Symantec

Endpoint Encryption

Symantec Encryption Desktop 10.4.1

Integration Guide

CryptoServer HSM

SecurityServer 4.10.0

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	2026-07-17
Status	PUBLISHED
Document No.	IG-2026-0070

Table of Contents

1 Introduction

This paper provides an integration guide explaining how to integrate a Utimaco CryptoServer Hardware Security Module (HSM) with Symantec Encryption Desktop 10.4.1 on a Windows Server 2012 R2 using the CNG interface to offload cryptographic operations from the server and to protect the private keys within the HSM.

Configuration details - especially relating to Active Directory Domain Services (ADDS) and Active Directory Certificate Services (ADCS) as well as Symantec Encryption Desktop - that go beyond normal configuration for the integration of hardware security module are not explained in this document. For more detailed information on these specific topics, please refer to the Microsoft Developer Network (MSDN) and to the documentation provided by Symantec.

2 Overview

Symantec Encryption Desktop provides comprehensive security for user endpoint computers, making it possible for enterprises, workgroups, and individuals to protect sensitive information without changing the existing IT infrastructure or disrupting work processes. This easy-to-use solution encrypts email, files, virtual volumes, and entire disks from a single desktop application by means of using OpenPGP.

OpenPGP is the most widely used email encryption standard. It is defined by the OpenPGP Working Group of the Internet Engineering Task Force (IETF) as a Proposed Standard in RFC 4880. OpenPGP was originally derived from the PGP software, created by Phil Zimmermann.

CryptoServer is a hardware security module developed by Utimaco IS GmbH. It is a physically protected specialized computing unit designed to perform sensitive cryptographic tasks and to securely manage and store cryptographic keys and data. It can be used as a shared independent security component for heterogeneous computer systems.

3 Requirements

Ensure that you have a copy of the *Microsoft CSP/CNG Integration Guide* from Utimaco. You should also have prepared a Windows Server 2012 R2 operating system.

HSM Model	CryptoServer Se Gen2-Series/ CSe-Series PCIe CryptoServer Se Gen2-Series/ CSe-Series LAN CryptoServer Simulator
HSM Firmware	SecurityServer Version 4.10.0
Software	Windows Server 2012 R2 Symantec Encryption Desktop 10.4.1

Table 1: Software and hardware requirements

3.1 Supported Systems

The integration of Symantec Encryption Desktop and CryptoServer was successfully tested with the following operating systems and CryptoServer firmware:

Operating System	Security Server Version	Symantec Encryption Desktop Version
Windows Server 2012 R2	4.10.0	10.4.1

Table 2: Supported systems

4 Prerequisites

This chapter covers the installation steps and post-deployment configuration that need to be performed for the various applications and services that are a prerequisite for the actual integration.

1. Install Symantec Encryption Desktop and skip the steps for generating a new PGP key. Refer to the Symantec Encryption Desktop documentation for more details regarding all necessary steps to install Symantec Encryption Desktop, including where to download the software, as well as performing the installation.
2. Install and configure the Utimaco CSP/CNG Provider as described in Chapter 2 of the *Microsoft CSP/CNG Integration Guide*.
3. Install Microsoft Windows Server Active Directory Domain Services and perform the necessary post-deployment configuration required to promote the server to a domain controller.
4. Install Microsoft Windows Server Active Directory Certificate Services and perform the necessary post-deployment configuration for Active Directory Certificate Services, and set up an Enterprise Certification Authority (CA). When asked to select a cryptographic provider, select **RSA#Utimaco CryptoServer Key Storage Provider**.

5 Configuration

Before PGP keys can be created and imported in Symantec Encryption Desktop that are generated and protected by the CryptoServer, the CA needs to be configured to:

1. Create a certificate template and issuing properties for a PGP User certificate.
2. Support the newly created PGP User certificate template.

5.1 Configure the CA to Create a Certificate Template and Issuing Properties for a PGP User Certificate

1. Open the Microsoft Management Console by typing in **mmc** in the **Run** dialog.
2. In the Microsoft Management Console select **File Add/Remove Snap-in…**
3. Select **Certificate Templates** in the list with available snap-ins, click **Add**, and then click **OK**.

