DATA SHEET

Cryptographic Security Platform (CSP) Cryptographic API

Cloud-friendly REST-like interface for cryptographic operations for use with Entrust platform's Key Management Vault deployments

The Entrust Cryptographic Security Platform Cryptographic API provides a REST-like API between applications requiring cryptographic key and data protection services and a key management system (KMS). The Cryptographic API RESTful attributes include:

- Well-defined URIs that uniquely identify "resources" (e.g.,keys/sign/verify.)
- 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 platform 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 using the universal HTTPS protocol.

Highlights

- Key management, signing, 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 140-3 certified hardware security modules (HSMs) or HSM cloud services
- The Entrust platform can be deployed on premises, as a service, or as a hybrid solution
- Unlimited keys
- Scalable to manage tens of millions of keys

Key Features and 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 the platform's 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 platform 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 Entrust Cryptographic Security Platform, the Cryptographic API utilizes the platform for centralized or decentralized key management.

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 or support software installation, and adjust your capacity up or down to meet demand while 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 the platform's key management vaults.

Getting Started With Entrust Cryptographic Security Platform Cryptographic API

You will need:

- An Entrust platform key management vault for Application Security with at least one key pack
- [Optionally] An Entrust nShield® Hardware Security Module (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.

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"
}
```

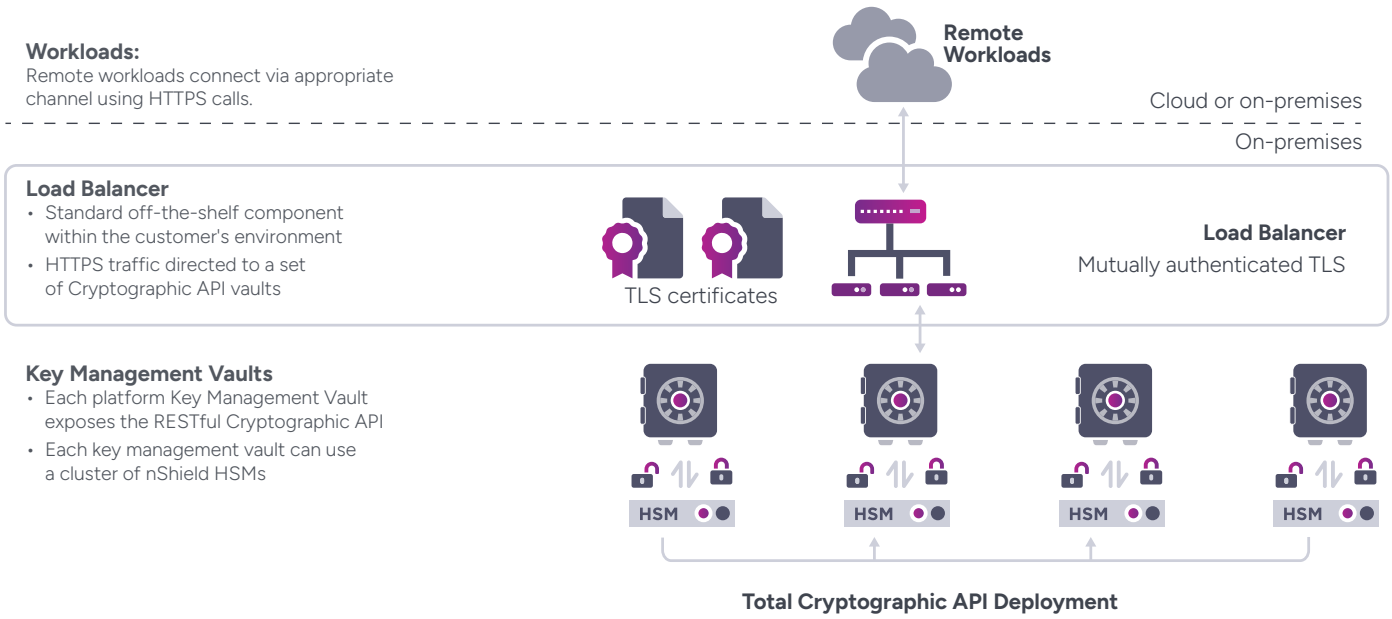
Key Rotation

