kept on smart cards
- Signature keys and master key parts are kept on different smart cards
- Each primary smart card will have a corresponding backup smart card
- Dual controlled functions require signatures from two administrators
- Administrators will use personal signatures (for example, each administrator will have a personal administrator signature key on smart card).
- Administrators will be divided in two groups with respect to the CA smart cards, such that no administrator will ever have access to both PIN1 and PIN2 for the CA smart card.
- Hyper Protect Crypto Services master keys will be composed of two key parts
- Key managers are divided in two teams, one team will manage first master key parts, and the other team will manage last key parts)
- Smart cards and PINs are kept in sealed envelopes when not in use
- Redundancy is achieved by having 4 administrators (2 more than required for dual controlled functions) and 4 key managers (2 in each key manager team)
- A supervisor will be required to direct ceremonies, record progress and deviations, and collect evidence.

5.1 Service instance initialization using smartcards

5.1.1 Purpose

The purpose of this procedure is to initialize Hyper Protect Crypto Services crypto units from scratch using smart cards:

- List prerequisites (presence of required people, equipment, material, etc.)
- Prepare a smart card zone with a CA smart card (and backups) and a number EP11 smart cards to hold administrator signature keys and master key parts (and backups).
- Generate administrator signature keys and store on EP11 smart cards (including backups)
- Add administrators to the Hyper Protect Crypto Services crypto units
- Activate the Hyper Protect Crypto Services access control system by setting signature and revocation thresholds
- Generate Hyper Protect Crypto Services master key parts and store on EP11 smart cards (including backups)
- Load master key parts to the Hyper Protect Crypto Services crypto units
- Commit and activate the master key
- Final verification of the Hyper Protect Crypto Services crypto unit configuration and collection of evidence

5.1.2 Participants

Role indication	Number of persons
CRYPTO UNIT ADMINISTRATOR 1	1
CRYPTO UNIT ADMINISTRATOR 2	1
SUPERVISOR	1
Other CRYPTO UNIT ADMINISTRATORs and MASTER KEY CUSTODIANs	2+4

5.1.3 Prerequisites

SUPERVISOR must bring

- A copy of this procedure.
- Sheets for documenting the Hyper Protect Crypto Services crypto units and smart card contents (for CA, Hyper Protect Crypto Services Administrator and Hyper Protect Crypto Services Master Key Part smart cards) – the sheets can be found in the appendix to this document
- Overview of the intended Hyper Protect Crypto Services management organization
- 14 empty smart cards (2 to use as CA smart card and backup, 8 to use as administrator smart cards and backups and 4 to use as key part smart cards and backups)
- Labels for smart cards and PINs and a marker pen
- Envelopes for smart cards and PINs. At least 30.

- Logbook for journaling the procedure

The Hyper Protect Crypto Services crypto units to be initialized must be in the initial/zeroized state.

At least one participant must have a valid user ID and password able to log in to the IBM cloud and must have the required Service administrator permissions on the Hyper Protect Crypto Services instance as outlined in https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-manage-access#roles

5.1.4 Evidence to be collected

All activities performed on the TKE workstation must be journaled in the logbook.

The journal must contain at least the following information:

- Date, time, and location
- Purpose of the procedure
- Identity and role of all people involved, including the supervisor
- Procedure steps completed and any deviations from the prescribed procedure
- Hyper Protect Crypto Services instance ID
- Crypto unit number and location of each crypto unit updated
- Subject key identifier and owner information for all administrator key pairs
- Key verification pattern of all master key parts
- Key verification pattern of the complete master key
- Where smart cards and PINs are stored after the procedure.
- Resulting Hyper Protect Crypto Services crypto unit set up (for example, screenshots of the 'Crypto units', 'Administrators', 'Signature thresholds' and 'Master keys' pages in the IBM Cloud Hyper Protect Crypto Services Trusted Key Entry application)
- Signature of all people involved, including the supervisor

The content of this logbook should be subject to internal/external audits.

In addition to the above, the inventory sheets should be updated.

5.1.5 Procedure steps

5.1.5.1 Create smart card zone

The following steps prepares numbers of smart cards for Hyper Protect Crypto Services management using Cloud TKE. The smart cards will be protected by 6-digit PINs and ready for storage of sensitive data.

The steps are performed using the IBM Cloud Hyper Protect Crypto Services Smart Card Utility Program.

A	CRYPTO UNIT ADMINISTRATOR 1 and 2	**Create CA smart card**

		The purpose of this step is to initialize a CA smart card for the smart card zone used to protect smart cards with Hyper Protect Crypto Services administrator signature keys and Hyper Protect Crypto Services master key parts. The CA smart card is protected with two 6-digit PINs. PIN1 and PIN2 must be selected by CRYPTO UNIT ADMINISTRATOR 1 and 2 respectively. To avoid any administrator ever gets to know both PINs, it should be decided and documented who are allowed access to which PIN. Evidence to be collected: • Zone description • Zone ID • Card ID • Name of administrators responsible for the two PINs • Serial number (if smart cards have printed unique serial numbers) Refer to the Hyper Protect Crypto Services documentation: **Initiate the CA card** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-prepare-management-utilities#initialize-ca-smart-card) for details.
B	CRYPTO UNIT CRYPTO UNIT ADMINISTRATOR 1 and 2	**Create backup of CA smart card** The purpose of this step is to create a backup of the CA smart card on another smart card. Evidence to be collected: • Card ID • Serial number (if smart cards have printed unique serial numbers) Refer to the Hyper Protect Crypto Services documentation: **Backup CA smart card** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-prepare-management-utilities#initialize-ca-smart-card) for details.
C	CRYPTO UNIT ADMINISTRATOR 1 and 2	**Initialize and enroll EP11 smart cards** The purpose of this step is to prepare EP11 smart cards for Hyper Protect Crypto Services administrator signature keys and Hyper Protect Crypto Services master key parts. All smart cards initialized and enrolled in this step will be part of the smart card zone represented by the CA smart card. Refer to the Hyper Protect Crypto Services documentation**: Initialize the EP11 smart card** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-prepare-management-utilities#initialize-ep11-smart-card) for details.
D	All CRYPTO UNIT ADMINISTRATORs	**Personalize administrator smart cards** This will let administrators take ownership of EP11 smart cards by defining PINs for the cards. These smart cards will be used to hold the administrators' personal signature keys. Each administrator must personalize two EP11 smart cards. The PIN on the two smart cards should be the same. Considerations: How will the smart cards be labelled for easy recognition? Evidence to be collected for each administrator smart card: • Card ID • Serial number (if smart cards have printed unique serial numbers))

		• Name of administrator Refer to the Hyper Protect Crypto Services documentation: **Personalize administrator smart cards** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-prepare-management-utilities#initialize-ep11-smart-card) for details.
E	MASTER KEY CUSTODIAN 1 and 2	**Personalize key part smart cards** This will let key managers take ownership of EP11 smart cards by defining PINs for the cards. In these procedures, key part smart cards are personalized smart cards that are not owned by individuals, but by the team of key managers who are authorized to load a specific key part. The key part card and corresponding PIN should therefore be available to the relevant key managers, stored in envelopes in a safe. MASTER KEY CUSTODIAN 1 and 2 must personalize two EP11 smart cards each. The PIN on the two smart cards must be the same. Evidence to be collected for each key part smart card: • Card ID • Serial number (if smart cards have printed unique serial numbers) • Name of key manager team Refer to the Hyper Protect Crypto Services documentation: **Personalize key part smart cards** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-prepare-management-utilities#initialize-ep11-smart-card) for details.
F	CRYPTO UNIT ADMINISTRATOR 1 and 2	**Archive CA smart cards** The CA smart cards will not be needed for the rest of the process and should be stored in sealed envelopes. Four envelopes are required. • CRYPTO UNIT ADMINISTRATOR 1 must mark two envelopes and put a CA smart card and a note with PIN1 in each envelope. • CRYPTO UNIT ADMINISTRATOR 2 must mark two envelopes and put a note with PIN2 in each envelope.

5.1.5.2 Log on Hyper Protect Crypto Services resource group and register crypto units

The following steps and the rest of the procedure is using the IBM Hyper Protect Crypto Services Trusted Key Entry application.

G	Person able to log on to the IBM Cloud	**Log on the Hyper Protect Crypto Services resource group** Refer to the following Hyper Protect Crypto Services documentation for instructions: • Before you begin: (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-prerequisite) • Manage resource groups: (https://cloud.ibm.com/docs/account?topic=account-rgs&interface=ui)
H	SUPERVISOR	**Gather information about Hyper Protect Crypto Services crypto units** The purpose of this step is to capture the information required to allow future identification of the Hyper Protect Crypto Services crypto units being managed. Evidence to be collected:

		• API endpoint • Resource group • Service instance ID • Crypto unit number and location of all crypto units The information should be documented in the Hyper Protect Crypto Services crypto units overview sheet Refer to the following Hyper Protect Crypto Services documentation for instructions: • Before you begin: (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-prerequisite) • Retrieving your instance ID: (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-retrieve-instance-ID)

5.1.5.3 Configure Hyper Protect Crypto Services administrators and access control

The following steps provides the administrators with personal signature keys and configures the access control system of the Hyper Protect Crypto Services crypto units, so only the administrators can manage the crypto units. In essence, the administrators take ownership.

I	All CRYPTO UNIT ADMINISTRATORs	**Generate administrator signature keys and backups** Each administrator must generate a signature key pair on their personal smart card, and each key pair must be copied to the respective administrator's backup smart card. Evidence to be collected for each administrator signature key: • Subject key ID (first 8 digits) • Card IDs Refer to the Hyper Protect Crypto Services documentation: **Generate signature keys** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-management-utilities#step1-generate-keys-management-utilities) for details.
J	All CRYPTO UNIT ADMINISTRATORs	**Add administrators to Hyper Protect Crypto Services crypto units** Each administrator must be added to the crypto units in order to be authorized to work with them. Refer to the Hyper Protect Crypto Services documentation: **Add administrators** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-management-utilities#step3-add-administrator-management-utilities) for details.
K	CRYPTO UNIT ADMINISTRATOR 1 and 2	**Configure signature thresholds (exit IMPRINT mode)** This moves the Hyper Protect Crypto Services crypto units out of imprint mode. When out of imprint mode, only the administrators can manage the crypto units, and the crypto units will enforce the signature requirements. The signature threshold and signature revocation threshold must both be set to 2. Considerations:

		Make sure ALL CRYPTO UNIT ADMINISTRATORs have been added to the crypto units before updating the thresholds. Refer to the Hyper Protect Crypto Services documentation: **Configure signature thresholds** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-management-utilities#step4-exit-imprint-mode-management-utilities) for details.

5.1.5.4 Generate and load Hyper Protect Crypto Services Master Key

L	MASTER KEY CUSTODIAN 1	**Generate 1st master key part and backup** The purpose of this step is to generate the first key part for the Hyper Protect Crypto Services master key and store it on a key part smart card owned by the group of key managers responsible for first key parts. The key part must be copied to a backup smart card. When prompted for a key part description, enter it in the following format: “<description> MK KP1, <YYYY-MM-DD>” (for example: *Production MK KP1, 2021-07-31*) Evidence to be collected: • AES-VP of key part (first 6 digits) • Card IDs Refer to the Hyper Protect Crypto Services documentation: **Generate master key** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-management-utilities#step1-generate-keys-management-utilities) for details.
M	MASTER KEY CUSTODIAN 2	**Generate 2nd master key part and backup** The purpose of this step is to generate the second (last) key part for the Hyper Protect Crypto Services master key on a key part smart card owned by the group of key managers responsible for last key parts. The key part must be copied to a backup smart card. When prompted for a key part description, enter it in the following format: “<description> MK KP2, <YYYY-MM-DD>” (for example: *Production MK KP2, 2021-07-31*) Evidence to be collected: • AES-VP of key part (first 6 digits) • Card IDs Refer to the Hyper Protect Crypto Services documentation: **Generate master key** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-management-utilities#step1-generate-keys-management-utilities) for details.
N	CRYPTO UNIT ADMINISTRATOR 1, MASTER KEY CUSTODIAN 1 and 2	**Load master key**

		The purpose of this step is to load the master key parts into the Hyper Protect Crypto Services crypto units to form the complete master key. It is recommended to load the key parts from the backup smart cards as an assurance that the backups are also readable. *When loading master key parts, it is important to verify and document the key verification patterns of the key parts being loaded as well as the verification pattern of the resulting master key. It can be extremely difficult or even impossible to restore the same master key in a recovery situation later if a wrong key part was loaded in the first place.* Evidence to be collected: • AES-VP of key parts loaded (first 6 digits) • VERIFICATION PATTERN of resulting master key (first 6 digits) Refer to the Hyper Protect Crypto Services documentation: **Load master key** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-management-utilities#step5-load-new-register-management-utilities) for details.
O	CRYPTO UNIT ADMINISTRATOR 1 and 2	**Commit the master key** Refer to the Hyper Protect Crypto Services documentation: **Commit the master key** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-management-utilities#step5-commit-new-register-management-utilities) for details.
P	CRYPTO UNIT ADMINISTRATOR 1 and 2	**Activate the master key** Refer to the Hyper Protect Crypto Services documentation: **Activate the master key** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-management-utilities#step5-activate-master-key-management-utilities) for details.

5.1.5.5 Collect evidence and archive smart cards

Q	SUPERVISOR	**Document resulting configuration of Hyper Protect Crypto Services crypto units** The easiest way to do this is by taking screen shots of the following pages in the IBM Cloud Hyper Protect Crypto Services Trusted Key Entry application: • Crypto units • Administrators • Signature thresholds • Master keys The screen shots should be added to the logbook
R	SUPERVISOR	**Verify collected evidence is correct and complete** • Hyper Protect Crypto Services Instances overview • CA Smart card overview • Hyper Protect Crypto Services Administrator smart card overview • Hyper Protect Crypto Services Master Key Part smart card overview

		- Screen shots showing resulting configuration of Hyper Protect Crypto Services crypto units - Execution of the procedure and any deviations The logbook must be signed by all people participating in the procedure.
S	All CRYPTO UNIT ADMINISTRATORs and MASTER KEY CUSTODIAN 1 and 2	**Archival of smart cards and PINs** - Each smart card is put in an envelope that is marked with a description of its content and then signed and sealed. - For each smart card, the corresponding PIN is also put in an envelope that is marked, signed, and sealed. The administrators and key managers are responsible for proper archival of their smart cards and PINs. The backup smart cards should be stored in a separate location.