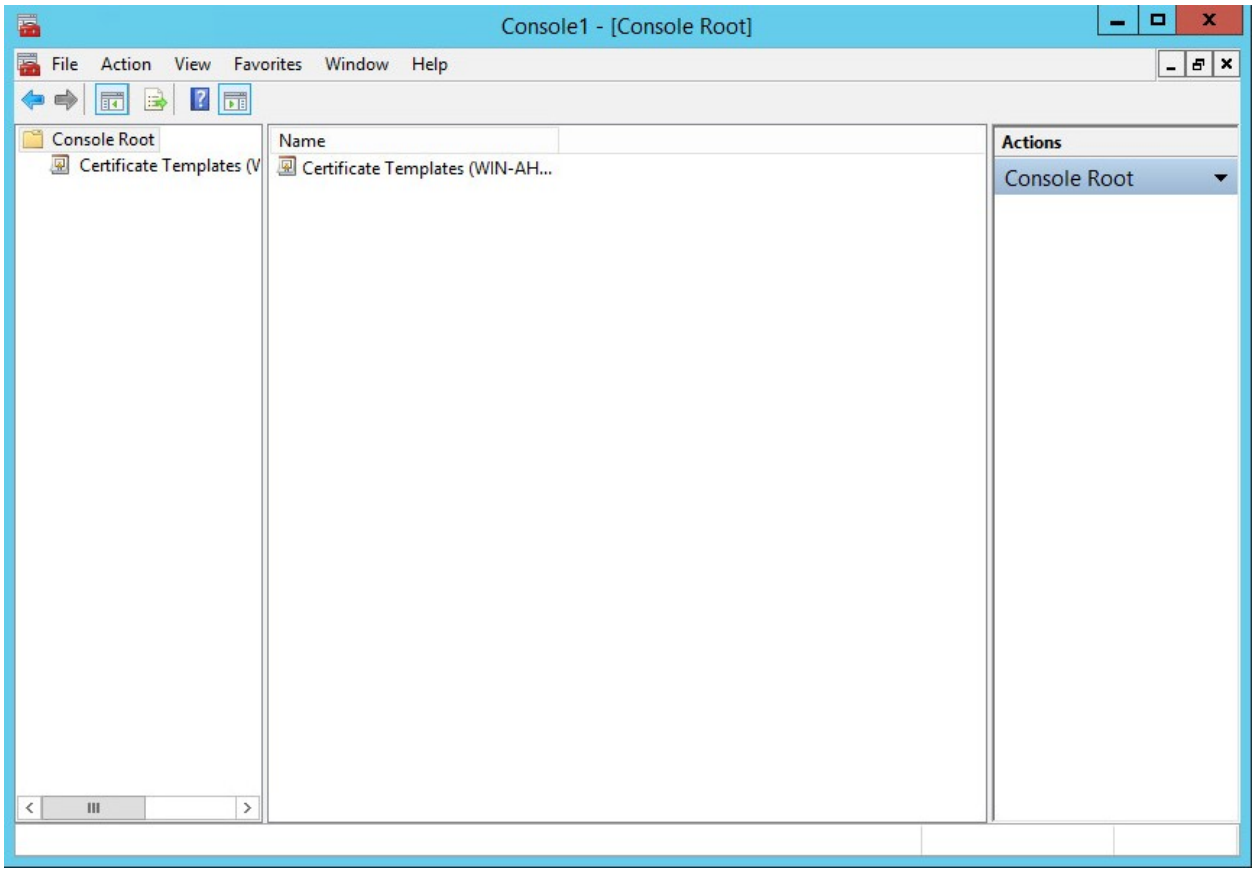

Figure 1 : Microsoft Management Console - certificate templates

4. Under Console Root, expand the **Certificate Templates** snap-in. In the middle section, all certificate templates available to the CA are listed.
5. Scroll down the list until the **User** template, right-click and click **Duplicate Template**.
6. In the pop-up dialog that appears, select the **General** tab.
7. Enter the Template display name, e.g. PGP User, and ensure that **Publish certificate in Active Directory** is selected.

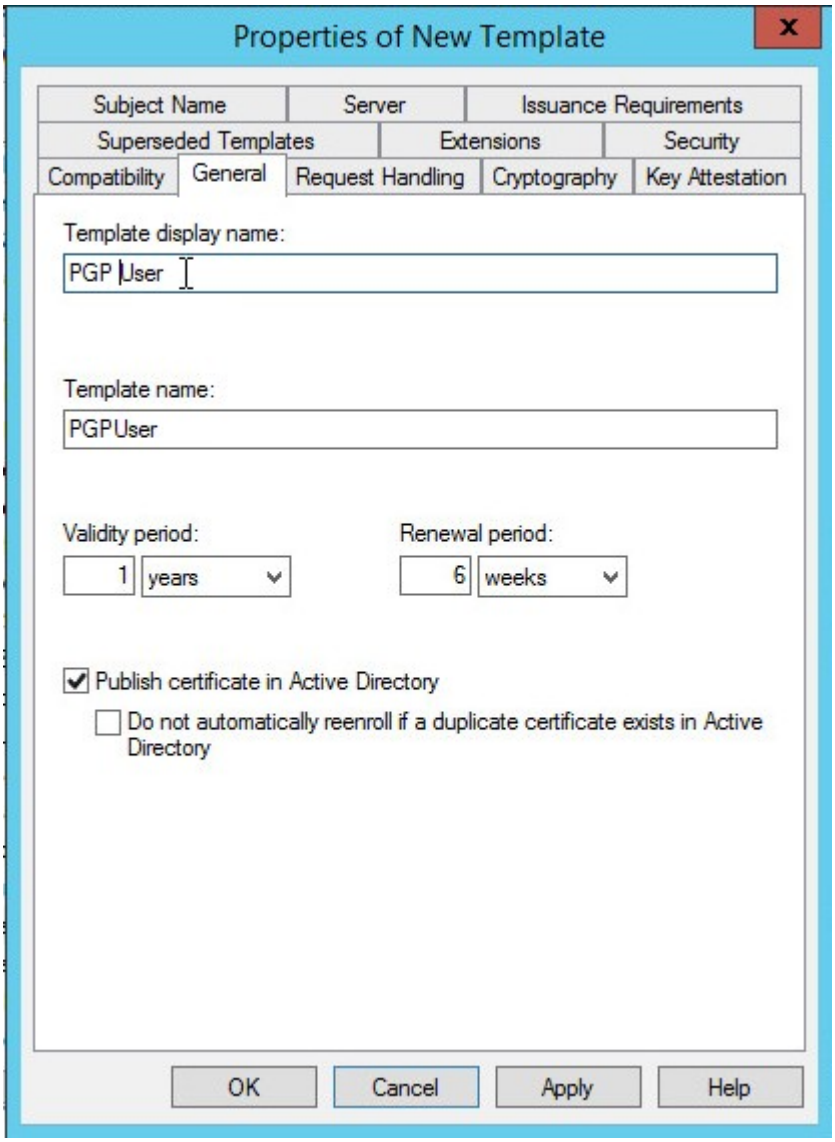

Figure 2 : Microsoft Management Console - properties of new template

8. Select the Compatibility tab and choose the following compatibility settings from the corresponding pulldown lists:

    a. Certification Authority: **Windows Server 2012 R2**.

    b. Certification recipient: **Windows 7 / Server 2008 R2**.

