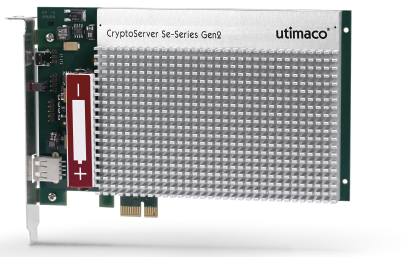
SecurityServer Se/CSe

Release Notes



utimaco®

Imprint

Copyright 2024	Utimaco IS GmbH Germanusstr. 4 D-52080 Aachen Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226) EMEA +49 800-627-3081 APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	4.90
Product Version	4.90
Date	2024-08-22
Document No.	2023-0032
Status	**PUBLISHED**

Table of Contents

1 Introduction

SecurityServer 4.90 introduces various enhancements and fixes issues found in previous releases. Please consult the following sections for details.

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.

2 Hardware platform - CryptoServer Models

The table below lists the compatible hardware platforms for this release.

Hardware 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

3 List of enhancements

This release has enhancements for an other hardware platform.

4 List of bug fixes

The following bugs were fixed in this release

Reference	Component	Issue
PHX-1822	DOC	#define CXI_KEY_ALGO_EC_EDWARDS Documentation now mentions value in hex 0x0000000B #define CXI_KEY_ALGO_X509 Documentation now mentions correct value in hex : 0x00000009 #define CXI_KEY_ALGO_X509_ATT Documentation now mentions correct value in hex : 0x0000000A
PHX-2005	FW	vrsa_pkcs1_pss_sign appears to be leaking memory
PHX-1940	FW	Audit log contains not understandable string for cmds AddUser (ECDSA user)
PHX-1823	DOC	cxi ModuleSpec CreateObj with AES did not mention 'VALUE' as mandatory
PHX-1746	CNG	Keys generated using cng tool , but cannot listed via cxitool
PHX-1708	FW	chsm-restore|full snapshot restored as data snapshot without migrate option (backward compatability))
PHX-1622	PKCS11	PKCS11 - lib can't be used anymore after an error CKR_DEVICE_REMOVED
PHX-757	CXI Java	CXI Java Sample: Inconsistent README.txt with folder content
PHX-122	PKCS11	PKCS#11 R3: Public exponent is now required when creating RSA private keys CKA_PUBLIC_EXPONENT is now a required attribute for C_CreateObject. A corresponding call without the attribute in the template is currently successful, but should return CKR_TEMPLATE_INCOMPLETE as it does if CKA_PRIVATE_EXPONENT or CKA_MODULUS are missing.
DOC-1158	DOC	CS_PD_SecurityServer_Algorithms.pdf does not list curve448/edwards448
DOC-1155	DOC	Ubuntu 18.04LTS and CentOS 7 not supported anymore
DOC-1154	DOC	Fixed documentation issue while using TCP and TLS setup via csxlan.conf
DOC-1077	DOC	RamInfoCSV, MemInfoCSV and GenRandom and now documented commands
DOC-1051	DOC	Command timeout is double as long as the set value
DOC-766	DOC	Added information about key replication
DOC-355	DOC	Improvements in PKCS11 Developper guide
DOC-56	DOC	Requirements for Linux simulator on CentOS/RHEL wrong
API-323	JCE	bug fix in rsa_pss_rsae_sha256 method

5 Known issues

The following issues are known in this release

Reference	Component	Issue
PHX-1633	cxitool	It is not possible to delete a key using the key specifier. Workaround : it is possible to use keyName to delete the key
PHX-1747	CNG	CNG config file located in C:\ProgramData\Utimaco\CNG\cs_cng.cfghas a default path which doesn't exists C:\ProgramData\Utimaco\CNG\keysas directory "keys" is missing.
OCTO-233	Driver	RHEL9.4 is currently not supported (kernel-5.14.0-427.XX.X.el9_4.x86_64). SecurityServer installation failed with kernels: ▪ kernel-5.14.0-427.26.1.el9_4.x86_64 ▪ kernel-5.14.0-427.24.1.el9_4.x86_64 Workaround: Downgrade to an earlier supported version like RHEL9.3 by setting it as new default. For example with grubby: ▪ grubby --set-default /boot/vmlinuz-5.14.0-362.13.1.el9_3.x86_64

