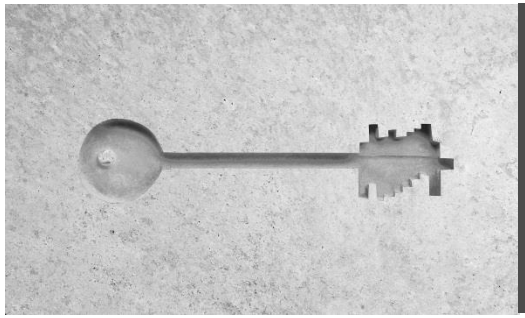


SecurityServer 4.51.0 for CryptoServer SeGen2/CSe Release Notes

Release Date: March 3, 2023

1 Introduction

SecurityServer 4.51.0 introduces numerous enhancements and new features, and fixes issues found in previous releases. Please consult the following sections for details.

If you have a valid maintenance contract for CryptoServer Se-Series Gen2 and/or CryptoServer CSe-Series Hardware Security Module(s), you are eligible to upgrade your HSM which are covered by this maintenance contract to SecurityServer 4.51.0. The SecurityServer 4.51.0 product bundle is available to you for download in our customer portal.

If you do not have a valid maintenance contract, or not all your CryptoServer Se-Series Gen2 and/or CryptoServer CSe-Series Hardware Security Module(s) are covered by this maintenance contract, you may not update these HSM(s)to SecurityServer 4.51.0. Please contact Utimaco Sales staff if you wish to update your HSM(s) to SecurityServer 4.51.0.

Please review this document to be informed of any new features and changes introduced by this new release, and especially any pre-conditions to notice. Please take special care to the installation instructions in chapter 6.

2 New Features and Improvements

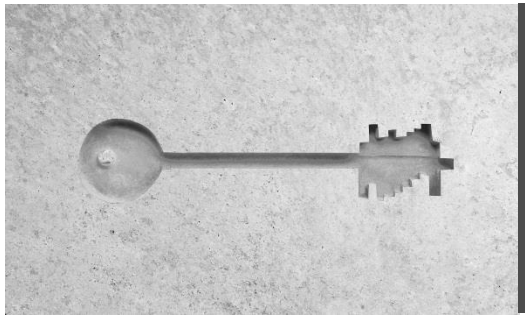
2.1 Support for Chinese Algorithms SM2, SM3 and SM4

SecurityServer 4.51.0 supports PKCS#11 Vendor Defined Mechanisms (VDM) for Chinese algorithms SM2, SM3 and SM4. These VDMs use the usual PKCS #11 Functions for key (pair) generation (SM4/SM2), signature creation/verification (SM2), hashing (SM3), encryption/decryption (SM4) and object deletion. Please consult the “CryptoServer PKCS #11 R3 Developer Guide” for details.

Crypto Provider administration tools p11tool2, P11CAT and cxitool support creation and management of SM2 and SM4 keys.

2.2 KeyAgreement class in JCE

The CryptoServer JCE provider now supports KeyAgreement Class with mechanisms ECCDH and ECCDHWITH<hash>KDF. Please consult the “CryptoServer JCE Provider” documentation for details.



SecurityServer 4.51.0 for CryptoServer SeGen2/CSe Release Notes

2.3 Microsoft SQL Server for external key storage

PKCS #11 R3 provider and PKCS #11 administration tools p11tool2 and P11CAT, as well as SQLEKM provider, support Microsoft SQL Server for external key storage. SecurityServer 4.51.0 thus enables customers building their infrastructure on Microsoft technology to use Microsoft SQL Server for external key storage for PKCS #11 and SQLEKM providers.

2.4 Documentation

- Updates of “CryptoServer PKCS#11 p11tool2 Reference Manual” and “CryptoServer PKCS#11 - P11CAT Manual” with information about Unique IDs of PKCS#11 objects.
- Improved description and examples for usage of (empty) <name>, <group> and <spec> parameters in “CryptoServer cxitool Manual” sections ‘Cryptographic Keys and Key Groups’, ‘ListKeys’, ‘KeyInfo’, ‘DeleteKey’, ‘BackupKey’ and ‘SetFipsUsage’.
- Improved description of SNMP object ‘cslclientsload’ in “CryptoServerLAN V5 Manual for System administrators”.

3 Legacy Features

The Utimaco PKCS#11 R3 provider stores newly created or imported objects in the key store specified by the "KeysExternal” item in the PKCS#11 configuration file, i.e. either in the internal or in the external keystore. When searching an object (C_FindObjects*) the search covers both the internal keystore and the external key store (if such external key store is configured).

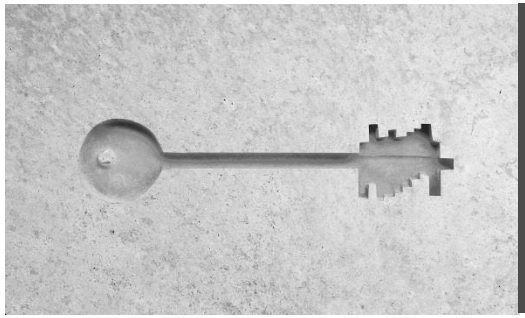
This behavior is unique to our PKCS#11 provider and has been adopted in PKCS#11 R3 for backwards compatibility to PKCS#11 R2 provider. All other Utimaco cryptographic provider switch between keystores.

The object search in internal and external keystore is declared as legacy with SecurityServer 4.50.0. We recommend you ensure that PKCS#11 slots use only one of internal key store or external key store, and don’t specify any setting in the [KeyStorage] section of the PKCS#11 configuration file when "KeysExternal” is set to false.

Future versions of the PKCS#11 R3 provider will exclusively use the internal or external key storage as configured.

4 Discontinued Features

None



SecurityServer 4.51.0 for CryptoServer SeGen2/CSe Release Notes

5 Release Details

5.1 CryptoServer models

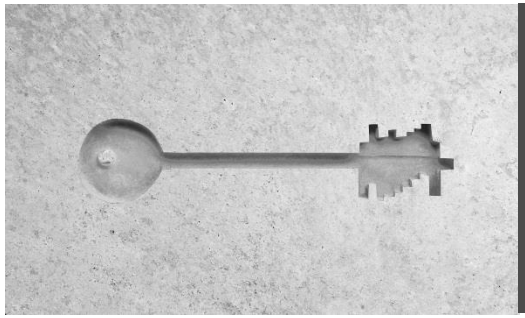
The following table lists CryptoServer models supported by SecurityServer 4.51.0:

CryptoServer Model	Hardware Platform
CryptoServer Se12/52/500/1500 PCIe	• CryptoServer Se-Series Gen2 PCIe card, hardware version >= 5.1.0.0, Bootloader >= 5.00.0.0
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 CSe10/CSe100 PCIe	• CryptoServer CSe-Series PCIe card, hardware version >= 4.0.2.0, Bootloader >= 4.0.0.0
CryptoServer CSe10/CSe100 LAN	• CryptoServer LAN V5, UTISYS003-AC, 19“ / 1U housing; redundant power supply, integrated CryptoServer CSe-Series PCIe card

5.2 Operating Systems

The following table lists the Operating Systems supported by SecurityServer 4.51.0.

Operating System	Version
Windows	
Windows	10, 11
Windows Server	2016, 2019, 2022
Linux	
Red Hat Enterprise Linux	8
CentOS	7
SUSE Linux Enterprise Server	12, 15
Ubuntu	18.04 LTS, 20.04 LTS



SecurityServer 4.51.0 for CryptoServer SeGen2/CSe Release Notes

Notice: Only 64-bit versions of these Operating Systems are supported. 32-bit applications running on such 64-bit Operating Systems are still supported, but 32-bit libraries (e.g. PKCS#11 provider, CNG provider) are not shipped with the product bundle anymore and instead provided as separate download on our customer support portal.

5.3 Java Runtime Environments

The following table lists the Java Runtime Environments supported by SecurityServer 4.51.0.