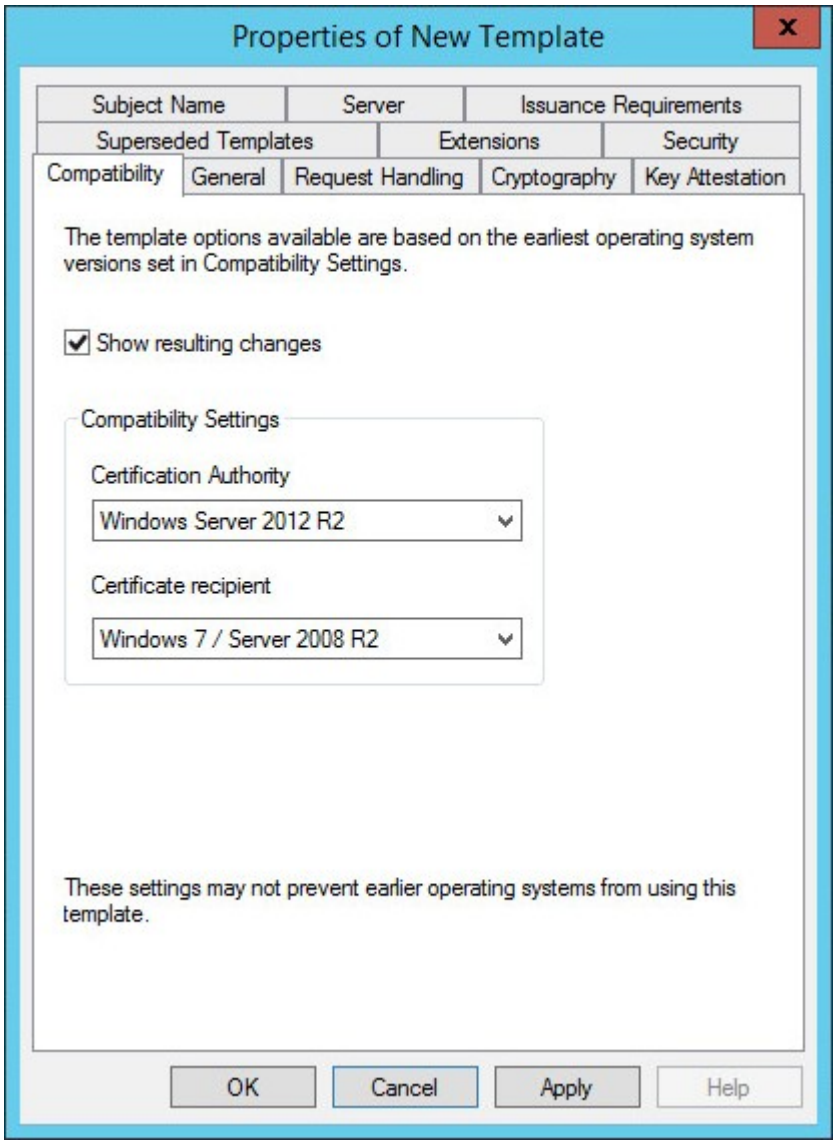

Figure 3 : Microsoft Management Console - properties of new template

9. Select the Cryptography tab and ensure that Provider Category **Key Storage Provider** is selected.

Choose **Request must use one of the following providers** and select **Utimaco CryptoServer Key Storage Provider**. Finally select the requested hash, e.g. SHA256.

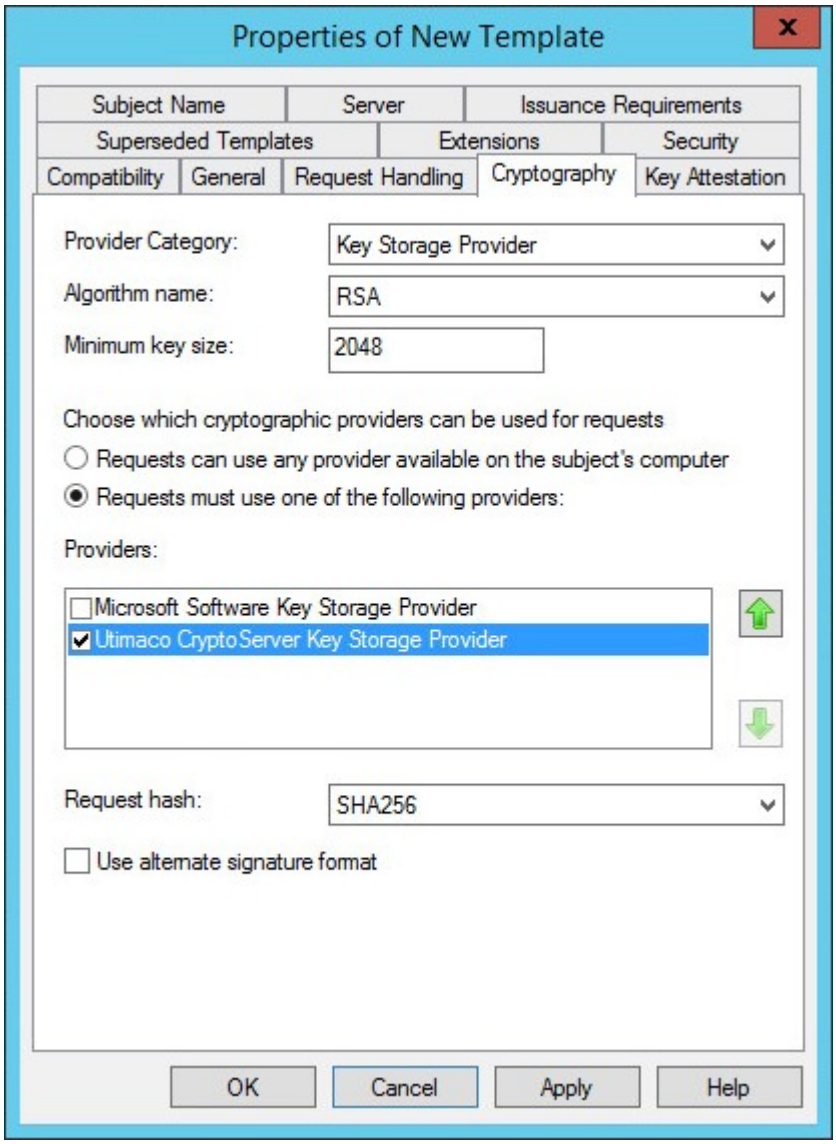

Figure 4 : Microsoft Management Console - properties of new template

10. Select the **Subject Name** tab and uncheck the **Include e-mail name in subject name** and **E-mail name** check boxes.