5.2 Restore Hyper Protect Crypto Services crypto units using smartcards

5.2.1 Purpose

The purpose of this procedure is to restore the configuration of one or more crypto units in a Hyper Protect Crypto Services instance, for example if crypto units were accidentally reset or new crypto units were added:

- Verify prerequisites (presence of required people, equipment, material, etc.)
- Add administrators to the Hyper Protect Crypto Services crypto units
- Activate the Hyper Protect Crypto Services access control system by setting signature and revocation thresholds
- Load master key parts to the Hyper Protect Crypto Services crypto units
- Commit and activate the master key
- Final verification of the Hyper Protect Crypto Services crypto unit configuration and collection of evidence

5.2.2 Participants

Role indication	Number of persons
CRYPTO UNIT ADMINISTRATOR 1	1
CRYPTO UNIT ADMINISTRATOR 2	1
MASTER KEY CUSTODIAN 1	1
MASTER KEY CUSTODIAN 2	1

All other CRYPTO UNIT ADMINISTRATORs	Depends on the set up
SUPERVISOR	1

5.2.3 Prerequisites

SUPERVISOR must bring

- A copy of this procedure
- Reference documentation for configuration to be restored, including the Subject Key Identifiers of the administrator signature keys, the AES-VPs of the master key parts and the Verification Pattern of the complete master key
- A pen and envelopes to replace envelopes opened during the procedure
- Logbook for journaling the procedure

All CRYPTO UNIT ADMINISTRATORs must bring:

- Their administrator smart cards
- Their 6-digit PINs for their administrator smart cards

MASTER KEY CUSTODIAN 1 must bring:

- The key part smart card with the first key part of the required master key
- The 6-digit PIN for the key part smart card

MASTER KEY CUSTODIAN 2 must bring:

- The key part smart card with the last key part of the required master key
- The 6-digit PIN for the key part smart card

At least one participant must have a valid user ID and password able to log in to the IBM cloud and must have the required Service administrator permissions on the Hyper Protect Crypto Services instance as outlined in https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-manage-access#roles

5.2.4 Evidence to be collected

All activities performed on the TKE workstation must be journaled in the logbook.

The journal must contain at least the following information:

- Date, time, and location
- Purpose of the procedure
- Identity and role of all people involved, including the supervisor
- Procedure steps completed and any deviations from the prescribed procedure
- Hyper Protect Crypto Services instance ID
- Crypto unit number and location of each crypto unit updated

- Where smart cards and PINs are stored after the procedure.
- Resulting Hyper Protect Crypto Services crypto unit set up (for example, screenshots of the ‘Crypto units’, ‘Administrators’, ‘Signature thresholds’ and ‘Master keys’ pages in the IBM Cloud Hyper Protect Crypto Services Trusted Key Entry application)
- Signature of all people involved, including the supervisor

The content of this logbook should be subject to internal/external audits.

In addition to the above, the inventory sheets should be updated.

5.2.5 Procedure steps

5.2.5.1 Log on Hyper Protect Crypto Services resource group and identify crypto units

The following steps and the rest of the procedure is using the IBM Cloud Hyper Protect Crypto Services Trusted Key Entry application.

A	Person able to log on to the IBM Cloud	**Log on the Hyper Protect Crypto Services resource group** Refer to the following Hyper Protect Crypto Services documentation for instructions: • Before you begin: (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-prerequisite) • Manage resource groups: (https://cloud.ibm.com/docs/account?topic=account-rgs&interface=ui)
B	SUPERVISOR	**Identify Hyper Protect Crypto Services crypto units** The purpose of this step is to identify the Hyper Protect Crypto Services crypto units and make sure working with the correct ones. Evidence to be collected: • API endpoint • Resource group • Service instance ID • Crypto unit number and location of all crypto units The supervisor must verify that any deviations from the information in the Hyper Protect Crypto Services crypto units overview sheet are as expected (i.e., only crypto units that are expected to be added or removed) If crypto units were added or removed, the Hyper Protect Crypto Services crypto units overview sheet should be updated to reflect the changes. Refer to the following Hyper Protect Crypto Services documentation for instructions: • Before you begin: (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-prerequisite) • Retrieving your instance ID: (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-retrieve-instance-ID)

5.2.5.2 Configure Hyper Protect Crypto Services administrators and access control

The following steps configures the Hyper Protect Crypto Services access control system so only the administrators can manage the Hyper Protect Crypto Services crypto units. In essence, the administrators take ownership.

C	All CRYPTO UNIT ADMINISTRATORs	**Add administrators to Hyper Protect Crypto Services crypto units** Each administrator must be added to the Hyper Protect Crypto Services crypto units. Evidence to be collected and compared with reference values for each administrator signature key: • Subject key Identifier (first 8 digits) Refer to the Hyper Protect Crypto Services documentation: **Add administrators** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-management-utilities#step3-add-administrator-management-utilities) for details.
D	CRYPTO UNIT ADMINISTRATOR 1 and 2	**Configure signature thresholds (exit IMPRINT mode)** This moves the Hyper Protect Crypto Services crypto units out of imprint mode. When out of imprint mode, only the administrators can manage the crypto units, and the crypto units will enforce the signature requirements. The signature threshold and signature revocation threshold must both be set to 2. Considerations: Make sure all administrators have been added to crypto units before updating the thresholds. Refer to the Hyper Protect Crypto Services documentation: **Configure signature thresholds** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-management-utilities#step4-exit-imprint-mode-management-utilities) for details.

5.2.5.3 Load Hyper Protect Crypto Services Master Key

E	CRYPTO UNIT ADMINISTRATOR 1, MASTER KEY CUSTODIAN 1 and 2	**Load master key** The purpose of this step is to load the master key parts into the Hyper Protect Crypto Services crypto units to form the complete master key. When providing the master key parts, the key managers must compare the AES-VP of their respective key parts with the reference documentation to make sure they are loading the correct key parts. They must also check the VERIFICATION PATTERN of the complete master key. Evidence to be collected and compared with expected values: • AES-VP of key parts loaded (first 6 digits) • VERIFICATION PATTERN of complete master key (first 6 digits)

		Refer to the Hyper Protect Crypto Services documentation: **Load master key** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-management-utilities#step5-load-new-register-management-utilities) for details.
F	CRYPTO UNIT ADMINISTRATOR 1 and 2	**Commit the master key** Refer to the Hyper Protect Crypto Services documentation: **Commit the master key** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-management-utilities#step5-commit-new-register-management-utilities) for details.
G	CRYPTO UNIT ADMINISTRATOR 1 and 2	**Activate the master key** Refer to the Hyper Protect Crypto Services documentation: **Activate the master key** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-management-utilities#step5-activate-master-key-management-utilities) for details.

