Entrust
Securing Digital Identities & Information

EntrustSecurity
@Entrust

Entrust Technical Integration Guide

Entrust Authority Security Manager 8.1 SP1 (with Patch 192895)
With Bull crypt2pay HR V12.01.02I

June 2016

Entrust.com
1-888-690-2424
Entrust@Entrust.com

Entrust®
Securing Digital Identities & Information

Contents

Introduction

This technical integration guide provides an overview of Bull crypt2pay integration with Entrust Authority Security Manager, hereafter referred to as Security Manager.

Thanks to the integration of Security Manager & Bull crypt2pay HR, the market can count on a complete solution to enable organizations to manage their encryption keys with reinforced confidentiality and integrity in compliance with the highest standards of security.

The robustness and high level of crypt2pay is substantiated by its FIPS 140-2 Level 3+, PCI HSM, and ICP Brazil or MEPS certifications. This can ensure current and future customers of Entrust that through this cooperation they can benefit from enhanced security for their application.

About Entrust

As a trusted provider of identity-based security solutions, Entrust empowers governments, enterprises and financial institutions in more than 5,000 organizations spanning 85 countries. Entrust's award-winning software authentication platforms manage today's most secure identity credentials, addressing customer pain points for cloud and mobile security, physical and logical access, citizen eID initiatives, certificate management and SSL. For more information about Entrust products and services, call 888-690-2424, email entrust@entrust.com or visit www.entrust.com.

About Bull

Bull is the Atos brand for its technology products and software, which are today distributed in over 50 countries worldwide. With a rich heritage of over 80 years of technological innovation, 2000 patents and a 700 strong R&D team supported by the Atos Scientific Community, it offers products and value-added software to assist clients in their digital transformation, specifically in the areas of Big Data and Cybersecurity.
Bull is the European leader in HPC and its products include bullx, the energy-efficient supercomputer; bullion, one of the most powerful x86 servers in the world developed to meet the challenges of Big Data; Evidian, the software security solutions for identity and access management; the robust hardware security modules crypt2pay & Proteccio, and Hoox, the ultra-secure smartphone. Bull is part of Atos.

For more information:
http://www.bull.com/protecting-e-transactions
http://www.facebook.com/BullGroup
http://twitter.com/bull_com

Partner Contact Information

Sales Contact

Andrea Lopez
Atos Cybersecurity Products
International Business Development
Global BDS
M. +33 (0)6 85 13 40 41
andrea.lopez@atos.net

Support Contact

Atos Global Cybersecurity Products, e-Transactions Security
crypt2pay Product Line
Rue Jean Jaures
BP 68
78340 Les Clayes-sous-Bois
FRANCE

HOT LINE : +(33) 1.30.80.62.00
e-mail: srv.hotline-bnt@atos.net
Fax: + (33) 1.30.80.76.36

Entrust Product Information

Entrust Authority Security Manager 8.1 SP1 (with Patch 192895)
Entrust Authority Security Manager Administration 8.1 SP1 (version 8.1.350)
Entrust Authority Security Manager PostgreSQL 8.3.23

Partner Product Information

Partner Name: Bull e-Transactions Security
Website: http://www.bull.com/protecting-e-transactions
Product Name: crypt2pay HR
Product Version: Firmware V12.01-02I, PKCS#11 v3.5.7
Platform and Service pack: Windows Server 2012 R2 with updates

Product Description

Crypt2pay is a network *Hardware Security Module* (HSM) providing cryptographic services to a server or a complete network (LAN) at TCP/IP level.
Sensitive data are only handled within the secure boundaries of the HSM and never exposed outside *in the clear*.

Security

Crypt2pay is built on a tamper resistant *Hardware Security Module*, ensuring physical and logical protection for cryptographic keys and preventing any unauthorized access to them.
Tamper detection mechanisms in place guarantee deletion of critical security data in case of violation attempts.
To prevent unavailability in case of power shortage, key storage memories and safety circuits are continuously powered by a dedicated battery.

High Performance

Crypt2pay takes care of cryptographic processing, providing host servers resources optimization in critical applications operations involving strong cryptography algorithms and sensitive key management.

Dual network interface

The dual network interface allows the deployment of crypt2pay on two different sub-networks to protect multiple security areas or provide redundancy within a single network. Support for two LANs can be used to enforce a strict separation between the administration and cryptographic services of the HSM as well.

Dual power supply

On HR (*High Range*) model, the power supply may be provided by the main power socket or through the Ethernet interface (POE - *Power Over Ethernet*).