11. Select the **Security** tab and:

    a. Add and provide the Read and Enroll permissions for the following:
        i. Authenticated Users.
        ii. Administrator b For Domain Admins and Enterprise Admins, make sure that Read, Write, and Enroll check boxes are ticked.

12. Click **Apply** and then **OK**.

13. Close the Microsoft Management Console.

5.2 Configure the CA to Support the Newly Created PGP User Certificate Template

1. From the Start menu select **Control Panel Administrative Tools Certification Authority**.
2. In the console tree (left-hand section), expand the CA. (It has a computer and a green tick next to it.).

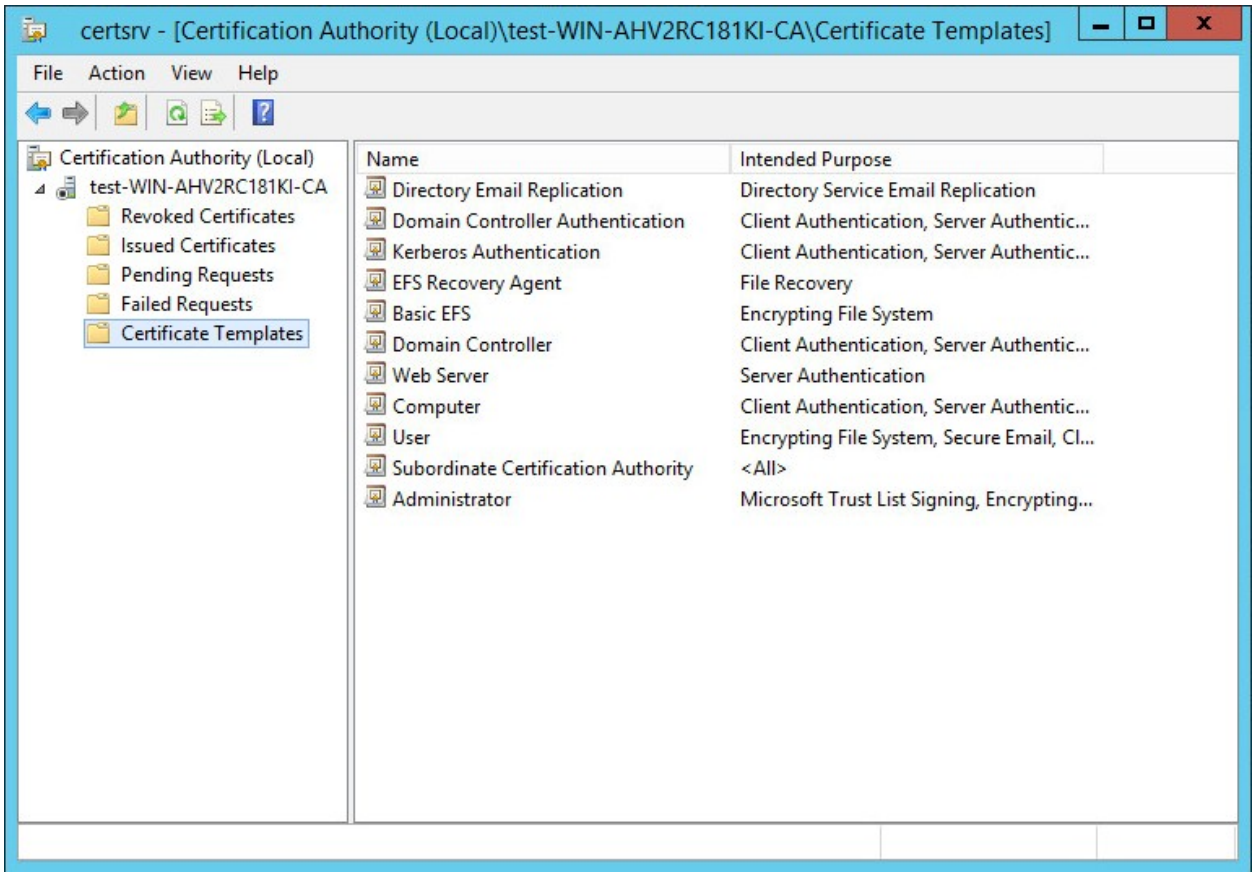

Figure 5 : Certification Authority

3. In console tree of the Certification Authority, right-click **Certificate Templates**, and then click **New Certificate Template to Issue**.
4. In Enable Certificates Templates, select the **PGP User** template and then click **OK**.

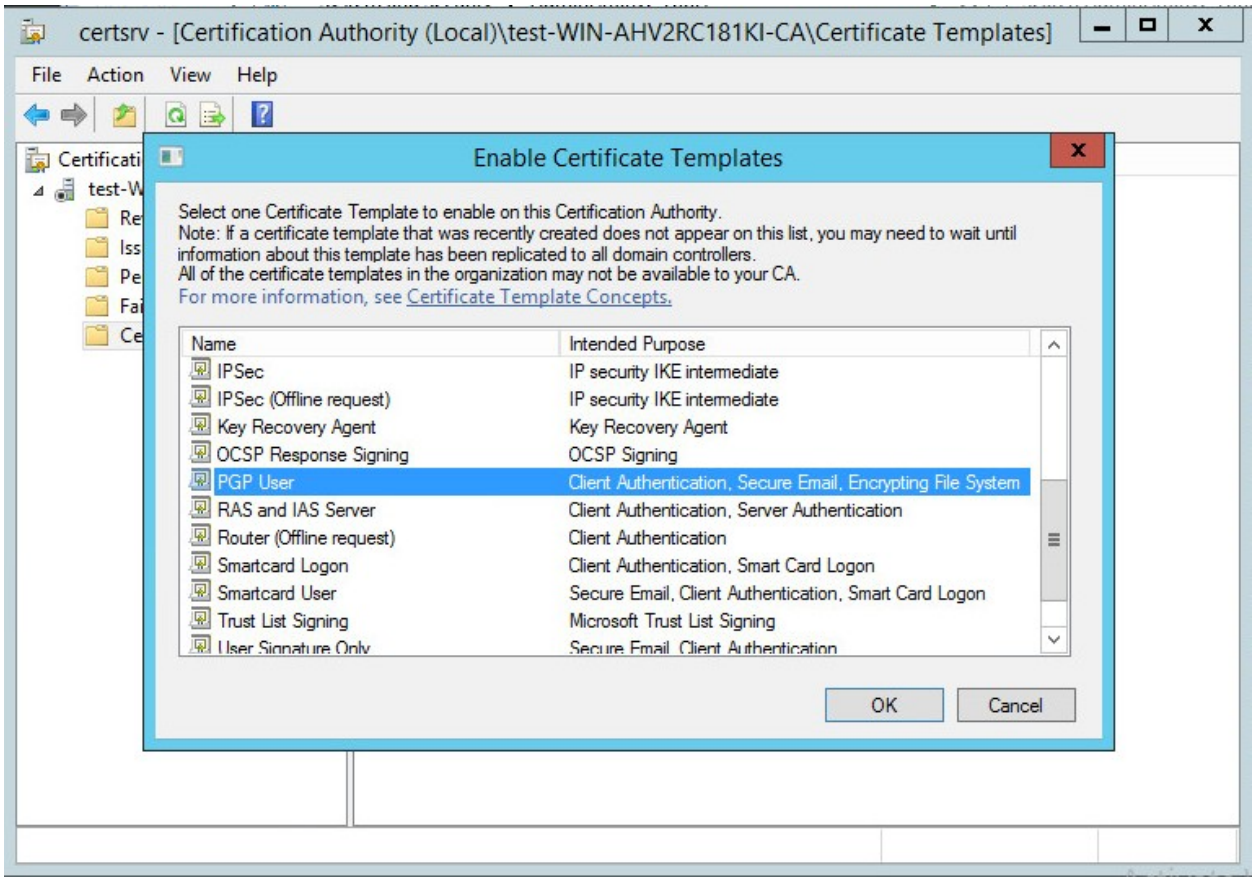

Figure 6 : Certification Authority - Enable Certificate Templates

5. Open Certificate Templates in the Certification Authority and verify that the modified certificate templates appear in the list.
6. Close the Certification Authority.

6 Creating a Key and Requesting a Certificate

Now the CA has been set up to issue PGP User certificates, we can enroll it and one can create a key and request a certificate.

1. Open the `certmgr.msc` from the location `C:\Windows\SysWow64`.
2. In the Microsoft Management Console that appears, right-click on the **Personal** folder and select **All Tasks Request New Certificate…**
3. Click **Next**, select **Active Directory Enrollment Policy** and then click **Next**. It will show the certificate template that has been configured, i.e. PGP User.
4. Click on **Details** and then **Properties**.
5. The Certificate Properties window will open. Select the **Subject** tab.
6. Select **Common Name** under **Subject Name** and provide the fully qualified domain name for the computer on which you are installing the certificate in the **Value** field. Click **Add**.
7. Click on **General** tab and provide the **Friendly Name**. For example, PGP User.
8. Click on **Private Key** tab, and ensure that *RSA,* **Utimaco CryptoServer Key Storage Provider** is selected as cryptographic service provider (CSP).