5.2.5.4 Collect evidence and archive smart cards

H	SUPERVISOR	**Document resulting configuration of Hyper Protect Crypto Services instances** The easiest way to do this is by taking screen shots of the following pages in the IBM Cloud Hyper Protect Crypto Services Trusted Key Entry application: • Crypto units • Administrators • Signature thresholds • Master keys The screen shots should be added to the logbook
I	SUPERVISOR	**Verify collected evidence is correct and complete** • Hyper Protect Crypto Services Instances overview • Screen shots showing resulting configuration of Hyper Protect Crypto Services crypto units • Execution of the procedure and any deviations The logbook must be signed by all people participating in the procedure.
J	All CRYPTO UNIT ADMINISTRATORs and MASTER KEY CUSTODIAN 1 and 2	**Archival of smart cards and PINs** • Each smart card is put in an envelope that is marked with a description of its content and then signed and sealed. • For each smart card, the corresponding PIN is also put in an envelope that is marked, signed, and sealed. The administrators and key managers are responsible for proper archival of their smart cards and PINs. The backup smart cards should be stored in a separate location.

5.3 Add Hyper Protect Crypto Services administrator using smartcards

5.3.1 Purpose

The purpose of this procedure is to add an administrator to the crypto units of an existing Hyper Protect Crypto Services instance using smart cards:

- List prerequisites (presence of required people, equipment, material, etc.)
- Generate administrator signature keys and store on EP11 smart cards (including backups)
- Add administrator to the Hyper Protect Crypto Services crypto units
- Final verification of the Hyper Protect Crypto Services crypto unit configuration and collection of evidence

5.3.2 Participants

Role indication	Number of persons
CRYPTO UNIT ADMINISTRATOR 1	1
CRYPTO UNIT ADMINISTRATOR 2	1
SUPERVISOR	1
New CRYPTO UNIT ADMINISTRATOR	1

5.3.3 Prerequisites

SUPERVISOR must bring

- A copy of this procedure.
- Overview of the intended Hyper Protect Crypto Services management organization
- 2 empty smart cards (to use as administrator smart card and backup)
- Labels for smart cards and PINs and a marker pen
- Envelopes for smart cards and PINs. At least 4.
- Logbook for journaling the procedure

CRYPTO UNIT ADMINISTRATOR 1 must bring:

- Their administrator smart card
- The 6-digit PIN for their administrator smart card
- The CA smart card
- The 6-digit PIN1 for the CA smart card

CRYPTO UNIT ADMINISTRATOR 2 must bring:

- Their administrator smart card

- The 6-digit PIN for their administrator smart card
- The 6-digit PIN2 for the CA smart card

At least one participant must have a valid user ID and password able to log in to the IBM cloud and must have the required Service administrator permissions on the Hyper Protect Crypto Services instance as outlined in https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-manage-access#roles

5.3.4 Evidence to be collected

All activities performed on the TKE workstation must be journaled in the logbook.

The journal must contain at least the following information:

- Date, time, and location
- Purpose of the procedure
- Identity and role of all people involved, including the supervisor
- Procedure steps completed and any deviations from the prescribed procedure
- Hyper Protect Crypto Services instance ID
- Crypto unit number and location of each crypto unit updated
- Subject key identifier and owner information for the new administrator key pair
- Where smart cards and PINs are stored after the procedure.
- Resulting Hyper Protect Crypto Services crypto unit set up (for example, screenshots of the 'Administrators' page in the IBM Cloud Hyper Protect Crypto Services Trusted Key Entry application)
- Signature of all people involved, including the supervisor

The content of this logbook should be subject to internal/external audits.

In addition to the above, the inventory sheets should be updated.

5.3.5 Procedure steps

5.3.5.1 Create administrator smart cards

The following steps prepares the smart cards to be used by the new administrator.

The steps are performed using the IBM Cloud Hyper Protect Crypto Services Smart Card Utility Program.

A	CRYPTO UNIT ADMINISTRATOR 1 and 2	**Initialize and enroll EP11 smart cards** The purpose of this step is to prepare two EP11 smart cards for the new administrator's personal signature key. Refer to the Hyper Protect Crypto Services documentation**: Initialize the EP11 smart card** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-prepare-management-utilities#initialize-ep11-smart-card) for details.

B	New CRYPTO UNIT ADMINISTRATOR	**Personalize administrator smart cards** This will let the new administrator take ownership of the two EP11 smart cards by defining the PIN for the smart cards. The smart cards will be used to hold the administrators' personal signature key. The administrator must personalize the two EP11 smart cards from the previous step. The PIN on the two smart cards should be the same. Consideration: How will the smart cards be labelled for easy recognition? Evidence to be collected for each smart card: • Card ID • Serial number (if smart cards have printed unique serial numbers) • Name of administrator Refer to the Hyper Protect Crypto Services documentation: **Personalize administrator smart cards** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-prepare-management-utilities#initialize-ep11-smart-card) for details.
C	CRYPTO UNIT ADMINISTRATOR 1 and 2	**Archive CA smart cards** The CA smart cards will not be needed for the rest of the procedure and should be put back in sealed envelopes. Four envelopes are required. 1. CRYPTO UNIT ADMINISTRATOR 1 must mark an envelope and put the CA smart card and a note with PIN1 in the envelope. 2. CRYPTO UNIT ADMINISTRATOR 2 must mark an envelope and put a note with PIN2 in the envelope.

5.3.5.2 Log on Hyper Protect Crypto Services resource group and verify crypto units

The following steps and the rest of the procedure is using the IBM Cloud Hyper Protect Crypto Services Trusted Key Entry application.

D	Person able to log on to the IBM Cloud	**Log on the Hyper Protect Crypto Services resource group** Refer to the following Hyper Protect Crypto Services documentation for instructions: • Before you begin: (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-prerequisite) • Manage resource groups: (https://cloud.ibm.com/docs/account?topic=account-rgs&interface=ui)
E	SUPERVISOR	**Identify Hyper Protect Crypto Services crypto units** The purpose of this step is to identify the Hyper Protect Crypto Services crypto units and make sure working with the correct ones. Evidence to be collected: • API endpoint • Resource group • Service instance ID • Crypto unit number and location of all crypto units

		The supervisor must verify that the information matches the information in the Hyper Protect Crypto Services crypto units overview sheet. Refer to the following Hyper Protect Crypto Services documentation for instructions: • Before you begin: (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-prerequisite) • Retrieving your instance ID: (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-retrieve-instance-ID)

5.3.5.3 Authorize administrator to Hyper Protect Crypto Services crypto units

The following steps provides the administrator with a personal signature key and adds the administrator to the Hyper Protect Crypto Services crypto units so the administrator can participate in management of the crypto units.

