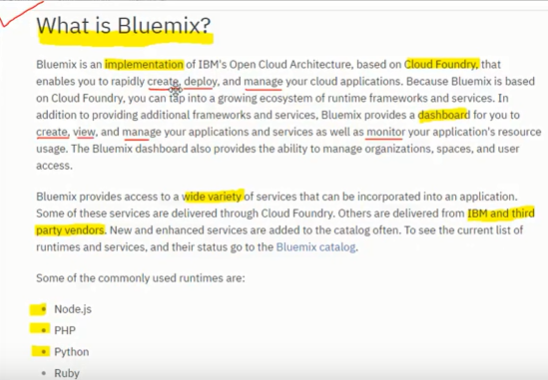
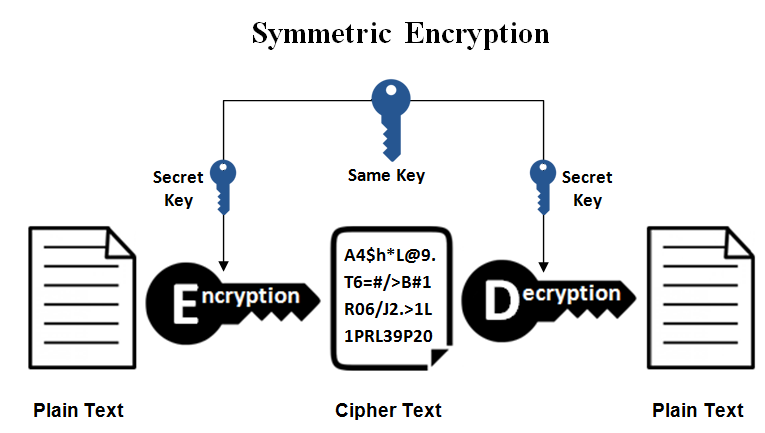
**IBM KEY PROTECT SERVICE**

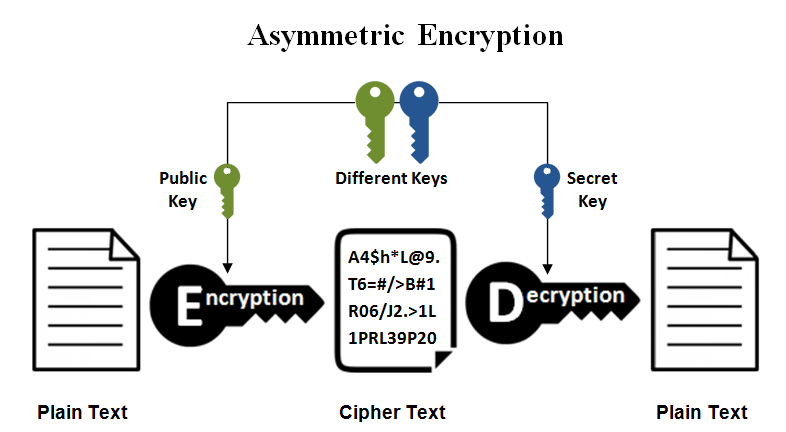
[**https://www.ibm.com/blogs/bluemix/2018/10/ibm-key-protect-is-now-available-for-ibm-cloud-kubernetes-service/**](https://www.ibm.com/blogs/bluemix/2018/10/ibm-key-protect-is-now-available-for-ibm-cloud-kubernetes-service/)

 to enable Key Protect for the Kubernetes secrets.



[**https://console.bluemix.net/docs/iam/login\_fedid.html#federated\_id**](https://console.bluemix.net/docs/iam/login_fedid.html#federated_id)





## **Difference Between Symmetric and Asymmetric Encryption**

* Symmetric encryption uses a single key that needs to be shared among the people who need to receive the message while asymmetrical encryption uses a pair of public key and a private key to encrypt and decrypt messages when communicating.
* Symmetric encryption is an old technique while asymmetric encryption is relatively new.
* Asymmetric encryption was introduced to complement the inherent problem of the need to share the key in symmetrical encryption model, eliminating the need to share the key by using a pair of public-private keys.
* Asymmetric encryption takes relatively more time than the symmetric encryption.

how to create and add existing cryptographic keys by using the Key Protect dashboard, so you can manage data encryption from one central location

**Root** keys are symmetric key-wrapping keys that you fully manage in Key Protect.You can use a root key to protect other cryptographic keys with advanced encryption.

**Standard** keys are symmetric keys that are used for cryptography. You can use a standard key to directly encrypt and decrypt data.

After adding root keys, **check wrapping keys**

<https://console.bluemix.net/docs/services/key-protect/wrap-keys.html#wrap-keys>

Wrapping keys

You can manage and protect your encryption keys with a root key by using the IBM® Key Protect API, if you are a privileged user.

When you wrap a data encryption key (DEK) with a root key, Key Protect combines the strength of multiple algorithms to protect the privacy and the integrity of your encrypted data.

To learn how key wrapping helps you control the security of at-rest data in the cloud, see [Envelope encryption](https://console.bluemix.net/docs/services/key-protect/concepts/envelope-encryption.html).

<https://console.bluemix.net/docs/services/key-protect/concepts/envelope-encryption.html>

# Envelope encryption

Envelope encryption is the practice of encrypting data with a data encryption key (DEK) and then encrypting the DEK with a root key that you can fully manage.