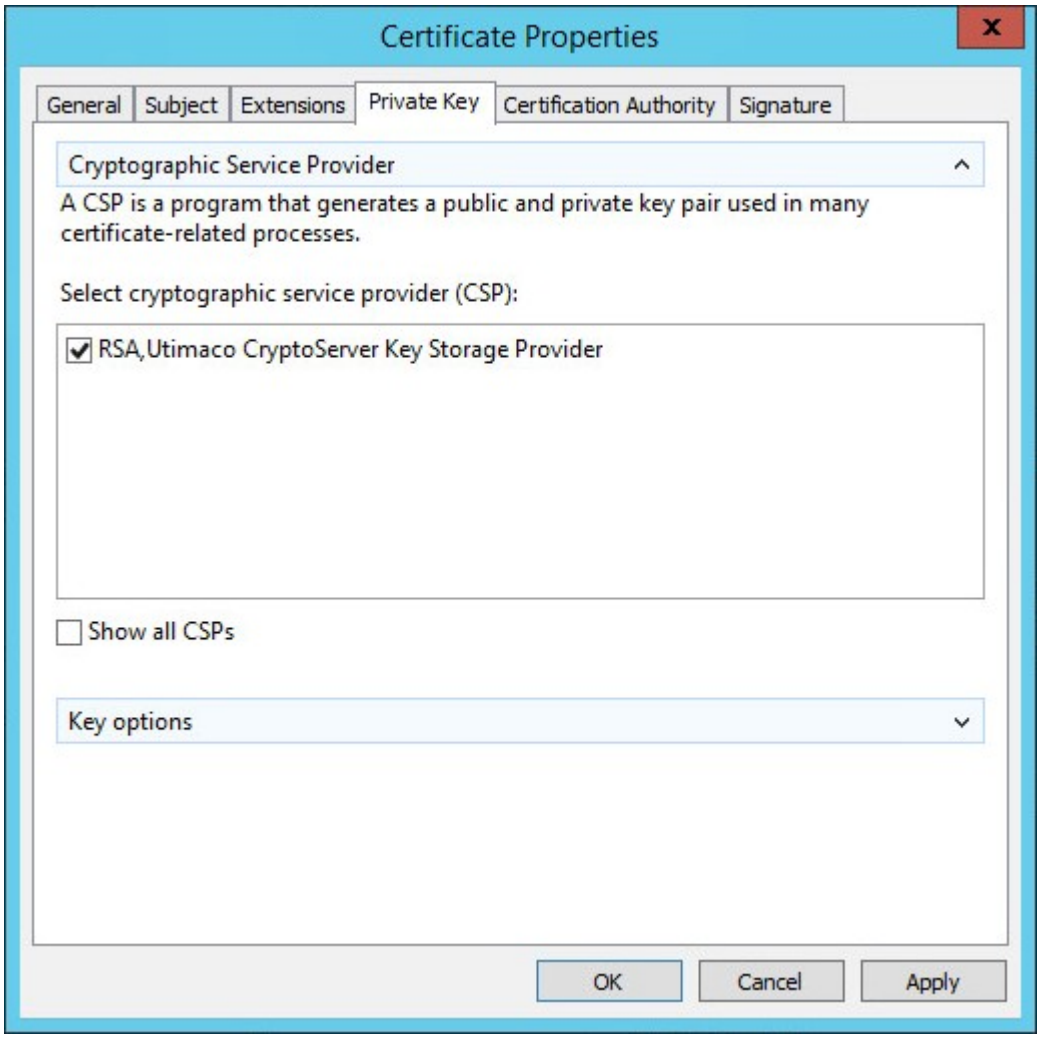

Figure 7 : Certificate Properties

9. Click on **Certificate Authority** tab and make sure that **Enterprise Root CA** is selected.
10. Click **Apply** and then **OK**.
11. Select the **PGP User** certificate template and click **Enroll**.

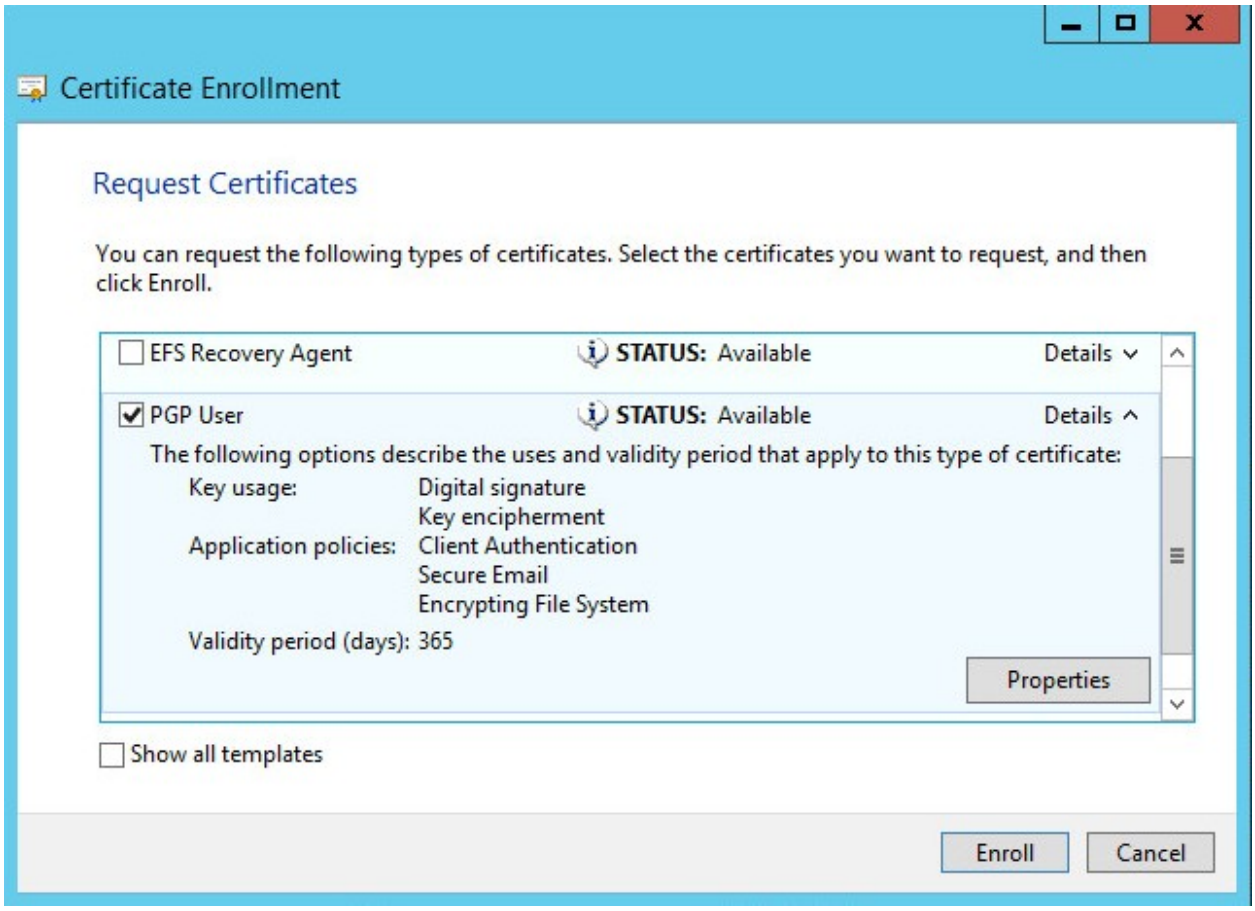

Figure 8 : Certificate Enrollment

12. When enrollment has succeeded, click **Finish**.
13. Make sure that the PGP User certificate is now available in the Personal Certificate store.
14. Double click on the certificate and see the **You have a private key that corresponds to this certificate** message.

