DATA SHEET

Entrust Cryptographic Security Platform (CSP) Cryptographic Command Line Interface (Crypto CLI)

DevOps-Friendly Command Line Tool for Cryptographic Operations for Use With Entrust Key Management Vault Deployments

The Entrust Cryptographic Security Platform Cryptographic CLI is a specialized command-line tool designed for executing cryptographic operations using the platform's 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 and Benefits

Integration With the Entrust Platform

As a component of the Entrust platform 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.

Multiple Deployment Methods

The platform 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 SGVsbG8slFdvcmxklQ==
{
        "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

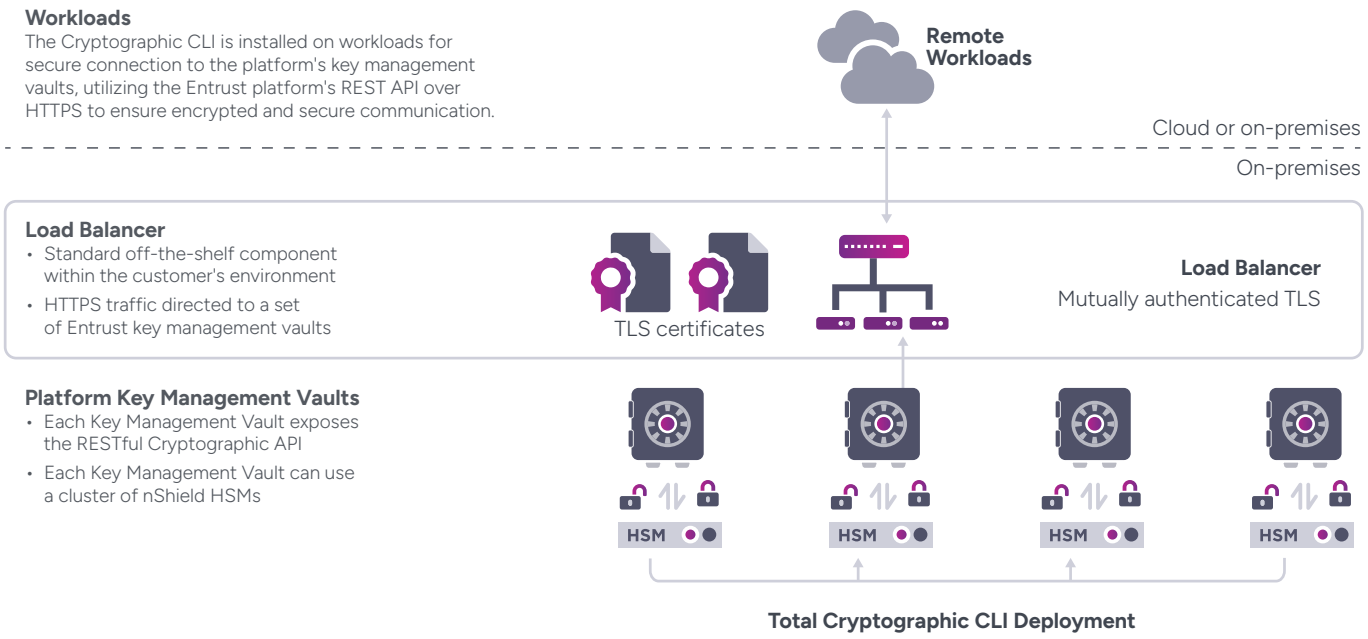
```
$ ./cryptocli export-key -k 35c741c8-56fc-406a-a78d-034381aa2309 -p pubkey.pem
{
        "wrapped_key": "Yr8CZL+xQ/mULgwR083HTL7e3odxx72peRp5XLkFhoQu1V-V60Js/iDkPgE7PScrlK4wXywlbfQ4/S1Q46wxCHAF3jMMz0mqqt-PAWxfcHqwWBapo1s9rHUDknRvC9FIKz7VCilEQp5LGTFevYwH-pGl0C05Cgj5L2JK5nijreVfTAh4QylbGmJ+S9KA/wog/Mx+y5DuNkkiRp//0lpgaxblT2CUx1WYvVhfEupJKsuSPttuecP-KYCEIklyNnkZamWpX9/CyZlMFEPa2TBvMd4tYB3N+kEu6CD-FmXqrMrozp1v8prPwJGaWc0XnbocFnaWGFSW0nCc7Yd/KGbZKPamRg6hus75JvplzE54D5PTrvRpJiRer7/AlaLlmMHrNr9D-kfx48YFVj5zw=",
        "result": "success"
}
```

