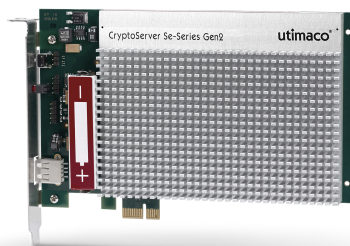


SecurityServer Se/CSe

Release Notes



utimaco[®]

Imprint

Copyright 2024	Utimatec 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 e-mail	https://support.hsm.utimatec.com/ support@utimatec.com
Document Version	6.0.0
Product Version	6.0.0
Date	2024-12-03
Document No.	2023-0032
Status	PUBLISHED

All rights reserved

No part of this documentation may be reproduced in any form (printing, photocopy or according to any other process) without the written approval of Utimatec IS GmbH or be processed, reproduced or distributed using electronic systems.

Utimatec IS GmbH reserves the right to modify or amend the documentation at any time without prior notice. Utimatec IS GmbH assumes no liability for typographical errors and damages incurred due to them. Any mention of the company name Utimatec in this documents refers to the Utimatec IS GmbH.

All trademarks and registered trademarks are the property of their respective owners.

Table of Contents

1	Introduction	5
2	Hardware platform - CryptoServer Models	6
3	List of enhancements	7
3.1	Backup and restore via csadm (From previous release to 6.0.0)	7
3.2	EdDSA support	7
3.3	Password enhancements in CAT	7
3.4	New parameter in pkcs#11 configuration file: SlotLoginRestriction.....	8
3.5	Larger key size for authentication	8
3.6	New JCE provider	8
3.6.1	New JCE provider: Benefits	9
3.6.2	New JCE provider: Supported wrap/unwrap mechanisms.....	10
3.6.3	New JCE provider: Known limitations.....	11
3.6.4	Migration from the old JCE provider.....	11
3.7	New Product Structure	12
4	List of bug fixes	13
5	Known issues	14
6	Supported operating systems	15
7	Supported Java runtime environments	16
8	Version and Driver (PCIe card)	17
9	Technical support	18
10	Legal Notices	19
11	Older Releases 4.90	20
11.1	List of bug fixes - 4.90	20
11.2	List of enhancements - 4.90	21
12	Older Releases 4.80	22
12.1	List of bug fixes - 4.80	22
12.2	List of enhancements - 4.80	22
13	Older Releases 4.70	23
13.1	List of bug fixes- 4.70	23
13.2	List of enhancements - 4.70	24
14	Older Releases - 4.60.0.2	25
14.1	List of bug fixes - 4.60.0.2	25

14.2	List of enhancements - 4.60.0.2	25
15	Older Releases - 4.60.0.1	26
15.1	List of bug fixes - 4.60.0.1	26
15.2	List of enhancements - 4.60.0.1	26
16	Older Releases - 4.60	27
16.1	List of bug fixes 4.60	27
16.2	List of enhancements 4.60	28
16.2.1	Replacement of Default Authentication data	28
16.2.2	Replacement of HMAC Authentication Data Set by Administrator	29
16.2.3	HMAC Authentication with PBKDF	29
16.2.4	Reconnection to lost external key storage connection	29

1 Introduction

SecurityServer 6.0.0 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

3.1 Backup and restore via csadm (From previous release to 6.0.0)

Database backup and user backup now include additional initialization vectors to enforce security of the backups.

Therefore, the backups are using a new format starting 6.0

Starting in 6.0, it is required

- to use `csadm backupdatabase` to backup the key database (and potentially other databases)
- to use `csadm backupusers` to backup the users

Release 6.0 still permits to use `csadm restoredatabase` to restore previous backups for backward compatibility, but this function will be disabled in later releases.

3.2 EdDSA support

In a previous release the support of EdDSA was added (4.70) to comply with the PKCS#11 3.0 standard.

In the 6.0.0 release, additional features were added to complete the full support of EdDSA as well as a migration utility.

Utimaco's utility `cxitool` now has an option to migrate keys from the old key type `CKK_EC` to `CKK_EC_EDWARDS` thus allowing users who were using the old key type in previous releases to migrate their keys to the correct key type. In future releases, the old key type `CKK_EC` will not be allowed for signing with Edward curves.

3.3 Password enhancements in CAT

When a user is logged in CAT, the user is prompted to enter the old password before providing the new password.

Admins users still have the possibility to change a user's password as before.

3.4 New parameter in pkcs#11 configuration file: SlotLoginRestriction

In previous releases of SecurityServer, the HSM was returning error messages "User already logged in" in the following cases:

- Multiple users try to login in pkcs#11 session, each user having a different role (Key Manager, Security Officers, or Crypto User)
- Multiple users try to login in pkcs#11 session, and the permission mask of these user has been greater than 2

Those restrictions were enforced to comply with pkcs#11, however in order to provide backward compatibility, the pkcs#11 configuration file now allows customer to choose whether this enforcement is necessary or not via a section [SlotLoginRestriction]

The default value is True. If set to False, the pkcs#11 library will accept multiple users or users with permission mask greater than 2 to be logged in at the same time.

3.5 Larger key size for authentication

Utimaco now ships by default a new smartcard applet (version 3.0.0)

This applet version is required to have keys greater than RSA 2048 on smartcards for user authentication.

3.6 New JCE provider

SecurityServer release 6.0.0 comes with two JCE providers.

- CryptoServerJCE: The JCE provider used in previous releases.
- SecurityServerJCE: The new JCE provider coming with this release.

The jar files have a different name to be able to differentiate them. From a java application though, the provider will be recognized as "CryptoServer" provider, thus avoiding to change anything on the application side to use the new provider.

The new JCE provider is built on UCAPI, thus it inherits load balancing and failover capabilities.

In addition, wrapping and unwrapping has been tested to be compatible with other JCE providers, such as BouncyCastle.

The Java version tested are 8,11,17, and 21.

New samples are provided in the new JCE provider directory. One sample allows testing the provider registration. The Readme file provides instruction on how to use the samples.

To use the new JCE provider

- Ensure the CLASSPATH points to the new jar file (by default, the installer points to the old JCE)
- Ensure the environment variable \$CRYPTOSERVER_JCE_CONFIG points to the correct configuration file
- Ensure your java.security only has the following line for the utimaco JCE provider: security.provider.XX=CryptoServerJCE.CryptoServerProvider (replace XX with appropriate number in sequence)
- Create the user JCE with permission 000007 (ex: csadm %auth% adduser=JCE,00000002{CXI_GROUP=*},hmacpwd,123456789), csadm logonpass=JCE,123456789 changeuser=JCE,12345678
- Run a sample: java -cp bin\samples.jar;"C:\my_path\bcprov-jdk18on-1.72.jar";..\lib\securityserver-jce.jar defaults.bench_RSA CryptoServer.cfg

3.6.1 New JCE provider: Benefits

- The new JCE provider is built on UCAPI, thus it inherits load balancing and failover capabilities.
- Compatible with the old provider (registers as CryptoServer)
- Compatible with old keys
- Supports wrap/unwrap and is compatible with BouncyCastle provider

- Support per key attributes for flag "exportable" and "plain exportable"
- Raw RSA is now supported

3.6.2 New JCE provider: Supported wrap/unwrap mechanisms

Wrapping Key	Wrapped Key	Supported transformations
RSA	ECC	<ul style="list-style-type: none"> ▪ RSA/ECB/PKCS1Padding ▪ RSA/ECB/OAEPPadding
	DES, DESede, AES	<ul style="list-style-type: none"> ▪ RSA/None/PKCS1Padding ▪ RSA/ECB/PKCS1Padding ▪ RSA/ECB/OAEPPadding
AES	DES, DESede, AES	<ul style="list-style-type: none"> ▪ AES/GCM/NOPADDING ▪ AES/CCM/NOPADDING ▪ AES/ECB/PKCS5PADDING ▪ AES/CBC/PKCS5PADDING ▪ AES/OFB/PKCS5PADDING
	RSA	<ul style="list-style-type: none"> ▪ AES/ECB/PKCS5PADDING ▪ AES/CBC/PKCS5PADDING ▪ AES/GCM/NOPADDING ▪ AES/CCM/NOPADDING ▪ AES/OFB/PKCS5PADDING
	ECC	<ul style="list-style-type: none"> ▪ AES/ECB/PKCS5PADDING ▪ AES/CBC/PKCS5PADDING ▪ AES/GCM/NOPADDING ▪ AES/CCM/NOPADDING ▪ AES/OFB128/PKCS5PADDING
3DES	DES, DESede, AES	<ul style="list-style-type: none"> ▪ DESede/ECB/PKCS5PADDING ▪ DESede/CBC/PKCS5PADDING

	RSA	<ul style="list-style-type: none"> ▪ DESede/CBC/PKCS5PADDING
	ECC	<ul style="list-style-type: none"> ▪ DESede/CBC/PKCS5PADDING

3.6.3 New JCE provider: Known limitations

- Supports only 1-tier certificate chain. This will be improved in later releases.
- Edward keys, ECDH and ECIES are not yet supported.
- No automatic storage of the public key when the private key is stored after the key pair generation.
- Limitation on failover when reading and writing keys. A patch is available to overcome limitation while reading keys. limitation of failover when writing keys will be addressed in later release.

3.6.4 Migration from the old JCE provider

The table below summarizes the compatibility of old and new JCE providers.

Key coming from the OLD JCE provider	Capabilities using the NEW JCE provider:
Key was generated in old JCE provider	<p>Keys are usable in new provider as before: 3DES, AES, RSA, ECC</p> <p>Keys are wrappable in the new provider: (RSA private keys, ECC private keys, 3DES and AES symmetric keys)</p> <p>Note: the function GetEncoded()</p> <ul style="list-style-type: none"> ▪ Does not work with ECC public keys ▪ Works with RSA public keys ▪ Works with 3DES/AES keys if key flag PLAIN EXPORTABLE is set ▪ Is not supported for privatekeys

<p>Key was imported in old JCE provider via keyfactory (plaintext)</p>	<p>AES, RSA, ECC, 3DES keys are usable in new provider</p> <p>3DES, AES, ECC keys are wrappable in the new provider</p> <p>RSA keys are NOT wrappable in the new provider. RSA keys, in order to be wrappable in the new provider, must be reimported, or newly generated in the new provider.</p>
<p>Key was imported in old provider via unwrapping</p>	<p>It is not possible to unwrap in the old provider since unwrap mechanisms are proprietary in the old provider.</p>

3.7 New Product Structure

The CD structure has been updated

- All user documentation is now in the folder named "Documentation"
- The admin, user guide, and operational guides for Segen2/CSe and u.trust Anchor Se are in separate folders
- There is an additional folder for FIPS documentation.

4 List of bug fixes

The following bugs were fixed in this release.

This list is not exhaustive and only indicates issues relevant to customers.

Reference	Component	Issue
PHX-2252	HOST	Secure messaging error reported while using multiple threads in CNG or JCE
PHX-2232	HOST	Cxtool help text fixed for generating EdDSA keys
PHX-2159	HOST	Csadm help mention only up to 4 MBK whereas it actually supports up to 256 (in MBK slot 0 .. 255)
PHX-1988	Host	C_GetMechanismList() now list EdDSA curves
PHX-1911	Host	SetMaxAuthFails command now logs FC in audit logs
PHX-1895	Host	When overwriting an existing key in external keystore the flag overwrite was ignored when the key has same name and spec
PHX-1888	Host	Fixed an error in internal MAC calculation
PHX-1845	FW	Correct error codes and transitions for user authentication
PHX-1736	Host	PKCS#11 config file is now parsed correctly when all devices are specified with carriage return
PHX-1671	FW	Fixed memory leak
PHX-1669	Host	Fixed issue with C_CopyObject which occurred while copying a session object to a persistent object (CKA_TOKEN=true)
PHX-1633	Cxtool	Fixed an issue which prevents to delete a key using key specifier
DOC-1282	DOC	Fixed wrong list of eddsa curves in documentation
DOC-1242	DOC	Fixed errors in documentation where PCI:0 was mentioned instead of PCI:0.x
DOC-1172	DOC	Fixed error in manual for set-time command, to be after changing default user credentials
DOC-1169	DOC	Fixed a wrong keyname in command example
DOC-1159	DOC	Improved driver installation steps
DOC-83	DOC	Behavior of SetGlobalconfig and SetSlotConfig is clarified

5 Known issues

The following issues are known in this release

Reference	Component	Issue
PHX-1747	CNG	CNG config file located in C:\ProgramData\Utimaco\CNG\cs_cng.cfg has a default path which does not exist. C:\ProgramData\Utimaco\CNG\keys as 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> grubby --set-default /boot/vmlinuz-5.14.0-362.13.1.el9_3.x86_64 The issue is apparently known for RHEL 9.4 and appears to be fixed in later version of RHEL 10.x
EGL-538	Host	When windows goes to hibernate mode and is awoken, it is not possible to establish a connection with the HSM - a reboot is required.
PHX-2402	Host	Restoring keys back and forth between internal and external storage, combined with new keys generated in the internal storage can cause restore issues.
PHX-2515	Host	Restoring keys back and forth between internal and external storage, combined with new keys generated in the external storage can cause restore issues.
PHX-2387	FW	CKM_DES3_RETAIL_MAC resolves to UNKNOWN in the logs.

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.

<i>Java Runtime Environment</i>	<i>Version</i>
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.

<i>Driver</i>	<i>Version</i>
Windows Driver	5.2.0.0
Linux Driver	5.32.0

SMOS firmware version for CSe: 4.7.0.0

SMOS firmware version for Segen2/Simulator : 5.7.0.0

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

Copyright © 2024 Utimaco IS GmbH. All rights reserved.

All trademarks and registered trademarks are the property of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms, or you otherwise have the prior permission in writing of the copyright owner.

11 Older Releases 4.90

11.1 List of bug fixes - 4.90

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	vrrsa_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

Reference	Component	Issue
DOC-355	DOC	Improvements in PKCS11 Developer guide
DOC-56	DOC	Requirements for Linux simulator on CentOS/RHEL wrong
API-323	JCE	bug fix in rsa_pss_rsae_sha256 method

11.2 List of enhancements - 4.90

This release has enhancements for an other hardware platform.

12 Older Releases 4.80

12.1 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

12.2 List of enhancements - 4.80

This release has enhancement for an other hardware platform.

13 Older Releases 4.70

13.1 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,cxtool	cxtool 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_SUPPORTED (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

13.2 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, Ed25519ctx, 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.

14 Older Releases - 4.60.0.2

14.1 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

14.2 List of enhancements - 4.60.0.2

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

15 Older Releases - 4.60.0.1

15.1 List of bug fixes - 4.60.0.1

This release only contains changes for another hardware platform.

15.2 List of enhancements - 4.60.0.1

This release only contains changes for another hardware platform.

16 Older Releases - 4.60

16.1 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 attempt
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	PKCS#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)

16.2 List of enhancements 4.60

16.2.1 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.

16.2.2 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.

16.2.3 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.

16.2.4 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.