Microsoft

Active Directory Rights Management Services (AD RMS)

Integration Guide

CryptoServer HSM

2.60.0

utimaco®

Imprint

Copyright 2026	Utimaco IS GmbH
	Krefelder Straße 220
	52070 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	2026-06-15
Status	PUBLISHED
Document No.	IG-2026-0053

Table of Contents

1 Introduction

This paper provides an explanation on how to integrate a Hardware Security Module (HSM) - SafeGuard CryptoServer PCI or SafeGuard CryptoServer LAN - with Microsoft Active Directory Rights Management Services (AD RMS). It is assumed that you have already prepared the Active Directory Rights Management Services infrastructure using the Microsoft Windows Server Active Directory Rights Management Services step-by-step guide published by Microsoft.

1.1 Concepts

Active Directory Rights Management Services protects information within a digital file, such as a Microsoft Office document. Once the protection is added, it stays with the file. By default, only the content owner is able to remove the protection from the file. The owner grants rights to other users to perform actions on the content, such as the ability to view, copy, or print the document. AD RMS requires the installation of Internet Information Services (IIS), where SSL (Secure Sockets Layer) encryption is highly recommended for https connections between each client using AD RMS and the AD RMS cluster.

IIS and Active Directory Certificate Services, which issue the SSL certificates with Microsoft Certificate Authority, can be secured by the SafeGuard CryptoServer as well. For further information about integrating SafeGuard CryptoServer into Microsoft Windows 2008 Server Active Directory Certificate Services and Internet Information Services, we refer to the corresponding documents; HowToW2K8Server-ADCS-CryptoServer and IIS7withSGCryptoServer. In this guide, a self-signed certificate for https connection between client and AD RMS server is created.

The SafeGuard CryptoServer is a hardware security module developed by Utimaco Safeware AG, i.e. a physically protected, specialized computer unit designed to perform sensitive cryptographic tasks and to securely manage cryptographic keys and data. In a SafeGuard CryptoServer system, security-relevant actions can be executed and security-relevant information can be stored. It can be used as a universal, independent security component for heterogeneous computer systems.

1.2 Overview

During the AD RMS installation an AD RMS Cluster Key is generated which is accessed while adding and verifying restricted document rights. The cluster key can be centrally managed by AD RMS and stored in the AD RMS configuration database using a strong password. It also can be protected within software or hardware based cryptographic service provider (CSP). As a best

security practice Microsoft recommends using hardware based CSP to protect the AD RMS cluster key.

2 Requirements

Ensure that you are familiar with the Microsoft Windows Server AD RMS step-by-step guide and have a copy of the CryptoServer Administration Guide. This document also assumes that the AD RMS infrastructure is already prepared, and the SafeGuard SecurityServer software is ready for installation on the ADRMS-SRV machine, where AD RMS will be installed and configured. If AD RMS is already installed, see chapter 3.2 for more information about removing AD RMS first.

HSM Model	SafeGuard CryptoServer CS-Series/S-Series/Se-Series PCI SafeGuard CryptoServer CS-Series/S-Series/Se-Series LAN SafeGuard CryptoServer Simulator
HSM Firmware Software	SafeGuard SecurityServer 2.60.0 SafeGuard SecurityServer 2.60.0 All components of AD RMS infrastructure

Table 1: Software and hardware requirements

2.1 Supported Systems

The interoperability of the SafeGuard CryptoServer solution, operating systems and Active Directory Rights Management Services have been tested successfully for the following combinations:

Operating System	SafeGuard SecurityServer Version	PCI Support	Ethernet Support
Microsoft Windows Server 2008	2.60.0	Yes	Yes

Table 2: List of supported systems

3 Procedures

To integrate the SafeGuard CryptoServer with Active Directory Rights Management Services, complete the following steps:

1. Set up the AD RMS Infrastructure.
2. Uninstall the AD RMS.
3. Install the SafeGuard CryptoServer hardware.
4. Install the SafeGuard CryptoServer software.
5. Configure Utimaco CSP.
6. Install AD RMS and IIS.
    a. Add ADRMSADMIN to Domain Admins group.
    b. Install and configure the Server Roles AD RMS and IIS.
    c. Create a self-signed certificate with IIS and complete the installation.
7. Verify the AD RMS functionality.

