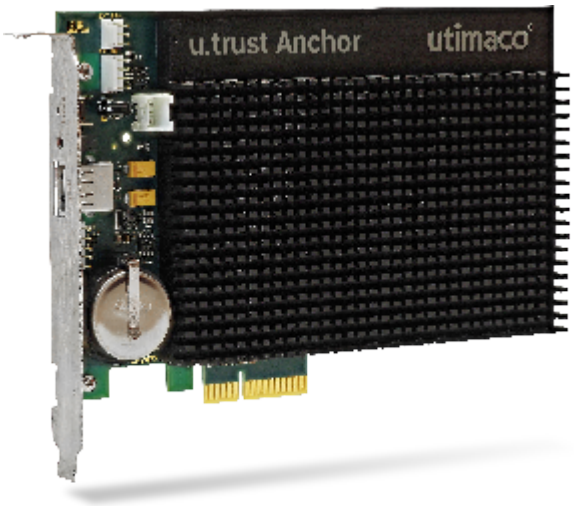
Security Server u.trust Anchor

Release Notes



utimaco®

Imprint

Copyright 2025	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	working version
Product Version	6.0.1 FIPS
Date	2025-03-21
Document No.	2024-0002
Status	**PUBLISHED**

Table of Contents

1 Introduction

SecurityServer 6.0.1 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

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

Hardware model	*Hardware platform*
SE100 PCIe SE2K PCIe SE5K PCIe	u.trust Anchor PCIe card 7.03.0.3
SE15K PCIe SE40K PCIe CSAR (standard/plus/premium) PCIe	u.trust Anchor PCIe card 7.03.0.3
SE15K LAN SE40K LAN CSAR (standard/plus/premium) LAN	CryptoServer LAN V5, UTISYS003-AC, 19“ / 1U housing; redundant power supply, integrated u.trust Anchor PCIe card V7.03.00.03
SE100 LAN SE2K LAN SE5K LAN	CryptoServer LAN V5, UTISYS003-AC, 19“ / 1U housing; redundant power supply, integrated u.trust Anchor PCIe card V7.03.00.03

3 List of enhancements

3.1 FIPS certification 140-3 Level 3

Release 6.0.1 is being submitted to NIST for FIPS 140-3 Level 3 certification. It is not certified yet but the process in ongoing.

Please refer to chapter "Older release - 6.0.0 - List of enhancement" to get all information related to specificities of this release and FIPS compliance

3.2 CKM_SHA256

The following 2 mechanisms CKM_SHA256_HMAC and CKM_SHA256_HMAC_GENERAL

were usually used in pkcs#11 with a generic secret pkcs#11 object.

It is now possible to use those signing mechanisms with AES key in the API.

PHX-2578	PKCS11	PKCS #11: CKM_SHA256_HMAC (with generic secrets or AES keys)
PHX-2577	PKCS11	PKCS #11: CKM_SHA256_HMAC_GENERAL (with generic secrets or AES keys)

3.3 AES CTR blocked in FIPS mode

AES CTR is blocked in CXI to comply with FIPS 140-3 requirement (in FIPS and FRA mode only).

3.4 AES-GCM

The C_Encrypt function with AES-GCM and internal IV in now compatible with pkcs#11 v2.40.

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-2133	SDK	SMOS: Function os_mem_get_type was returning -1 for stacks in secure RAM.
EGL-790	SDK	eca_dp_find_oid / ecdsa_key_gen now returns the correct values instead of error 0xB00A800E
PHX-2729 EGL-780 EGL-581 PHX-2728	SDK DOC	RSA Key Generation - if Exponent length is greater modulus length now returns the correct error message Documentation updated accordingly
API-1216	JCE2	Wrong hash computation with update when offset greater than zero
API-995	JCE2	ECC key imported from keyfactory via JCE then wrapped, was not working when importing in SUNJCE
API-1121	JCE2	The java app returns an error when the key is wrapped the second time
API-990	JCE2	An exception (KEYSTORAGE_INVALID_STORAGE_ID = 0xb9080005) is thrown when a key is generated in a ECDH key agreement.
API-1066	JCE2	UCAPI and JCE now have the same log levels

5 List of 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 exists C:\ProgramData\Utimaco\CNG\keysas directory "keys" is missing.
EGL-507	FW	After using gladm system-fetch-log the HSM returns an error message that should not be present: "Failed to write CPU temperature to SMBUS"
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 The issue is apparently known for RHEL 9.4 and appears to be fixed in later version of RHEL 10.x Note : This is fixed in a more recent version of securityServer release
PHX-2212	SDK	There is no NVRAM available on u.trust Anchor. Therefore when loading files into NVRAM (for example via csadm command), the file is actually loaded into flash.
EGL-538	HOST	When windows goes to hibernate mode and is awaken, it is not possible to establish connection with the HSM - a reboot is required.
PHX-2090	GLADM	gladm system-restart should work locally and remotely. But currently this command only works remotely Example: ▪ gladm -d /dev/cs2.0 $auth system-restart doesn't work. ▪ gladm -d 192.168.140.146 $auth system-restart : works To restart the driver locally, either use gladm device-restart Or alternatively echo "REBOOT" > /proc/driver/cs2.0

Reference	Component	Issue
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. Note : This is fixed in a more recent version of securityServer release
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 Note : This is fixed in a more recent version of securityServer release
PHX-1777	GLAD	If some Utimaco default modules are deleted in a container, they will reappear when the snapshot is restored. A workaround is to delete the modules manually if not needed.
PHX-2212	FW	Loading files in nvram should return an error. Note : This is fixed in a more recent version of securityServer release
PHX-2211	CSADM	loadFwDecKey is not working. It is currently blocked. Note : This is fixed in a more recent version of securityServer release
PHX-2478	FW	csadm settime allows to set a delta between the time of a cHSM and the hypervisor (to adjust the time, timezone etc.). This delta is lost when the cHSM is restarted.
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.

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 the Driver)

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

Driver	*Version*
Windows Driver	5.2.0.0
Linux Driver	5.32.0

9 Technical support

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

Download product information from the 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 Release - 6.0.0

11.1 List of enhancements - 6.0.0

11.1.1 FIPS certification 140-3 Level 3

Release 6.0.0 is being submitted to NIST for FIPS 140-3 Level 3 certification. It is not certified yet but the process in ongoing.

The release 6.0 contains two firmware images which are packaged with a different list of templates. The templates in the two images are built from the same source code.

Image 1 templates :	*Image 2 templates :*	*Description*
SecurityServer	SecurityServer	Standard firmware
SecurityServer-FIPS	SecurityServer-FIPS	Standard firmware that applies the restriction required by NIST to comply with FIPS 140-3 Level 3
SecurityServer-SDK	-	Standard firmware, allows to load custom code
SecurityServer-FIPS-SDK	-	Standard firmware that applies the restriction required by NIST to comply with FIPS 140-3 Level 3 and allows custom code to be loaded

Depending on the list of available templates, the information returned by the hypervisor (GLAD) and the cHSMs in regards to the FIPS status may change to reflect accurately the status of the HSM configuration and compliance.

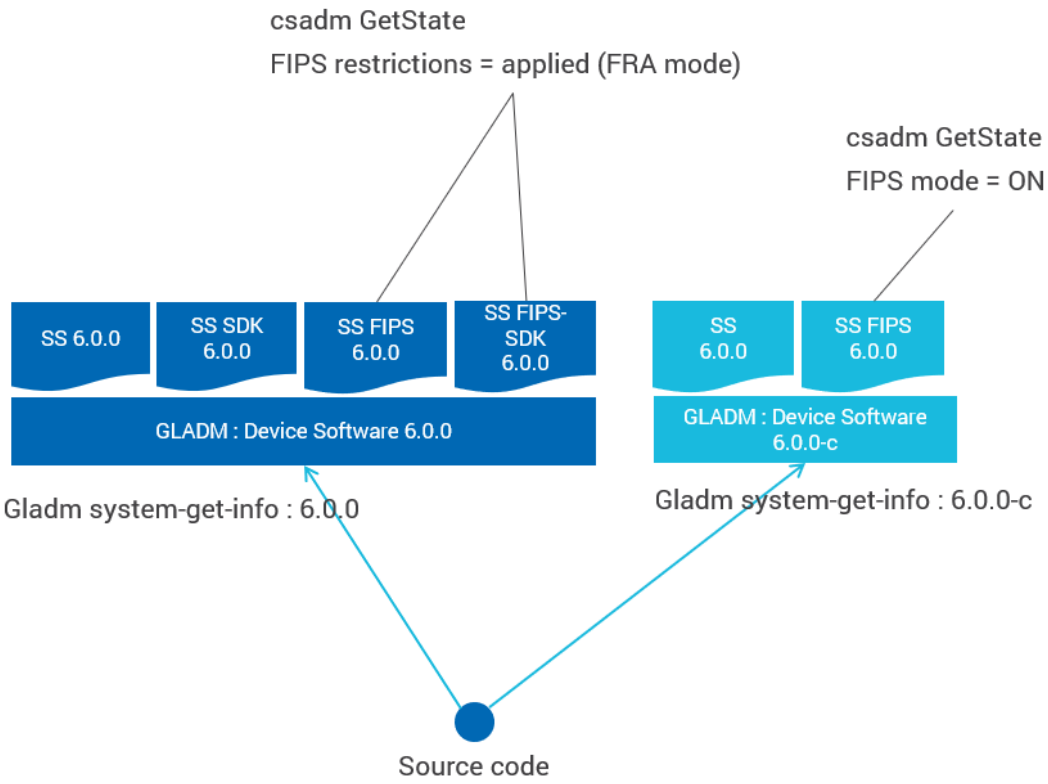
11.1.1.1 Identification via hypervisor (via gladm command)

The SDK template is not permitted by FIPS since they allow to load custom code. Therefore the hypervisor will differentiate images that are strictly compliant to FIPS by appending a suffix '-c' to its version number.

11.1.1.2 Identification in cHSM (via csadm command)

Depending on whether the suffix '-c' is present, the cHSM will either return "FIPS mode = ON" or "FIPS restriction = applied" as soon as the FIPS restrictions are present in the cHSM template.

See the below picture for a summary of templates, images and indications on the FIPS status.



11.1.1.3 Certification status

Strict FIPS compliance is achieved only when the three conditions are fulfilled:

- The HSM is operated with firmware image 6.0.0
- The Hypervisor (glad) outputs suffix -c via gladm system-get-info
- The cHSM outputs "FIPS Mode = ON" via csadm GetState

In addition to the above the following information must be checked via gladm system-get-information

- Sensory controller is in version 3.02.0.8
- Hardware revision number : 7.03.0.3

Finally, ensure the corresponding information on NIST website are valid.

At the moment this release is being submitted to NIST, and there is no certificate yet.

11.1.1.4 FIPS restriction = applied

Available for customers who need to load custom modules on an HSM that runs a version identical to FIPS, but not strictly, as additional code must be loaded.

A cHSM with FIPS restriction will return "FIPS Mode = ON" when GLAD returns -c

A cHSM with FIPS restriction will return "FIPS restriction = applied" when GLAD doesn't return -c

11.1.2 Transition from non-FIPS to FIPS

In order to switch from a non-FIPS certified release to a FIPS-certified release, NIST requires the end user to perform a zeroization of the key material. Therefore when switching for example from 6.0.0 ↔ 6.0.0-c the end user must

- Short press external erase (<3s).
- Wait for reboot (~1min).
- Type `gladm system-clear` to erase all users and keys.
- Set up the HSM again.
- Instantiate the container and restore keys and users.

11.1.3 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, as required by NIST.

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 of users, for backward compatibility, but this function will be disabled in later releases.

When an old backup format is used and restored in 6.0, the cHSM will restore the data and re-encrypt them including a new IV.

11.1.4 Backup and restore via csadm (From previous release to 6.0.0 FIPS container)

FIPS does not accept restoring keys with a 0-IV. If you want to backup from an older version (non FIPS container) and restore into FIPS container, you have to

- Backup your old container / from your old version
- Restore the databases into a non-FIPS container 6.0.0(-c) this will generate the required IV)
- Backup from the non-FIPS container and restore into the FIPS container.

11.1.5 Backup and restore via snapshot (From previous release to 6.0.0)

A Snapshot taken in a previous release can be restored in 6.0.

A snapshot of a template type can only be restored on a template of the same type (for example a SecurityServer cannot be restored as SecurityServer-FIPS), as this is required by certification.

A snapshot can only be restored in a version equivalent or greater than its current version (no downgrade possible).

11.1.6 Backup and restore via snapshot (From previous release to 6.0.0 FIPS container)

A snapshot of a template type can only be restored on a template of the same type (for example a SecurityServer cannot be restored as SecurityServer-FIPS), as this is required by certification.

If you have a snapshot from an older version and a template that is non FIPS (SecurityServer template), and you want to migrate to the FIPS template:

- restore you snapshot on 6.0.0 using the same template
- backup your users and keys via csadm backupdatabase and csadm backupusers
- restore your users and keys via csadm into the FIPS container
- snapshot the FIPS container

11.1.7 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.

11.1.8 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.

11.1.9 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.

11.1.10 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.

11.1.11 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

11.1.11.1 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

11.1.11.2 New JCE provider: Supported wrap/unwrap mechanisms

Wrapping Key	Wrapped Key	Supported transformations
RSA	ECC	▪ RSA/ECB/PKCS1Padding ▪ RSA/ECB/OAEPPadding

	DES, DESede, AES	▪ RSA/None/PKCS1Padding ▪ RSA/ECB/PKCS1Padding ▪ RSA/ECB/OAEPPadding
AES	DES, DESede, AES	▪ AES/GCM/NOPADDING ▪ AES/CCM/NOPADDING ▪ AES/ECB/PKCS5PADDING ▪ AES/CBC/PKCS5PADDING ▪ AES/OFB/PKCS5PADDING
	RSA	▪ §AES/ECB/PKCS5PADDING ▪ AES/CBC/PKCS5PADDING ▪ AES/GCM/NOPADDING ▪ AES/CCM/NOPADDING ▪ AES/OFB/PKCS5PADDING
	ECC	▪ AES/ECB/PKCS5PADDING ▪ AES/CBC/PKCS5PADDING ▪ AES/GCM/NOPADDING ▪ AES/CCM/NOPADDING ▪ AES/OFB128/PKCS5PADDING
3DES	DES, DESede, AES	▪ DESede/ECB/PKCS5PADDING ▪ DESede/CBC/PKCS5PADDING
	RSA	▪ DESede/CBC/PKCS5PADDING
	ECC	▪ DESede/CBC/PKCS5PADDING

11.1.11.3 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

11.1.11.4 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	Key are usable in new provider as before: 3DES, AES, RSA, ECC Keys are wrappable in the new provider: (RSA private keys, ECC private keys, 3DES and AES symmetric keys) Note: the function GetEncoded() ▪ Doesn't 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
Key was imported in old JCE provider via keyfactory (plaintext)	AES,RSA,ECC, 3DES keys are usable in new provider 3DES,AES,ECC keys are wrappable in the new provider 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.
Key was imported in old provider via unwrapping	It is not possible to unwrap in the old provider since unwrap mechanisms are proprietary in the old provider.

11.1.12 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.

11.2 List of bug fixes - 6.0.0

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	Cxitool help text fixed for generating EdDSA keys
PHX-2159	HOST	Csadm help mentions 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 existing key in external keystore the flag overwrite was ignored when the key has the 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	Cxitool	Fixed an issue which prevents to delete a key using key specifier
DOC-1282	DOC	Fixed wrong list of eddsa curves in documentation
DOC-1262	DOC	NTP module is managed at gladm level on u.trust Se HSM. Therefore the NTP module is no longer mentioned in cHSM manuals
DOC-1249	DOC	slot-set-quota and slot-get-quota were missing in the Administration Manual

Reference	Component	Issue
DOC-1242	DOC	Fixed errors in documentation where PCI:0 was mentioned instead of PCI:0.x
DOC-1175	DOC	Clarified the steps top bring HSM into factory state via external erase and system clear.
DOC-1172	DOC	Fixed error in manual for set-time command, to be after changing default user credentials
DOC-1171	DOC	Fixed a wrong output of chsm-create command
DOC-1169	DOC	Fixed a wrong keyname in command example
DOC-1168	DOC	Fixed error in command example of user-change-credential
DOC-1159	DOC	Improved driver installation steps
DOC-83	DOC	Behavior of SetGlobalconfig and SetSlotConfig is clarified
OCTO-250	Driver	Driver installation fails on ubuntu 20 / kernel 5.15.0-119-generic

11.3 List of known issues - 6.0.0

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 exists C:\ProgramData\Utimaco\CNG\keysas directory "keys" is missing.
EGL-507	FW	After using gladm system-fetch-log the HSM returns an error message that should not be present: "Failed to write CPU temperature to SMBUS"

Reference	Component	Issue
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 The issue is apparently known for RHEL 9.4 and appears to be fixed in later version of RHEL 10.x
PHX-2212	SDK	There is no NVRAM available on u.trust Anchor. Therefore when loading files into NVRAM (for example via csadm command), the file is actually loaded into flash.
EGL-538	Host	When windows goes to hibernate mode and is awaken, it is not possible to establish connection with the HSM - a reboot is required.
PHX-2090	gladm	gladm system-restart should work locally and remotely. But currently this command only works remotely Example: ▪ gladm -d /dev/cs2.0 $auth system-restart doesn't work. ▪ gladm -d 192.168.140.146 $auth system-restart : works To restart the driver locally, either use gladm device-restart Or alternatively echo REBOOT > /proc/driver/cs2.0
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-1777	GLAD	If some Utimaco default modules are deleted in a container, they will reappear when the snapshot is restored. A workaround is to delete the modules manually if not needed.
PHX-2212	FW	Loading files in nvram should return an error.
PHX-2211	csadm	loadFwDecKey is not working. It is currently blocked. It will be enabled in an upcoming release.

Reference	Component	Issue
PHX-2133	FW	Function os_mem_get_type returns -1 when allocating memory.
PHX-2448	FW	csadm settime allows to set a delta between the time of a cHSM and the hypervisor (to adjust the time, timezone etc.). This delta is lost when the cHSM is restarted.
PHX-2387	FW	CKM_DES3_RETAIL_MAC resolves to UNKNOWN in the logs.

12 Older Release - 4.47.3

12.1 Older Release - 4.47.3 - Information

SecurityServer 4.47.3 is a special release, allowing to update the image signing key and upgrade to further release 6.0.x

Once an HSM is upgraded to 4.47.3, it will start using the new ISK (image signing key). Therefore it is not possible to downgrade back to previous release. The only way forward is to upgrade to later release 6.0.x.

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.

12.2 List of enhancements - 4.47.3

There aren't any enhancements in this release.

12.3 List of bug fixes - 4.47.3

There aren't any bug fixes in this release

12.4 List of known issues - 4.47.3

There aren't any known issues in this release.

13 Older Release - 4.47.2

13.1 List of enhancements - 4.47.2

This release only contains bug fixes.

13.2 List of bug fixes - 4.47.2

The following bugs were fixed in this release.

Reference	Component	Issue
EGL-501	FW	Acceleration ship is sometimes not detected correctly

14 Older Release - 4.47.1

14.1 List of enhancements - 4.47.1

New image signing key

A new signing key has been introduced on the u.trust Anchor HSM. The purpose is to enhance security by using a new key with greater length and elliptic curves. The new signing key is NIST512.

This ISK (image signing key) is specific to this release covered by the FIPS certification. It is therefore not possible to upgrade/downgrade from/to that release to a newer or older version. This will be possible when the next FIPS-certified release will be available.

14.2 List of bug fixes - 4.47.1

The following bugs were fixed in this release.

Reference	Component	Issue
PHX-1188	Host	Backport of HSM-11554 : fix issue related to load balancing
PHX-1187	Host	Backport of HSM-1114 : When a session is closed (Cluster::logout_all) and a device is not reachable, an exception is logged and the logout stops, i.e. not all sessions to all devices are closed.
PHX-1186	Host	Backport of HSM-11301 : wrong PKCS#1 v1.5 or PSS padding at least when creating signatures with mechanisms CKM_SHA*_RSA_PKCS and CKM_SHA*_RSA_PKCS_PSS.
PHX-1185	Host	Backport of HSM-11591 : Fix incorrect signature with RSASSA-PSS {SHA256:{MGF1;SHA256}
PHX-1184	Host	Backport of HSM-11795 : Fix issue with key derivation including KDF flag
PHX-1183	FW	Backport of HSM-11620 : during certificate chain verification in secure messaging handshakes, a subject-issuer mismatch is detected and the verification fails.
PHX-1182	FW	Backport of HSM-12609 : Fix problem with function CopyObject (modifies key cache)
PHX-1180	cxitool	Backport of HSM-11934 : cxitool key group visible to non-group member
PHX-1175	FW	Backport of HSM-11731 : cxitool: fails in signature verification