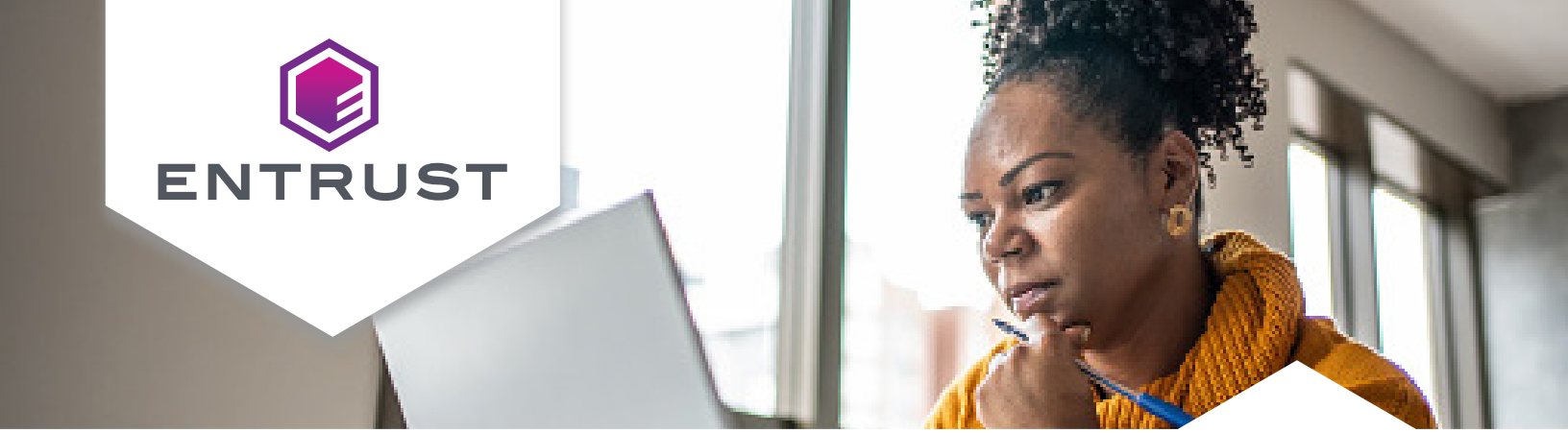


Entrust KeyControl Cryptographic API

Cloud-friendly REST-like interface for cryptographic operations for use with KeyControl Vault deployments

The Entrust KeyControl Cryptographic API provides a RESTlike API between applications requiring cryptographic key and data protection services and a FIPS-certified key management system (KMS). The Cryptographic API RESTful attributes include:

- Well-defined URIs that uniquely identify “resources” e.g., / keys / sign / verify etc.
- HTTP methods as verbs to perform actions on that resource e.g., GET for read operations such as listing keys, POST for write operations such as creating keys, DELETE for delete operations such as deleting keys.

The Entrust KeyControl solution performs a variety of cryptographic functions including key management, encryption, decryption, signing, and verification. These core functions are now available to applications through a simple web-service interface utilizing the universal HTTPS protocol.

HIGHLIGHTS

- Key management, signing, and encryption and random number generation services
- Access to high-security data protection solution from cloud, data center, or on-premises applications
- Enables fast and scalable dynamic application deployment
- Flexible OS and architecture support
- Optional hardware key protection using FIPS 140-2 certified hardware security modules (HSMs) or HSM cloud services

Learn more about the Entrust KeyControl Cryptographic API at entrust.com

Entrust KeyControl Cryptographic API

KEY FEATURES & BENEFITS

- **Efficient access to remote cryptographic services from the cloud, data center, or on-premises applications**
  Applications that reside anywhere, whether in the cloud, in remote data centers, or locally, can access KeyControl services through HTTPS-based web service calls via the REST-like API, bringing greater flexibility to today's varied computing environments.