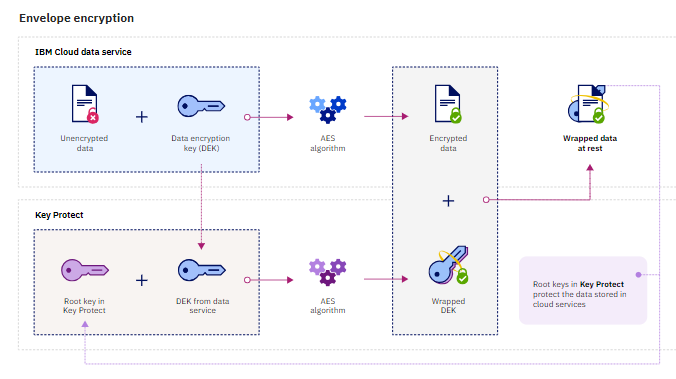
## Definition - What does *Data Encryption Key (DEK)* mean?

A data encryption key (DEK) is a type of key designed to encrypt and decrypt data at least once or possibly multiple times. DEKs are created by an encryption engine. Data is encrypted and decrypted with the help of the same DEK; therefore, a DEK must be stored for at least a specified duration for decrypting the generated cipher text.

## **How it works**

Envelope encryption combines the strength of multiple encryption algorithms to protect your sensitive data in the cloud. It works by wrapping one or more data encryption keys (DEKs) with advanced encryption by using a root key that you can fully manage. This key wrapping process creates wrapped DEKs that protect your stored data from unauthorized access or exposure. Unwrapping a DEK reverses the envelope encryption process by using the same root key, resulting in decrypted and authenticated data.

The following diagram shows a contextual view of the key wrapping functionality.



## **Key types**

The service supports two key types, root keys and standard keys, for the advanced encryption and management of data.

**Root keys**

Root keys are primary resources in Key Protect. They are symmetric key-wrapping keys used as roots of trust for wrapping (encrypting) and unwrapping (decrypting) other keys stored in a data service. With Key Protect, you can create, store, and manage the lifecycle of root keys to achieve full control of other keys stored in the cloud. Unlike a standard key, a root key can never leave the bounds of the Key Protect service.

**Standard keys**

Standard keys are encryption keys that are used for cryptography. Generally, standard keys directly encrypt data. With Key Protect, you can create, store, and manage the lifecycle of standard keys. After you import or generate a standard key in the service, you can export it to an outside data resource, such as a storage bucket, to encrypt sensitive information. Standard keys that encrypt stored data are called data encryption keys (DEKs), which can be wrapped with advanced encryption. Wrapped DEKs are not stored in Key Protect.

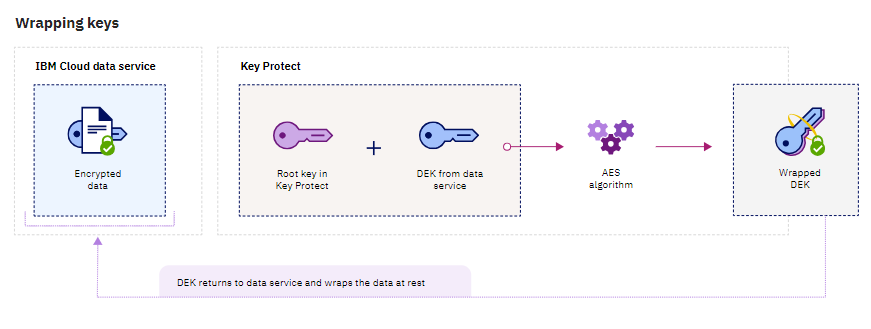
After you create keys in Key Protect, the system returns an ID value that you can use to make API calls to the service. You can retrieve the ID value for your keys with the Key Protect GUI or the [Key Protect API](https://console.bluemix.net/apidocs/key-protect).

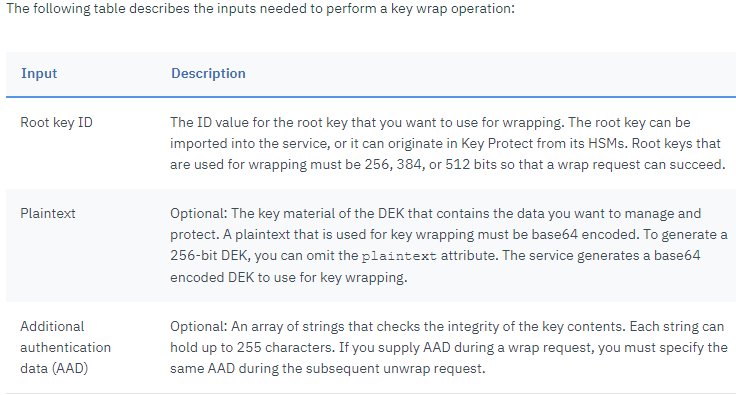
<https://console.bluemix.net/apidocs/key-protect>

## **Wrapping keys**

Root keys help you group, manage, and protect data encryption keys (DEKs) stored in the cloud. You can wrap one or more DEKs with advanced encryption by designating a root key in Key Protect that you can fully manage.

After you designate a root key in Key Protect, you can send a key wrap request to the service by using the Key Protect API. The key wrap operation provides both confidentiality and integrity protection for a DEK. The following diagram shows the key wrapping process in action:





If you send a wrap request without specifying the plaintext to encrypt, the AES-GCM encryption algorithm generates and converts a plaintext to an unintelligible form of data called a ciphertext. This process outputs a 256-bit DEK with new key material. The system then uses an AES key-wrapping algorithm, which wraps the DEK and its key material with the specified root key. A successful wrap operation returns a base64 encoded wrapped DEK that you can store in an IBM Cloud app or service

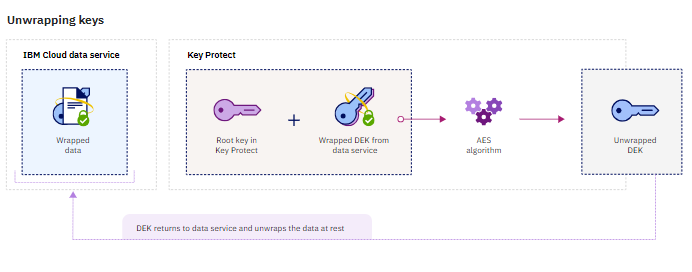
## **Unwrapping keys**

Unwrapping a data encryption key (DEK) decrypts and authenticates the contents within the key, returning the original key material to your data service.

If your business application needs to access the contents of your wrapped DEKs, you can use the Key Protect API to send an unwrap request to the service. To unwrap a DEK, you specify the ID value of the root key and the ciphertextvalue returned during the initial wrap request. To complete the unwrap request, you must also supply the additional authenticated data (AAD) to check the integrity of the key contents.

The following diagram shows key unwrapping in action.

## **Wrapping keys by using the API**



After you send the unwrap request, the system reverses the key wrapping process by using the same AES algorithms. A successful unwrap operation returns the base64 encoded plaintext value to your IBM Cloud data at rest service.

**DEMO:**

## **Wrapping keys by using the API**

You can protect a specified data encryption key (DEK) with a root key that you manage in Key Protect.

**Important:** When you supply a root key for wrapping, ensure that the root key is 256, 384, or 512 bits so that the wrap call can succeed. If you create a root key in the service, Key Protect generates a 256-bit key from its HSMs, supported by the AES-GCM algorithm.

1. **Log in to IBM Cloud with the**[**IBM Cloud CLI**](https://console.bluemix.net/docs/cli/index.html#overview).

rajbir\_sood@PTL06625 MINGW64 /c/sandbox/devops\_docs (master)

$ ibmcloud config --check-version=false

rajbir\_sood@PTL06625 MINGW64 /c/sandbox/devops\_docs (master)

$ **ibmcloud login --apikey ggZAdoNYcqUJfJljBL\_3NkRxSyYalUjS4CCIFE5EKoo\_**

API endpoint: https://api.eu-gb.bluemix.net

Authenticating...

OK

1. **To start managing encryption keys, install the Key Protect CLI plug-in.**
2. rajbir\_sood@PTL06625 MINGW64 /c/sandbox/devops\_docs (master)

**$ ibmcloud plugin install key-protect**

1. Looking up 'key-protect' from repository 'Bluemix'...
2. Plug-in 'key-protect/kp 0.1.1' found in repository 'Bluemix'
3. Attempting to download the binary file...
4. 10.27 MiB / 10.27 MiB 100.00% 53ss5s
5. 10764288 bytes downloaded
6. Installing binary...
7. OK
8. Plug-in 'key-protect 0.1.1' was successfully installed into C:\Users\rajbir\_sood\.bluemix\plugins\key-protect. Use 'C:\Program Files\IBM\Cloud\bin\ibmcloud.exe plugin show key-protect' to show its details.

rajbir\_sood@PTL06625 MINGW64 /c/sandbox/devops\_docs (master)

rajbir\_sood@PTL06625 MINGW64 /c/sandbox/devops\_docs (master)

**$ ibmcloud plugin list**

Listing installed plug-ins...

Plugin Name Version

container-registry 0.1.329

container-service/kubernetes-service 0.1.575

dev 2.1.4

key-protect 0.1.1

sdk-gen 0.1.12

cloud-functions/wsk/functions/fn 1.0.22

1. **Select the account that contains your provisioned instance of Key Protect**.

You can run ibmcloud resource service-instances to list all service instances that are provisioned in your account.

rajbir\_sood@PTL06625 MINGW64 /c/sandbox/devops\_docs (master)

$ **ibmcloud resource service-instances**

Retrieving service instances in resource group Default and all location under account IBM as rajbsood@in.ibm.com...

OK

Name Location State Type Tags

Continuous Delivery us-south active service\_instance

Key Protect-raj eu-gb active service\_instance

1. **Retrieve the Cloud Resource Name (CRN) that uniquely identifies your Key Protect service instance.**

rajbir\_sood@PTL06625 MINGW64 /c/sandbox/devops\_docs (master)

$ **ibmcloud resource service-instance "Key Protect-raj" --id**

crn:v1:bluemix:public:kms:eu-gb:a/90488ffecf50473ba57279d415e24aef:0cb9bd07-e60d-42ae-a761-bf11c40c7174:: 0cb9bd07-e60d-42ae-a761-bf11c40c7174

## **Forming your API request**

When you make an API call to the service, structure your API request according to how you initially provisioned your instance of Key Protect.

To build your request, pair a [regional service endpoint](https://console.bluemix.net/docs/services/key-protect/regions.html) with the appropriate authentication credentials. For example, if you created a service instance for the us-south region, use the following endpoint and API headers to browse keys in your service:

curl -X GET \

https://keyprotect.us-south.bluemix.net/api/v2/keys \

-H 'accept: application/vnd.ibm.collection+json' \

-H 'authorization: Bearer <access\_token>' \

-H 'bluemix-instance: <instance\_ID>' \

## **Before you begin**

https://console.bluemix.net/docs/services/key-protect/manage-access-api.html#manage-access-api

To work with the API, generate your authentication credentials, such as your [access token](https://console.bluemix.net/docs/services/key-protect/access-api.html#retrieve-token) and [instance ID](https://console.bluemix.net/docs/services/key-protect/access-api.html#retrieve-instance-ID). You also need the ID of the Key Protect key that you want to manage access for.