Signature of Data using RSA 2048 and SHA 256

```
$ ./cryptocli sign -k 99dc2344-50cd-4910-89db-1566fb88b579 -m RSA_SHA256 -d SGVsbG8slFdvcmxklQ==
{
        "signature": "gjAwWho8KHb9uzUZ5WElQx7K21lF2qGGL/Jq4ny/1FJaWl7pIlt-sL65kX5kk9xU6MCEgNWm8EPRRF+e2UKEOCQ5NdSJq0P0X-DvYIKy7xkqG/l0BMLz5YHthqDUVd1YFHO4bSd8aDOSrNpZs-S3OZeYklG04y6YFAOTCpvjWQr4l6aJlhLcjhjA18Uifv0Mtf//b/bBOb/yZTyMsCHApQcn/O0jP6uydKlYK9zbLDKQk/OJBJYE-8HUtHSQ7Zt0Glgx4LfP2MP40vthGUTr6EeMXySopGpWh/Nk9ZDqtbU8+vrmZ8bys/cmMplmV4ZpLyoedO2cfYSKDYQyqljY-WGr4Tw=="
}
```


ENTRUST
SECURING A WORLD IN MOTION

How It Works



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:

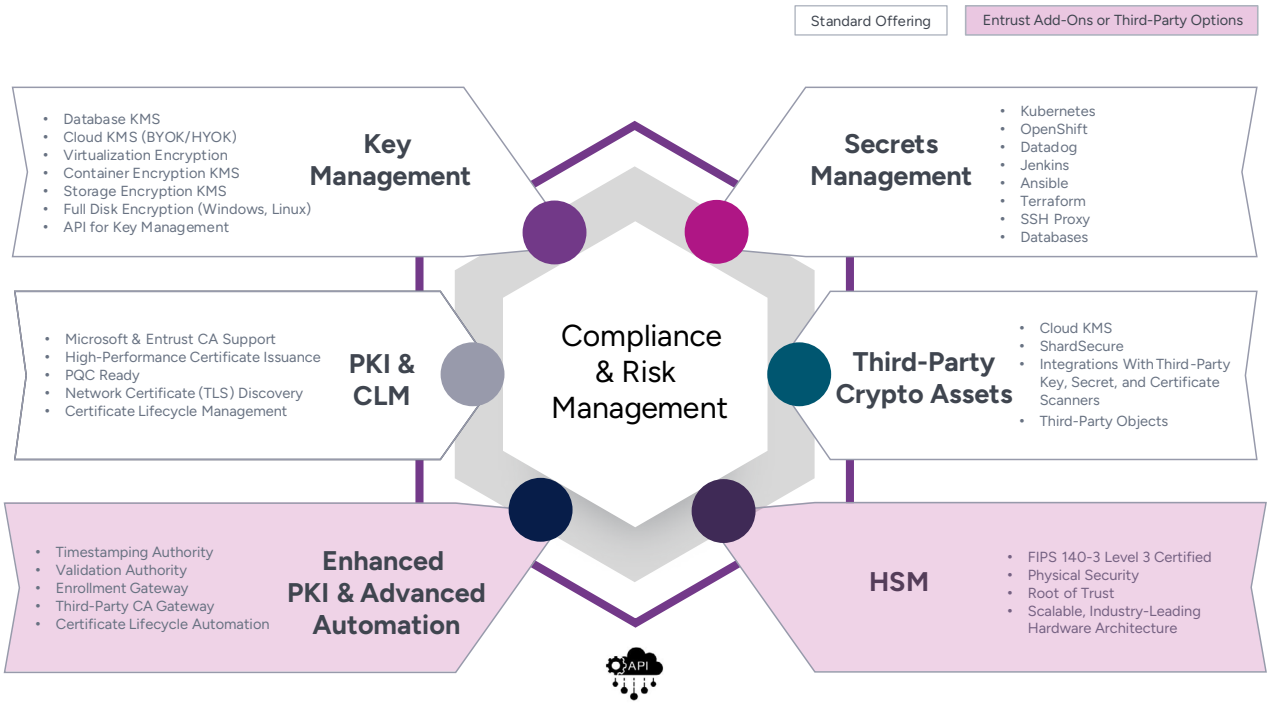
- RSA_OAEP_SHA1, RSA_OAEP_SHA256, RSA_OAEP_SHA384, RSA_OAEP_SHA512

ENTRUST
SECURING A WORLD IN MOTION

Entrust Cryptographic Security Platform

The Entrust Cryptographic Security Platform provides a comprehensive solution for discovering and managing the lifecycles of certificates, cryptographic keys, secrets, tokens, libraries, protocols, and configurations.

By centralizing cryptographic asset management, it enhances security, helps ensure compliance, and streamlines operations, enabling seamless integration across both on-premises and cloud environments.



entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION