

[print](#) | [close](#)

Check Your Cryptographic Access Provider LPP for Bugs and Support

[System iNetwork Systems Management Newsletter](#)

[Carsten Flensburg](#)

Carsten Flensburg

Wed, 07/20/2005 (All day)

It seems that the installation of the OS/400 Cryptographic Access Provider licensed program products at times have a problem. Carsten has run up against this problem, and I experienced the same problem when configuring a system for Kerberos (Network Authentication Service) for Single Sign-on.

It appears that under some circumstances, a recovery situation arises where the Display Software Resources (DSPSFWRSC) command verifies the Cryptographic Access Provider licensed program as being installed, yet the product had to be reinstalled because the _CIPHER MI instruction claimed that the algorithm needed was not supported. We have not yet seen a PTF to fix this problem.

For this issue, Carsten has provided a utility to let you easily check what cryptographic support is available on your machine. Depending on the presence -- and version -- of the Cryptographic Access Provider licensed program product, a variety of cryptographic algorithms and cipher key lengths are supported.

[Click here for a list of the Cryptographic Access Providers LPPs and their corresponding support.](#)

Provided here is the new CL command CHKCRPSPT (Check Cryptographic Support). The command verifies the current status of the Cryptographic software functions provided on the machine.

The command has the following format:

CHKCRPSPT ALGORITHM(*LIST)

The ALGORITHM parameter specifies the cryptographic algorithms should be checked for support on your machine. The allowable values are:

- *LIST – Check all algorithms for support
- *MAC - Message Authentication Code
- *MD5 - The MD5 algorithm
- *SHA_1 - The Secure Hash Algorithm
- *DES_E - The Data Encryption Standard algorithm (encrypt only)
- *DES – The Data Encryption Standard
- *RC4 - The RC4 algorithm
- *RC5 - The RC5 algorithm
- *DESX - The DESX algorithm
- *TDES - The Triple-DES algorithm
- *DSA - The Digital Signature Algorithm
- *RSA - The Rivest-Shamir-Adlem algorithm

- *DIFHEL - The Diffie-Hellman algorithm
- *CDMF - The Commercial Data Masking Facility algorithm
- *RC2 - The RC2 algorithm
- *AES - The Advanced Encryption Standard algorithm

The default option of *LIST returns an informational message for each cryptographic algorithm currently supported, but it's also possible to check a specific algorithm (e.g. *AES).

Here is a sample of the resulting message in case of the algorithm being supported:

AES algorithm supported with maximum key length 256.

The following source code is included:

- CBX940 - Command RPG/IV CPP
- CBX940H - Command help text panel group
- CBX940X - Command definition source

See each source member for compile instructions.

You can download a zip file containing all the source code from the following URL:

<http://www2.systeminetwork.com/noderesources/code/clubtechcode/ChkCrpSpt.zip>

Source URL: <http://iprodeveloper.com/security/check-your-cryptographic-access-provider-lpp-bugs-and-support>