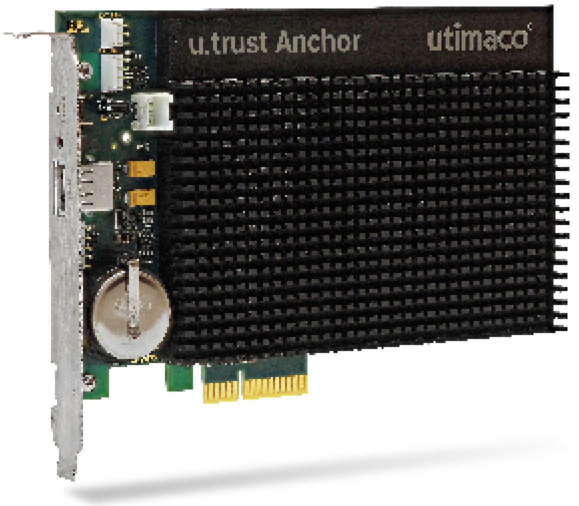
Security Server u.trust Anchor

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	6.2
Product Version	6.2
Date	2025-07-09
Document No.	2023-0031
Status	**PUBLISHED**

Table of Contents

1 Introduction

SecurityServer 6.2 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 - u.trust Anchor models

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	u.trust Anchor PCIe card 7.03.0.3
SE15K LAN SE40K 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 New Setup state

This change is a step needed in order to support different configuration modes operating in u.trust Anchor.

The device has now a new command, namely device-setup, which is used to bring the device from a setup state to an operational state. When u.trust Anchor is in a factory state, it starts with an initial admin and GIAK and is in setup state. In this state, the device operates with restrictions, allowing only a small set of commands to be executed (currently, the same ones that were allowed with GIAK). Then, to go to an operational state, the command device-setup -o must be executed (and all administrators must have the GIAK replaced by a GAAK).

The main point of the command is the following:

- It is possible to replace the initial admin by an initial set of admins (using the -n and -u options). This allows to create multiple users still in setup state (to in the future set a device configuration or if the device is under dual control).
- It is possible to replace the GIAK by the GAAK and still be in a setup state (which is required to in the future set a device configuration).

As the device configuration is yet to be done and users might want to be in an operational state with a single command (as now), instead of calling user-change-credentials to replace the GIAK by a GAAK, bringing the device to an operational state is possible by executing: device-setup -o -k=<token> .

3.2 Configurable Secure RAM size quota per cHSM

Currently, all cHSMs/slots have a share of 256 kb of secure RAM. This is to allow cHSMs to be instantiated in the 31 available slots given the total amount of secure RAM available for cHSMs. With this new feature, the amount of secure RAM of the slot can be configured from 256 kb to 4 MB (in intervals of 256 kb) via gladm slot-set-quota. cHSMs can be created in the slots as long as the limit of cHSMs allowed in the license file is satisfied and the sum of secure RAM of occupied slot does not exceed 8 MB (maximum of secure RAM for cHSMs).

The amount of used/free secure RAM can be seen either via csadm RamInfo and the amount of secure RAM that is not allocated to cHSMs can be seen via gladm-system-get-metrics with the new metric csar_chsm_smem_free_bytes_total.

3.3 Enhanced load balancing and key replication

This feature (available for pkcs#11 provider) is the first step towards making the broadcast mechanism of state changing command more resilient. Currently, when a state changing command is executed (generation of new key, or user for example) it requires all cHSM in the cluster to be available.

It is now possible to determine the behavior of the mechanism. It has two configurations:

- SynchornizationOnline = Enforced | Relaxed: the synchronization online configuration allows to choose what happens when the state-changing command is being executed. In Enforced mode, there is a checking of the status of each device in the cluster (if it is it up and running, and reconnects if needed) and then the command is executed in every device. If there is at least one device offline, the command is not executed. There might be a slight performance impact because of this status checking to avoid the cluster to be out of sync. In Relaxed mode, the devices that are offline are skipped, to possibly be synchronized later (but there are still attempts to reconnect to known failed devices).
- SynchornizationOffline = Backups | None. In case of the Relaxed mode, the cluster could be be out of sync. In this case, the synchronization offline configuration allows to choose if/how to bring the device back to a synchronized state. With the Backups option, when the device is offline, a list of created/updated/deleted user and key entries is maintained, and when the device is back online, another device that is in a synchronized state has these entries backed up and restored into the device that was offline. For the Backups option, it is necessary to have an administrator configured in the PKCS #11 configuration file (AutoLogin). The None option, as the name says, does nothing to synchronize out of sync devices, and it is not recommended to be used with the Relaxed mode.

