

Member of Microsoft Intelligent Security Association

Microsoft Security

Time Stamp Option Pack

nShield[®] HSM Integration Guide for Microsoft 365

© 2023 Entrust Corporation. All rights reserved.

Table of Contents

1. Introduction
1.1. Requirements
2. Setup
2.1. Install the root certificate of TSS on the client machine
2.2. Edit the registry settings
3. Procedures
3.1. Add a signature line to a document
3.2. Sign the signature line in a document
4. Troubleshooting

Chapter 1. Introduction

Microsoft 365 (previously called Microsoft Office) is a productivity suite for Microsoft Windows. The Microsoft 365 applications include Microsoft Word, Microsoft Excel, and Microsoft PowerPoint. Microsoft 365 also permits users to create, control, and digitally sign documents.

You can integrate Microsoft 365 with a Entrust Time Stamp Option Pack to permit the use of time stamping to seal documents. The Entrust Time Stamp Option Pack is referred to in this guide as Time Stamp Server (TSS). TSS is a time stamp appliance, which uses the industry-standard IETF RFC 3161 protocol to provide time stamps. TSS also provides a secure auditable trail of time for the purposes of nonrepudiation. In this way, you can time stamp an Microsoft document to validate that document's authenticity at the time it was time stamped.

1.1. Requirements

Entrust has successfully tested the integration between TSS and Microsoft 365 in the following configurations:

Operating System	Microsoft 365 version	TSS version	HSM	Security World Version	Firmwar e
Microsoft Windows Server 2019 (x64)	Microsoft 365 2022	8.0	Solo XC	12.80.5	12.80.5



Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

Chapter 2. Setup

To enable Microsoft 365 to use a specified TSS appliance for its default time stamp service, you must:

- Install the root certificate of TSS on the client machine.
- Edit the registry settings.

2.1. Install the root certificate of TSS on the client machine

To install the root certificate of TSS on the client machine:

- 1. Log into the TSS as the security officer (**superuser**).
- In the left pane, navigate to **TSA Management** > **Operational Status**. For example:



- 3. Select the TSA Name, then select Cert Info.
- 4. Select the certificate and **Export** it to a .cer file. For example:

	TIME STAMP SERVER		
TSA Management Operational Status Configuration	TCA Vou Ctatua:	TSA Certificate Info - tsaid_0	
Clock Management Time Stamps Issued Server Management Cogging User Management About Log out		V3 6310 BCD5 3842 F753 1648 471D 4D36 B386 RSA with SHA-256 CN=Test1;OU=nShield TSS ESN:5C0F-03E0-D947;O=Er 2022/09/01 14:08:21 (UTC) 2023/09/01 14:08:21 (UTC) RSA - 2048 3082 0122 300D 0609 2A86 4886 F70D 0101 0105 0003 8	

- 5. On the client machine, enter **certmgr** on the Windows **Start** menu to start the Microsoft Certificate Manager.
- In the left pane, navigate to Certificates > Trusted Root Certificate Authorities > Certificates.
- 7. Import the exported .cer file. For example:

File Action View Help					
🗢 🔿 📶 📋 🙆 💀 🛛 🖬					
🙀 Certificates - Local Computer 🔺	Issued To	^	Issued By	^	
> 🚞 Personal	🗔 AAA Ce	rtificate Services	AAA Certificate Services		
Trusted Root Certification	AddTrus	t External CA Root	AddTrust External CA Root		
Certificates			Baltimore CyberTrust Root		
> Enterprise Irus All Tasks	; >	Import	Certum CA		
> Intermediate C	>	rusted Network CA	Certum Trusted Network CA		
> Instanted Publish		ublic Primary Certificat	Class 3 Public Primary Certificatio		
Third-Party Ro		D RSA Certification Au	COMODO RSA Certification Auth		
Trusted People	ist	t (c) 1997 Microsoft C	Copyright (c) 1997 Microsoft Corp.		
Client Authent Help		CorporateCA	DatacardCorporateCA		
> Preview Build Koots		-CorporateCA	DatacardCorporateCA		
> 📔 Test Roots	🗔 DigiCert	Assured ID Root CA	DigiCert Assured ID Root CA		
> 📔 AAD Token Issuer	🔄 🗔 DigiCert	Global Root CA	DigiCert Global Root CA		
> 🚞 Dell Trust	🔤 DigiCert	Global Root G2	DigiCert Global Root G2		
> in eSIM Certification Authori	🗔 DigiCert	Global Root G3	DigiCert Global Root G3		
> 📋 Homegroup Machine Cer	DigiCert	High Assurance EV Ro	DigiCert High Assurance EV Root		
K 🤗 Remote Derkton	<			. *	
Add a sectificate to a store	-			_	

