

IBM Technology



G-Cloud 15

IBM – Hyper Protect Crypto – Key Management
Service & HSM

Service Definition Document

Email: ukcat@uk.ibm.com

Contact: Anne-Marie Wheeler



IBM Cloud Hyper Protect Crypto Services

Except as noted below, the terms of the IBM Cloud Service Description apply.

1. Cloud Service

IBM Cloud Hyper Protect Crypto Services (Hyper Protect Crypto Services) provides a cloud hardware security module (HSM) for a dedicated key management service. Hyper Protect Crypto Services helps Client encrypt its data according to the highest security standards utilizing FIPS 140-2 compliant hardware security modules.

1.1 Offerings

The Client may select from the following available offerings.

1.1.1 IBM Cloud Hyper Protect Crypto Services

Hyper Protect Crypto Services integrates with IBM Key Protect for IBM Cloud APIs to generate and encrypt keys. The Cloud Service provides network access to Hardware Security Module (HSM) Hardware that has been designed to meet FIPS 140-2 lvl 4 certification requirements. Keep Your Own Keys (KYOK) allows imprinting (initializing) and management of the HSM with customer generated administrator certificates and master keys.

2. Data Processing and Protection Data Sheets

The Data Sheet applicable for this service and the terms of this section provides the details and terms, including Client responsibilities, around use of this service. The following Data Sheet(s) apply to this service: <https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=46E9C81025D811E895B382FBC780E8BA>

3. Service Levels and Technical Support

3.1 Service Level Agreement

The service level agreement set forth in the base IBM Cloud Service Description applies to this service.

3.2 Technical Support

The support terms set forth in the base IBM Cloud Service Description apply to this service.

4. Charges

4.1 Charge Metrics

The charge metric(s) for the Cloud Service are specified in the Transaction Document. The following charge metrics apply to this Cloud Service:

- Hour is an hour of use of the Cloud Services. For this Cloud Service Client will be charged for:
- Each Hour a Crypto Unit is available to or managed by the Cloud Service.

- Each Hour the Unified Key Orchestrator feature is enabled.
- Item is an occurrence of a specific item that is managed by, processed by, or related to the use of the Cloud Service. For this Cloud Service an Item is either an internal keystore or an external keystore

5. Additional Terms

For Cloud Service Agreements (or equivalent base cloud agreements) executed prior to January 1, 2019, the terms available at <https://www.ibm.com/acs> apply.

5.1 Open-Source Licenses

The following describe open source packages and their licenses used:

- IBM/Plex Font: The Cloud Service uses the IBM/plex font within the IBM Cloud dashboard under the SIL Open Font License: <https://opensource.org/licenses/OFL-1.1/>.
- distribute-0.6.34/docs/build/html/_sources/index.txt:
<https://creativecommons.org/licenses/by/3.0/>
- golang/text: <https://creativecommons.org/licenses/by-sa/3.0/>
- golang/gopher: <https://creativecommons.org/licenses/by-sa/3.0/>
- howto.diveintomark: <https://creativecommons.org/licenses/by-sa/2.5/>

5.2 Client Responsibilities

Client is responsible for keeping copies of signature keys and master key parts as the Cloud Service does not retain copies. If the Cloud Service fails, or hardware replacement or upgrade is made, Client may need to reinitialize the HSM using Client's saved keys and certificates to fully restore usage of the Cloud Service and all Content.

5.3 Sample and Demo Software

The Cloud Service may include some components in source code form (Source Components) and other materials that will be identified as "Sample Materials". Client may copy and modify Source Components and Sample Materials for internal use only. Client may not alter or delete any copyright information or notices contained in the Source Components or Sample Materials. IBM provides the Source Components and Sample Materials as-is, without warranties of any kind.

5.4 Administrative Access

IBM Cloud Hyper Protect Crypto Services do not include any interface in the product that enables IBM Cloud provider administrative access to Client or Customer Personal Data and other key material in the



production runtime environment. "Administrative Access" means the right and possibility to access, read, export, modify or delete unencrypted customer data (e.g., database content, log files and key material). Service log files do not contain any Personal Data or key material. IBM Cloud Satellite
Except as noted below, the terms of the IBM Cloud Service Description apply.