- **Streamlined development process**
  The efficient, modern Cryptographic API improves the speed with which applications can be developed to access Entrust KeyControl cryptographic services.

- **Single user-friendly console with comprehensive administrative role separation.**
  The Cryptographic API offers an administration WebUI designed to support security principles such as separation of duties and least privilege principles. It also features multi-tenancy capabilities and provides granular access control over the keys.

- **No need for client-side integration**
  By using the web services REST-like API, developers benefit from reduced deployment complexity.

- **Centralized or decentralized key management**
  As a component of the KeyControl platform, the Cryptographic API utilizes the KeyControl Vault for centralized or decentralized key management, with up to FIPS 140-2 Level 3 key security.

- **Flexible OS and architecture support**
  The REST-like interface of the Cryptographic API is independent of client application infrastructure and requires no OS specific software local to the application, thus simplifying integration, particularly in custom environments.

- **Dynamic scalability**
  Spin up new or additional application workloads without requiring further configuration, support software installation; adjust your capacity up or down to meet demand easily including vault nodes.

- **Support load balancing using dedicated COTS appliances**
  The Cryptographic API allows the KMS workload to be managed using commercial off-the-shelf (COTS) load balancers ensuring the best utilization of a pool of KeyControl Vaults.

Getting started with Entrust KeyControl Cryptographic API

You will need:

- A KeyControl Vault for Application Security with at least one key pack
- [Optionally] An nShield HSM, or a cloud HSM sevice subscription

To use the REST-like API, the nShield WSOP is installed on an nShield client server, activating the service and making it available for direct and immediate connections from applications.

Learn more about the Entrust KeyControl Cryptographic API at entrust.com

Entrust KeyControl Cryptographic API

EXAMPLES OF CRYPTOGRAPHIC API REQUESTS

Creation of an AES 256 key

```
$ curl --request POST \
         --url https://sedemo.yourcorp.com/token/1.0/key/ \
         --header 'Content-Type: application/json' \
         --header 'x-token-auth:[…] ' \
         --data '{
 "cipher": "AES-256",
"description": "Production key for application app1",
"keyset_guid": "6df6ac54-f739-498f-a7c4-aeaec51a6837",
"name": "key_aes256_prod_app3"
}'
Response sample:
{
         "keyguid": "35c741c8-56fc-406a-a78d-034381aa2309",
         "result": "success"
}
```

Tokenization of a credit card number

```
$ curl --request POST \
         --url https://sedemo.yourcorp.com/token/1.0/token/ \
         --header 'Content-Type: application/json' \
         --header 'x-token-auth:[…] ' \
         --data '{
"policyName": "credicard_pol_01",
"tokenData": "1234-1234-1234-1238"
}'
Response sample:
{
         "keyGuid": "9e70dfc1-f41a-47cd-a21f-21ba2ec4dca2",
         "value": "1234-4263-8713-0431"
}
```

Key rotation

```
$ curl --request POST \
         --url https://sedemo.yourcorp.com/token/1.0 key/
              53ab4254 -9cbd-4e2c-abe4-e8ae6e09735e/rotate/ \
         --header 'Content-Type: application/json' \
         --header 'x-token-auth:[…] '
Response sample:
{
         "result": "success"?
         "newkeyguid": "ccb6fe81-e458-43fb-b3e4-
                       09a5659581043
}
}
```

Signature of data using RSA

```
$ curl --request POST \
         --url https://sedemo.yourcorp.com/token/1.0/sign/ \
         --header 'Content-Type: application/json' \
         --header 'x-token-auth:[…] ' \
         --data '{
"keyGuid": "99dc2344-50cd-4910-89db-1566fb88b579",
"data": "SGVsbG8sIFdvcmxkIQ==",
"mode": "RSA_SHA256"}'
Response sample:
{
         "signature": "[…]"
}
```

Learn more about the Entrust KeyControl Cryptographic API at entrust.com

Entrust KeyControl Cryptographic API

TECHNICAL SPECIFICATIONS

Supported symmetric algorithms:

- DES, DES3/TDEA
- AES128, AES192, AES256
- SEED128
- ARIA128, ARIA192, ARIA256

Supported asymmetric algorithms:

- RSA1024, RSA2048, RSA3072, RSA4096
- Secp256k1
- Nistp256r1, Nistp348r1, Nistp521r1

Supported signing algorithms:

- RSA, RSASSA-PKCS1-v1_5, RSASSA-PSS
- ECDSA

Supported tokenization methods:

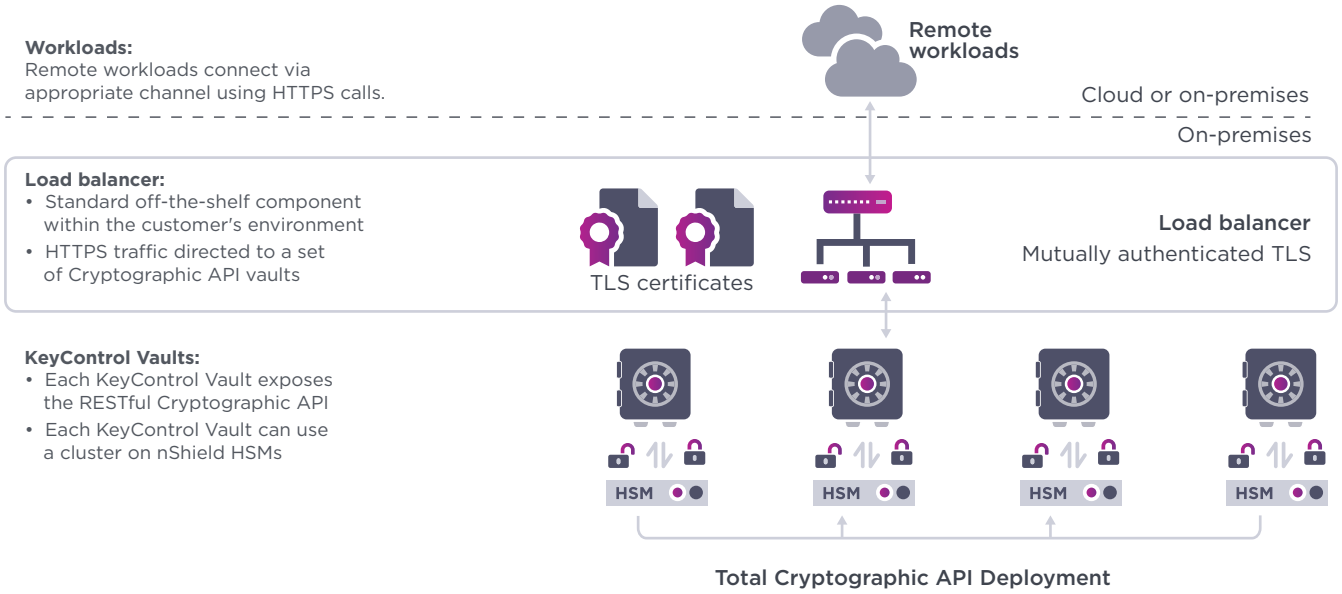
- Format Preserving Encryption
- Partial tokenization
- Dynamic data masking

Supported hashing algorithms:

- HMAC MD5
- HMAC SHA1, HMAC SHA224, HMAC SHA256, HMAC
- SHA384, HMAC SHA512
- HMAC128, HMAC192, HMAC256
- AES-CMAC128, AES-CMAC192, AES-CMAC256

Supported wrapping algorithms:

- RSA_OAEP_SHA1, RSA_OAEP_SHA256, RSA_OAEP_SHA384, 'RSA_OAEP_SHA512

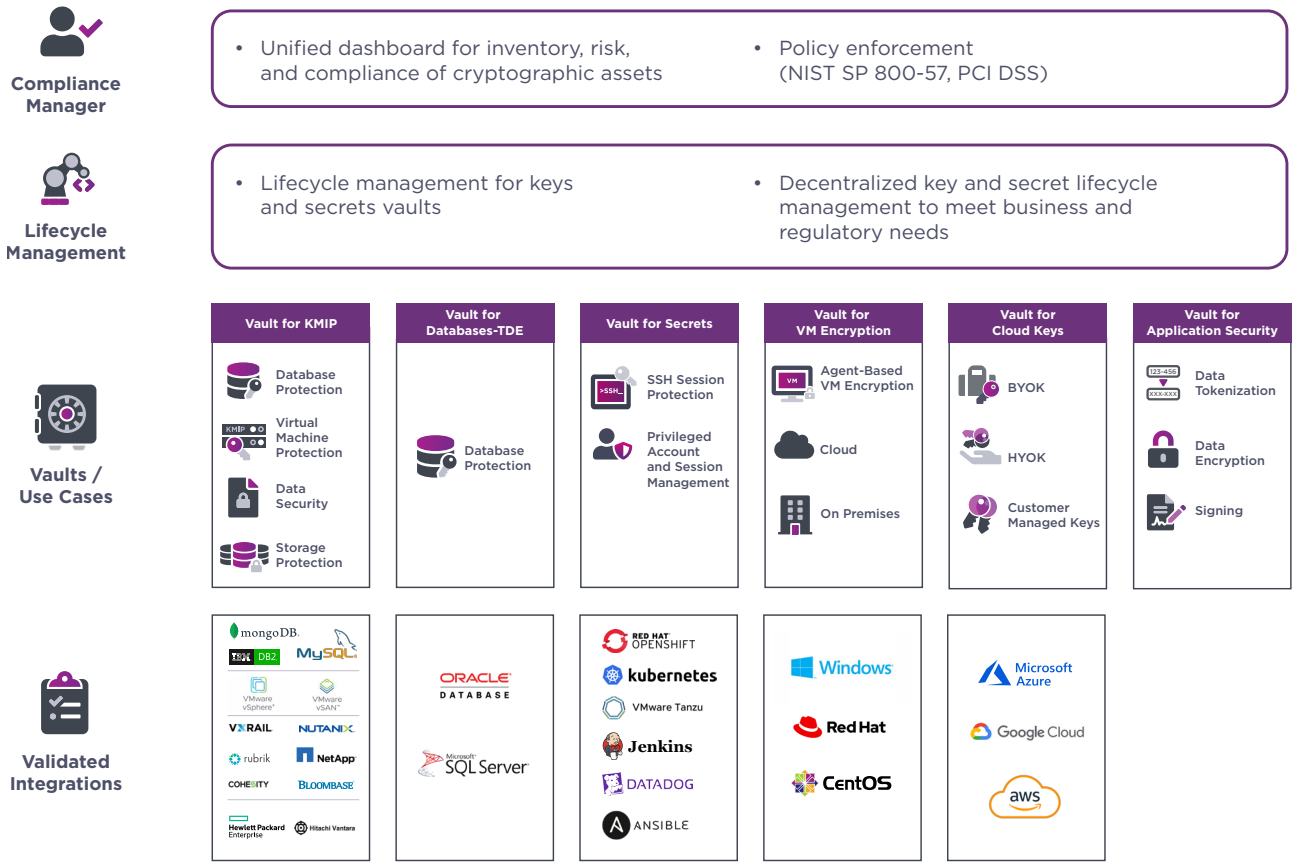


Learn more about the Entrust KeyControl Cryptographic API at entrust.com

Entrust KeyControl Cryptographic API

Entrust KeyControl Platform

Entrust KeyControl Cryptographic API is part of a suite of products designed to manage key lifecycles at scale for encrypted workloads in virtualized environments across on-premises, multicloud, and hybrid deployments.



Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223