```
$ 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": "[...]"
}
```

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:

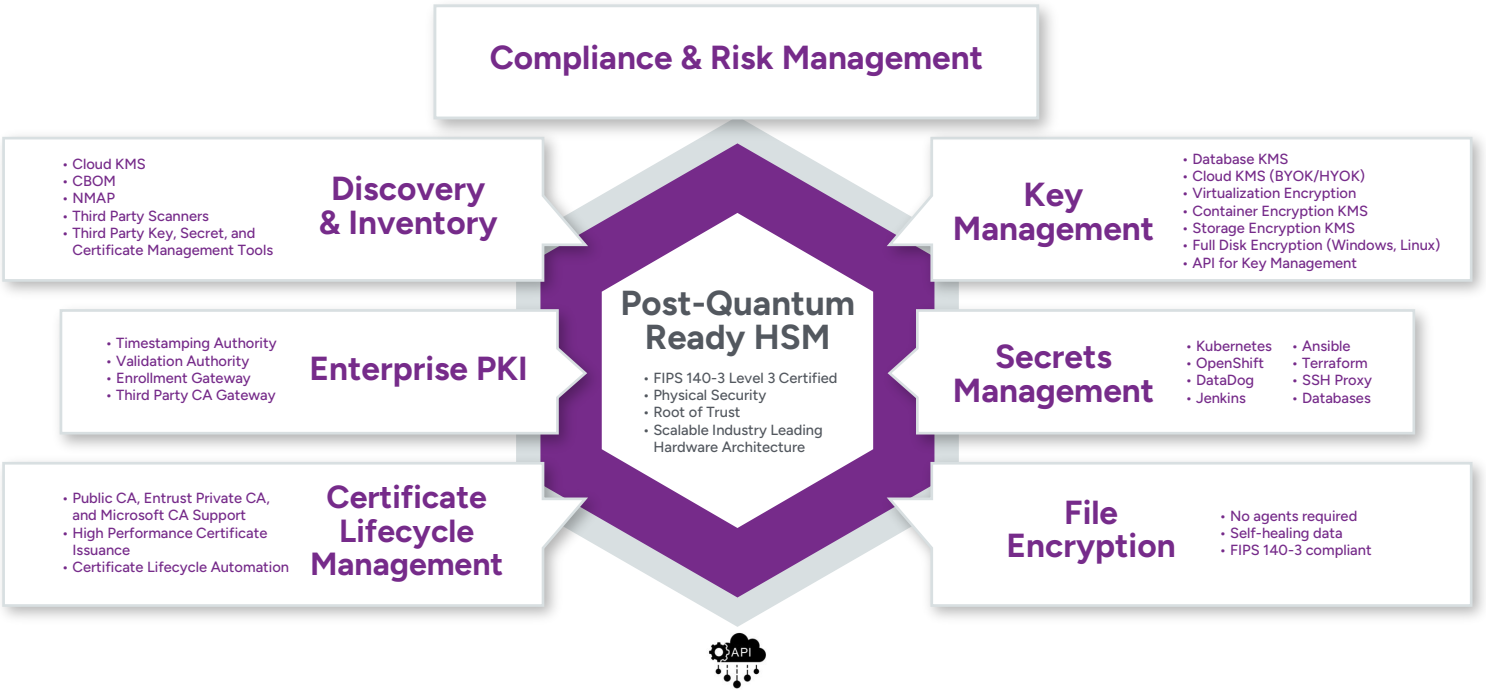
- RSA_OAEP_SHA1, RSA_OAEP_SHA256, RSA_OAEP_SHA384, RSA_OAEP_SHA512

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