## **Retrieving an access token**

You can authenticate with Key Protect by retrieving an access token from Cloud Identity and Access Management. With a [service ID](https://console.bluemix.net/docs/iam/serviceid.html#serviceids), you can work with the Key Protect API on behalf of your service or application on or outside IBM Cloud, without needing to share your personal user credentials.

<https://console.bluemix.net/docs/services/key-protect/access-api.html#retrieve-token>

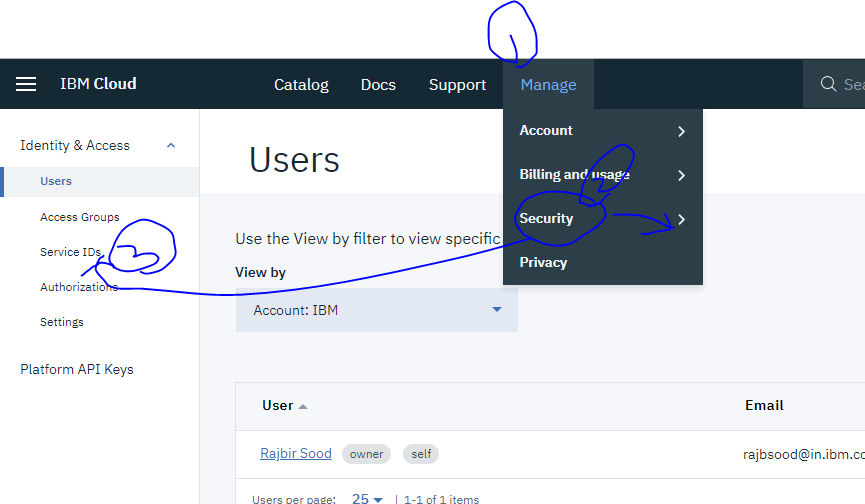
rajbir\_sood@PTL06625 MINGW64 /c/sandbox/devops\_docs (master)

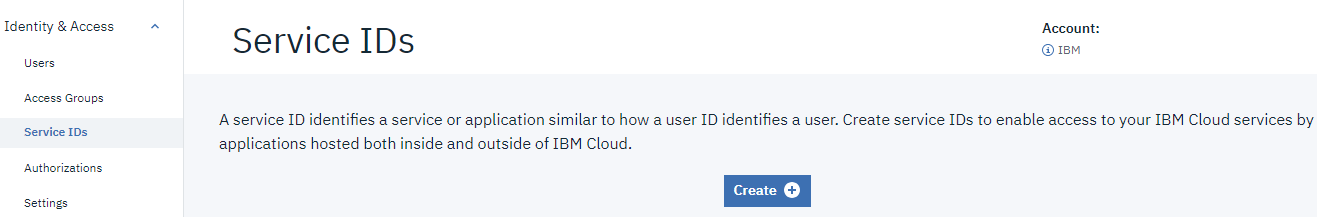
$ **ibmcloud iam oauth-tokens**

IAM token: Bearer eyJraWQiOiIyMDE3MTAzMC0wMDowMDowMCIsImFsZyI6IlJTMjU2In0..arOXo5lQOWb-62x2YuAprPkJk4dG0vKRNFc8i7F4etyPiSXYHwWIBd1yHn3YTG\_a3e9ZjEcc\_fNqTIgp4VBkNqXXlyxW5Ycx9wNjtJq\_kY7xtllrFdzM2JJuNHWs\_VoWoBAhui5GkYeSNuqKV05-5mY08-PXTKKbqdH5nBxAQKc-Zvqd6SeoVewi8zVAtWgfRcWQTEzUW1nit8PgzLesKDns0mzn\_6I-SOIDmM3iIigqMR5hAgrI4ekVqTKVReVg1lL-olgUc4YsDbxGJ3LwNHx9V1H4V8sjbzhehcLxxXbRp1BGcLBONEsaNNSvOYCK1dFUO8JQPRDp-JyBCflQ

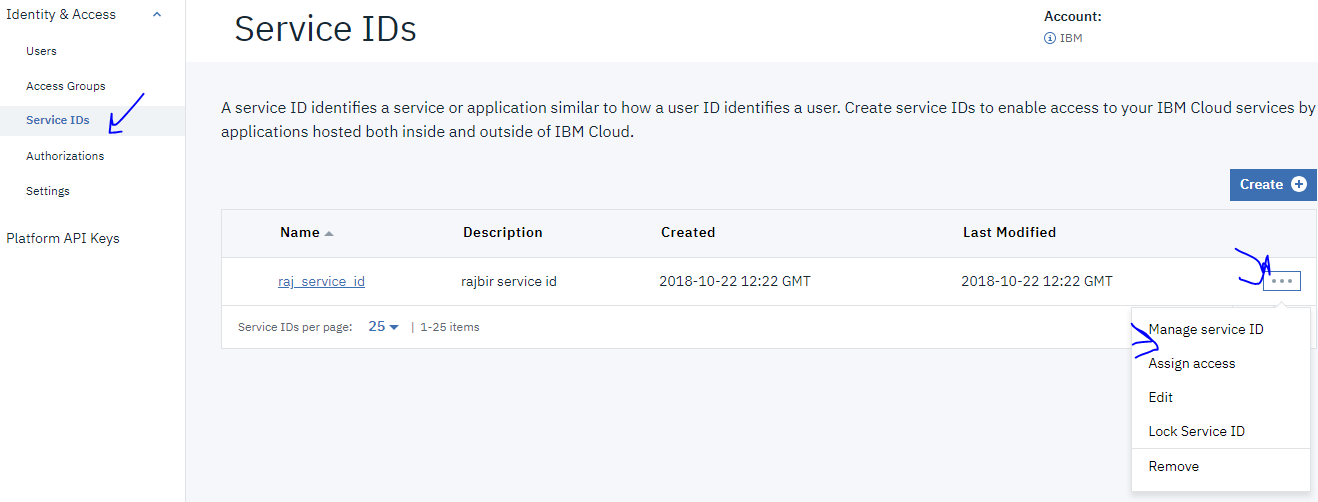
**Complete the following steps to retrieve an access token**:

1. **In the IBM Cloud console, go to Manage > Security > Identity and Access > Service IDs. Follow the process to**[**create a service ID**](https://console.bluemix.net/docs/iam/serviceid.html#creating-a-service-id)**.**

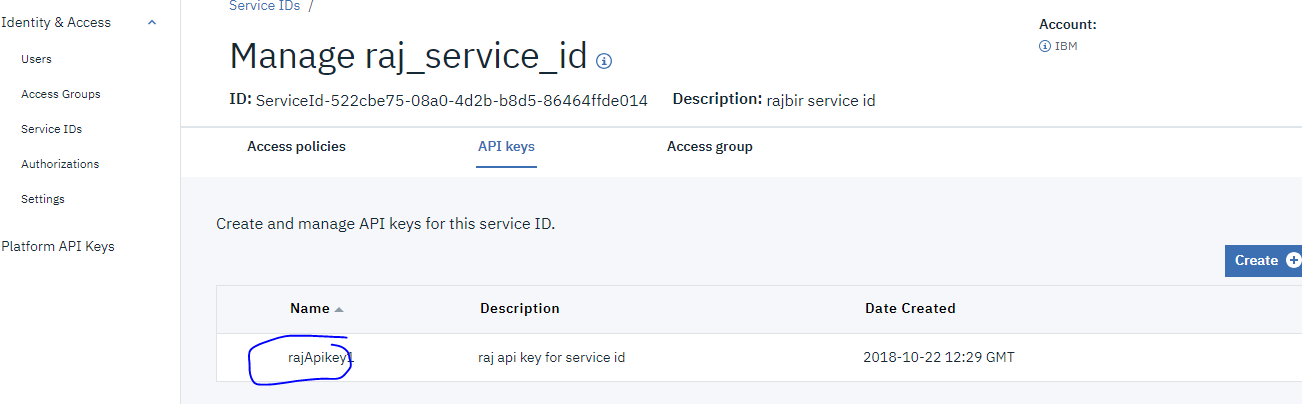




1. **Use the Actions menu to**[**define an access policy for your new service ID**](https://console.bluemix.net/docs/iam/serviceidaccess.html).



1. **Use the API keys section to**[**create an API key to associate with the service ID**](https://console.bluemix.net/docs/iam/serviceid_keys.html#serviceidapikeys)**. Save your API key by downloading it to a secure location**.



1. **Call the Cloud Identity and Access Management API to retrieve your access token.**

curl -X POST \

"https://iam.bluemix.net/identity/token" \

-H "Content-Type: application/x-www-form-urlencoded" \

-H "Accept: application/json" \

-d "grant\_type=urn%3Aibm%3Aparams%3Aoauth%3Agrant-type%3Aapikey&apikey=<API\_KEY>" \

In the request, replace <API\_KEY> with the API key that you created in step 3. The following truncated example shows the token output:

rajbir\_sood@PTL06625 MINGW64 /c/sandbox/devops\_docs (master)

$ curl -X POST \

> "https://iam.bluemix.net/identity/token" \

> -H "Content-Type: application/x-www-form-urlencoded" \

> -H "Accept: application/json" \

> -d "grant\_type=urn%3Aibm%3Aparams%3Aoauth%3Agrant-type%3Aapikey&apikey=Si6gePHdIWRHEV2wD03LBCnzdwXFwJYk3MU15OmUAk" \

>

% Total % Received % Xferd Average Speed Time Time Time Current

Dload Upload Total Spent Left Speed

100 2316 100 2205 100 111 1308 65 0:00:01 0:00:01 --:--:-- 1457{"access\_token":"eyJraWQiOiIyMDE3MTAzMC0wMDowMDowMCIsImFsZyI6IlJTMjU2In0..ah336ZLUrDXBiH1T2BL7c6T3ps3eAfgVKH\_k3YTLRnvTDMaxsuZ7ZA7N2BpUNENlR84tLco8kSfDydnE8bpuNosg3QpmPgRyfS7wqlxtkWqGnNIo7bBxsy2R1owB4g1Q6AvfDiOklpvenefTa7JPO4LYmaEYRi0IV4xfIxcFrAKVUUdhS314-acHMAztU1EvPnj0Vyz0ejoqqVsfnjlmbbmvYom4vd59wUw7E3bh3jOH3jnmYIChaY47hMbe92sxNGjzuRpIAb95M6789gUo8bDUEUpVnrbVi8dvWfvSKBgU6TgOPsoH\_42-qLOhPk7kh09DH9E38mTnkBcq0w2-DA","refresh\_token":"J1DBhIH\_O9xqsP3QvFfvLLggOE2uG7PRckyzc6yMv6ICryFjynqV5kih6fnzB8Z7VSZ8NjNgtyHYPEHv7BAIWX6lHL-X4Uo46TCMSrlYwDGBNG3vhtTSlqZLmQUq\_Z9sETEHx70R-tybI6bJwNQNfAZwpIRcALsMFskxCQm2DrurAOUV1Hh1O-08bbf8zaFffAJZa-dvQsRvNhF3lPqhup-DVAUAtKiEG7gPSymdLUtbnG9-fucUQVo5j1Ih9s4iwfqWWifWfI45mvWIY5bpuJsonqZzK3\_xe1Hx6g3gCwS8cddlY3HzL-W8amWQVK1DSp02a-l9c\_plR\_Cn6fC7GRyDDiJtGj6tBbY9TdC9zqUTpqhVVhgxNmvPUNkL9iaBzGS109hL2tCzkSjvjCS0GmujbSiki3tbewiGQVGKtQ-0N4Co5dApCw82ZE-4Y0clQ\_-BcIuPFBKdS1kIxQn5iBLHTi4Ub95towiSPOGg4h-\_8j5887QWcQTLobTjQQyJ70GWyrETfQkNoUXhhfXSRyRRIasJtLDnxds8gVnv1Dos5n4wN-5Uy1XhVENq\_469Wp2utTqBXVOULUx6-2ySTuuWN8XyDyN2ut5HWt4agfCvRpTjG9x\_3hZAFu2cAZKrYuaJXguHrd6V2tHxdqRjSgcadaRciBC-074qRy9VswU-FkhkLkXwpbykP6-QDzCvvPnqqt0LR4ffe-jhjwTQNGqc\_oMUvQGIX3osLCfo8Hl1ZiPV6st6nP1oaTEXfczza6C\_tNY6pNkveWGDtb3ib-vvPZPkM2IP\_nbZazpt0MrHjxbDs2DV4aCQBwJh1H15Rzqb709e2oXggpdtTCoLkrCze7TEKtVf7-XHs9IbKxONxNZdknK1BKUr0rQDtZShaVs4mhsx4ghoYmfsS2-qvdsZSPKpvOi5Z8BdOmuhO2pyWbwoPDRHinJ2q9lTFZ8cgHZnTQcRnu53EpOYv2Mvc6r7","token\_type":"Bearer","expires\_in":3600,"expiration":1540215439,"scope":"ibm openid"}

Example as above json format

{

"access\_token": "eyJraWQiOiIyM...",

"expiration": 1512161390,

"expires\_in": 3600,

"refresh\_token": "...",

"token\_type": "Bearer"

}

**NOTE: Access tokens are valid for 1 hour, but you can regenerate them as needed. To maintain access to the service, refresh the access token for your API key on a regular basis by calling the Cloud Identity and Access Management API.**

**Key protect geo location**

[**https://console.bluemix.net/docs/services/key-protect/regions.html#regions**](https://console.bluemix.net/docs/services/key-protect/regions.html#regions)

## **Retrieving your instance ID**

rajbir\_sood@PTL06625 MINGW64 /c/sandbox/devops\_docs (master)

$ **ibmcloud resource service-instances**

Retrieving service instances in resource group Default and all location under account IBM as rajbsood@in.ibm.com...

OK

Name Location State Type Tags

Continuous Delivery us-south active service\_instance

Key Protect-raj eu-gb active service\_instance

rajbir\_sood@PTL06625 MINGW64 /c/sandbox/devops\_docs (master)

$ **ibmcloud resource service-instance "Key Protect-raj" --id**

crn:v1:bluemix:public:kms:eu-gb:a/90488ffecf50473ba57279d415e24aef:0cb9bd07-e60d-42ae-a761-bf11c40c7174:: 0cb9bd07-e60d-42ae-a761-bf11c40c7174

rajbir\_sood@PTL06625 MINGW64 /c/sandbox/devops\_docs (master)

**The 0cb9bd07-e60d-42ae-a761-bf11c40c7174 value is an example instance ID.**

## **Forming your API request**

When you make an API call to the service, structure your API request according to how you initially provisioned your instance of Key Protect.

To build your request, pair a [regional service endpoint](https://console.bluemix.net/docs/services/key-protect/regions.html) with the appropriate authentication credentials. For example, if you created a service instance for the us-south region, use the following endpoint and API headers to browse keys in your service:

curl -X GET \

https://keyprotect.us-south.bluemix.net/api/v2/keys \

-H 'accept: application/vnd.ibm.collection+json' \

-H 'authorization: Bearer <access\_token>' \

-H 'bluemix-instance: <instance\_ID>' \

[**https://console.bluemix.net/apidocs/key-protect**](https://console.bluemix.net/apidocs/key-protect)

**api docs**

curl -X GET \

https://keyprotect.eu-gb.bluemix.net/api/v2/keys \

-H 'accept: application/vnd.ibm.collection+json' \

-H 'authorization: Bearer eyJraWQiOiIyMDE3MTAzMC0wMDowMDowMCIsImFsZyI6IlJTMjU2In0..Ng9JNIsgQelptxm7yjP11JiuwUHGNjdN93yw6WwHCyEr3TAGybTI\_qVAOP4efCyR\_I8QqegtPD7rUpSqpOtY8-xtpXVZJYiJWKte1rT9UkrPcpptV1k4RW9q0Q\_MGfipFto0yZmY6R0A1oOuUwFrjDE3xZAvuBEnMDGv1HdIzdxC0HIiKjRry7Bytm-PbzM7v1k7FPUAKFNM298rJvL0MXWoHII14C2l07Zvk-nWOwsMm2Z3inlw4hdvuTHZOG9YAqBFGxr7KsPvkG1QiIBTxAv9FqBXMcx6MpA1Z\_O6-\_DYtMHhZFofeb5LhOF83cuhCw-O2rE\_vbpuRQ0OAISxhA' \

-H 'bluemix-instance: 0cb9bd07-e60d-42ae-a761-bf11c40c7174' \

## **Viewing keys with the API**

[**https://console.bluemix.net/docs/services/key-protect/view-keys.html#view-keys**](https://console.bluemix.net/docs/services/key-protect/view-keys.html#view-keys)

You can retrieve the contents of your keys by using the Key Protect API.

### Retrieving a list of your keys

For a high-level view, you can browse keys that are managed in your provisioned instance of Key Protect by making a GET call to the following endpoint.

https://keyprotect.<region>.bluemix.net/api/v2/keys

Run the following cURL command to view general characteristics about your keys.

curl -X GET \

https://keyprotect.<region>.bluemix.net/api/v2/keys \

-H 'accept: application/vnd.ibm.collection+json' \

-H 'authorization: Bearer <IAM\_token>' \

-H 'bluemix-instance: <instance\_ID>' \

-H 'correlation-id: <correlation\_ID>' \

rajbir\_sood@PTL06625 MINGW64 /c/sandbox/devops\_docs (master)

$ curl -X POST \

> 'https://keyprotect.eu-gb.bluemix.net/api/v2/keys/b8ac229d-6655-4465-925d-4813305055ae?action=wrap' \

> -H 'accept: application/vnd.ibm.kms.key\_action+json' \

> -H 'authorization: Bearer eyJraWQiOiIyMDE3MTAzMC0wMDowMDowMCIsImFsZyI6IlJTMjU2In0..EmDdKujuFT5HM1HCsh-EGbSA6dW9\_9OZIcnLVO-SmTcmnpeCTgApNtbug6HN0jw0gcOqa6ruIi\_D3dOKP5kszqICaSj-\_LR9kWtAS1xqOE1lpA9hptZ6jg1342pzajWA4-ZkZmp1kFM4NicmOuJEeWY5rG2cAvZfmfgFoZK7FYcSkUB7aIEfxeyMLGCrAksn0Pp8jH7E4H9hiHNQYWbhTyYlk4QgYtf7LkgpbEqFt\_NFtYviHDCdc4m\_OMKBXPKb1-LXNIS0XIfClvnZ5XsTz03li4uR5Jaf\_xLEiNj71Qfay0wZ-ut4Pkng3c5GSSIfdM-AjDv7JKaf5-aOnoQANQ' \

> -H 'bluemix-instance: 0cb9bd07-e60d-42ae-a761-bf11c40c7174' \

> -H 'content-type: application/vnd.ibm.kms.key\_action+json' \

> -H 'correlation-id:' \

> -H 'prefer: return=representation' \

> -d '{

> "plaintext": "dGhpcyBpcyB0ZXN0IGV4YW1wbGUgdG8gdXNlIHdyYXAga2V5cyB0byBlbmNyeXB0IGRhdGE=",

> "aad": ["<additional\_data>", "<additional\_data>"]

> }' \

>

% Total % Received % Xferd Average Speed Time Time Time Current

Dload Upload Total Spent Left Speed

100 707 100 558 100 149 337 90 0:00:01 0:00:01 --:--:-- 388{"plaintext":"this is test example to use wrap keys to encrypt data","ciphertext":"eyJjaXBoZXJ0ZXh0IjoiNEhtV04yWFM2ZGx0czlxYUhzaEZZOGlKQXk3UW02ODJNRC9tSEtxZWlvZDIyMnRSaHo1ZlNrMlVWZHRLYnQzSFRxb1A2aU56YUJSR0tIL1R6VDhFdEQ0PSIsImhhc2giOiI1c2tndGFnUm0vcnJpcW83QVUwdHlpTkNPSFZBUWF0UGRRMU50dXg5N3NKcWJ3dENHaG0zSXFyRUN1R3JEdDQxWjYwQTFFOTljdUFFVktDTUtjOWt5UT09IiwiaXYiOiJ3WGVTRUhCSGxDUWZPT3RjRERycWVRPT0iLCJ2ZXJzaW9uIjoiMi4wLjAiLCJoYW5kbGUiOiJiOGFjMjI5ZC02NjU1LTQ0NjUtOTI1ZC00ODEzMzA1MDU1YWUifQ==","aad":["\u003cadditional\_data\u003e","\u003cadditional\_data\u003e"]}

# Integrating with IBM Cloud Object Storage

**https://console.bluemix.net/docs/services/key-protect/integrations/integrate-cos.html#integrate-cos**

Your wrapped key, containing the base64 encoded key material, is returned in the response entity-body. The following JSON object shows an example returned value.

{

"plaintext": "VGhpcyBpcyBhIHNlY3JldCBtZXNzYWdlLg==",

"ciphertext": "eyJjaXBoZXJ0ZXh0Ijoic3VLSDNRcmdEZjdOZUw4Rkc4L2FKYjFPTWcyd3A2eDFvZlA4MEc0Z1B2RmNrV2g3cUlidHphYXU0eHpKWWoxZyIsImhhc2giOiJiMmUyODdkZDBhZTAwZGZlY2Q3OGJmMDUxYmNmZGEyNWJkNGUzMjBkYjBhN2FjNzVhMWYzZmNkMDZlMjAzZWYxNWM5MTY4N2JhODg2ZWRjZGE2YWVlMzFjYzk2MjNkNjA5YTRkZWNkN2E5Y2U3ZDc5ZTRhZGY1MWUyNWFhYWM5MjhhNzg3NmZjYjM2NDFjNTQzMTZjMjMwOGY2MThlZGM2OTE3MjAyYjA5YTdjMjA2YzkxNTBhOTk1NmUxYzcxMTZhYjZmNmQyYTQ4MzZiZTM0NTk0Y2IwNzJmY2RmYTk2ZSJ9"

"aad": ["data1", "data2"]

}

## **Unwrapping keys by using the API**

You can unwrap a data encryption key (DEK) to access its contents by using the IBM® Key Protect for IBM Cloud API, if you are a privileged user. Unwrapping a DEK decrypts and checks the integrity of its contents, returning the original key material to your IBM Cloud data service.

1. Copy the ID of the root key that you used to perform the initial wrap request.

You can retrieve the ID for a key by making a GET /v2/keys request, or by viewing your keys in the Key Protect GUI.

1. Copy the ciphertext value that was returned during the initial wrap request.
2. Run the following cURL command to decrypt and authenticate the key material.

curl -X POST \

'https://keyprotect.<region>.bluemix.net/api/v2/keys/<key\_ID>?action=unwrap' \

-H 'accept: application/vnd.ibm.kms.key\_action+json' \

-H 'authorization: Bearer <IAM\_token>' \

-H 'bluemix-instance: <instance\_ID>' \

-H 'content-type: application/vnd.ibm.kms.key\_action+json' \

-H 'correlation-id: <correlation\_ID>' \

-H 'prefer: <return\_preference>' \

-d '{

"ciphertext": "<encrypted\_data\_key>",

"aad": ["<additional\_data>", "<additional\_data>"]

}'

rajbir\_sood@PTL06625 MINGW64 /c/sandbox/devops\_docs (master)

$ curl -X POST 'https://keyprotect.eu-gb.bluemix.net/api/v2/keys/b8ac229d-6655-4465-925d-4813305055ae?action=unwrap' -H 'accept: application/vnd.ibm.kms.key\_action+json' -H 'authorization: Bearer eyJraWQiOiIyMDE3MTAzMC0wMDowMDowMCIsImFsZyI6IlJTMjU2In0..EmDdKujuFT5HM1HCsh-EGbSA6dW9\_9OZIcnLVO-SmTcmnpeCTgApNtbug6HN0jw0gcOqa6ruIi\_D3dOKP5kszqICaSj-\_LR9kWtAS1xqOE1lpA9hptZ6jg1342pzajWA4-ZkZmp1kFM4NicmOuJEeWY5rG2cAvZfmfgFoZK7FYcSkUB7aIEfxeyMLGCrAksn0Pp8jH7E4H9hiHNQYWbhTyYlk4QgYtf7LkgpbEqFt\_NFtYviHDCdc4m\_OMKBXPKb1-LXNIS0XIfClvnZ5XsTz03li4uR5Jaf\_xLEiNj71Qfay0wZ-ut4Pkng3c5GSSIfdM-AjDv7JKaf5-aOnoQANQ' -H 'bluemix-instance: 0cb9bd07-e60d-42ae-a761-bf11c40c7174' -H 'content-type: application/vnd.ibm.kms.key\_action+json' -H 'correlation-id:' -H 'prefer: return=representation' -d '{

"ciphertext": "eyJjaXBoZXJ0ZXh0IjoiNEhtV04yWFM2ZGx0czlxYUhzaEZZOGlKQXk3UW02ODJNRC9tSEtxZWlvZDIyMnRSaHo1ZlNrMlVWZHRLYnQzSFRxb1A2aU56YUJSR0tIL1R6VDhFdEQ0PSIsImhhc2giOiI1c2tndGFnUm0vcnJpcW83QVUwdHlpTkNPSFZBUWF0UGRRMU50dXg5N3NKcWJ3dENHaG0zSXFyRUN1R3JEdDQxWjYwQTFFOTljdUFFVktDTUtjOWt5UT09IiwiaXYiOiJ3WGVTRUhCSGxDUWZPT3RjRERycWVRPT0iLCJ2ZXJzaW9uIjoiMi4wLjAiLCJoYW5kbGUiOiJiOGFjMjI5ZC02NjU1LTQ0NjUtOTI1ZC00ODEzMzA1MDU1YWUifQ==",

"aad": ["<additional\_data>", "<additional\_data>"]

}'

% Total % Received % Xferd Average Speed Time Time Time Current

Dload Upload Total Spent Left Speed

100 571 100 89 100 482 57 312 0:00:01 0:00:01 --:--:-- 359{"plaintext":"dGhpcyBpcyB0ZXN0IGV4YW1wbGUgdG8gdXNlIHdyYXAga2V5cyB0byBlbmNyeXB0IGRhdGE="}

# Managing user access

[**https://console.bluemix.net/docs/services/key-protect/manage-access.html#manage-access**](https://console.bluemix.net/docs/services/key-protect/manage-access.html#manage-access)

**SAMPLE APP**

[**https://github.com/IBM-Cloud/key-protect-helloworld-python**](https://github.com/IBM-Cloud/key-protect-helloworld-python)

cf login -a https://api.ng.bluemix.net -u apikey -p ThisValueIsYourAPIKey

**https://console.bluemix.net/docs/cli/reference/ibmcloud/cf\_index.html#cf**

**login using powershell only**

To log in by using the Cloud Foundry CLI, specify apikey as the user name and the API key string as the password:

1. cf login
2. API endpoint: https://api.ng.bluemix.net
3. Email> apikey
4. Password>
5. Authenticating...
6. OK

Above NOT working.

PS C:\Users\rajbir\_sood> cf login --sso

API endpoint: https://api.eu-gb.bluemix.net

One Time Code (Get one at https://login.eu-gb.bluemix.net/UAALoginServerWAR/passcode)>

Authenticating...

OK

Targeted org rajbsood@in.ibm.com

Targeted space dev