F	New CRYPTO UNIT ADMINISTRATOR	**Generate administrator signature key and backup** The administrator must generate a signature key pair on their personal smart card, and the key pair must be copied to the administrator's backup smart card. Evidence to be collected: • Subject key ID (first 8 digits) • Card IDs Refer to the Hyper Protect Crypto Services documentation: **Generate signature keys** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-management-utilities#step1-generate-keys-management-utilities) for details.
G	CRYPTO UNIT ADMINISTRATOR 1 and 2 and New ADMINISTRATOR	**Add administrator to Hyper Protect Crypto Services crypto units** The new administrator must be added to the crypto units in order to be authorized to work with them. Refer to the Hyper Protect Crypto Services documentation: **Add administrators** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-management-utilities#step3-add-administrator-management-utilities) for details.

5.3.5.4 Collect evidence and archive smart cards

H	SUPERVISOR	**Document resulting configuration of Hyper Protect Crypto Services crypto units** The easiest way to do this is by taking a screen shot of the following page in the IBM Cloud Hyper Protect Crypto Services Trusted Key Entry application: • Administrators The screen shot should be added to the logbook
I	SUPERVISOR	**Verify collected evidence is correct and complete** • Hyper Protect Crypto Services Administrator smart card overview

		• Screen shots showing resulting configuration of Hyper Protect Crypto Services crypto units • Execution of the procedure and any deviations The logbook must be signed by all people participating in the procedure.
J	CRYPTO UNIT ADMINISTRATOR 1 and 2 and New CRYPTO UNIT ADMINISTRATOR	**Archival of administrator smart cards and PINs** • Each smart card is put in an envelope that is marked with a description of its content and then signed and sealed. • For each smart card, the corresponding PIN is also put in an envelope that is marked, signed, and sealed. The administrators are responsible for proper archival of their smart cards and PINs. The new administrator’s backup smart card should be stored in a separate location.

5.4 Remove Hyper Protect Crypto Services administrator using smartcards

5.4.1 Purpose

The purpose of this procedure is to remove an administrator from the crypto units of an existing Hyper Protect Crypto Services instance. After removal, the administrator will no longer be able to manage the crypto units.

The procedure includes:

- List prerequisites (presence of required people, equipment, material, etc.)
- Remove administrator from the Hyper Protect Crypto Services crypto units
- Final verification of the Hyper Protect Crypto Services crypto unit configuration and collection of evidence

If another administrator is going to replace the administrator, make sure to add the new administrator (using the corresponding procedure) before removing the old administrator.

5.4.2 Participants

Role indication	Number of persons
CRYPTO UNIT ADMINISTRATOR 1	1
CRYPTO UNIT ADMINISTRATOR 2	1
SUPERVISOR	1

5.4.3 Prerequisites

SUPERVISOR must bring

- A copy of this procedure.
- Overview of the Hyper Protect Crypto Services management organization
- Logbook for journaling the procedure

CRYPTO UNIT ADMINISTRATOR 1 must bring:

- Their administrator smart card
- The 6-digit PIN for their administrator smart card

CRYPTO UNIT ADMINISTRATOR 2 must bring:

- Their administrator smart card
- The 6-digit PIN for their administrator smart card

At least one participant must have a valid user ID and password able to log in to the IBM cloud and must have the required Service administrator permissions on the Hyper Protect Crypto Services instance as outlined in https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-manage-access#roles

5.4.4 Evidence to be collected

All activities performed on the TKE workstation must be journaled in the logbook.

The journal must contain at least the following information:

- Date, time, and location
- Purpose of the procedure
- Identity and role of all people involved, including the supervisor
- Procedure steps completed and any deviations from the prescribed procedure
- Hyper Protect Crypto Services instance ID
- Crypto unit number and location of each crypto unit updated
- Subject key identifier and owner information of the administrator being removed
- Resulting Hyper Protect Crypto Services crypto unit set up (for example, screenshot of the 'Administrators' page in the IBM Cloud Hyper Protect Crypto Services Trusted Key Entry application)
- Signature of all people involved, including the supervisor

The content of this logbook should be subject to internal/external audits.

In addition to the above, the inventory sheets should be updated.

5.4.5 Procedure steps

5.4.5.1 Log on Hyper Protect Crypto Services resource group and verify crypto units

The following steps and the rest of the procedure is using the IBM Hyper Protect Crypto Services Trusted Key Entry application.

A	Person able to log on to the IBM Cloud	**Log on the Hyper Protect Crypto Services resource group** Refer to the following Hyper Protect Crypto Services documentation for instructions: • Before you begin: (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-prerequisite) • Manage resource groups: (https://cloud.ibm.com/docs/account?topic=account-rgs&interface=ui)
B	SUPERVISOR	**Identify Hyper Protect Crypto Services crypto units** The purpose of this step is to identify the Hyper Protect Crypto Services crypto units and make sure working with the correct ones. Evidence to be collected:

		- API endpoint - Resource group - Service instance ID - Crypto unit number and location of all crypto units The supervisor must verify that the information matches the information in the Hyper Protect Crypto Services crypto units overview sheet. Refer to the following Hyper Protect Crypto Services documentation for instructions: - Before you begin: (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-prerequisite) - Retrieving your instance ID: (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-retrieve-instance-ID)

5.4.5.2 Remove administrator from Hyper Protect Crypto Services crypto units

The following steps removes the administrator from the crypto units so the administrator can no longer participate in management of the crypto units.

C	CRYPTO UNIT ADMINISTRATOR 1 and 2	**Remove administrator from Hyper Protect Crypto Services crypto units** Before removing the administrator, make sure to compare the administrators Name and Subject Key ID with the values from the inventory documentation, so you are sure to remove the correct administrator. Evidence to be collected: - Name of administrator being removed - Subject key ID of administrator being removed (first 8 digits) Refer to the Hyper Protect Crypto Services documentation: **Remove administrator** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-management-utilities#step3-add-administrator-management-utilities) for details.

5.4.5.3 Collect evidence and archive smart cards

D	SUPERVISOR	**Document resulting configuration of Hyper Protect Crypto Services crypto units** The easiest way to do this is by taking a screen shot of the following page in the IBM Cloud Hyper Protect Crypto Services Trusted Key Entry application: - Administrators The screen shot should be added to the logbook
E	SUPERVISOR	**Verify collected evidence is correct and complete** - Hyper Protect Crypto Services Administrator smart card overview - Screen shots showing resulting configuration of Hyper Protect Crypto Services crypto units - Execution of the procedure and any deviations

		The logbook must be signed by all people participating in the procedure.
F	CRYPTO UNIT ADMINISTRATOR 1 and 2	**Archival of administrator smart cards and PIN** - Each smart card is put in an envelope that is marked with a description of its content and then signed and sealed. - For each smart card, the corresponding PIN is also put in an envelope that is marked, signed, and sealed. The administrator is responsible for proper archival of their smart cards and PIN.

5.5 Rotate Hyper Protect Crypto Services master key using smart cards

5.5.1 Purpose

The purpose of this procedure is to rotate the master key for a Hyper Protect Crypto Services instance. Use this procedure when the instance already contains a master key and this master key should be renewed.

- Verify prerequisites (presence of required people, equipment, material, etc.)
- Generate Hyper Protect Crypto Services master key parts for new master key and store on EP11 smart cards (including backups)
- Load master key parts to the Hyper Protect Crypto Services crypto units
- Commit and activate the new master key
- Final verification of the Hyper Protect Crypto Services crypto unit configuration and collection of evidence

5.5.2 Participants

Role indication	Number of persons
CRYPTO UNIT ADMINISTRATOR 1	1
CRYPTO UNIT ADMINISTRATOR 2	1
MASTER KEY CUSTODIAN 1	1
MASTER KEY CUSTODIAN 2	1
SUPERVISOR	1

5.5.3 Prerequisites

SUPERVISOR must bring

- A copy of this procedure
- A pen and envelopes to replace envelopes opened during the procedure
- Logbook for journaling the procedure

The ADMINISTRATORs must bring:

- Their administrator smart cards
- The 6-digit PINs for their administrator smart cards

MASTER KEY CUSTODIAN 1 must bring:

- The key part smart card to hold the first key part of the new master key
- The corresponding backup key part smart card
- The 6-digit PIN for the key part smart cards

MASTER KEY CUSTODIAN 2 must bring:

- The key part smart card to hold the last key part of the new master key
- The corresponding backup key part smart card
- The 6-digit PIN for the key part smart cards

At least one participant must have a valid user ID and password able to log in to the IBM cloud and must have the required Service administrator permissions on the Hyper Protect Crypto Services instance as outlined in https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-manage-access#roles

5.5.4 Evidence to be collected

All activities performed on the TKE workstation must be journaled in the logbook.

The journal must contain at least the following information:

- Date, time, and location
- Purpose of the procedure
- Identity and role of all people involved, including the supervisor
- Procedure steps completed and any deviations from the prescribed procedure
- Hyper Protect Crypto Services instance ID
- Crypto unit number and location of each crypto unit updated
- Key verification pattern of the new master key parts
- Key verification pattern of the complete new master key
- Where smart cards and PINs are stored after the procedure.
- Resulting Hyper Protect Crypto Services crypto unit set up (for example, screenshot of the ‘Master Keys’ page in the IBM Cloud Hyper Protect Crypto Services Trusted Key Entry application)
- Signature of all people involved, including the supervisor

The content of this logbook should be subject to internal/external audits.

In addition to the above, the inventory sheets should be updated.

5.5.5 Procedure steps

5.5.5.1 Log on Hyper Protect Crypto Services resource group and identify crypto units

The following steps and the rest of the procedure is using the IBM Cloud Hyper Protect Crypto Services Trusted Key Entry application.

A	Person able to log on to the IBM Cloud	**Log on the Hyper Protect Crypto Services resource group** Refer to the following Hyper Protect Crypto Services documentation for instructions: • Before you begin: (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-prerequisite) • Manage resource groups: (https://cloud.ibm.com/docs/account?topic=account-rgs&interface=ui)
B	SUPERVISOR	**Identify Hyper Protect Crypto Services crypto units** The purpose of this step is to identify the Hyper Protect Crypto Services crypto units and make sure working with the correct ones. Evidence to be collected: • API endpoint • Resource group • Service instance ID • Crypto unit number and location of all crypto units The supervisor must verify that the information matches the information in the Hyper Protect Crypto Services crypto units overview sheet. As an extra assurance, it is recommended to verify that the VERIFICATION PATTERN of the CURRENT MASTER KEY REGISTER in all crypto units for the Hyper Protect Crypto Services instance matches the value recorded in the Hyper Protect Crypto Services crypto units overview sheet to make sure the right crypto units are being updated. Refer to the following Hyper Protect Crypto Services documentation for instructions: • Before you begin: (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-prerequisite) • Retrieving your instance ID: (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-retrieve-instance-ID)

5.5.5.2 Generate and load new Hyper Protect Crypto Services Master Key

C	MASTER KEY CUSTODIAN 1	**Generate 1st master key part and backup** The purpose of this step is to generate the first key part for the new Hyper Protect Crypto Services master key and store it on the key part smart card owned by the group of key managers responsible for first key parts. The key part must be copied to the backup smart card. When prompted for a key part description, enter it in the following format:

		“<description> MK KP1, <YYYY-MM-DD>” (for example: *Production MK KP1, 2021-07-31*) Evidence to be collected: • AES-VP of key part (first 6 digits) • Card IDs Refer to the Hyper Protect Crypto Services documentation: **Generate master key** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-management-utilities#step1-generate-keys-management-utilities) for details.
D	MASTER KEY CUSTODIAN 2	**Generate 2nd master key part and backup** The purpose of this step is to generate the second (last) key part for the new Hyper Protect Crypto Services master key on the key part smart card owned by the group of key managers responsible for last key parts. The key part must be copied to the backup smart card. When prompted for a key part description, enter it in the following format: “<description> MK KP2, <YYYY-MM-DD>” (for example: *Production MK KP2, 2021-07-31*) Evidence to be collected: • AES-VP of key part (first 6 digits) • Card IDs Refer to the Hyper Protect Crypto Services documentation: **Generate master key** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-management-utilities#step1-generate-keys-management-utilities) for details.
E	CRYPTO UNIT ADMINISTRATOR 1, MASTER KEY CUSTODIAN 1 and 2	**Load master key** The purpose of this step is to load the master key parts into the Hyper Protect Crypto Services crypto units to form the complete master key. It is recommended to load the key parts from the backup smart cards as an assurance that the backups are also readable. *When loading master key parts, it is important to verify and document the key verification patterns of the key parts being loaded as well as the verification pattern of the resulting master key. It can be extremely difficult or even impossible to restore the same master key in a recovery situation later if a wrong key part was loaded in the first place.* Evidence to be collected: • AES-VP of key parts loaded (first 6 digits) • VERIFICATION PATTERN of resulting master key (first 6 digits) Refer to the Hyper Protect Crypto Services documentation: **Rotating master keys by using smart cards and the Management Utilities** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-rotate-master-key-smart-cards) for details.
F	CRYPTO UNIT ADMINISTRATOR 1 and 2	**Commit the master key**

		Refer to the Hyper Protect Crypto Services documentation: **Rotating master keys by using smart cards and the Management Utilities** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-rotate-master-key-smart-cards) for details.
G	CRYPTO UNIT ADMINISTRATOR 1 and 2	**Rotate the master key** **WARNING:** You must use the **Rotate** button to do this. Do not use the **Set Immediate** button, as this might result in loss of keys in the key store. Refer to the Hyper Protect Crypto Services documentation: **Rotating master keys by using smart cards and the Management Utilities** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-rotate-master-key-smart-cards) for details.