Java Runtime Environment	Version
Oracle Java	8, 11, 15
OpenJDK	8, 11,15

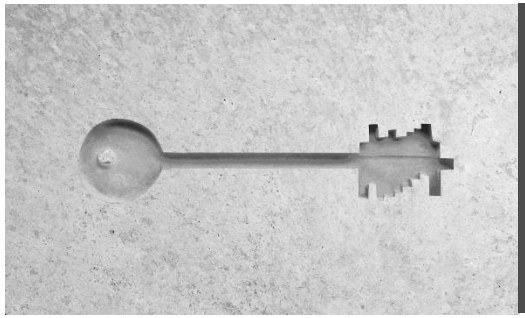
Please notice

When encountering an exception "java.awt.AWTError: Assistive Technology not found: org.GNOME.Accessibility.AtkWrapper" on Linux when starting CAT or P11CAT please check that full JDK/JRE is installed and not just the headless version. Alternatively, delete or comment the line ‘assistive_technologies’ in file /etc/java-X-openjdk/accessibility.properties.

5.4 Firmware packages and modules

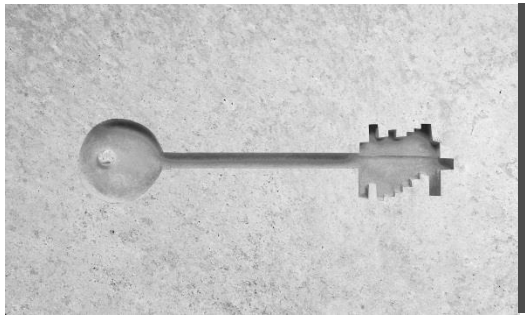
The following table shows the version of each firmware module included in the SecurityServer 4.51.0 firmware packages. Firmware modules are listed by ascending FunctionCode, as shown by a ‘csadm listfirmware’ command or executing Show Firmware in the administration tool CAT:

Firmware Package	**SecurityServer-Se2-Series-4.51.0.1.mpkg**	**SecurityServer-CSe-Series-4.51.0.1.mpkg**
CryptoServer Model	**CryptoServer Se12/52/500/1500 PCIe / LAN**	**CryptoServer CSe10/100 PCIe / LAN**
Firmware Module		
SMOS	5.6.8.0	4.6.8.0
POST	2.2.5.0	2.2.5.0



SecurityServer 4.51.0 for CryptoServer SeGen2/CSe Release Notes

Firmware Package	SecurityServer-Se2-Series-4.51.0.1.mpkg	SecurityServer-CSe-Series-4.51.0.1.mpkg
CryptoServer Model	CryptoServer Se12/52/500/1500 PCIe / LAN	CryptoServer CSe10/100 PCIe / LAN
Firmware Module		
HCE	3.0.3.0	---
EXAR	2.2.1.3	---
CXI	2.4.13.0	2.4.6.6*
VDES	2.2.5.0	2.2.5.0
PP	1.4.3.0	1.4.3.0
CMDS	3.8.8.0	3.8.8.0
VRSA	2.2.5.0	2.2.5.0
SC	1.2.2.0	1.2.2.0
UTIL	3.0.10.0	3.0.10.0
ADM	3.1.6.0	3.1.6.0
DB	2.0.2.0	2.0.2.0
HASH	2.2.5.0	2.2.5.0
AES	2.2.5.0	2.2.5.0
DSA	2.2.5.0	2.2.5.0
LNA	2.2.5.0	2.2.5.0
ECA	2.2.5.0	2.2.5.0
ASN1	2.2.5.0	2.2.5.0



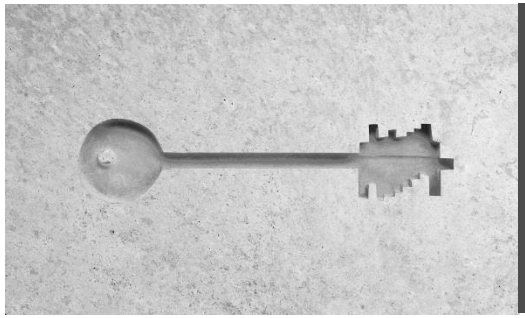
SecurityServer 4.51.0 for CryptoServer SeGen2/CSe Release Notes

Firmware Package	SecurityServer-Se2-Series-4.51.0.1.mpkg	SecurityServer-CSe-Series-4.51.0.1.mpkg
CryptoServer Model	CryptoServer Se12/52/500/1500 PCIe / LAN	CryptoServer CSe10/100 PCIe / LAN
Firmware Module		
MBK	2.5.4.0	2.5.4.0
NTP	1.2.3.0	1.2.3.0
ECDSA	2.2.5.0	2.2.5.0
CRYPT	2.2.5.0	2.2.5.0
STUN	1.0.2.0	1.0.2.0

5.5 Administration Tools

The following table lists the administration tools shipped with SecurityServer 4.51.0:

Tool	Version
Command-line administration tool “csadm”	2.9.0
GUI administration tool “CAT”	2.2.9.0
PKCS #11 command-line administration Tool “p11tool2”	3.3.1
PKCS #11 GUI administration tool “P11CAT”	3.05
CNG Key Management Tool “cngtool”	1.5.0
CXI Key Management Tool “cxitool”	1.13.1
Remote PIN Pad Daemon (PPD)	1.5.0



SecurityServer 4.51.0 for CryptoServer SeGen2/CSe Release Notes

5.6 Cryptographic Interface Libraries

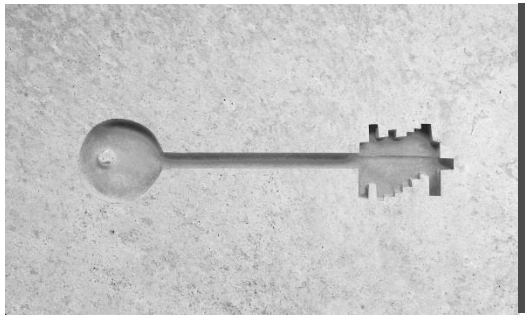
The following table lists the cryptographic interface libraries shipped with SecurityServer 4.51.0:

Cryptographic Interface Libraries	Version
PKCS #11 R3 library “cs_pkcs11_R3.dll” (Windows), “libcs_pkcs11_R3.so” (Linux)	1.28
JCE Provider “CryptoServerJCE.jar” (Windows, Linux)	1.76
CSP Provider “cs2csp.dll” (Windows)	3.4.0
CNG Provider “cs2cng.dll” (Windows)	2.5.0
MS SQL Extensible Key Management Provider “cssqlekm.dll” (Windows)	2.0.3.0
CXI library for C/C++ “cxi.dll” (Windows), “libcxi.so” (Linux)	1.11.0
CXI library for Java “CryptoServerCXI.jar” (Windows, Linux)	1.86

5.7 Driver

The following table lists the PCIe card driver shipped with SecurityServer 4.51.0:

Driver	Version
Windows driver	5.1.1
Linux driver	5.19.0



SecurityServer 4.51.0 for CryptoServer SeGen2/CSe Release Notes

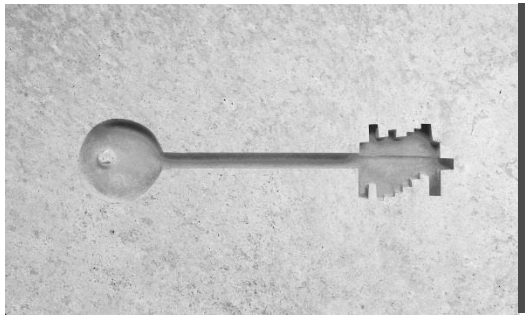
6 Installation

Follow the steps described in the CryptoServer Administration Manual section ‘Setup’ for installation of the product bundle.

When updating an existing installation prior SecurityServer 4.40.0, you should first uninstall your existing installation to cure the vulnerability described in CVE-2020-26155: Right click on the Windows Start button, then select ‘Apps & Features’. Start typing “CryptoServer” in the search field of the Apps & Features window, and Windows will find the CryptoServer app. Click on the CryptoServer app and press the ‘Uninstall’ button to uninstall the current installation. Alternatively, you may open the Control Panel, and select ‘Uninstall a program‘ from the ‘Programs’ section, and Windows will find the CryptoServer program. Either double-click on the CryptoServer program or press the ‘Uninstall’ button to uninstall the current installation. When being asked whether you want to uninstall the previous installation, select “Yes” to uninstall the previous version. To be sure that a possible exploitation of the vulnerability gets fixed, it is important that the previous installation is removed completely. You should therefore open Windows File Explorer, a command shell or PowerShell and check that the previous installation has been removed completely, i.e. there is no more directory “Utimaco” in “C:\Program Files”. In case the “Utimaco” directory has not been removed, delete it manually. Configuration files will not be removed from directory C:\ProgramData\Utimaco during uninstallation. Then run the installation wizard “SecurityServer-4.51.0.1.msi” that will guide you through the installation process. You find it on top-level of the SecurityServer 4.51.0 product bundle.

Important notice:
Loading a new firmware package SecurityServer-<platform>-4.51.0.1.mpkg with CryptoServer Administration Tool CAT or the command line tool csadm of a SecurityServer version prior 4.45.0 will throw an error. You must use CAT or csadm from the SecurityServer 4.51.0 product bundle for updating the firmware of your HSM(s) with firmware package SecurityServer-<platform>-4.51.0.1.mpkg.

Use the CryptoServer Administration Tool CAT or the command line tool csadm to update the HSM firmware and load the firmware package SecurityServer-Se2-Series-4.51.0.1.mpkg or SecurityServer-CSe-Series-4.51.0.1.mpkg depending on your type of HSM.



SecurityServer 4.51.0 for CryptoServer SeGen2/CSe Release Notes

7 Resolved issues

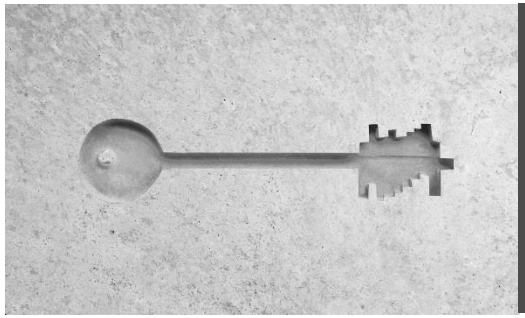
The following issues have been resolved in SecurityServer 4.51.0:

Reference	Component	Issue
PHX-564	PKCS#11 R3	Unwrapping a key with AES GCM succeeds although AAD not correct
PHX-454 / PHX-85	PKCS#11 R3	Memory leak in libcs_pkcs11_R3.so of SecurityServer 4.50.0
PHX-236	Simulator	Incorrect return value of Startsim.sh when simulator start failed.
PHX-195	CXI API	AES-GCM call for large amount of data, with data length not a multiple of 16 bytes, returns error 0xB08B0001
PHX-132	JCE	In JCE when using external key storage, a call to KeyStore#aliases seems to always return an empty list of key names. On the other hand, searching for keys directly using KeyStore#getKey occassionally fails with UnrecoverableKeyException and nested CryptoServerException.
PHX-76	JCE	JCE method key_Generate.java used with setting StoreKeysExternal = true (with given KeyStorePath) sometimes crashes on Linux.
EGL-40	PKCS#11 R3	Changes to keys in an ODBC external key store may cause C_FindObjects to return keys multiple times (one for each change).

8 Known issues

The following issues are known with SecurityServer 4.51.0:

Reference	Component	Issue
HSM-14404	JCE	Exception in thread "main" java.lang.IllegalAccessError: superinterface check failed: class CryptoServerJCE.CryptoServerKey … on Java 19. Workaround: start your Java application with “java --add-opens=java.base/sun.security.util=ALL-UNNAMED -jar <your Java application>”



SecurityServer 4.51.0 for CryptoServer SeGen2/CSe Release Notes

9 Technical support

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

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

Contact us at http://hsm.utimaco.com/contact/ .

Send an email to support@utimaco.com , including your hardware serial number(s), software version number(s), operating system(s) and patch level(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

10 Legal notices