Physical Security

The *tamper-resistant* envelope and active circuits ensure secure memory *zeroization* in case of physical attack detection.
Two security levels are implemented, providing protection for both secure memories used for symmetric encryption key (DES, Triple DES, AES, etc.), asymmetric keys (RSA, ECC, etc.) and sensitive data storage.
A dedicated battery provides emergency power for safety circuits in case of power supply shortage. A procedure for changing the battery allows the user to replace it without loss of configuration and without opening the device.
Crypt2pay contains a certified physical random number generator providing a 256-bit entropy source ensuring a high level of security in probabilistic cryptographic schemes and key management operations.
CHR platform is **FIPS140-2 level 3+** validated.

Availability and Scalability

The crypt2pay contains no mechanical element and thus provides a high level of reliability and availability.
Crypt2pay introduces no limitation on the number of keys or HSMs connected to a server.
The cryptographic functions of crypt2pay can be updated and activated using the remote web administration interface. The level of performance itself can be dynamically adjusted to customer needs (*HR model*).

Integration Details

The technical integration is based on the two following main steps:

1. crypt2pay setup and configuration,
2. Entrust setup and configuration.

Crypt2pay setup and configuration require:

1 hardware deployment,
2 PKCS#11 client setup,
3 PKCS#11 client configuration.

References

[1] C2P LP54008 User Guide v3.3
[2] C2P LP54006 Reference Manual v3.15
[3] C2PAPI LP54016 PKCS11 API User Guide v2.18
[4] C2PENV LP54022 Quickstart v1.2
[5] KMC LP54002 Reference_Manual V4.9.7

Crypt2pay setup and configuration

Hardware deployment

Crypt2pay is a network HSM and requires being reachable from client application (two Ethernet interfaces may be configured through the web administration interface).

Besides network reachability, a *Master Key* has to be generated or imported.

Note: *in test environments, a pre-generated test Master Key may be used.*
To activate test Master Key, check the TEST option (requires a TEST HSM).

In order to supply proper cryptographic abilities regarding Security Manager integration, the following options have to be enabled through the web administration interface (“Options” menu):

```
BASIC, ENCRYPT, MULTI_C, PKCS11.
```

Refer to [1] *to get more details about* crypt2pay *hardware deployment.*

PKCS#11 client setup

The Bull crypt2pay PKCS#11 client may be installed using the dedicated installer supplied with crypt2pay HSM.

Note: *Security Manager requires x83 (32-bit) environment.*
Be careful to choose the “32-bit” option during PKCS#11 client installation process.

The installer creates **two directories**:

1. the first one is dedicated to PKCS#11 client *binaries* (library and tools),
2. the second one is dedicated to *data* (keys and configuration file).

Default path for binaries is `C:\Program Files (x86)\Bull\c2p`; default path for data is `C:\ProgramData\Bull\c2p`.

Those may be changed during installation process.
They are needed to perform the checking operations described in the "Validation" paragraph.

Note: *in test environments, you may use the QuickStart Package to deploy a test PKCS#11 client (check the "QuickStart Package" option during PKCS#11 client setup).*

Refer to [4] *to get more details about QuickStart Package.*

PKCS#11 client configuration

The Bull crypt2pay PKCS#11 client relies on a **dynamic library** (`pkcs11c2p.dll`), a **key store** (regular directory for key files) and a **configuration file**.

The configuration file sets PKCS#11 client parameters including crypt2pay IP address.

Refer to [3] *to get more details about the* crypt2pay *PKCS#11 client configuration file.*

PKCS#11 keys are stored in *key stores* dedicated to each PKCS#11 slot defined in the configuration file.

Note: *in a regular Security Manager deployment, only one slot is used. However, if the HSM is used to protect the db key, then a second slot is used.*

Only one key store is discussed in the following procedure.

Entrust Certification Authority key files stored in the *key store* are encrypted using a Distribution Key (KDK) (managed by C2P and unknown to Security Manager).

The KDK itself is encrypted using the crypt2pay Master Key (so it is the only device able to decrypt the KDK and then the key store).

Note: *when several* crypt2pay HSMs *are used in a cluster (for performance, load-balancing and failover), the same KDK is encrypted*

using each crypt2pay *Master Key, so they are all able to decrypt and access the keys in a same key store.*

Both master keys and KDK are generated during a Key Ceremony with the Key Management Center (Bull software dedicated to secure key generation).

Note: *the use of a crypt2pay HSM with the Key Management center requires the* `CGDC` *option to be enabled.*

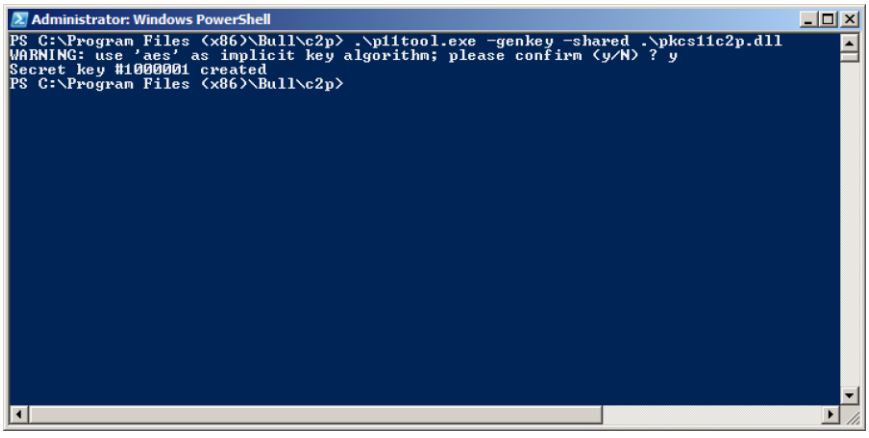
Refer to [5] to get more details about Master Key and Distribution Key management using the Key Management Center.

Validation

Successful deployment of crypt2pay and its PKCS#11 client may be checked by the generation of a key using the Bull `p11tool` utility.
From the Bull PKCS#11 binaries locations (`C:\Program Files (x86)\Bull\c2p`, by default), run the following symmetric key creation command:

```
.\p11tool.exe -genkey -shared pkcs11c2p.dll
```

The shell may require a confirmation (use of default algorithm), type "y" or "yes".

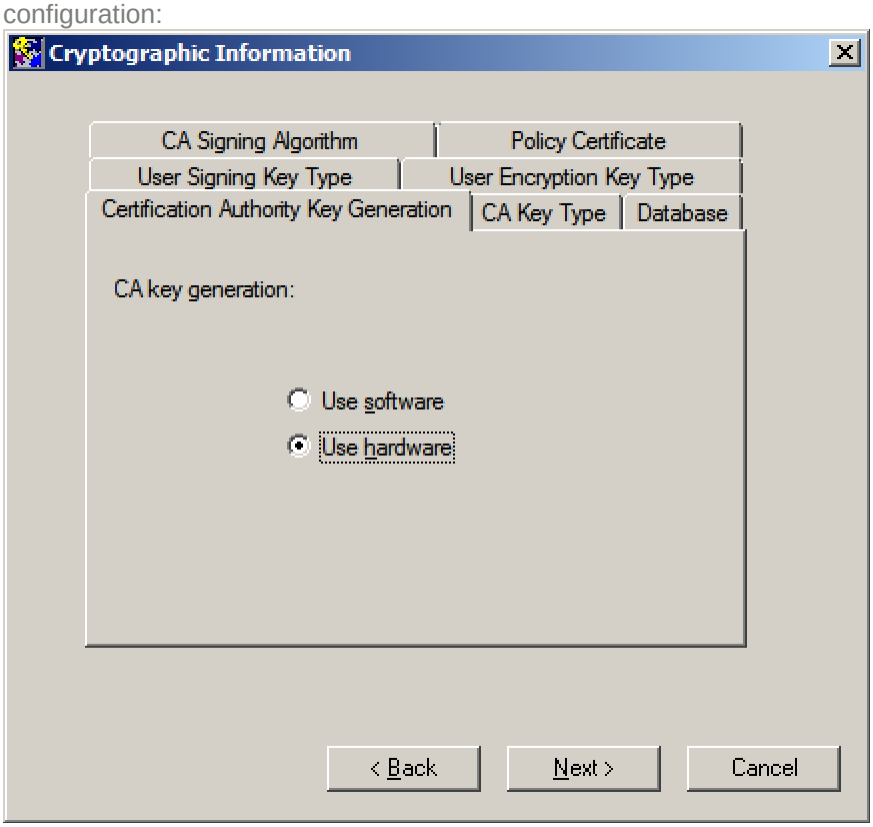


Once successful, the p11tool utility print the "`Secret key #XXXXXXXX created`" message (and a net key file is available in the key store directory)

Install, Configure, and Initialize Security Manager

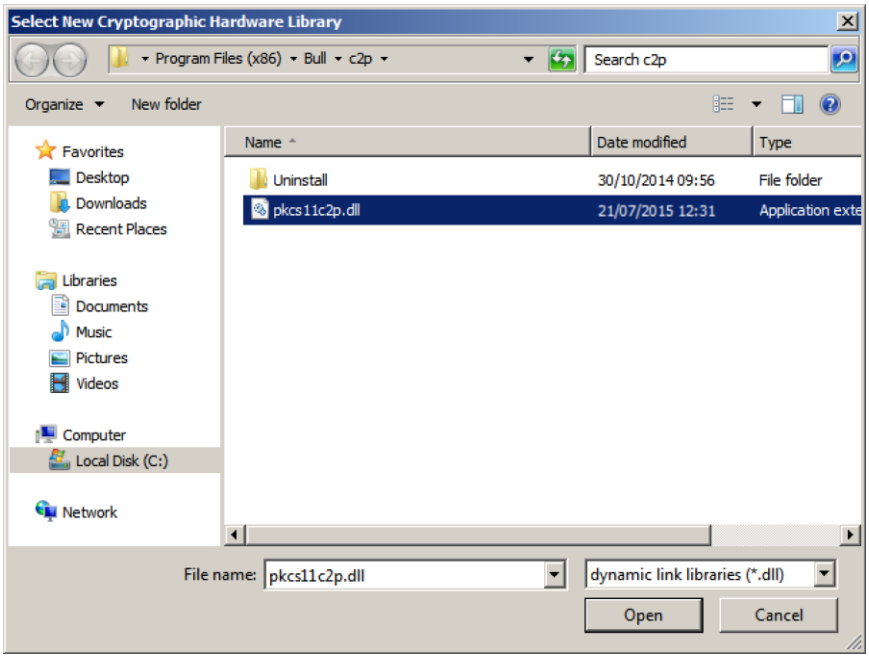
Install, configure and initialize the Security Manager in accordance with the *Entrust Authority Security Manager Installation Guide*.

Crypt2pay usage by Security Manager is enabled during configuration process (after installation) and consists of choosing “Use hardware” instead of “Use software” option after CA cryptographic keys configuration:



After you click on the Next button, you are prompted to select the HSM.

After Cryptographic configuration, and if the Bull PKCS#11 client is not automatically detected, select the `pkcs11c2p.dll` library (in the PKCS#11 client binaries directory – `C:\Program Files (x86)\Bull\c2p` by default, if not change during PKCS#11 client setup):



System Behavior/Limitations

FIPS Mode

While crypt2pay is FIPS140-2 level 3+ validated, the current integration with Security Manager does not support running in FIPS mode.

TCP connections

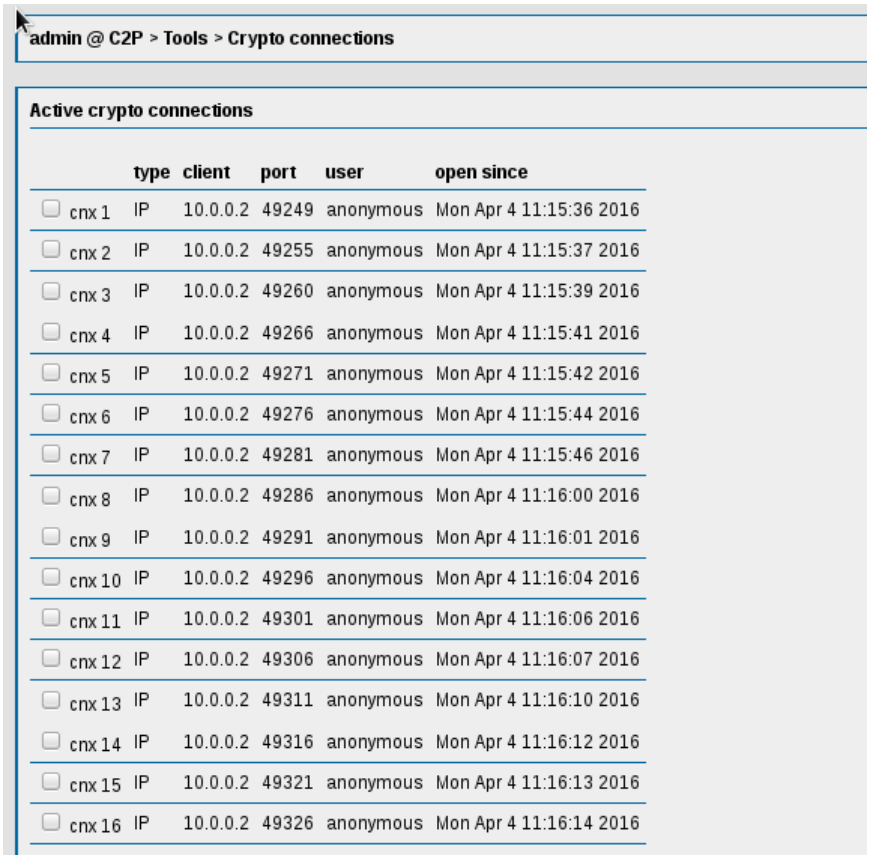
Crypt2pay communications with its PKCS#11 client are performed through TCP connections.
Up to **16** simultaneous TCP connections can be managed by crypt2pay.

Security Manager defines a specific number of processes to each of its subsystems that comprise the service (which may be checked using the "`service status`" command).
Those processes may preempt one or more TCP connections.

In default installation, the number of processes used by the Security Manager service is 14. Operations requiring more than 16 TCP connections at the same time would require clustering several HSMs together to avoid a TCP shortage.

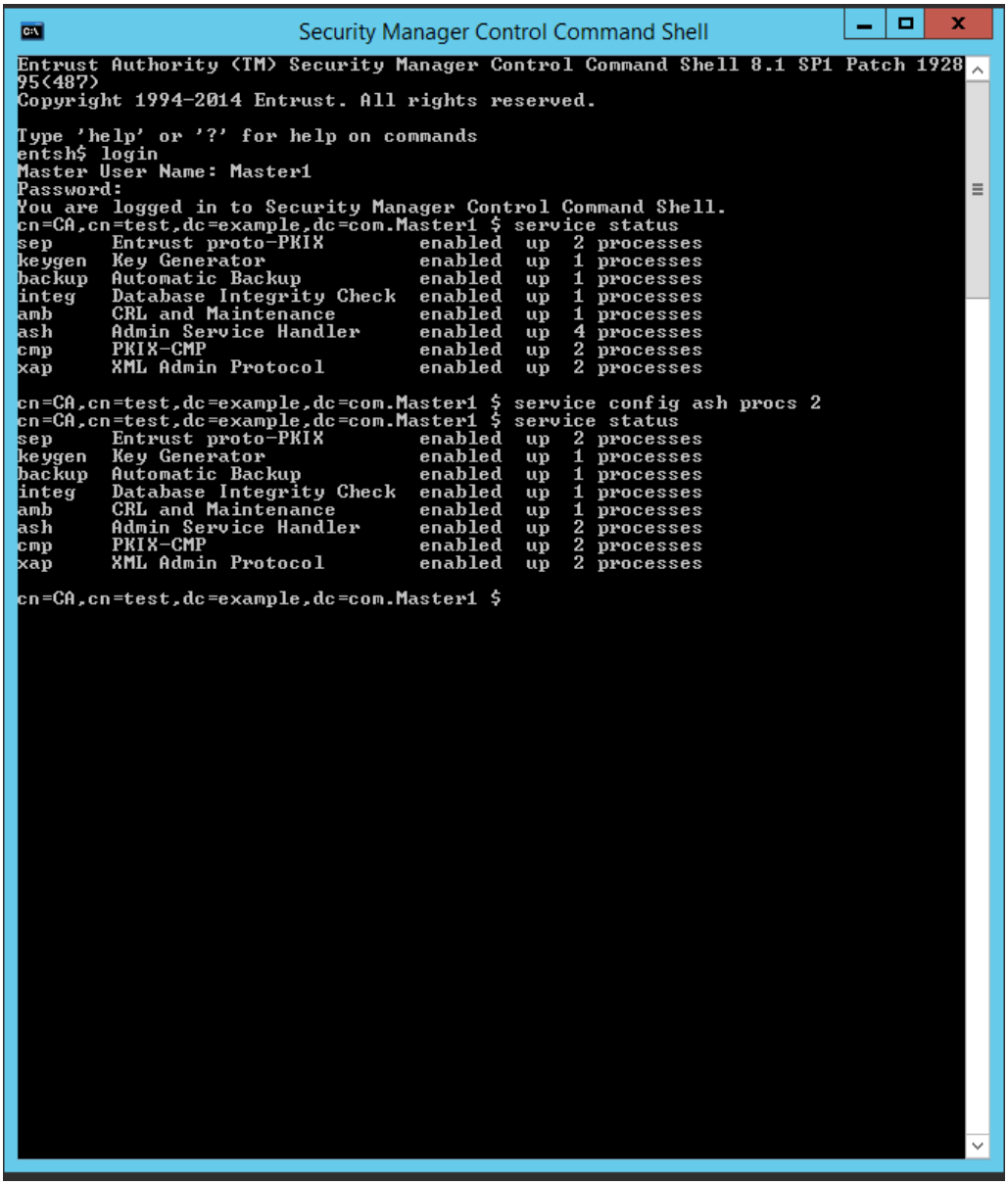
Note: *active TCP connections to* crypt2pay *can be monitored through the web administration interface (*`Crypto Connections` *menu).*
In case of persistent inability of starting the Security Manager services, the number of processes attached to each service may have to be decreased (`service config <service name> procs <number`

of processes>).



	type	client	port	user	open since
cnx 1	IP	10.0.0.2	49249	anonymous	Mon Apr 4 11:15:36 2016
cnx 2	IP	10.0.0.2	49255	anonymous	Mon Apr 4 11:15:37 2016
cnx 3	IP	10.0.0.2	49260	anonymous	Mon Apr 4 11:15:39 2016
cnx 4	IP	10.0.0.2	49266	anonymous	Mon Apr 4 11:15:41 2016
cnx 5	IP	10.0.0.2	49271	anonymous	Mon Apr 4 11:15:42 2016
cnx 6	IP	10.0.0.2	49276	anonymous	Mon Apr 4 11:15:44 2016
cnx 7	IP	10.0.0.2	49281	anonymous	Mon Apr 4 11:15:46 2016
cnx 8	IP	10.0.0.2	49286	anonymous	Mon Apr 4 11:16:00 2016
cnx 9	IP	10.0.0.2	49291	anonymous	Mon Apr 4 11:16:01 2016
cnx 10	IP	10.0.0.2	49296	anonymous	Mon Apr 4 11:16:04 2016
cnx 11	IP	10.0.0.2	49301	anonymous	Mon Apr 4 11:16:06 2016
cnx 12	IP	10.0.0.2	49306	anonymous	Mon Apr 4 11:16:07 2016
cnx 13	IP	10.0.0.2	49311	anonymous	Mon Apr 4 11:16:10 2016
cnx 14	IP	10.0.0.2	49316	anonymous	Mon Apr 4 11:16:12 2016
cnx 15	IP	10.0.0.2	49321	anonymous	Mon Apr 4 11:16:13 2016
cnx 16	IP	10.0.0.2	49326	anonymous	Mon Apr 4 11:16:14 2016

Note: *for environments requiring more processes than available, several* crypt2pay HSMs *may be used in a cluster to increase the number of available TCP connections.*



CA key generation or update

The Shell may have to be restarted after CA key generation or update.

Database Encryption

By default, the <cipherOptimisation> tag of the c2p.xml configuration file is set to “On”. In order to perform key generation for database encryption, this tag must be set to **off**.

```
<cipherOptimisation>Off</cipherOptimisation>
```

NB: this tag is within the <C2Pconfig></C2Pconfig> tag.

Please refer to “C2P_LP54016_PKCS11_API_User_Guide_V2 18_EN”.

Unsupported cryptographic algorithms

The CAST algorithm is not supported (and cannot be used for database encryption). Trying to select CAST5-CBC-128 algorithm for hardware protection of Security Manager Database fails with an error message: “(-188) Bad key length. Error creating symmetric key in hardware”.

RSA modulus length cannot exceed 4096 bits. As a consequence, RSA-6144 cannot be used in signature algorithms.

Named curves with an order lower than 192 are not supported:

Name	OID
EC-ansix9p160k1	06 05 2B 81 04 00 09
EC-ansix9p160r1	06 05 2B 81 04 00 08
EC-ansix9p160r2	06 05 2B 81 04 00 1E

Regarding Brainpool curves, only the following are available for signature:

Name	OID
EC-brainpoolP192r1	06 09 2B 24 03 03 02 08 01 01 03
EC-brainpoolP224r1	06 09 2B 24 03 03 02 08 01 01 05
EC-brainpoolP256r1	06 09 2B 24 03 03 02 08 01 01 07
EC-brainpoolP320r1	06 09 2B 24 03 03 02 08 01 01 09
EC-brainpoolP384r1	06 09 2B 24 03 03 02 08 01 01 0B
EC-brainpoolP512r1	06 09 2B 24 03 03 02 08 01 01 0D