3.1 Set up the AD RMS Infrastructure

For setting up the AD RMS infrastructure, we refer to the Microsoft Windows Server AD RMS step-by-step guide: http://go.microsoft.com/fwlink/?LinkId=185635. You will need to prepare four different operating systems and install corresponding applications and services on four separate machines:

1. Active Directory Domain Controller on ADRMS-DC with Windows Server 2003 (SP2) and Domain Name System (DNS).
2. Database computer on ADRMS-DB with Windows Server 2003 (SP2) and Microsoft SQL Server 2005 (SP2).
3. AD RMS root cluster on ADRMS-SRV with Windows Server 2008 and Internet Information Services (IIS) 7.0.
4. Client computer on ADRMS-CLNT with Windows Vista and MS Office Word 2007 Enterprise Edition.

Do not install AD RMS until SafeGuard CryptoServer is installed and configured.

3.2 Uninstall AD RMS

If AD RMS was already installed before, uninstall it to provide a more secure, hardware-based cryptographic service provider for the RMS cluster key in further installations. For this purpose, complete the following steps:

1. Open Server Manager (**Start** → **Administrative Tools** → **Server Manager**).
2. Start the Remove Roles Wizard (**Roles** → **Remove Roles**) and click **NEXT**.
3. Unselect the roles **Active Directory Rights Management Services** and **Internet Information Services** and click **NEXT**.
4. Click **REMOVE**.
5. Reboot the machine as soon as the wizard is done.
6. After login, wait until the installation is complete.
7. AD RMS clients use a service connection point (SCP) to automatically discover the AD RMS Custer. To unregister the old SCP, download the RMS Administration Toolkit with SP2 and install it.
8. Open a command prompt (Start → Run → type in `cmd`), navigate to the installation folder:
    - cd C:\Program Files\RMA SP2 Administration Toolkit\ADScpRegister\ and unregister SCP:
    - ADScpRegister.exe unregisterscp.

3.3 Install SafeGuard CryptoServer Hardware

For the installation and setup of SafeGuard CryptoServer hardware, we refer to the SafeGuard CryptoServer PCI Installation and Operating Manual and the *SafeGuard CryptoServer LAN* Installation and Operating Manual respectively.

3.4 Install SafeGuard CryptoServer Software

For the installation of SafeGuard CryptoServer software, we refer to the CryptoServer Administration Guide. Select CSP/CNG - Cryptographic Service Provider (Microsoft) during the installation of SafeGuard SecurityServer. Please ensure that the `CXI` firmware module has been loaded after the installation (chapter 3.4.1). Otherwise load the firmware package `SecurityServer-2.60.0.mpkg` to the SafeGuard CryptoServer.

3.4.1 Check Firmware Installation

- Start the CryptoServer Administration Tool (CAT) (**Start** → **All Programs** → **Utimaco** → **SafeGuard CryptoServer**).
- Connect to your SafeGuard CryptoServer device.
- Press button **LIST FIRMWARE** to list all installed firmware modules. The `CXI` module should be listed like this: `68 CXI 2.0.9.10 INIT_OK`.

3.4.2 Install Firmware

If `CXI` module has not been installed on the SafeGuard CryptoServer, follow these steps to load the firmware module:

1. Start the CryptoServer Administration Tool (CAT) (**Start** → **All Programs** → **Utimaco** → **SafeGuard CryptoServer**).
2. Connect to your SafeGuard CryptoServer device.

In case of SafeGuard CryptoServer Se-Series, log in as user with administration privileges (e.g. ADMIN) as next.

3. Open the dialog Setup CryptoServer (**Firmware Management** → **Setup CryptoServer**).

- Enter the license file if necessary, or leave it blank.
- Select the firmware package file; `SecurityServer-2.60.2.mpk`.
- Either chose **UPDATE** or **NEW INSTALLATION** as installation type. (Select **UPDATE** option if you want to update the existing firmware modules and keep your key databases

unchanged, or select NEW INSTALLATION if you want to remove all key databases and firmware modules before upload of the new ones.).

- To start uploading the firmware package, press SETUP.
- You will be prompted to authorize the installation. Select either smartcard authorization or key file token authorization and press the OK button.

The SafeGuard CryptoServer will restart after the installation of the SecurityServer firmware package.

To check if your setup was successful, refer to the steps of chapter 3.4.1.

3.5 Configure Utimaco CSP

The SafeGuard CryptoServer Cryptographic Service Provider (CSP) has to be configured before it can be used in the integration with the Microsoft Active Directory Rights Management Services. The CSP has to be aware of the SafeGuard CryptoServer device(s) to be used. Each CryptoServer device has to be registered in the CSP. Generally there are two types of key storage options available for the CSP:

- The most common way is to store the keys inside the SafeGuard CryptoServer. This is the best protection against physical and logical attacks.
- In a cluster or failover scenario, keys are stored externally. Normally the external storage is a media device e.g. shared network device (SAN or ISCSI) or a hard drive.

The next steps assume that an internal storage of keys is used:

1. Start the SafeGuard CryptoServer CSP configuration tool (**Start → Control Panel → Utimaco CryptoServer CSP**).

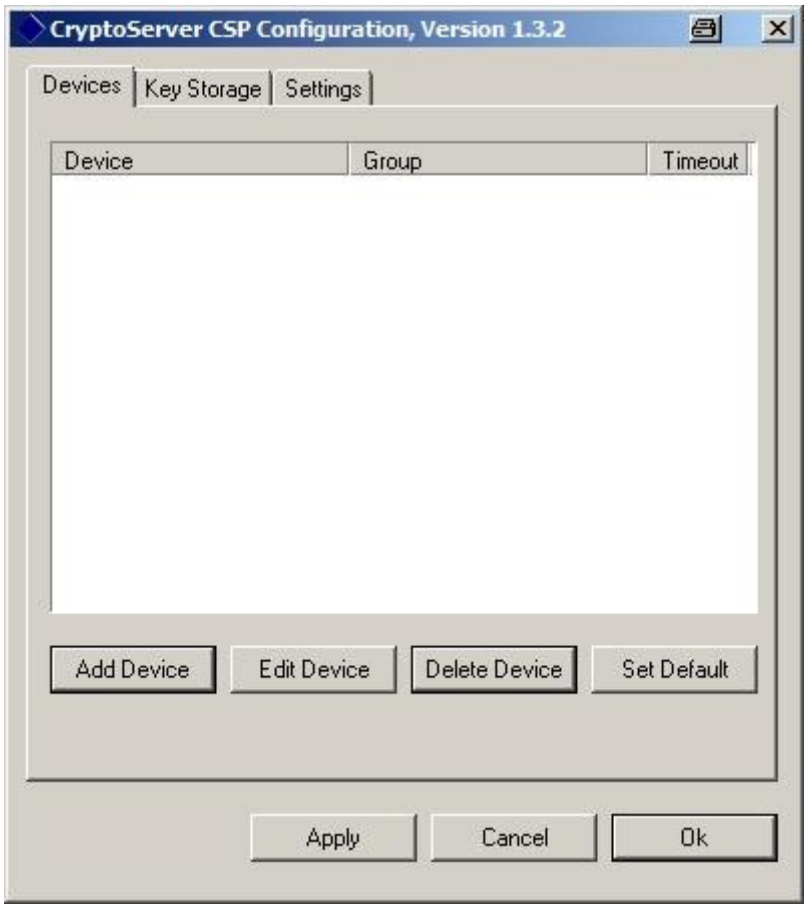

Figure 1 : CryptoServer CSP configuration

2. Add a device to the list by pressing **ADD DEVICE** and enter the device specifier, e.g.:
    a. IP address of SafeGuard CryptoServer LAN.
    b. `PCI:0` in case of SafeGuard CryptoServer PCI(e).
    c. `3001@127.0.0.1` in case of SafeGuard CryptoServer Simulator.
3. Choose a group name for the new generated keys. Usually, the name of the workstation is chosen here. Confirm the settings by pressing **OK**.

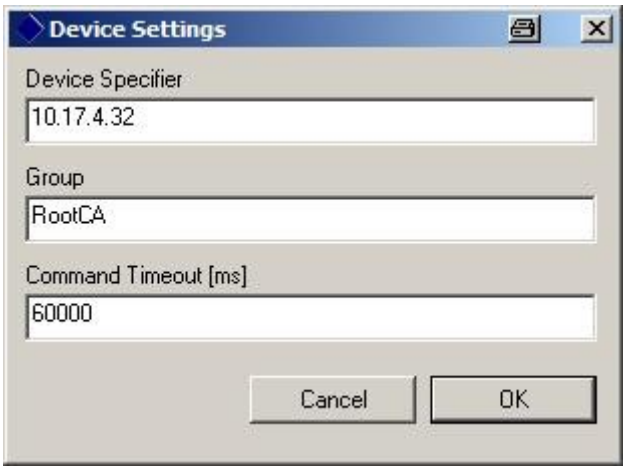

Figure 2 : Device settings

4. Now, you are prompted for a CryptoServer user logon. Only a user with administrative privileges can log on here. For example, select the default **ADMIN** user and press the **LOGON** button.

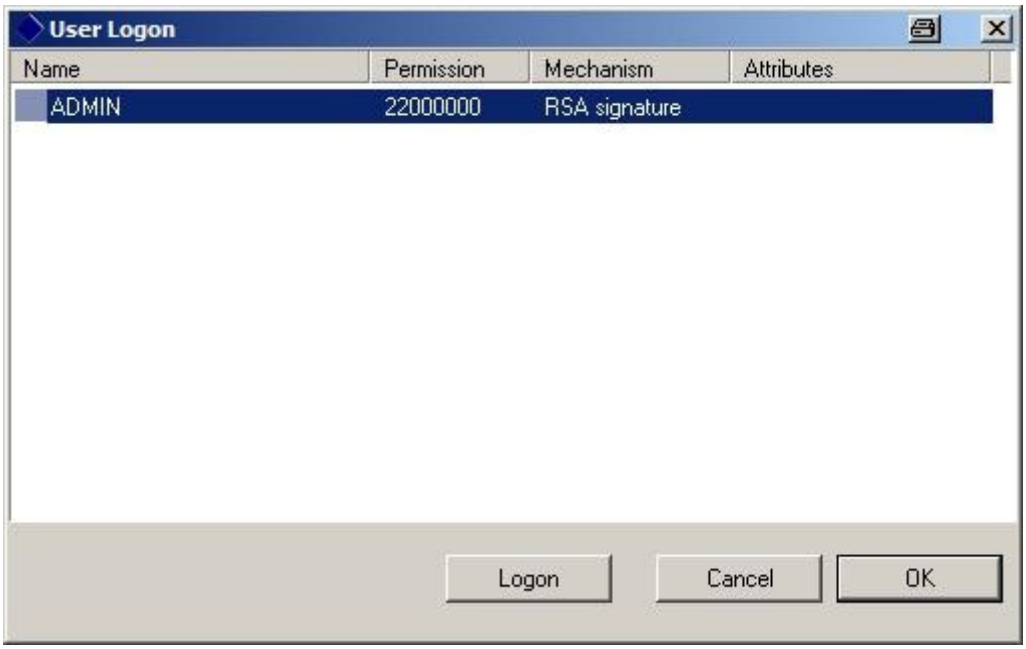

Figure 3 : User logon

5. The user credentials must be provided here. If you have selected a key-based user, you are prompted for the user key. Enter the source of the private user key and press **OK**.

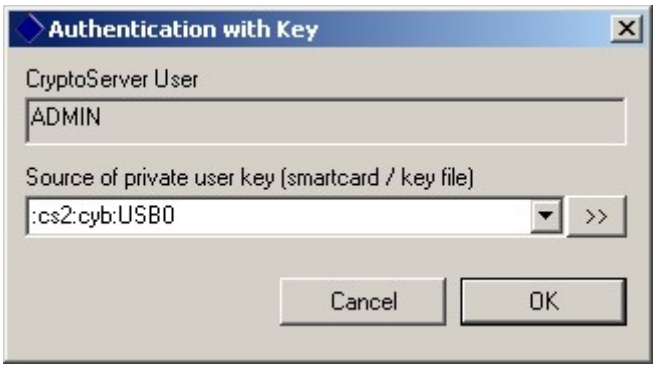

Figure 4 : Authentication with key

6. After a successful authentication, the user is logged on. Press the **OK** button to close the dialog.

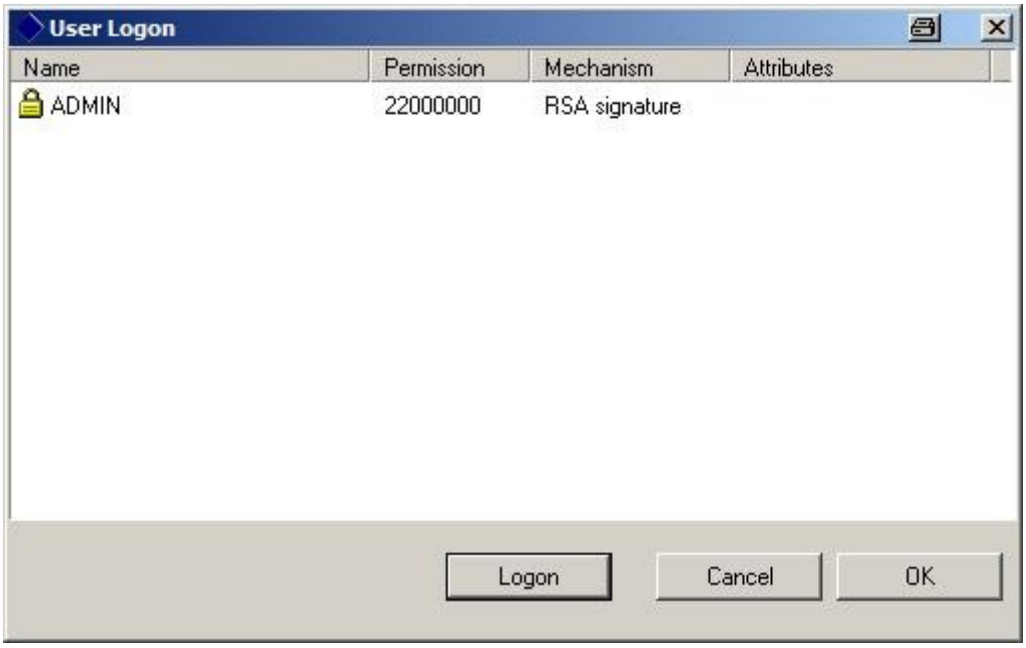

Figure 5 : User logon

7. The new registered device is shown in the list of known devices.

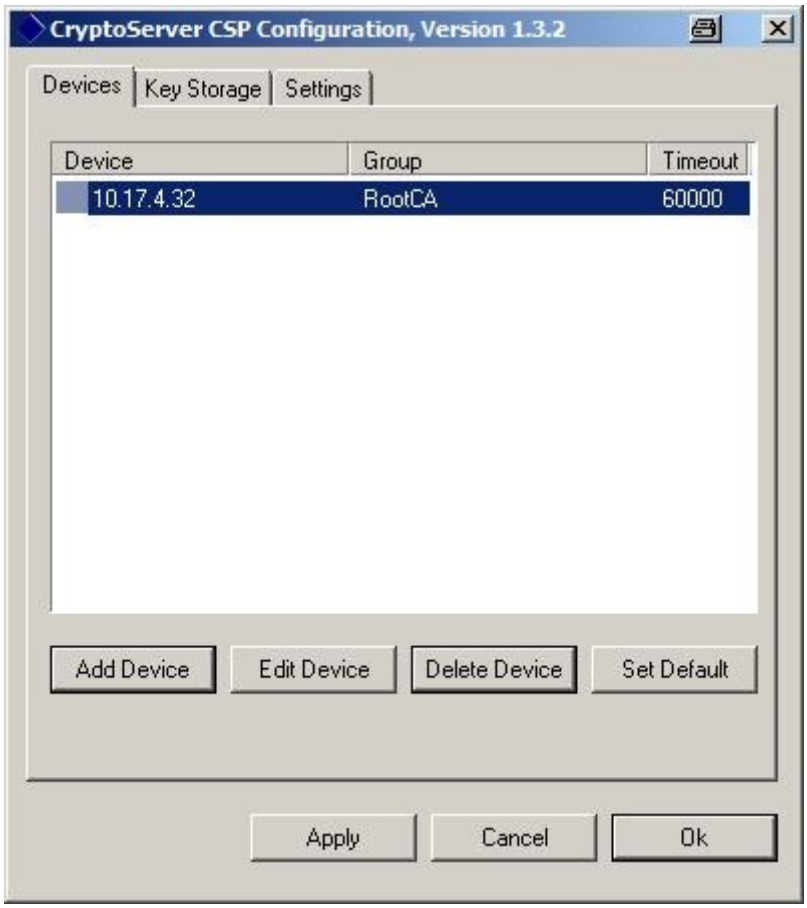

Figure 6 : CryptoServer CSP configuration

8. Select the device in the list and set it as default by pressing the SET DEFAULT button. In case of a cluster or failover scenario several other devices may be defined and shown here.

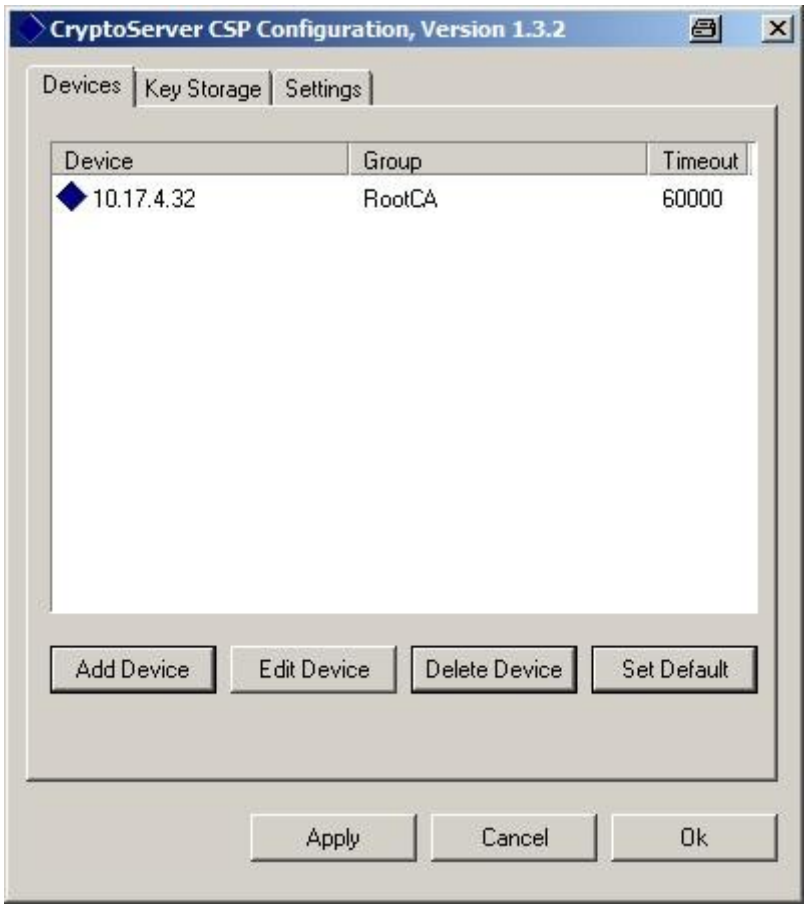

Figure 7 : CryptoServer CSP configuration

9. As the next step, the key storage export policy can be adjusted. Switch to the **KEY STORAGE** tab and set the key export policy as shown in the next figure. Then, click **OK** to leave the CryptoServer CSP Configuration window.

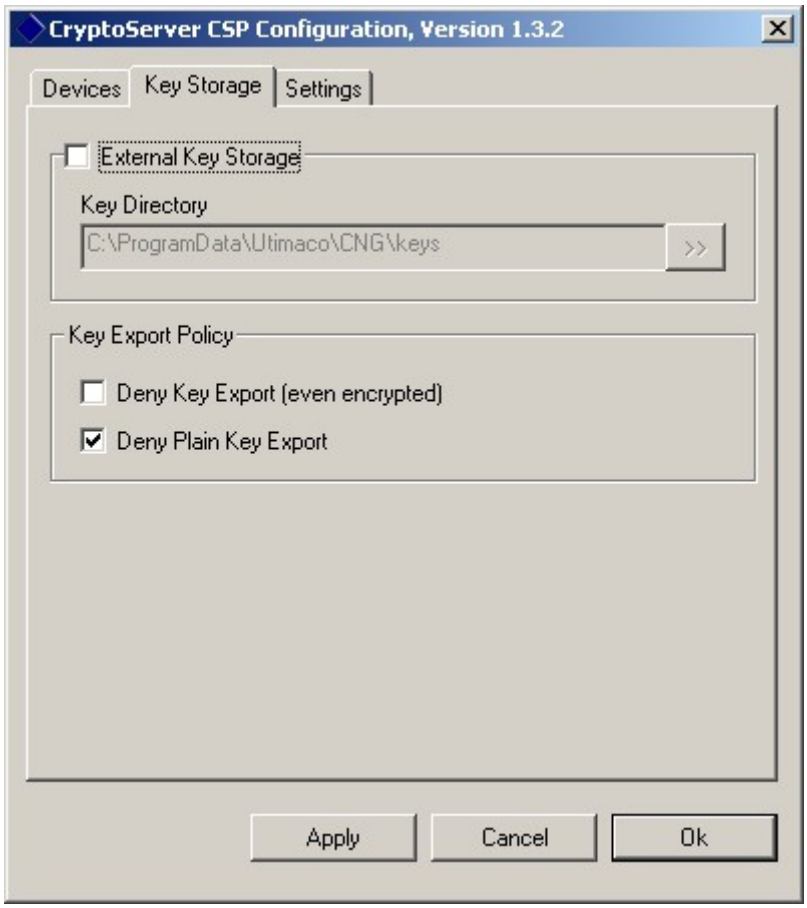

Figure 8 : CryptoServer CSP configuration

3.6 Install AD RMS and IIS

AD RMS is one of the available server roles in Windows Server 2008. You can add and configure it through the Server Manager. AD RMS root cluster may be composed of one or more AD RMS servers. This guide shows how to install and configure a single-server AD RMS root cluster. In this guide, the chosen domain name is utimaco.com.

3.6.1 Add ADRMSADMIN to Domain Admins group

For registering the service connection point (SCP), the installing user account must be a member of the Active Directory Enterprise Admin group:

1. Log on to ADRMS-DC as utimaco\Administrator (or any other user account in Domain Admins group).
2. Launch ACTIVE DIRECTORY USERS AND COMPUTERS (**Start → Administrative Tools → Active Directory Users and Computers**).

3. In the console tree, expand utimaco.com, double-click **USERS** and then double-click **ENTERPRISEADMINS**.
4. Click the Members tab and then click **ADD**.
5. Type adrmsadmin@utimaco.com, and then click **OK**.

3.6.2 Install and Configure the Server Roles AD RMS and IIS

1. Log on to ADRMS-SRV as utimaco\ADRMSADMIN.
2. To install AD RMS you have to add it to your current server installation. Start Server Manager (**Start → Administrative Tools → Server Manager**).
3. Click **ADD ROLES** in the Roles Summary Box and the Add Roles Wizard is started.
4. Click **NEXT** after reading the **BEFORE YOU BEGIN** section.
5. Select **ACTIVE DIRECTORY RIGHTS MANAGEMENT SERVICES** on the Server Role page. It informs you about dependent role services and features.
6. Internet Information Services (IIS) should be listed as such dependent role. Click **ADD REQUIRED ROLE SERVICES** and then click **NEXT**.
7. Click **NEXT** after reading the AD RMS introduction page.
8. Make sure the **Active Directory Rights Management Server** check box is selected on the **Select Role Services** page, and click **NEXT**.
9. Select the option **CREATE A NEW AD RMS CLUSTE**R and click **NEXT**.
10. Check **USE A DIFFERENT DATABASE SERVER**, click **SELECT** button, type ADRMS-DB into the **Select Computer** dialog box and confirm by clicking **OK**.
11. Select default as database instance, click **VALIDATE**, and click **NEXT**.
12. Click **Specify**, type in utimaco\ADRMSSRVC and the password of the account, click **OK** and **NEXT**.

ADRMSSRVC is the name of the AD RMS service account, which was created during user configuration with the Active Directory Domain Controller.

13. Check the **USE CSP KEY STORAGE** option for storing the AD RMS cluster key, and click **NEXT**.

14. Now you should be able to select **UTIMACO CRYPTOSERVER CSP** as the cryptographic service provider.
15. Ensure that a new key will be created with the selected CSP, and click **NEXT**.
16. Verify that **DEFAULT WEB SITE** is marked as the web site where the AD RMS will be hosted.
17. Select the option **CHOOSE A CERTIFICATE FOR SSL ENCRYPTION** later, and click **NEXT**.
18. Type in adrms-srv.utimaco.com (same as FQDN) as a friendly certificate name, and click **NEXT**.
19. Select **REGISTER THE AD RMS SERVICE CONNECTION POINT NOW** to register the AD RMS service connection point (SCP) in Active Directory during the installation, and click **NEXT**.
20. Click **NEXT** after reading the IIS introduction page.
21. Keep the default check box selections for the Web Server installation, and click **NEXT**.
22. Click **Install** to start the AD RMS installation, and click **Close** as soon the installation is complete.

Read the next chapter to create a self-signed certificate for SSL connection, and to complete the installation.