5.5.5.3 Collect evidence and archive smart cards

H	SUPERVISOR	**Document resulting configuration of Hyper Protect Crypto Services crypto units** The easiest way to do this is by taking screen shot of the following page in the IBM Cloud Hyper Protect Crypto Services Trusted Key Entry application: • Master keys The screen shot should be added to the logbook
I	SUPERVISOR	**Verify collected evidence is correct and complete** • Screen shot from previous step • Execution of the procedure and any deviations The logbook must be signed by all people participating in the procedure.
J	All CRYPTO UNIT ADMINISTRATORs and MASTER KEY CUSTODIAN 1 and 2	**Archival of smart cards and PINs** • Each smart card is put in an envelope that is marked with a description of its content and then signed and sealed. • For each smart card, the corresponding PIN is also put in an envelope that is marked, signed, and sealed. The administrators and key managers are responsible for proper archival of their smart cards and PINs. The backup smart cards should be stored in a separate location.

5.6 Freeze Hyper Protect Crypto Services instance using smart cards

5.6.1 Purpose

The purpose of this procedure is to remove the master key from the crypto units of a Hyper Protect Crypto Services instance. This prevents anyone from using the Hyper Protect Crypto Services instance. To enable the use of the Hyper Protect Crypto Services instance again, the master key must be reloaded (see separate procedure).

- Verify prerequisites (presence of required people, equipment, material, etc.)
- Remove the current master key
- Final verification of the Hyper Protect Crypto Services crypto unit configuration and collection of evidence

5.6.2 Participants

Role indication	Number of persons
CRYPTO UNIT ADMINISTRATOR 1	1
CRYPTO UNIT ADMINISTRATOR 2	1
SUPERVISOR	1

5.6.3 Prerequisites

SUPERVISOR must bring

- A copy of this procedure
- A pen and envelopes to replace envelopes opened during the procedure
- Logbook for journaling the procedure

The ADMINISTRATORs must bring:

- Their administrator smart cards
- The 6-digit PINs for their administrator smart cards

At least one participant must have a valid user ID and password able to log in to the IBM cloud and must have the required Service administrator permissions on the Hyper Protect Crypto Services instance as outlined in https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-manage-access#roles

5.6.4 Evidence to be collected

All activities performed on the TKE workstation must be journaled in the logbook.

The journal must contain at least the following information:

- Date, time, and location
- Purpose of the procedure
- Identity and role of all people involved, including the supervisor
- Procedure steps completed and any deviations from the prescribed procedure
- Hyper Protect Crypto Services instance ID
- Crypto unit number and location of each crypto unit updated
- Key verification pattern of the master key that was removed
- Where smart cards and PINs are stored after the procedure.
- Resulting Hyper Protect Crypto Services crypto unit set up (for example, screenshot of the 'Master Keys' page in the IBM Cloud Hyper Protect Crypto Services Trusted Key Entry application)
- Signature of all people involved, including the supervisor

The content of this logbook should be subject to internal/external audits.

In addition to the above, the inventory sheets should be updated.

5.6.5 Procedure steps

5.6.5.1 Log on Hyper Protect Crypto Services resource group and identify crypto units

The following steps and the rest of the procedure is using the IBM Hyper Protect Crypto Services Trusted Key Entry application.

A	Person able to log on to the IBM Cloud	**Log on the Hyper Protect Crypto Services resource group** Refer to the following Hyper Protect Crypto Services documentation for instructions: • Before you begin: (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-prerequisite) • Manage resource groups: (https://cloud.ibm.com/docs/account?topic=account-rgs&interface=ui)
B	SUPERVISOR	**Identify Hyper Protect Crypto Services crypto units** The purpose of this step is to identify the Hyper Protect Crypto Services crypto units and make sure working with the correct ones. Evidence to be collected: • API endpoint • Resource group • Service instance ID • Crypto unit number and location of all crypto units The supervisor must verify that the information matches the information in the Hyper Protect Crypto Services crypto units overview sheet.

		As an extra assurance, it is recommended to verify that the VERIFICATION PATTERN of the CURRENT MASTER KEY REGISTER in all crypto units for the Hyper Protect Crypto Services instance matches the value recorded in the Hyper Protect Crypto Services crypto units overview sheet to make sure the right crypto units are being updated. Refer to the following Hyper Protect Crypto Services documentation for instructions: • Before you begin: (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-prerequisite) • Retrieving your instance ID: (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-retrieve-instance-ID)

5.6.5.2 Remove the current Hyper Protect Crypto Services Master Key

C	CRYPTO UNIT ADMINISTRATOR 1 and 2	**Clear current master key** The purpose of this step is to remove the master key from the Hyper Protect Crypto Services crypto units effectively preventing use of the Hyper Protect Crypto Services instance. Evidence to be collected: • VERIFICATION PATTERN of master key removed (first 6 digits) Refer to the Hyper Protect Crypto Services documentation: **Remove master key**(https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-management-utilities#step5-load-master-key-management-utilities) for details.

5.6.5.3 Collect evidence and archive smart cards

D	SUPERVISOR	**Document resulting configuration of Hyper Protect Crypto Services crypto units** The easiest way to do this is by taking screen shot of the following page in the IBM Cloud Hyper Protect Crypto Services Trusted Key Entry application: • Master keys The screen shot should be added to the logbook
E	SUPERVISOR	**Verify collected evidence is correct and complete** • Screen shot from previous step • Execution of the procedure and any deviations The logbook must be signed by all people participating in the procedure.
F	CRYPTO UNIT ADMINISTRATOR 1 and 2	**Archival of smart cards and PINs** • Each smart card is put in an envelope that is marked with a description of its content and then signed and sealed. • For each smart card, the corresponding PIN is also put in an envelope that is marked, signed, and sealed.

		The administrators and key managers are responsible for proper archival of their smart cards and PINs.

5.7 Reload Hyper Protect Crypto Services master key using smart cards

5.7.1 Purpose

The purpose of this procedure is to reload the master key into the crypto units of a Hyper Protect Crypto Services instance. This is required to reactivate a Hyper Protect Crypto Services instance after the master key has been deleted (for example after freezing the Hyper Protect Crypto Services instance)

- Verify prerequisites (presence of required people, equipment, material, etc.)
- Load master key parts to the Hyper Protect Crypto Services crypto units
- Commit and activate the master key
- Final verification of the Hyper Protect Crypto Services crypto unit configuration and collection of evidence

5.7.2 Participants

Role indication	Number of persons
CRYPTO UNIT ADMINISTRATOR 1	1
CRYPTO UNIT ADMINISTRATOR 2	1
MASTER KEY CUSTODIAN 1	1
MASTER KEY CUSTODIAN 2	1
SUPERVISOR	1

5.7.3 Prerequisites

SUPERVISOR must bring

- A copy of this procedure
- A pen and envelopes to replace envelopes opened during the procedure
- Logbook for journaling the procedure

The ADMINISTRATORs must bring:

- Their administrator smart cards
- The 6-digit PINs for their administrator smart cards

MASTER KEY CUSTODIAN 1 must bring:

- The key part smart card holding the first key part of the master key

- The 6-digit PIN for the key part smart card

MASTER KEY CUSTODIAN 2 must bring:

- The key part smart card holding the last key part of the master key
- The 6-digit PIN for the key part smart card

At least one participant must have a valid user ID and password able to log in to the IBM cloud and must have the required Service administrator permissions on the Hyper Protect Crypto Services instance as outlined in https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-manage-access#roles

5.7.4 Evidence to be collected

All activities performed on the TKE workstation must be journaled in the logbook.