6 Supported operating systems

The following table lists the Operating Systems supported by SecurityServer

Windows	*Version*
Windows	10 11
Windows Server	2016 2019 2022

Linux	*Version*
RHEL	8 9 *9.4 (see known issues)
SUSE LES	12 15
Ubuntu	20.04LTS 22.04LTS

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 versions of tools and libraries are not shipped with the product bundle anymore.

7 Supported Java runtime environments

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

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

8 Version and Driver (PCIe card)

All components delivered with this release now match the release number except Driver and SMOS firmware package:

The following table lists the PCIe card driver shipped with SecurityServer.

Driver	*Version*
Windows Driver	5.2.0.0
Linux Driver	5.29.0

SMOS firmware version : 4.6.14.0

9 Technical support

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

Download product information from Utimaco website[1].

Consult the Utimaco support portal[2] or find here contact information[3] to contact us via email or telephone. Please make sure to have your HSM information at hand, including your hardware serial number(s), software version number(s), operating system(s) and patch level(s), as well as the text of any error messages.

1 https://utimaco.com/products/categories/hardware-security-modules-hsm/hsms-general-purpose-use-cases/securityserver
2 https://support.hsm.utimaco.com/support
3 https://support.hsm.utimaco.com/support/contact/

10 Legal Notices

11 Older Releases 4.80

11.1 List of bug fixes- 4.80

The following bugs were fixed in this release

Reference	Component	Issue
PHX-1660	FW	Improve speed of AES-GCM
PHX-1632	FW	CMDS module specification now list I as valid attribute with meaningful explanations
PHX-1628	Host	ODBC can't overwrite existing keys
PHX-1452	Host	Connections to MS database are not getting closed/ removed
PHX-610	SDK	CS2_SDK flag removed from docs and code samples
PHX-522	csadm,FW	Loadpkg=x,forceclear hangs when trying to load the first module
DOC-999	DOC	CKK_EC_EDWARDS and CKK_EC_MONTGOMERY listed as unsupported whereas they are in the firmware/api
CM-1075	CM	Simulator 4.70 fails to start in Windows now fixed
API-323	JCE	rsa_pss_rsae_sha256 was throwing error in JCE provider

11.2 List of enhancements - 4.80

This release has enhancement for an other hardware platform.

12 Older Releases 4.70

12.1 List of bug fixes- 4.70

The following bug were fixed in this release

Reference	Component	Issue
PHX-1150	Simulator	Fixed memory allocation in Simulator
PHX-1279	SDK	SDK headers for CRYPT built with platform are missing information (cmake build)
PHX-999	SDK	CryptoServer SDK exmp_host.c does not build - Old reference to cs_xtrace
PHX-998	CXI	Fixed memory allocation error
PHX-320	cxi,cxitool	cxitool BackupKey: The same successfully imported keys cannot be backed up (error: os_mem_failed)
PHX-225	p11tool2	p11tool2 PIN-related commands: Examples in help text use deprecated 6-digit PIN
DOC-719	DOC	New paramter in CS_PKCS11_R3.cfg for ODBC reconnections
PHX-1073	EKM	cssqlekm.cfg mentions ucapi in the example for KeyStorageConfig
DOC-875	DOC	Fixed error in documentation saying ECDSA was not supported for user authentication
PHX-175	SDK	[FW] PATHDEFS in Windows make_clean.bat in SDK\... \mak
PHX-1637	P11CAT	P11CAT | Generate keypair from file' using key Templates(key_SM2) is not working
PHX-1580	SDK	CS-SDK envsetup.sh script does not work (wrong path using Linux/x86-64)
PHX-1579	SDK	CS-SDK Build exmp using make CFG=sim5 does not work on Linux
PHX-1400	p11tool2	p11tool2: Wrong Error text during setpin
PHX-1339	p11tool2	[Host] p11tool2 SetPIN wrong behavior
PHX-1242	cng	Default log path for cs_cng.cfg does not work
PHX-1019	CXI	[FW] CXI DeriveKey with ECDH_COF, SHA-256 should allow longer AES output keys
PHX-636	P11CAT	[Host] P11CAT shows wrong data type for Unique ID
PHX-532	cngtool	[Host] cngtool: No output when stdout is e.g. send through a pipe
PHX-173	cxi	[FW] cxi GenerateKeyPair: Public exponent of public template is ignored

Reference	Component	Issue
PHX-128	p11tool2	[Host] p11tool2 GenerateKeyPair: Generating a key pair with a template file and oid:secp256r1 returns CKR_CURVE_NOT_SUPPORT (while executing without a template works)
PHX-121	pkcs11	[Host] Fallback in PKCS11 R3 not working/breaks failover
PHX-117	cxitool	[Host] cxitool SelfSignedCert: Supported KeyUsage parameter is said unknown
PHX-107	pkcs11	[Host] PKCS11: Re-Initialize Slot does not delete keys in external keystore
PHX-84	pkcs11	[Host] PKCS#11 R3: Error when accessing slots with ID > 255
OCTO-148	Driver	PCIe driver: resynch after external erase

12.2 List of enhancements - 4.70

New operating systems

This version of SecurityServer 4.70 has been tested on the operating systems RHEL/CentOS 9, and Ubuntu 22.04LTS.

Versioning

Starting with this release, firmware modules and host side utilities will report the same version number as the product CD (i.e. 4.70) to ease version identification of the product.

Support of Edward curves

This release adds support of Edward curves: Ed25519 and Ed448. This release supports both variants (Pure and Pre-Hashed) with or without context data.

The schemes supported are Ed25519, Ed25519cts,Ed25519ph, Ed448, and Ed448ph.

Prevent weak mechanisms for HMAC users

If an HSM user cannot login due deprecated hash algorithms (HMAC-PBKDF with hash=MD5 or Rd160), the administrator will see an audit log entry that helps to understand the issue.

It is no longer possible to create or restore users with md5 and Rd160 hash algorithms.

13 Older Releases - 4.60.0.2

13.1 List of bug fixes - 4.60.0.2

The following issues have been resolved in SecurityServer.

Reference	Component	Issue
PHX-1150	Firmware	Fixed memory allocation error

13.2 List of enhancements - 4.60.0.2

This is a maintenance release. It only contains bug fixes.

14 Older Releases - 4.60.0.1

14.1 List of bug fixes - 4.60.0.1

This release only contains changes for another hardware platform.

14.2 List of enhancements - 4.60.0.1

This release only contains changes for another hardware platform.

15 Older Releases - 4.60

15.1 List of bug fixes 4.60

The following issues have been resolved in SecurityServer.

Reference	Component	Issue
PHX-735	CryptoServer JCE	u.trust_anchor_product_bundle CryptoServerJCE.jar shows wrong version information in MANIFEST.MF
PHX-735	CryptoServer JCE	Wrong version in CXI_JAVA and JCE sample
PHX-733	Cmds,csadm	Error in User Database changing user password after user invalid authentication attemp
PHX-835	csadm	Unexpected error trying to perform FW downgrade after installing feature that requires change of Initial ADMIN credentials
PHX-916	Csadm,pkcs11	Access cHSMs via host using the Windows driver
PHX-389	PKCS#11	PCKS#11 C_Sign: Resulting MAC has double of the expected size with CKM_AES_MAC and CKM_DES3_MAC
PHX-637	PKCS#11	PKCS #11 C_SignUpdate: C_Verify on a C_SignUpdate created signature fails (ECDSA)
PHX-560	gladm	gladm system-clear: Interruption of u.trust Anchor after repeated system-clear executions
PHX-775	CXI	cxi: Memory allocation error when encrypting several (large) files
PHX-970	SDK,vdx	vdx_host sample cannot run due to p11 initial credentials unchanged (SO, User)
PHX-934	SDK	VDX example module does not build under linux & Windows (obsolete memutil.h)
PHX-344	CryptoServer CXI	JVM crash from CP5.getchallenge and pkcs11 reports secure messaging failed
PHX-709	gladm	gladm tests failing on Windows for Release 4.55 - device_ready test
PHX-731	gladm	gladm tests failing on Windows for Release 4.55 - test_quorum_requirements_unparsable_values
PHX-704	gladm	CSAR - error CHAI_SNAPSHOT_TEMPLATE_UNAVAILABLE while cloning snapshot on v4.51.0.1
PHX-783	Csadm	csadm test for connection timeouts failing on Linux side
PHX-638	PKCS#11	PKCS#11 R3: No errorcode in C_OpenSession when err != CKR_OK
PHX-831	CAT	The I Attribute of Users Display I[$01] Instead of I[1]

Reference	Component	Issue
PHX-799	CryptoServer CXI	CryptoServerCXI: Linux CXI_Java reproducible JVM crash when ignoring timeout on session
PHX-823	cmds	Possible to add multiple users with the same long name - Shortname displayed to users
PHX-829	CAT	It is Not Possible to Get I=0 Only Using CAT
PHX-830	CAT	After Failing to Login a User with Unchanged Credentials on CAT the Connection to the Hsm is terminated
PHX-832	csadm	Load File shadow.msc visible in AuditLogs
PHX-991	PKCS#11	ucapi: Key replication error - CKR_GENERAL_ERROR when creating PKCS #11 keys on CSAR and SeXk (with multiple cHSMs configured in the configuration file)

15.2 List of enhancements 4.60

15.2.1 Replacement of Default Authentication data

No authentication can be done using the ADMIN key provided in the product CD. Customers cannot execute any commands before changing
the default credentials.

Further implications:

- Existing customers that have an ADMIN user with the default key are not impacted.
- Ready to use simulator already has a replaced ADMIN key. The key named ADMIN_SIM should be used.
- New credentials for the ADMIN user must not be same or equal to old credentials.
- It is possible to change credentials in alarm state.

- If a command does not require authentication and credentials are provided, then first the authentication takes place and it is checked if the
credentials are changed or not. If the credentials are not changed, the command execution will not take place.

15.2.2 Replacement of HMAC Authentication Data Set by Administrator

HMAC users are now required to change their password. Users cannot execute any commands without changing their password.
Further implications are:
- Existing users are not impacted. Restored users are not considered new users. However, if a new user is restored without changing
the password, then a password change is required.
- Whilst changing the password, the password cannot be same as the previous one.

15.2.3 HMAC Authentication with PBKDF

The HMAC Authentication has been replaced by the HMAC-PBKDF Authentication. This functionality is not visible externally. The iteration
count of PBKDF was chosen to lead to an authentication delay of no more than ~0.5secs. It is recommended to use keep alive sessions. The
functionality is implemented with backward compatibility, which means an older version of host software with firmware 4.60 and an older
version of firmware with software 4.60 will fall back to the old HMAC authentication. In the August release of 2024, this backward compatibility
will be deprecated as part of deprecation roadmap.

15.2.4 Reconnection to lost external key storage connection

PKCS#11 uses ODBC to connect to a database on the host side. If the connection with the database is lost, PKCS#11 did not try to re-
establish a connection. This means that the application needed to be restarted to re-establish a connection. Now, PKCS#11 tries to
automatically re-establish lost connections with the database.