The default options are Enforced and None.

Failures that cannot be recovered are logged with error and throw an exception, while failures that can be recovered are logged with warning. All log entries related to cluster synchronization have the same prefix [ClusterSync] to enable automated log analysis.

3.4 Improvements to in field license updates

Displaying the AcceleratorCredits in the gladm system-get-license-info command, so that it is possible to distinguish the products Se2k and Se15k, because both will have the same product name (u.trust Anchor) and the same number of cHSMs.

Throwing an error in case a wrong license file was issued.

Changing the name of a product with corrupted license file to “Device Unlicensed”, because if there is no license file, the product can be any.

3.5 FIPS simulator

This release contains a package allowing customers to emulate FIPS restriction in the Utimaco's HSM simulator.

3.6 JCE log enhancements

JCE provider can now log into multiple files The parameters are the following :

Parameter	***Description***	***Default***
LogFile	The base name for log file paths, both JCE logs and ucapi logs. For JCE logs, log file names will include a number (starting with zero) before the extension defined in the base name (e.g. logfile.0.log, logfile.1.log, ... for logfile.log) to distinguish log files that are rotated. For ucapi logs, the log file name will include a suffix (-ucapi) before the extension defined in the base name for the main log file, and an additional suffix (.bak) for the secondary rotating log (e.g. logfile-ucapi.log and logfile-ucapi.log.bak for logfile.log).	-
LogNumberFiles	The number of files in which the JCE logs will rotate.	2
LogSizeUcapi	Maximum log file size in bytes for ucapi log files. If not present, LogSize will be used for ucapi logs.	10000

JCE now also support jul-to-slf4j bridge so that JCE logs can be managed by other Java logging frameworks (such as log4j or logback).

3.7 JCE enhancements to multithreading

Added support for configurable OS locking, thus improving resilience for multithreaded scenarios (similar to PKCS#11 api)

3.8 Other enhancements

Reference	Component	Issue
PHX-2778	PKCS11	Minimal example of using multiple threads in PKCS #11
PHX-2400	GLAD	gladm system-monitor: new command to display battery metrics, (these metrics are in system-get-metrics too) but this command does not require authentication, so it can be executed even when the device is in setup state/with GIAK.
PHX-2549 PHX-2450	cxitool	cxitool sign/verify supporting EdDSA signature schemes (Ed25519, Ed448, Ed25519 and Ed448ph).
PHX-3015	SDK	The fields family/serial/crc of the EID of the UTIL module was before a virtual serial number of the hardware (this is not Utimaco's serial number!). Now, it shows a unique serial number linked to the hardware. This serial number can be access via SDK code. Utimaco's serial number is still only available via gladm system-get-info
PHX-1777	GLAD	gladm chsm-restore in the same firmware version now does not re-introduce deleted modules. Previously, the snapshot did not contain information about deleted modules in the snapshot. Now, when restoring a snapshot in the same firmware version, these modules remain deleted. Note that when upgrading, the modules are back again as it is not possible to distinguish modules that were deleted and new modules that were introduced in the new firmware version.
PHX-2723	CSADM	csadm gives a warning if the order of the chain of trust certificates is incorrect (and then the chain of trust will not be verified). Before, this was a silent error.
PHX-2559 PHX-2561	CXITOOL	The command cxitool KeyMigration has now the option GenerateUUID, which generates UUID to all keys in the database that do not contain an UUID (legacy keys). The UUID is generated for all keys that the authenticated user has permission to manage.