The journal must contain at least the following information:

- Date, time, and location
- Purpose of the procedure
- Identity and role of all people involved, including the supervisor
- Procedure steps completed and any deviations from the prescribed procedure
- Hyper Protect Crypto Services instance ID
- Crypto unit number and location of each crypto unit updated
- Key verification pattern of the master key
- Where smart cards and PINs are stored after the procedure.
- Resulting Hyper Protect Crypto Services crypto unit set up (for example, screenshot of the 'Master Keys' page in the IBM Cloud Hyper Protect Crypto Services Trusted Key Entry application)
- Signature of all people involved, including the supervisor

The content of this logbook should be subject to internal/external audits.

In addition to the above, the inventory sheets should be updated.

5.7.5 Procedure steps

5.7.5.1 Log on Hyper Protect Crypto Services resource group and identify crypto units

The following steps and the rest of the procedure is using the IBM Cloud Hyper Protect Crypto Services Trusted Key Entry application.

A	Person able to log on to the IBM Cloud	**Log on the Hyper Protect Crypto Services resource group** Refer to the following Hyper Protect Crypto Services documentation for instructions:

		- Before you begin: (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-prerequisite) - Manage resource groups: (https://cloud.ibm.com/docs/account?topic=account-rgs&interface=ui)
B	SUPERVISOR	**Identify Hyper Protect Crypto Services crypto units** The purpose of this step is to identify the Hyper Protect Crypto Services crypto units and make sure working with the correct ones. Evidence to be collected: - API endpoint - Account - Resource group - Service instance ID - Crypto unit number and location of all crypto units The supervisor must verify that the information matches the information in the Hyper Protect Crypto Services crypto units overview sheet. As an extra assurance, it is recommended to verify that the VERIFICATION PATTERN of the CURRENT MASTER KEY REGISTER in all crypto units for the Hyper Protect Crypto Services instance are empty to make sure the right crypto units are being updated. Refer to the following Hyper Protect Crypto Services documentation for instructions: - Before you begin: (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-prerequisite) - Retrieving your instance ID: (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-retrieve-instance-ID)

5.7.5.2 Load Hyper Protect Crypto Services Master Key

C	CRYPTO UNIT ADMINISTRATOR 1, MASTER KEY CUSTODIAN 1 and 2	**Load master key** The purpose of this step is to load the master key parts to form the complete master key. When providing the master key parts, the key managers must compare the AES-VP of their respective key parts with the reference documentation to make sure they are loading the correct key parts. They must also check the VERIFICATION PATTERN of the complete master key. Evidence to be collected and compared with expected values: - AES-VP of key parts loaded (first 6 digits) - VERIFICATION PATTERN of complete master key (first 6 digits) Refer to the Hyper Protect Crypto Services documentation: **Load master key** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-management-utilities#step5-load-new-register-management-utilities) for details.
D	CRYPTO UNIT ADMINISTRATOR 1 and 2	**Commit the master key** Refer to the Hyper Protect Crypto Services documentation: **Commit the master key** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-

		management-utilities#step5-commit-new-register-management-utilities) for details.
E	CRYPTO UNIT ADMINISTRATOR 1 and 2	**Activate the master key** Refer to the Hyper Protect Crypto Services documentation: **Activate the master key** (https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-initialize-hsm-management-utilities#step5-activate-master-key-management-utilities) for details.

5.7.5.3 Collect evidence and archive smart cards

F	SUPERVISOR	**Document resulting configuration of Hyper Protect Crypto Services crypto units** The easiest way to do this is by taking screen shot of the following page in the IBM Cloud Hyper Protect Crypto Services Trusted Key Entry application: • Master keys The screen shot should be added to the logbook
G	SUPERVISOR	**Verify collected evidence is correct and complete** • Screen shot from previous step • Execution of the procedure and any deviations The logbook must be signed by all people participating in the procedure.
H	All CRYPTO UNIT ADMINISTRATORs and MASTER KEY CUSTODIAN 1 and 2	**Archival of smart cards and PINs** • Each smart card is put in an envelope that is marked with a description of its content and then signed and sealed. • For each smart card, the corresponding PIN is also put in an envelope that is marked, signed, and sealed. The administrators and key managers are responsible for proper archival of their smart cards and PINs.

6. Appendix

Hyper Protect Crypto Services Security Organization overview

Security organization - roles

Organizational role	Role description
CRYPTO UNIT ADMINISTRATOR 1	Security administrator: • Responsible for signing updates to Hyper Protect Crypto Services crypto units • Responsible for CA smart cards • Responsible for 1st PIN for CA smart cards
CRYPTO UNIT ADMINISTRATOR 2	Security administrator: • Responsible for signing updates to Hyper Protect Crypto Services crypto units • Responsible for 2nd PIN for CA smart cards
MASTER KEY CUSTODIAN 1	Key manager: • Responsible for first key part of Hyper Protect Crypto Services master keys
MASTER KEY CUSTODIAN 2	Key manager: • Responsible for last key part of Hyper Protect Crypto Services master keys
SUPERVISOR	Supervisor of ceremonies: • Responsible for directing Hyper Protect Crypto Services ceremonies according to procedures, documenting progress and deviations, as well as collecting evidence needed for audit purposes.

Security organization – people

Full name	Organizational role(s)

Date updated: **Updated by:**

Hyper Protect Crypto Services crypto units overview

API Endpoint: ______________________________

Account: ______________________________

Resource group: ______________________________

Crypto units

SERVICE INSTANCE	CRYPTO UNIT NUM	LOCATION

Master key VERIFICATION PATTERN (first 6 digits): ____________

Notes:

Date updated:

Updated by:

Hyper Protect Crypto Services CA Smart cards

Zone Description: ____________________

Zone ID: ____________________

Used with SERVICE INSTANCE(s): ____________________

CA Smart cards

Administrators of PIN 1	Administrators of PIN 2	Card ID	Serial number (if printed on card)	Type	Storage location (location and/or envelope ID)
				Master	
				Backup	

Notes:

Date updated:

Updated by:

Hyper Protect Crypto Services Administrator smart cards

Zone Description: ______________________________

Zone ID: ______________________________

Used with SERVICE INSTANCE(s): ______________________________

Administrator or Team	Subject Key Identifier (first 8 digits)	Card ID	Serial number (if printed on card)	Type	Storage location (location and/or envelope ID)
				Master	
				Backup	
				Master	
				Backup	
				Master	
				Backup	
				Master	
				Backup	

Notes:

Date updated:

Updated by:

Hyper Protect Crypto Services Master Key Part smart cards

Zone Description:

Zone ID:

Used with SERVICE INSTANCE(s):

Master key VERIFICATION PATTERN (first 6 digits):

Key part	AES-VP	Key manager team	Card ID	Serial number	Type	Storage location
(first/last)	(first 6 digits)			(if printed on card)		(location and/or envelope ID)
First					Master	
					Backup	
Last					Master	
					Backup	

Notes:

Date updated:

Updated by: