Microsoft
Azure HYOK

Integration Guide

CryptoServer HSM

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	2026-05-18
Status	PUBLISHED
Document No.	IG-2026-0040

Table of Contents

1 Introduction

More and more companies are moving into the cloud; some even apply a “cloud first” strategy. If public clouds such as Microsoft Azure are used, data must be protected sufficiently, also to meet legal requirements. Such protection can be achieved with encryption. Necessary encryption keys could be stored in the cloud, for example in the key management systems of the cloud providers. However, in doing so, companies will give up control of their keys, it might be difficult to migrate the keys to another provider, and multi-cloud strategies are impossible.

Hosting your own keys is a viable alternative, especially if you already own an HSM. Then, a VPN tunnel between your cloud installation and the on-premise HSM can be created, and the applications running in the cloud can perform cryptographic operations using the local HSM. Depending on the internet connectivity of your company, higher latency must be considered.

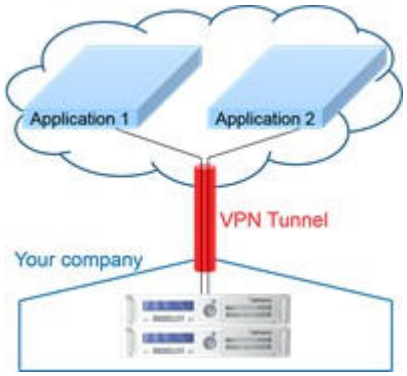

Figure 1 : VPN tunnel

In this scenario, you have full control of your HSM, including physical access required e.g., for key ceremonies. Moreover, your in-house applications can also have access to the HSMs. Last but not least, the full feature set of Utimaco CryptoServer HSMs is available, including applications written with CryptoServer SDK or CryptoScript and running on - and thus protected by - the HSM.

This integration guide shows how to set up such an HYOK scenario with Azure. We assume that the reader is familiar with Azure and has already set up a Virtual Network (VN) with a Virtual Machine (VM). The reader should also be familiar with installing the Utimaco SecurityServer software and with using the CryptoServer HSM.

2 VPN Setup

Setting up the Virtual Private Network (VPN) connection requires work in Azure and locally. Before starting, please check that you have a gateway device that was tested by Microsoft (see VPN devices documentation) or that your device supports the IPsec/IKE parameters described in that document. You may also consult your device manufacturer for integration guides. Detailed VPN setup is beyond this integration guide; please ask your networking staff for further assistance.

2.1 Azure Setup

In the following, we assume a Site-to-Site or a Multi-Site connection. Please check the About VPN Gateways document for an explanation and more options.

Setup on Azure is described very well in the VPN site-to-site tutorial. In short, you have to create a virtual network gateway (including a local subnet and a public IP address), a local network gateway, and a VPN connection between them. Make sure to select the correct VPN type (route-based or policy-based) depending on your needs and/or your VPN gateway requirements. If your only intention is to connect one or more on-premise HSMs to Azure, you can rely on static routing and you do not need to enable BGP in the local network gateway. Instead, you should specify the IP range of your local internal network where the HSMs are located.

2.2 Local Setup

If your gateway was tested by Microsoft, you can find links to the configuration guides in the *VPN devices documentation*. Typically, you have to setup IKE and IPsec with the given pre-shared key for authentication. Note that only Diffie-Hellman group 2 (MODP 1024) is possible. For policy based VPNs, we recommend to use AES256 and SHA256 for IKE encryption and hashing; for route based VPNs, you should use AES-GCM256. With static routing, you also need to announce the virtual network's subnet that should have access to the HSM(s).

2.3 Connection Check

After the VPN connection has been established, the HSM can be accessed from an Azure VM. For the rest of the document, we assume that the environment variable CRYPTOSERVER is set to the IP address of the HSM, reachable via the VPN. Then, running `csadm getstate` should return status information of the CryptoServer.

3 Additional Security

Since SecurityServer release 4.10, the CryptoServer HSM can also authenticate against the user/host application. Thus, your application running in an Azure VM can be sure to talk to the right HSM. To enable this feature, export the public HSM authentication key to a file:

›_ Console

```
csadm GetHSMAuthKey > hsmkey.txt
```

We recommend to perform this operation on-premise as close as possible to the HSM and to copy the resulting file to the VM. On the VM, set the environment variable CS_AUTH_KEYS to the file path.

Now, each time an application wants to authenticate against the HSM, the HSM also needs to authen-ticate against the application (“mutual authentication”). You can check by renaming or moving the file or by changing the CSxxxxxx number in the file – an error will occur when you try `csadm Login…`.

4 Conclusion

Setting up a HYOK scenario with Azure is usually simple and straightforward. The creation of a VPN tunnel between your company and Azure is independent from the HSM, and once the tunnel has been established the HSM can be reached via IP as if it was on a local network. Mutual Authentication provides additional security for such remote connection scenarios.

5 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.