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-2699	CXITOOL	Before, the parameter timeout in cxitool was ignored if not set as first parameter. Now an error is thrown to indicate the incorrect syntax.
PHX-2772	FW	SecurityServer crashed if C_Sign was called with mechanism CK_RSA_PKCS_PSS_PARAM and salt length = 0.
PHX-2923	CSADM	csadm Restart did not work remotely using smartcard authentication (csadm restart=:cs2:AUTO:USB0). .
PHX-2904	FW	RSA Bulk Signing had performance decrease, in the new release the issue has been fixed.
PHX-2851	SDK	aes_gcm_data had a memory leak if it is being called with more than 64k (1024*64) bytes at once.
PHX-2754	FW	gladm device-restart without -d (device) caused segmentation fault.
PHX-2477	SDK	vdx_mdl example had warning during compilation (and were removed).
PHX-2394	CNG	CNG API crashed when the simulator or HSM became unavailable.
PHX-3052	FW	Failed device part of load balancing and failover in PKCS #11 was shown as successfully reconnected when the phisical device was reachable but the cHSM was not. The log message has been changed to “Unauthenticated connection re-established to <device>".
PHX-3017	PKCS#11	In PKCS #11, when the EdDSA signature schemes Ed25519ph, Ed25519, and Ed448ph were used, the parameters were not sent to the firmware, leading to the firmware to execute Ed25519 or Ed448 instead. For pre-hash, it was assumed the pre-hash part was done by the client application, which is not fully compliant with the standard. This was also changed in 6.2 to do the pre-hashing on the host (PHX-3164).
PHX-3027	PKCS#11	Calling PKCS #11 C_GetInterface without initializing the pointer of the parameter of ppInterface leads to a segmentation fault (scenario of the integration with p11-kit > v0.25). The segmentation fault was fixed.
PHX-3204	CAT	The functionality to reboot CSLAN via CAT (or csadm) caused a crash when triggering reboot using AuthReset = 1 in CSLAN.

Reference	Component	Issue
PHX-1893	CAT	CAT showed HSM restart as successful if it was not successful because the return value was not being displayed.
PHX-3205	CAT	Permissions of users can be in the range 0-F for each group. If a user had a permission for a group between A and F, this user could successfully login in CAT, but when executing commands, errors occurred (the authentication failed).
PHX-3095	HOST	When executing concurrent key generation (mainly via PKCS #11), due to a collision of group and specifier, the concurrent key generation (while executing key replication) fails. This occurs only if keys are stored in the HSM.
PHX-1448	CSADM	csadm Restart with a local card on Windows failed.
API-1548	JCE	When performing an "unwrapKey" operation and the transport key is "Legacy" then a "record not found" error was returned.
API-1403	JCE	Errors and coredumps (SIGSEGV) occur randomly when the number of threads and cHSMs is under very high load for long enough duration. Fixed
API-1351	JCE	optimized memory consumption for some MAC classes
API-1274	JCE	removes a timestamp present in the logfiles for backward compatibility with old JCE provider
API-1132	JCE	There is now an explicit way to call for delete and release memory of ephemeral keys, thus avoiding increasing memory consumption when creating a huge amount of keys.
API-1013	JCE	Fixed an issue EXCEPTION_ACCESS_VIOLATION with native memory (parameter NoNativeGC=true)

5 List of known issues

The following issues are known in this release:

Reference	Compone nt	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"
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 OCTO-252	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-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.
PHX-2969	SDK	vdx_mdl Example: Example SDK modules do not compile due to the need of internal headers
PHX-3252	CSADM	csadm RestoreUser: Shortname causes issues
HSM-1545 5	EKM	EKM sometimes does not load on windows 2019 and MSSQL 2019 and shows errors.
PHX-2992	FW	In FIPSmode 1 key can have only 1 padding type. This is no longer applicable as NIST relaxed this restriction. Will be fixed in next release.
API-996	JCE	Error with keytool when JCE is located in path with whitespaces
QA 905	DRIVER	Error messages are thrown while compiling the driver on RHEL 8.10 ,Ubuntu 20, Windows 11 and Windows 2016. The issue only occurs with the PCI express version of the HSM and the operating system mentioned above. The issue has already been fixed. If you are facing this issue you can download an updated version of the driver 5.39 on Utimaco support portal
OCTO-401	HOST	This known issue only affect windows 11 and windows server 22 environments and only PCIe HSM cards. A recent update from windows update (may) actually makes the HSM unreachable from the host. This issue is being investigated. It is recommended to not apply the recent updates of Windows if you are using the PCIe version of the HSM

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
SUSE LES	12 15
Ubuntu	20.04LTS 22.04LTS
CentOSStream	9

Notice: Only 64-bit versions of these Operating Systems are supported. 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

The following table lists the Java Runtime Environments supported by SecurityServer (new) JCE provider

Java Runtime Environment	*Version*
Oracle 8	1.8.0_211
Oracle 11	11.0.3
Oracle 17	17.0.10
Oracle 21	21.0.2
Oracle 23	23.0.1
OpenJDK 8	8.0.422
OpenJDK 11	11.0.8
OpenJDK 17	17.0.2
OpenJDK 21	21.0.2
OpenJDK 23	23.0.1

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	5.38.0

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 by email or telephone. Please make sure to have the 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 - 6.1.1

11.1 List of enhancements - 6.1.1

11.1.1 In-field license upgrade

This version of SecurityServer allow end users to upgrade their license file. Thus it is possible to upgrade the speed of the HSM, the number of cHSM, and the number of template available (for example, it is possible to enable SecurityServer-SDK template).