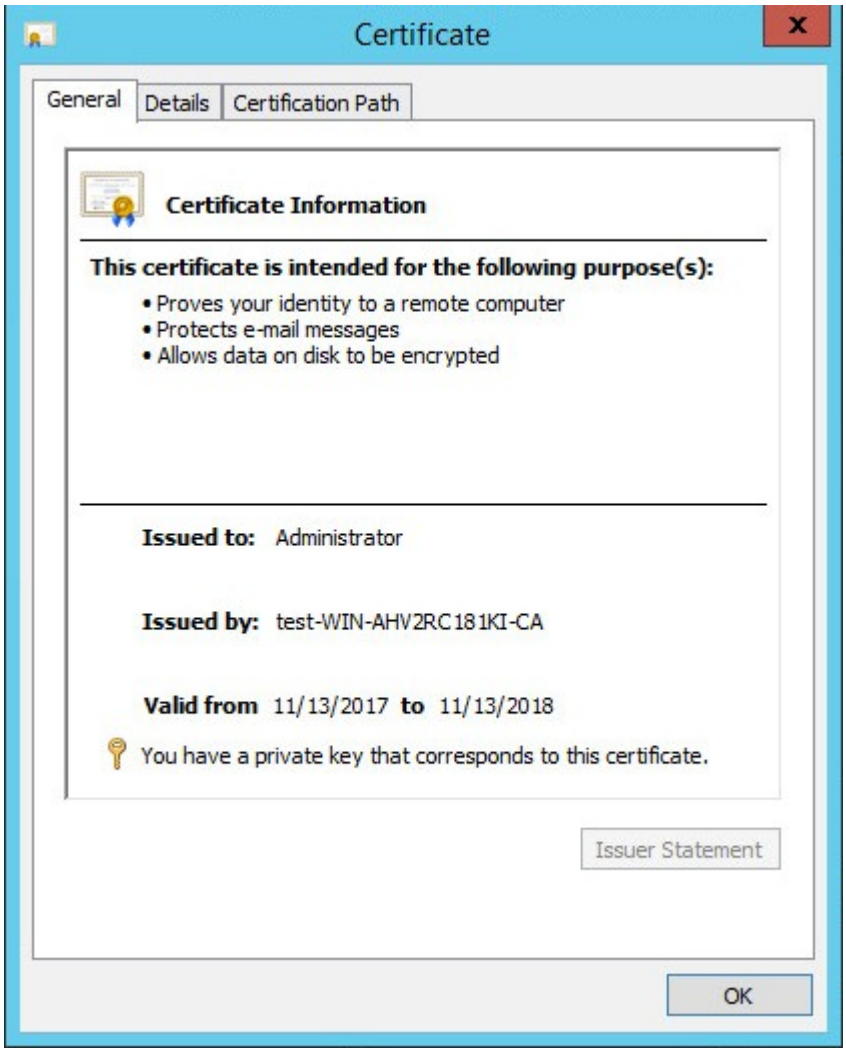

Figure 9 : Certificate

15. The keys for this certificate have been generated on the CryptoServer. You can list the keys on the CryptoServer by means of invoking the cngtool ListKeys command from the command prompt.

7 Importing and Using the Keys in Symantec Encryption Desktop

To be able to use the keys/certificates protected by the CryptoServer with Symantec Encryption Desktop, it is necessary to import them in the current key ring files:

1. Open the Symantec Encryption Desktop and select **PGP Keys** on the left side of the window.

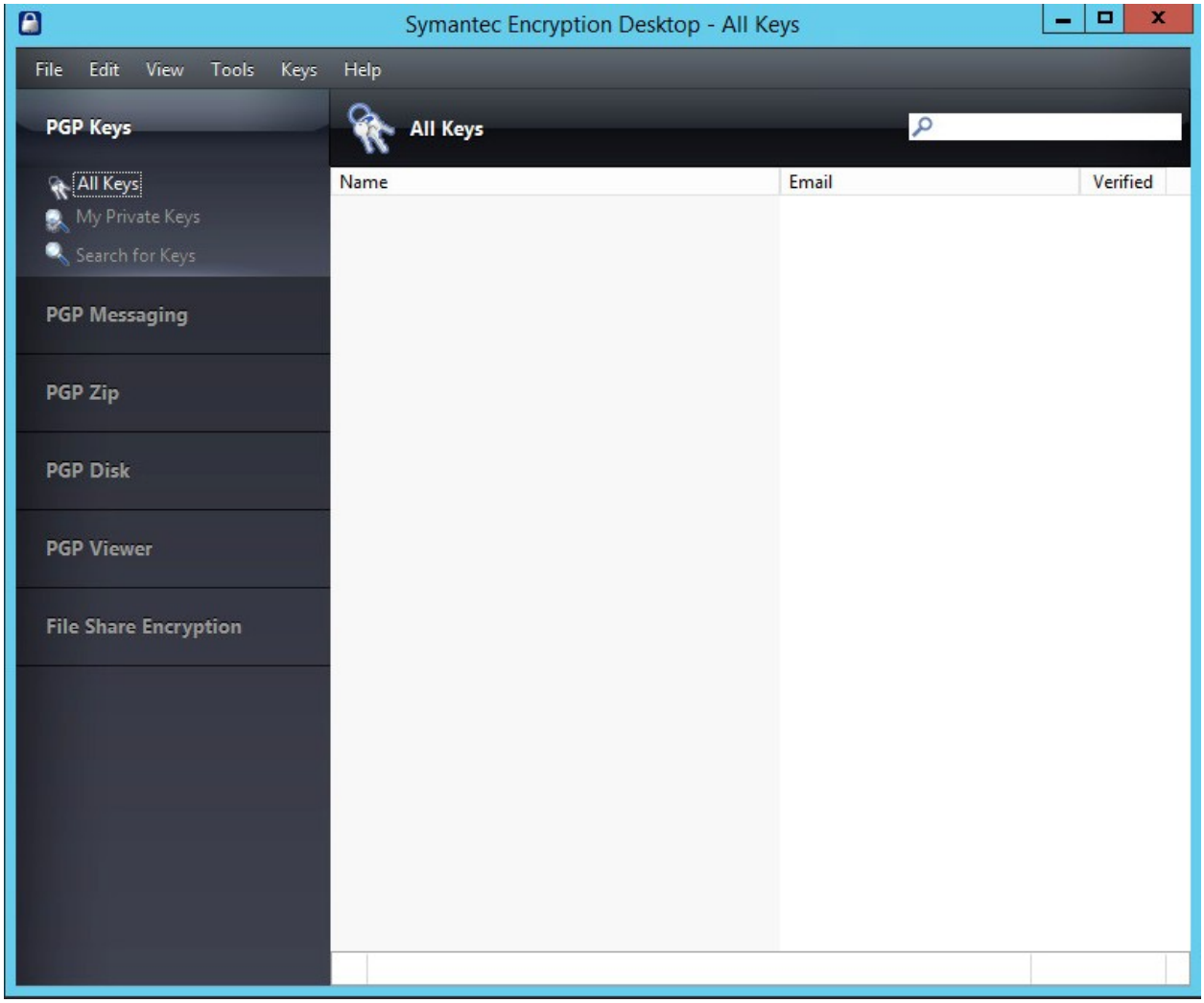

Figure 10 : Symantec Encryption Desktop - All Keys

2. From the File menu choose **Import Personal Certificate(s)…**, click **Finish**.
3. Confirm the list of certificates found to be imported into the PGP Key Ring. Double click to open the properties window to see the details.

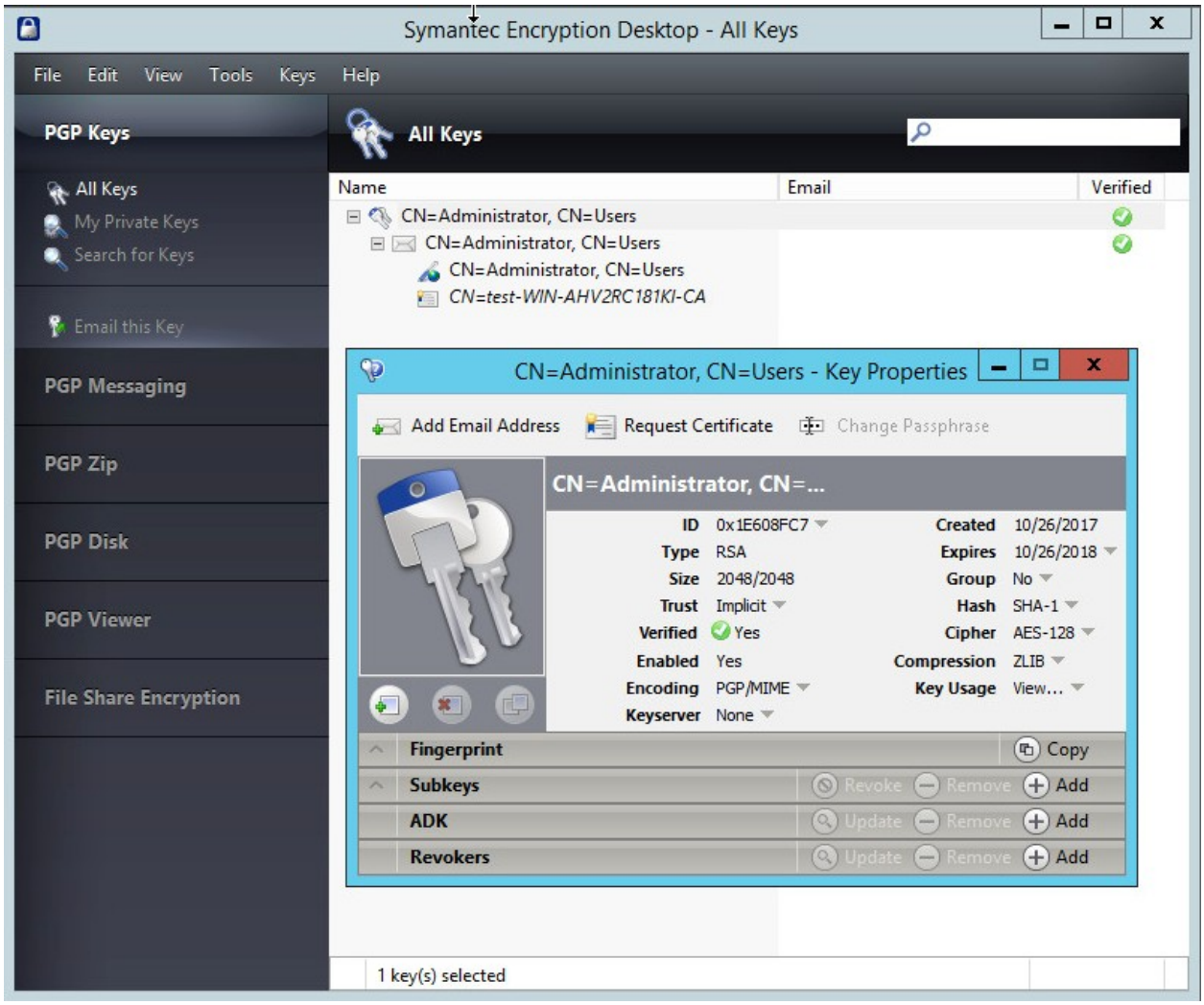

Figure 11 : Symantec Encryption Desktop - All Keys

4. The certificate protected by the CryptoServer can now be used in all PGP applications. After importing the keys/certificates in Symantec Encryption Desktop, the keys protected by the CryptoServer can be used in the same way as any other keys available in the PGP key ring.

8 Further Information

This document forms a part of the information and support which is provided by Utimaco IS GmbH.

Additional documentation can be found on the product CD in the documentation directory.

9 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.