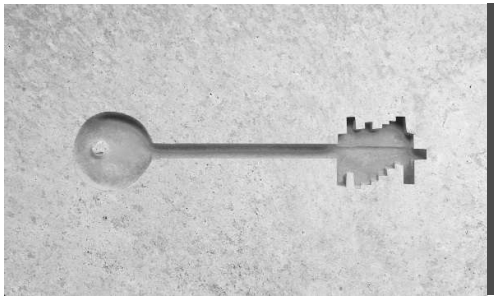


CryptoServer CP5 5.1.2 Release Notes

July 1st, 2025

1 Introduction

CryptoServer CP5 5.1.2 is a recertified maintenance update

The common criteria portal is not updated yet but the new certificate can be found here :
https://www.trustcb.com/common-criteria/nscib/nscib-certificates/

2 New features

2.1 Increased key length for secure messaging

Secure messaging protocol now uses 3K DH keys (instead of 2K).

2.2 Increased key length for user authentication

RSA user authentication via csadm now support keys greater than 2048 (3K and 4K keys).

This feature requires a new smartcard applet (so new smartcards are required).

To verify the smartcard applet version it must be V3.x:

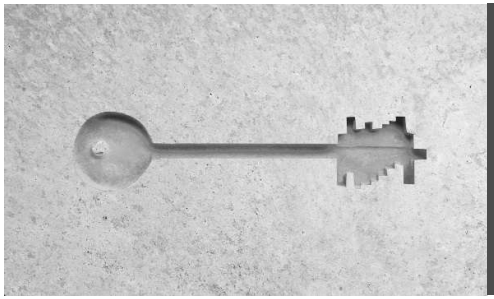
csadm GetCardInfo=:cs2:cjo:USB0

Utimaco Smartcard version: 3.0.0.0

3 Bugfixes

OCTO-101 : Every 497 days the HSM no longer processes commands with certain buffer size and HSM must be rebooted. This is fixed.

PHX-343 : execution of command openKey is possible even if audit log is full.



CryptoServer CP5 5.1.2 Release Notes

July 1st, 2025

HSM-15166 : fixed memory leak in cxial_saek_generate_key_blob

HSM-11575 : Fixed error in C_DeriveKey ASN.1 (with mechanism CKM_ECDH1_DERIVE)

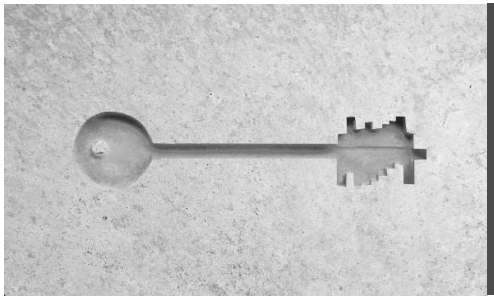
4 Release Details

4.1 CryptoServer models

The following table lists CryptoServer models supported by CryptoServer CP5 5.1.2:

CryptoServer Model	Hardware Platform
CryptoServer Se12/52/500/1500 PCIe	• CryptoServer Se-Series Gen2 PCIe card, hardware version 5.01.4.0, Bootloader 5.01.4.0
CryptoServer Se12/52/500/1500 LAN	• CryptoServer LAN V5, UTISYS003-AC, 19“ / 1U housing; redundant power supply, integrated CryptoServer Se-Series Gen2 PCIe card • CryptoServer LAN V4c*, Mayflower-ID/G1820TE1D; 19“ / 2U housing; redundant power supply, integrated CryptoServer Se-Series Gen2 PCIe card

Notice: CryptoServer models resp. hardware platforms marked with * have passed End of Sales but are still supported.



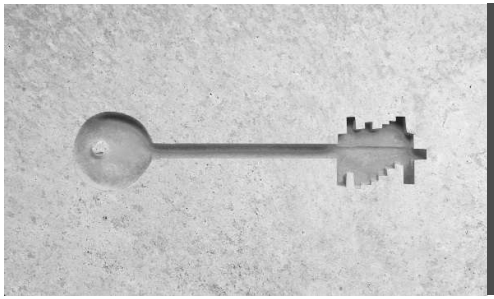
CryptoServer CP5 5.1.2 Release Notes

July 1st, 2025

4.2 Operating Systems

The following table lists the Operating Systems supported by CryptoServer CP5 5.1.2.

Operating System	Se-Series Gen2
Windows	
Windows 7 / 8 / 8.1 / 10	✓
Windows Server 2008 / 2008 R2	✓
Windows Server 2012 / 2012 R2	✓
Windows Server 2016	✓
Linux	
Red Hat Enterprise Linux 6.4 / 6.5 / 6.6 / 6.9 Red Hat Enterprise Linux 7.0 / 7.1 / 7.2 / 7.3 Red Hat Enterprise Linux 8.10 *	✓
SUSE Linux Enterprise Server 11	✓
Debian 7 “Wheezy”, Debian 8 “Jessie”, Debian 9 “Stretch”	✓



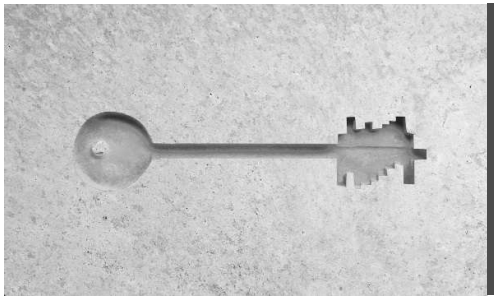
CryptoServer CP5 5.1.2 Release Notes

July 1st, 2025

4.3 Firmware packages and modules

The following table shows the version of each firmware module included in the CryptoServer CP5 5.1.2 firmware packages. Firmware modules are listed by ascending FunctionCode, as shown by a “list firmware” command:

Firmware Package	**CryptoServerCP5-Se2-Series-5.1.2.mpkg**
CryptoServer Model	**CryptoServer Se12/52/500/1500 PCIe / LAN**
Firmware Module	
SMOS	5.6.6.1
POST	1.0.0.2
HCE	2.2.2.3
EXAR	2.2.1.1
CXI	2.2.3.7
CXIAL	1.0.0.1
VDES	1.0.9.4
CMDS	3.6.0.13
VRSA	1.3.6.5
UTIL	3.0.5.3
ADM	3.0.25.5
DB	1.3.2.4
HASH	1.0.12.1
AES	1.4.1.7
LNA	1.2.4.4



CryptoServer CP5 5.1.2 Release Notes

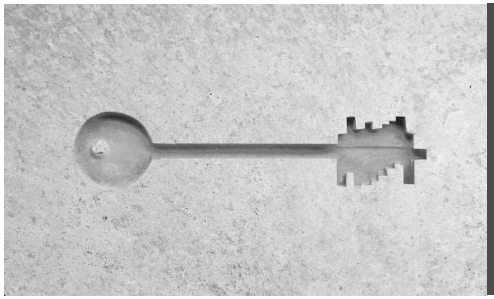
July 1st, 2025

Firmware Package	CryptoServerCP5-Se2-Series-5.1.2.mpkg
CryptoServer Model	CryptoServer Se12/52/500/1500 PCIe / LAN
Firmware Module	
ECA	1.1.12.4
ASN1	1.0.3.8
MBK	2.3.0.0
ECDSA	1.1.16.2

4.4 Administration Tools

The following table lists the administration tools shipped with CryptoServer CP5 5.1.2 Product CD:

Tool	Version
Command-line administration tool “csadm”	2.3.8
PKCS#11 R2 command-line administration Tool “p11tool2”	2.0.20
PKCS#11 R2 GUI administration tool “P11CAT”	2.28
CNG Key Management Tool “cngtool”	1.3.11 for CP5
CXI Key Management Tool “cxitool”	1.6.26 for CP5



CryptoServer CP5 5.1.2 Release Notes

July 1st, 2025

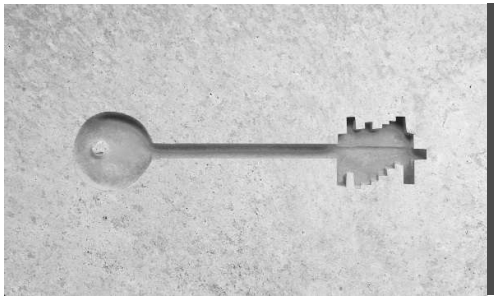
4.5 Cryptographic Interface Libraries

The following table lists the cryptographic interface libraries shipped with CryptoServer CP5 5.1.2 Product CD:

Cryptographic Interface Libraries	Version
PKCS#11 R2 library “cs_pkcs11_R2.dll” (Windows), “libcs_pkcs11_R2.so” (Linux)	2.92
CSP Provider “cs2csp.dll” (Windows)	3.2.5
CNG Provider “cs2cng.dll” (Windows)	2.0.10
CXI library for C/C++ “cxi.dll” (Windows), “libcxi.so” (Linux)	1.7.18

The following table lists the cryptographic interfaces that are supported by CryptoServer CP5 5.1.2 on the respective Operating System:

	PKCS#11 R2	Microsoft CSP	Microsoft CNG	CXI
Windows				
Windows 7 / 8 / 8.1 / 10	✓	✓	✓	✓
Windows Server 2012 / 2012 R2	✓	✓	✓	✓
Windows Server 2016	✓	✓	✓	✓
Linux (32 and 64 bit)				
Red Hat Enterprise Linux 6.4 / 6.5 / 6.6 / 6.9 Red Hat Enterprise Linux 7.0 / 7.1 / 7.2 / 7.3 Red Hat Enterprise Linux 8.10	✓	n.a.	n.a.	✓
SUSE Linux Enterprise Server 11	✓	n.a.	n.a.	✓
Debian 7 “Wheezy”, Debian 8 “Jessie”, Debian 9 “Stretch”	✓	n.a.	n.a.	✓



CryptoServer CP5 5.1.2 Release Notes

July 1st, 2025

4.6 Driver

The following table lists the PCIe card driver shipped with CryptoServer CP5 5.1.2:

Driver	Version
Windows driver	5.2
Linux driver	5.38

5 Known issues

There aren't any known issues in CryptoServer CP5 5.1.2.

6 Technical support

You can find technical support for Utimaco products in any of these ways:

Download product information from https://support.hsm.utimaco.com/support

Contact us at https://utimaco.com/company/contact-us

Send an email to support@utimaco.com including your hardware serial number(s), software version number(s), operating system(s) and patch level(s), log file(s) and the text of any error messages.

Contact our support hotline: EMEA +49 800-627-3081, Americas +1-844-UTIMACO (+1 844-884-6226), APAC +81 800-919-1301

7 Legal notices