Using an RDBMS for key storage

Integration Guide

CryptoServer

utimaco®

Imprint

Copyright 2020	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	1.0.0
Date	06/10/2025
Status	PUBLISHED
Document No.	IG-2025-0003

Table of Contents

1 Version Information

Partner Name	
Product Name	Using an RDBMS for key storage
Partner v[Version]	
Document Type	Integration Guide
Utimaco Product	CryptoServer
Utimaco v[Version]	
Document Image	
Document Number	IG-2025-0003
Document Version	1.0.0
Status	PUBLISHED

2 Overview

CryptoServer is the Utimaco family of general-purpose hardware security modules (HSMs), i.e. physically protected, specialized computing units, designed to perform sensitive cryptographic tasks and to securely manage cryptographic keys and data objects. General-purpose HSMs from Utimaco aggressively protect the cryptographic identity - the digital keys - of your enterprise.

The CryptoServer lines are certified by NIST, to FIPS 140-2 Level 3 (the Se Gen2), or Level 4 for physical security, Level 3 overall ("Level 3+", the CSe). Additionally, the CP5 variant is certified to EAL4+ for Common Criteria, according to EN 419221-5 *Protection Profiles for TSP Cryptographic Modules*.

The HSMs themselves are standard format PCIe (1U, full height, half-length) cards, and can be supplied in two form factors: Either as the card itself, or as clusterable 1U, 19" rack-mount appliances for use in HA/FT environments. The PCIe form-factor does *not* come with server software , it is considered for use as an offline Root CA; it is not network addressable and can only be used on the workstation in which it is installed.

The CryptoServer line is also programmable; Utimaco can provide different SDKs that an enterprise will use to create private software modules that run directly on the HSM. Use of the SDK allows you to protect your cryptographic keys and the IP that uses them. These private methods can be either for performance optimization or to implement custom cryptographic algorithms or mechanisms. Performance optimization allows multiple, chained cryptographic operations to run with a single HSM call, and custom cryptography is useful for Post-Quantum Cryptography or when non-standard curves or symmetric encryption or hashing is required. Available SDKs are for C- or Lua-based modules, or for PKCS#11 Vendor-defined-mechanisms.

In a CryptoServer-based security system, security-relevant actions can be executed, and security-relevant information (i.e., cryptographic keys) can be stored. Given its general-purpose nature and extreme programmability, the Utimaco CryptoServer CSLAN form-factor is used as a universal, independent security component in heterogeneous computer systems, supporting multiple use cases, concurrently, and from different hosts.

Utimaco HSMs are priced according to protection level and performance, *not* by number of users, applications or algorithms available.

3 Getting to know the tools

This document relies on `csadm Help=<command>` throughout, as the syntax or capability of a given tool or command may change based on which version of the SecurityServer you are using. For brevity, this is generally shown as `csadm <command>` , the `Help=` is assumed.

```
csadm Help
csadm Help=BackupDatabase
```

Keep in mind that the database commands for backup and restore require system-, and/or user-admin-level authorization, and which auth level depends on both the tool used and the database that you are trying to back up.

For example, the `user.db` requires a " `user admin` " authorization (`csadm`), `CXIKEY.db` can be backed up as a single file with " `system admin` " authorization (`csadm`), or a specific user can backup their own keys using " `cryptographic user` " level authorization (`cxitool`).

See the SecurityServer documentation for how the authorization mechanism works. The CryptoServer Manual for System Administrators, section 2.14 'Users, User Groups and Authentication', is a good place to start. [V4.2x]

The `csadm BackupDatabase` and `RestoreDatabase` commands are not permitted when the HSM is running "FIPS" or "CC" firmware. In this case, backup and restore must use one of the API tool commands, `cxitool BackupKey` for example.

3.1 Backup

Backing up user.db requires both CryptoServer Admin, as well as at least one User Admin (`12000000`), while the CXIKEY.db requires only a CryptoServer Admin (`02000000`). footnote: [Please see the SecurityServer administration documentation for more on permission masks and authorization levels provided, and how they are used.] Backing up individual keys or groups of keys based on their Group value, using an API's tool like `cxitool`, require Cryptographic User (`00000002`), *plus* the correct key CXI Group for the targeted keys. CXI_GROUP is a regular-expression attribute of the user, and Group is an attribute of the key, and regex matching rules are applied to provide or restrict access.

In general, to run an arbitrary command requires an authorization value of '2' in a specific field. CXI Group, key Group and "Cryptographic User" authorization (`00000002`) has the added requirement that the authorization supplied by a Cryptographic User is specifically that user's CXI Group. A user with `00000002` in CXI Group "ExmpKey", and a user with `00000000` in CXI Group "ProdKey", cannot make backups of keys in Group "ProdKey", as those "users" in the "ProdKey" group don't reach the `00000002` authorization state needed for cryptographic operations on that group.

A recommendation to use `csadm` and `BackupDatabase` to capture the entire database, or use `cxitool` and only make backups of specific key groups/keys will be case dependent. The simplicity in capturing an entire database may conflict with the level of granularity required, and, as always, **security** should not take a back seat to **convenience**.

The primary data to be backed up reside in the `user.db` (authorized CryptoServer users) and `CXIKEY.db` (the CXI key database). If you have custom, SDK-generated private database files, you can also use `csadm BackupDatabase` to capture those.

The command-line tools generally allow you to "stack" operations.

For 4.20 SecurityServer, the following script can be used as a starting point.

```
csadm \
LogonSign=AdminUserA,:cs2:cjo:USB0 \
LogonSign=AdminUserB,:cs2:cjo:USB0 \
BackupDatabase=user.db BackupDatabase=CXIKEY.db
```

The command "stacks" two `BackupDatabase` commands, to capture the user and internal key databases. If you have custom databases, you can add additional `BackupDatabase=<file>.db` commands at the end of this command. The commands populate the working directory with the copies, which should then be treated as directed by local policy (immediate off-site copy via sftp or scp, etc).

Security-relevant data in these backup files are encrypted using the device MBK.

The combined permission for the above command should be at least (`12000000`). The 2 in slot 6 allows the `BackupDatabase` command to be run, and the 1 in slot 7 provides the authentication requirement to make a backup of the CryptoServer *users* database. Without the `10000000` , the command would fail at attempting the backup of `user.db` , and *all following commands would not be run*.

The SecurityServer command line tools will execute command-line arguments, in general, left to right. The current session state of the command is maintained from one stacked command to the next. In the event an exception is thrown by one command, the remainder of the commands are ignored, and the session is torn down on return to the command line. You do, however, need to provide all Logon details after setting the Device (if needed), and prior to issuing any parameter, argument or command.

3.2 Restore

Restoring the databases or other data requires the inverse command steps. For 4.20 SecurityServer, the following script can be used as a starting point.

```
csadm \
LogonSign=AdminUserA,:cs2:cjo:USB0 \
LogonSign=AdminUserB,:cs2:cjo:USB0 \
RestoreDatabase=user.db RestoreDatabase=CXIKEY.db
```

The `csadm` command stacks two `RestoreDatabase` commands, to upload the user and internal key databases from the working directory. If you have custom databases, you can add additional `RestoreDatabase=<file>.db` commands at the end of this command. The commands are sourcing the backup files from the working directory, and will load them into the CryptoServer, where they will be immediately available.

Database restores are done line-by-line, not by replacing the resident file with a different one. This means that if there is a user in the HSM, but not in the backup, that user will **still** be in the HSM `user.db` after the restore.

Make sure that you have deleted the factory-default 'ADMIN' user prior to making backups of the `user.db` database.

The combined permission for the above command should be at least (`12000000`). The 2 in slot 6 allows the `RestoreDatabase` command to be run, and the 1 in slot 7 provides the authentication requirement to make a restore of the CryptoServer *users* database.

If the MBK used to back up the artifacts is different from the one resident on the target CryptoServer, the command will fail and the existing databases will not be modified.

Because commands and command syntax may change between releases, this document shows which commands are used to perform which tasks, but it does not, in general, explicitly show the syntax necessary for that command. Also, the commands you have available to you may have options that you can take advantage of for your local policies. Issue the help command to get the syntax for the variant of the command, and options, available in the tools you have.

4 Bill of Materials/Artifacts

While a 'Sharpie' or other indelible ink pen can write on the plastic smart cards, friction and simple wear and tear can rub the ink off, over time. To prevent this, use a strip of tape to cover the markings, or use a label maker and print out the information, and attach it to the cards.

A CSLAN in a box on a shelf will drain the 'carrier' battery. The exterior battery usable life is **18 months**, the 'carrier' battery is **6 months**. A CSLAN that has been in a box on a shelf for 2 years has drained batteries.

5 Making Backups

```
export CRYPTOSERVER=/dev/cs2a
csadm getstate
```

6 Restoring from Backups

```
Error B0830063
      CryptoServer module CMDS, Command scheduler
      illegal challenge length requested
```

7 What else to back up/Other Considerations

7.1 Governance Files

.

8 Further Information

This document forms a part of the information and support provided by Utimaco IS GmbH. Additional documentation can be found on the product CD in the documentation directory. All Utimaco CryptoServer documentation is also available at the Utimaco IS GmbH Website: https://www.utimaco.com/services/support

If you have questions about this document, suggestions for improvement on unclear wording, or see any typographical errors, please email support@utimaco.com, with the subject line *Doc Comments on IG RDBMS Key Store*.

While we cannot guarantee a targeted response to your questions or suggestions, they will be considered when generating later versions of this document.