This capability is available via 2 new commands.

Gladm system-update-license : This command loads a license file in the HSM. The license is signed using ECDSA NIST P512 / SHA-512 and the signature is verified during the loading process. A valid license file (with correct signature issued by Utimaco) is required.

Gladm system-get-license-info : This command allows customer to verify which license is loaded on the HSM and displays license properties including :

- License file version
- Product name
- Serial number
- Number of cHSMs
- Included templates in license (this gives a list of templates with their names)

11.1.2 User's password policy

Utimaco's HSM has a default password policy which requires the password of HSM users to be at least 8 characters long (and password to be changed at first login).

It is now possible to harden the configuration of the HSM by using a signed configuration file to enforce stronger password requirements.

Typical example of password policy hardening :

```
[PasswordRequirements]
MinLength = 8
RequireLowerCase = true
```

```
RequireUpperCase = true
RequireNumber = true
RequireSpecialChars = true
MinNumRestrictions = 2
UsernameAllowed = false
```

- MinLength: Specifies the minimum length of the password. If it is lower than 8 (current minimum requirements), it is ignored.
- RequireLowerCase: If true, the password must contain at least one lowercase letter. Default is false.
- RequireUpperCase: If true, the password must contain at least one uppercase letter. Default is false.
- RequireNumber: If true, the password must contain at least one number. Default is false.
- RequireSpecialChars: If true, the password must contain at least one special character (from `~!@#$%^&*()-_=+|[{}];:'",<.>/? Or blank space). Default is false.
- MinNumRestrictions: The password must contain at the minimum at least a subset from the four groups above. It should be from 0 to a number lower than or equal to the number of "true" for the required groups. The default is the number of required groups. If MinNumRestrictions is inconsistent with the number of "trues" for the groups, then MinNumRestrictions is adjusted as equal to the number of trues.
- UsernameAllowed: If false, the password cannot be the same as the user name.

11.1.3 Device clusters

In PKCS#11 configuration file it was possible to define multiple clusters with the [Cryptoserver] section.

This release adds the capability to define multiple cluster and manage HSMs individually (access to a given slot on a given HSM).

There is a new section called [HSMCluster] allowing to define a cluster ID. Each Cluster can have multiple slots and multiple HSMs.

Each slot ID has 8 digits. The first 4 digits contain the value of the cluster ID and the last 4 digits represent the slot number in that cluster.

Example In the picture below :

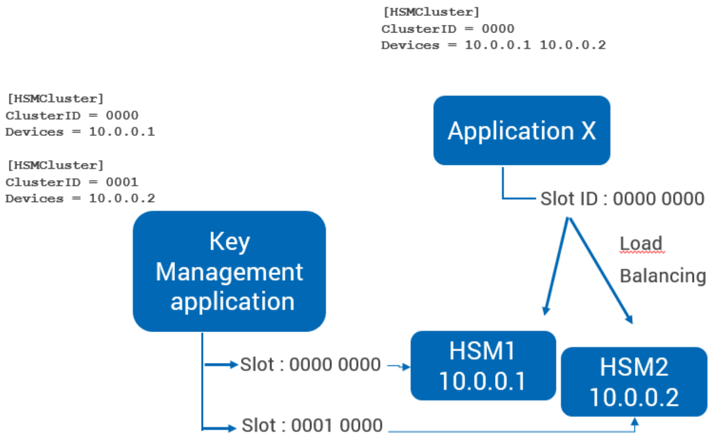
"Application X" uses a single cluster of 2 HSMs and a single slot : slot 00000000.

With the new feature, the "key management app" in the picture will have 2 clusters defined, one for each HSM.

Slot 0000 0000 : which is the slot 0 on the first HSM.

Slot 0001 0000 : which is the slot 0 on the second HSM.

Therefore, just via a config file, an application can either login on a slot bound to an HSM cluster (for high availability and load balancing), or login on a particular slot number on a particular HSM.



```
[HSMCluster]
ClusterID = 0000
Devices = 10.0.0.1 10.0.0.2
```

```
[HSMCluster]
ClusterID = 0000
Devices = 10.0.0.1

[HSMCluster]
ClusterID = 0001
Devices = 10.0.0.2
```

The tool p11tool2 also supports this capability via the new parameter to the command : p11tool2 Cluster=0001 Slot=0000

11.1.4 IP and port ranges

It is now possible to define port ranges and IP ranges in the pkcs11 config file.

Ports are expanded : 8000-8005, expands to 8000, 8001, 8002, 8003, 8004, 8005 (the range is inclusive).

IPV4 addresses are expanded : xxx.xxx.xxx.100-105, expands to xxx.xxx.xxx.100, xxx.xxx.xxx.101, xxx.xxx.xxx.102, xxx.xxx.xxx.103, xxx.xxx.xxx.104, xxx.xxx.xxx.105 (the range is inclusive).

So for example, if configuring 2 u.trust Anchor SE40K, which have IP addresses 10.1.20.200 and 10.1.20.202, which have 12 cHSMs each, just takes a single line in the configuration file :

Devices = { 3001-3012@10.1.20.200-202 }

11.1.5 Load encrypted firmware module in SDK

This capability was originally available in the old Se and CSe HSM and has now been reintroduced.

The command LoadFWDecKey is now available.

11.1.6 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)

11.1.7 Auto-Login

In pkcs#11 config file, the section [Autologin] now allows to define one or multiple users to automatically login, whatever the type of user and whatever authentication method of the users is.

The new [Autologin] replaces the former Autologin and also sections ExtendedLoginUser and ExtendedLoginSO.

The utility p11tool2 also reads the pkcs11 config file and do not require user credentials if the autologin parameters are set.

11.1.8 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).

11.1.9 Documentation changes

csadm, cxitool manuals are now part of the cHSM administration manual, in appendix, rather than separated manuals.

11.2 List of bug fixes - 6.1.1

Unable to render include or excerpt-include. Could not retrieve page.

11.3 List of known Issues - 6.1.1

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"
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.

Reference	Component	Issue
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-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-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.
PHX-2772	FW	When performing an RSA PSS signature without salt (i.e., deterministic) via P11 (sLen = 0) the HSM fails and returns NO_DEVICE_AVAILABLE
PHX-2904	FW	RSA performances in bulk mode are lower this release. This only affects bulk mode, Single signing is not affected.

12 Older Releases - 6.0.0

12.1 List of enhancements - 6.0.0

12.1.1 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.

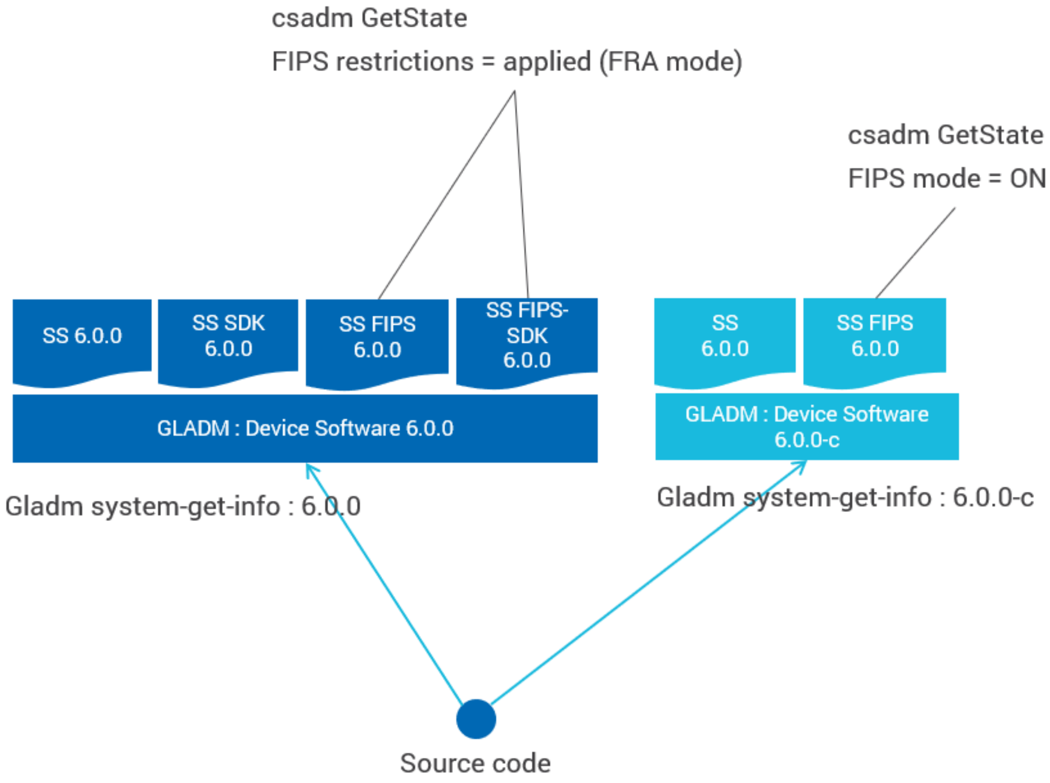
12.1.1.1 Identification via hypervisor (via gladm command)

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.

12.1.1.2 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.


csadm GetState
FIPS restrictions = applied (FRA mode)
csadm GetState
FIPS mode = ON
SS 6.0.0
SS SDK 6.0.0
SS FIPS 6.0.0
SS FIPS-SDK 6.0.0
SS 6.0.0
SS FIPS 6.0.0
GLADM : Device Software 6.0.0
GLADM : Device Software 6.0.0-c
Gladm system-get-info : 6.0.0
Gladm system-get-info : 6.0.0-c
Source code

12.1.1.3 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.

12.1.1.4 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

12.1.2 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.

12.1.3 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.

12.1.4 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.

12.1.5 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).

12.1.6 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

12.1.7 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.

12.1.8 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.

12.1.9 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.

12.1.10 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.

12.1.11 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

12.1.11.1 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

12.1.11.2 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

12.1.11.3 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

12.1.11.4 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.

12.1.12 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.

12.2 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

12.3 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.

13 Older Releases - 4.90

13.1 List of enhancements - 4.90

FIPS 140-3 compliance

Although not directly visible to customers, this release contains significant number of enhancements in order to comply for FIPS 140-3 L3 requirements.

Documentation changes

Manuals for u.trust Anchor Se is now unified across all product variants.

13.2 List of bug fixes - 4.90

The following bugs were fixed in this release.

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

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

Reference	Component	Issue
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-1074	DOC	Internal battery in u.Trust Anchor manuals was wrong
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

14 Older Releases - 4.80

14.1 List of enhancements - 4.80

Snaphot behavior

In releases <= 4.80 it was possible to make two types of snapshot : "full" or "data"

- full snapshot take a whole image of the containerized cHSM
- data snapshot take a full image of the user's data (including custom firmware modules, database of keys and database of users)

In release 4.80 the full snapshot option has been removed to ease certification process.

From a user's perspective this does not change since the data snapshots are allowing to restore a containerized HSM in a working state, including all cHSM configuration, data, keys, users, and custom firmware modules if present.

This is a summary of the situation:

Snapshot taken in <=4.70	--migrate	Restore in UTA version <= 4.70
Full	No	Restores if firmware version = snapshot version
Full	Yes	Restores if firmware version >= snapshot version
Data	Yes	Restores is firmware version >= snapshot version
Data	No	Restores is firmware version = snapshot version

In releases prior to 4.80, you can use both full and data snapshot and restore them.

Snapshot taken in <=4.70	--migrate	Restore in UTA version 4.80 and beyond
Full	No	Error since no full snapshot with version 4.80 possible.
Full	Yes	Restores if firmware version >= snapshot version
Data	Yes	Restores if firmware version >= snapshot version
Data	No	Error since snapshot version is from 4.70 and firmware version is 4.80

In release 4.80 and beyond, you can use data snapshot only and restore them.

If you try to restore an old snapshot, made with the --full option, you can restore as well but must use the --migrate option.

The --migrate option actually updates the version number in the snapshot metadata indicating in which release the snapshot was created, as this release number is checked by the HSM firmware for verification.

***If an Utimaco module is deleted (only modules from Utimaco are present in the base firmware) and a snapshot is taken, the deleted module will still be present upon restoring the snapshot. This will be addressed in further release.**

FIPS 140-3 enhancement

Release 4.80 contains a number of enhancements which are required for the FIPS 140-3 certification including additional self tests and security enhancements to store keys and users in the HSM in order to comply with NIST requirements.

Multi-tenancy now available on all Se-series HSMs

The scope covers all Se-series HSMs including Se100, Se2K, Se5K, Se15K and Se40K. Before 4.80, if a user wanted to use different cHSMs for different use cases (including different configuration, users, keys etc.), it was required to instantiate the first cHSM via *gladm chsm-create*, and then duplicate the cHSM via snapshots, and optionally reconfigure the snapshot independently via csadm.

Now with 4.80, a user can instantiate any amount of cHSMs using gladm chsm-create command. The maximum number of cHSMs is still limited by license (for example 12 cHSMs on Se40K).

This capability allows customer to ease cHSM instantiation for multi-tenant use cases, unify the setup steps and configuration across all Se-series HSMs.

This capability will be enabled on all new devices starting to ship with 4.80 in June 2024 from Utimaco factory. It is currently not possible to upgrade the license file in-field.

pcsadm is still present on the product CD, but should no longer be used to setup the HSMs. It will be removed in later releases.

User documentation still does not reflect that change but will be updated in a later release.

14.2 List of bug fixes - 4.80

The following bugs were fixed in this release.

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

Reference	Component	Issue
PHX-1660	FW	Improve speed of AES-GCM
PHX-1628	Host	ODBC can't overwrite existing keys
PHX-1576	FW	csadm getauditlog shows SMOS version partially in hexadecimal
PHX-1421	Host	Correct error message displayed while using gladm operator secret with both -g and -t options
PHX-1364	FW	Fixed error during poweron self test
PHX-1325	SDK	UTA SDK - vs code properties json uses the path for PKCS11_R2 instead of R3
PHX-1068	Host/FW	Full snapshot are now disabled to prevent loading module into a container, for FIPS 140-3 compliance --full option is no longer available previous full snapshot are restored as data snapshot
DOC-1022	DOC	fixed error in documentation regarding full snapshot (gladm manual)
DOC-1020	DOC	Fixed typo in documentation, cryptoserver SDK page 28 Correct: csadm Model=*c7s* MMCSignKey=<path_to_your_AMSK.key> MakeMTC=EXMP.so
DOC-1003	DOC	Documentation updated regarding uninstallation of PCIedriver
DOC-999	DOC	CKK_EC_EDWARDS and CKK_EC_MONTGOMERY listed as unsupported whereas they are in the firmware/api
DOC-991	DOC	Documentation updated to reflect HSM are now shipping in secure bags
DOC-977	DOC	Clarified gladm restore --migrate
DOC-829 DOC-828	DOC	u.trust Anchor PCIe technical data PDF - battery information now refers to correct battery type
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

15 Older Releases - 4.70

15.1 List of enhancements - 4.70

New operating systems

This version of SecurityServer 4.70 has been tested on the operating system 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 (ie 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, 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.

Features for FIPS 140-3 compliance

Adding new power-up self test : PBKDF , RSAAE-PKCS-v1_5, RSA PSSS, RSAES-OAE, DSA Sign/Verify.

Adding new class of Audit log "Action needed".

Operator secret on smartcards

In previous releases, the operator secret was only managed via single key file and tools of the operating system. This option is still available for backward compatibility.

In this release, the operator secret can now be managed via multiple smartcards. The command gladm key-set-operator-secret has new option '-g' to generate operator secret shares and store them on smartcards. It is possible to specify a quorum (ie 2/3 or 2/5). 2 is minimum, 255 is the maximum. The operator secret shares are generated in turn and saved to multiple smartcards, then automatically wrapped by the Key Wrapping Key downloaded from the HSM, and the operator secret is finally securely combined and loaded in the HSM. All in a single operation.

The command gladm key-set-operator-secret can now also load the operator secret from multiple smartcards (wrapping and loading only, if generated previously)

If a single file is used for operator secret (in previous releases),

- It can still be loaded as a single file in the HSM as in previous release, (requires manual wrapping, and loading in the HSM)
- It can be wrapped and loaded via gladm : use gladm key-set-operator-secret with path to the file, without any token value.
- It cannot be split from single file to multiple files to allow the quorum : quorum is only available on smartcards
- It can be split from single file to multiple smartcards to use the quorum (using gladm smartcard-copy-secret command)

Copying operator secret share from smartcards to keyfile is not possible.

mTLS support

The application can now use either regular TCP connections (with secure messaging) or mTLS.

mTLS is a new feature and requires the latest version of the LAN OS : 5.8c.0.

If your HSM has been delivered with a version prior to 4.70, the LANOS is certainly in an older version. Please ensure you upgrade your LANOS to 5.8c.0 to get mTLS support.

mTLS is only supported on Linux operating systems (client side)

Upgrade and New Image Signing Key

A new signing key has been introduced on the u.trust Anchor HSM since release 4.60.0.3 (previous release).

The purpose is to enhance security by using a new key with greater length and elliptic curves. The new signing key is NIST512.

The release 4.70 is signed with this new ISK.

Upgrading to release 4.70 therefore requires to be at least in 4.60.0.3.

If you are in an older release, you have to upgrade to 4.60.0.3 first, then upgrade to 4.70.

After each upgrade: Restart the HSM with the command gladm system-restart, then reboot the LAN appliance after (if you are using the LAN appliance)

USB port support

USB port is now enabled so it is possible to connect the pinpad to the HSM's USB port for MBK loading and user authentication.

15.2 List of bug fixes - 4.70

The following bug were fixed in this release

Reference	Component	Issue
PHX-1065	csadm	csadm VendorRootCert: Using certificates that have an empty file behaves as if no certificate is provided
PHX-1150	Simulator	Fixed memory allocation in Simulator
PHX-1274	FW	SMOS logs wrong version in bootlog
PHX-1311	SDK	u.trust SDK Dockerfile uses version gcc-arm-9.2 instead of gcc-arm-11.2.0
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

Reference	Component	Issue
PHX-818	gladm	gladm device-restart: Wrong error message when executing the command without a device
PHX-561	gladm	Update glad spec. with Audit Log entry description for self-test errors
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
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

Reference	Component	Issue
PHX-84	pkcs11	[Host] PKCS#11 R3: Error when accessing slots with ID > 255
OCTO-148	Driver	PCIe driver: resynch after external erase

15.3 Known issues - 4.70

List of known issues on this release

Reference	Component	Issue

HSM-15097	pkcs11	The pkcs11 config file requires the list of devices to be added with carriage return
		`Device = {`
		`     <dev1>`
		`     <...>`
		`     <devN>}`

HSM-15086	Host	The setup scripts provided with the api samples have errors. Workaround is to edit the script and add the corresponding test users manually The file pom.xml is also in rong version so prevent JCE sample to be built.
HSM-15115	Host	The installer of 4.70 doesn't detect/warn/remove previous SecSrv/UTA installations It is adviced to remove older installation first before performing new installation of Security Server software

16 Older Releases - 4.60.0.3

16.1 List of enhancements - 4.60.0.3

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.

Release 4.60.0.3 is a new release that contains two firmware images;

- Image signed with old ISK : u.trust_Anchor-4.60.0.3-RSA-Signed.raucb
- Image signed with new ISK : u.trust_Anchor-4.60.0.3-ECA2024-Signed.raucb

When upgrading from release prior to 4.60.0.3 : use the image signed with the old ISK. Loading this image will verify the signature with the old signing key, and replace the signature verification key on the HSM.

Then, any later upgrade will require image signed with the new ISK.

The second image, signed with the new ISK, is present in this version if you upgrade to a later version (greater than 4.60.0.3) and wish to downgrade back to 4.60.0.3 later on.

Upgrade

Once the firmware of the HSM has been upgraded to 4.60.0.3, it is not possible to downgrade later, as the ISK will be different.

16.2 List of bugfixes - 4.60.0.3

Only enhancements have been added to this release.

17 Older Releases - 4.60.0.2

17.1 List of enhancements - 4.60.0.2

This release contains bugfixes for another hardware platform.

17.2 List of bugfixes - 4.60.0.2

The following issues have been resolved in SecurityServer.

Reference	Component	Issue
PHX-1150	Host	Memory Allocation Error on Simulator

18 Older releases - 4.60.0.1

18.1 List of enhancements - 4.60.0.1

The following issues have been resolved in SecurityServer.

Reference	Component	Issue
PHX-1150	Host	u.trust_anchor_product_bundle CryptoServerJCE.jar shows wrong version information in MANIFEST.MF
CM-827	Driver	PCIe registry entries not set by driver (Windows driver installation issue)

18.2 List of bug fixes - 4.60.0.1

The following issues have been resolved in SecurityServer.

Reference	Component	Issue
CM-827	Driver	PCIe registry entries not set by driver (Windows driver installation issue)

19 Older releases - 4.60

19.1 List of enhancements - 4.60

19.1.1 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.

19.1.2 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 the same as the previous one.

19.1.3 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.

19.1.4 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.

19.1.5 Gladm system-restart and device-restart -h

These new commands are available now. Please follow the product documentation to learn more about the usage and application.

19.1.6 Windows Support to Gladm with a PCIe card

Gladm now supports connectivity to a Windows PCIe Node and user u.trust Anchor with a local PCIe.

19.2 List of bugfixes - 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]
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

Reference	Component	Issue
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)