



Entrust KeyControl Cryptographic Command Line Interface (Crypto CLI)

Devops-friendly command line tool for cryptographic operations for use with KeyControl Vault deployments

The Entrust KeyControl Cryptographic CLI is a specialized command-line tool designed for executing cryptographic operations using the KeyControl key management solution. This tool streamlines various cryptographic tasks, enabling users to efficiently manage cryptographic keys and encrypt and sign data, as well as hash data. The Cryptographic CLI supports a broad spectrum of cryptographic algorithms, making it a versatile choice for various security applications.

Highlights

- **Versatility in Cryptographic Operations**
Beyond basic key management, the Cryptographic CLI can handle a wide range of cryptographic tasks, adapting to the diverse needs of different security environments.
- **User-Friendly Command-Line Interface**
The command-line interface of the Cryptographic CLI is particularly beneficial for administrators who prefer or require a command-line approach for managing cryptographic operations. This can be due to the need for automation, scripting capabilities, or simply a preference for a command-line environment.

Key features & benefits

- **Integration with KeyControl**
As a component of the KeyControl solution, the Cryptographic CLI is tailored to work seamlessly within this environment, leveraging its security and cryptographic features.
- **Platform-Agnostic Design**
The Cryptographic CLI is versatile and can operate seamlessly across various operating systems, including Windows, Linux, and macOS.
- **Support for Multiple Cryptographic Algorithms**
The Cryptographic CLI handles a wide array of cryptographic algorithms, catering to diverse security requirements or use cases.
- **User and Access Policy Management**
It allows for the administration of user access and security policies, ensuring that only authorized personnel can access certain cryptographic functions or keys.
- **KeyControl can be deployed on premises, as a service, or as a hybrid solution.**
- **Scalable to manage tens of millions of keys**
As organizations scale they need to manage increasing numbers of keys and secrets.



Examples of Cryptographic CLI commands

Creation of an AES 256 key

```
$ ./cryptocli create-key -c AES-256 -d "Production key for application app1" -n "key_aes256_prod_app1" -k 6df6ac54-f739-498f-a7c4-aeaec51a6837
{
  "keyguid": "35c741c8-56fc-406a-a78d-034381aa2309",
  "result": "success"
}
```

Symmetric encryption of data using AES GCM

```
$ ./cryptocli encrypt -k 35c741c8-56fc-406a-a78d-034381aa2309 -i a3e2b0a45dd2aeb658252c18c37747fd -m AES_GCM -d SGVsbG8sIFdvcmxkIQ==
{
  "data": "SOeds64owtmWyR58JjTD9NXaeMPGYUMg+2rFLps="
}
```

Rotation of a key

```
$ ./cryptocli rotate-key -k 6df6ac54-f739-498f-a7c4-aeaec51a6837
{
  "result": "success",
  "newkeyguid": "f89056db-53d3-4d9f-ba1f-e8c73db9c619"
}
```

Tokenization of a credit card number

```
$ ./cryptocli tokenize -n credicard_pol_02 -d 377511772089935 {
  "keyGuid": "9e70dfc1-f41a-47cd-a21f-21ba2ec4dca2",
  "value": "017206027424997"
}
```

Export of a key

```
$ ./cryptocli export-key -k 35c741c8-56fc-406a-a78d-034381aa2309 -p pubkey.pem
{
  "wrapped_key":
"Yr8CZL+xQ/mULgwR083HTL7e3odxx72peRp5XLkFhoQu1VV60Js/iDkPgE7PScr1K4wXyw1bfQ4/S1Q46wxCHAF3jMMz0mqqtPAWxfCH-qwWBapo1s9rHUDknRvC9FIKz7VCi1EQp5LGTFeYwHpG10C05Cg-j5L2JK5nijreVfTAh4Qy1bGmJ+S9KA/wog/Mx+y5DuNkKiRp//01p-gaxblT2CUx1WYvVhfEupJKsuSPttuecPKYCEIkIyNnkZamWpX9/CyZ1MFEPa2TBvMd4tYB3N+kEu6CDFmXqrMrozp1v8prPwJGawc0XnbocF-naWGFsw0nCc7Yd/KGbZKPamRg6hus75JvpIzE54D5PTrvRjJiRer7/AIaL-ImMHRnr9Dkfx48YFVj5zw=",
  "result": "success"
}
```

Signature of data using RSA 2048 and SHA 256

```
$ ./cryptocli sign -k 99dc2344-50cd-4910-89db-1566fb88b579 -m RSA_SHA256 -d SGVsbG8sIFdvcmxkIQ==
{
  "signature":
"gjAwWho8KHb9uzUZ5WE1Qx7K211F2qGGL/Jq4ny/1FJaW17pIIt-sL65kX5kk9xU6MCEgNWm8EPRRF+e2UKE0CQ5NdSJq0P0XDvYIKy7x-kqG/10BMLz5YHthqDUVd1YFH04bSd8aD0SrNpZsS30ZeYk1G04y6Y-FAOTCpvjWQr4l6aJIhLejhjA18UiFv0Mtf//b/bB0b/yZTyMsCHApQcn/00jp6uydK1YK9zbLDKQk/OJBjYE8HUtHSQ7Zt0GIgx4LP2MP40vth-GUTr6EeMXySopGpWh/Nk9ZDqtbU8+vrnz8bys/cmMplmV4ZpLyoeD02c-fYSKDYQyqljYwGr4Tw=="
}
```

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

Workloads:

The Cryptographic CLI is installed on workloads for secure connection to KeyControl vaults, utilizing KeyControl's REST API over HTTPS to ensure encrypted and secure communication.



Remote workloads

Cloud or on-premises

On-premises

Load balancer:

- Standard off-the-shelf component within the customer's environment
- HTTPS traffic directed to a set of Entrust KeyControl vaults



TLS certificates



Load balancer

Mutually authenticated TLS

KeyControl Vaults:

- Each KeyControl Vault exposes the RESTful Cryptographic API
- Each KeyControl Vault can use a cluster of nShield HSMs



Total Cryptographic CLI Deployment

Entrust KeyControl Platform

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