3.6.3 Create a Self-Signed Certificate with IIS and Complete the Installation

1. Open the INTERNET INFORMATION SERVICES (IIS) MANAGER (**Start → Administrative Tools → Internet Information Services (IIS) Manager**).
2. Select ADRMS_SRV (UTIMACO\adrmsadmin) on the left.
3. Scroll down to IIS in the ADRMS_SRV Home window and double-click **SERVER CERTIFICATES**.
4. Click the **CREATE SELF-SIGNED CERTIFICATE** link on the right.
5. Type in adrms-srv.utimaco.com as a friendly name and click **OK**.
6. Expand **SITES** in the menu on the left and click **DEFAULT WEB SITE**.
7. Click the link **BINDINGS** on the right.

8. Select the HTTPS connection in the list and click **EDIT** or **ADD** one if it doesn't exist.
9. Then, you should be able to select the previously created, self-signed certificate as SSL certificate. Click **OK** and **CLOSE**.
10. Finally, right-click **DEFAULT WEB SITE** and select **SET WEB SITE DEFAULTS**. Make sure https is set as enabled protocol.
11. Click **RESTART** (on the right) to restart the IIS Server.
12. Log off from the server and then log on again as utimaco\ADRMSADMIN to update the security token of the logged-on user account.
13. You can start AD RMS now (**Start → Administrative Tools → Active Directory Rights Management Services**).

Any user who is logged on after AD RMS server role installation is automatically made a member of the AD RMS Enterprise Administrators local group.

3.7 Verify AD RMS functionality

Since MS Windows Vista is running on ADRMS-CLNT, an additional installation of AD RMS client is not required. For earlier versions of the Windows operating systems an AD RMS client is available to download. For verifying the AD RMS functionality, we refer to the third step of the Windows Server AD RMS step by step guide. You might perform the following actions on ADRMS-CLNT for the users to work with right-protected content:

1. Add the URL of the AD RMS cluster (https://adrms-srv.utimaco.com) to the LOCAL INTRANET SECURITY ZONE in Internet Explorer for all users.
2. Log on as utimaco\NHOLLIDA and restrict permissions of a Microsoft Word 2007 document that only utimaco@engineering group may access but not change (**Microsoft Office Button → Prepare → Restrict Permission → Restricted Access**).
3. Log on as utimaco\SRAILSON and verify that permissions to read the document are granted, since this user is a member of the engineering group.
4. Log on as utimaco\LHENIG and verify that this user is not allowed to open the document.

4 Troubleshooting

The following table lists problems you might encounter when you integrate Active Directory Rights Management Services with SafeGuard CryptoServer.

Problems	Solutions
Removing AD RMS fails.	Uninstall AD RMS without uninstalling IIS simultaneously first. Then reboot and uninstall IIS.
While installing AD RMS the following error occurs: *"Attempt to configure Active Directory Rights Management Server failed. The AD RMS installation could not determine the certificate hierarchy..."*	Unregister old AD RMS Service Connection Point (SCP) with RMS Administration Toolkit SP2 (chapter 3.2) and rerun the installation.
While validating access to the database server during AD RMS installation: *"An error has occurred while establishing a connection to the server. When connecting to SQL Server 2005, this failure may be caused by the fact that under the default settings SQL Server does not allow remote connections."*	Activate local and remote connections on ADRMS-DB: *Start → Programs → MS SQL Server → Configuration Tools → Configuration → SQL Surface Area Configuration → Services and Connections → Database Engine*, then start SQL Server Browser.
While configuring bindings of Default Web Site setting up a new SSL certificate fails. (*"A specified logon session does not exist."*)	Do it again (confirm the error message, keep the bindings settings and click OK again).

Problems	Solutions
It is not possible to add protection to a document on ADRMS-CLNT.	1. Try to ping every instance within the AD RMS infrastructure. 2. Make sure an email address is configured for the user on the domain controller. 3. Make sure "https" is set as "Enabled Protocol": *Start → Administration Tools → IIS Manager*, then navigate to *ADRMS-SRV → Sites*, right click on *Default Web Site* in the middle of the window and select *Set Web Site Defaults*. 4. Watch the events of AD RMS and IIS in the *Server Manager.*

Table 3: List of problems and their solutions

5 Further Information

This document forms a part of the information and support which is provided by the Utimaco Safeware. Additional documentation can be found on the product CD in the documentation directory.

6 Contact and Support Information

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Krefelder Str. 220
52070 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Krefelder Str. 220
52070 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.