The certificate is added.

2.2. Edit the registry settings

To edit the registry settings:

- 1. On the Microsoft 365 computer, enter **regedit** on the Windows **Start** menu to start the Registry Editor.
- 2. In the left pane, navigate to **Computer** > **HKEY_CURRENT_USER**.
- 3. Export the **HKEY_CURRENT_USER** registry settings as a backup before you continue. For example:



 Navigate to the following registry path: Computer\HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Signatures.



If the registry path does not already exist, you must create it.

5. Add the following variables to the registry path:

Name	Туре	Data
MinXAdESLevel	REG_DWORD	2
Timestamp Required	REG_DWORD	1
TSALocation	REG-SZ	http:// <tss_ip_address>/ TSS/HttpTspServer</tss_ip_address>
XAdESLevel	REG_DWORD	5

In this table, <TSS_IP_address> is the IP address of the TSS appliance. You may use a host name instead of an IP address.

Chapter 3. Procedures

To test and use the time stamping functionality:

- Add a signature line to a document.
- Sign the signature line in a document.

These procedures are described in the following sections.

3.1. Add a signature line to a document

To add a signature line to a document:

- 1. Open the document in Microsoft Word.
- 2. Click the location in the document where you want to add the signature line.
- 3. On the ribbon, select the **Insert** tab and locate the **Text** group.
- 4. Click the arrow next to **Signature Line**, and then select **Microsoft Office Signature Line**. For example:



5. The Signature Setup dialog appears. For example:

Signature Setup	?	×			
Suggested <u>s</u> igner (for example, John Doo	Suggested <u>s</u> igner (for example, John Doe):				
Suggested signer's <u>t</u> itle (for example, Manager):					
Suggested signer's <u>e</u> -mail address:					
Instructions to the signer:					
Before signing this document, verify that the content you are signing is correct.					
Allow the signer to add <u>c</u> omments in the Sign dialog					
Show sign <u>d</u> ate in signature line					
OK Cancel	I				

6. Click **OK**.

3.2. Sign the signature line in a document

When you sign the signature line in an Microsoft 365 document, you add both a visible representation of your signature and a digital signature.

To sign the signature line in a document:

- 1. Open the document in Microsoft Word.
- 2. In the document, double-click the signature line where your signature is requested.
- 3. In the **Sign dialog**, add the required information. For example:

Sign	? ×				
① See additional information about what you are signing					
Before signing this document, verify that the content you are sign	iing is correct.				
Type your <u>n</u> ame below, or click Select Image to select a picture to signature:	o use as your				
X John Doe	Select Image				
To include information about the signer, click the details button	1. <u>D</u> etails				
Signing as: f4d9cfb4-1132-41ab-91fe-ee96e45d120c Issued by: MS-Organization-Access	C <u>h</u> ange				
Sign	Cancel				



Ensure the signer you choose is in the Trusted Certificates.

4. Click Sign.

A message about the certificate selected not being verified may appear. In this case, you can click **OK** to continue.

The document is signed. For example:

(i) MARKED AS FINAL An author has marked this document as final to discourage editing	. Edit Anyway
Recoverable Signature	
X John Doe	
John Doe	
Data Signed by: f4d9cfb4-1132-41ab-91fe-ee96e45d120c	

5. Click on the signed section of the document to confirm that the signature is valid. The signature type should be **XAdES-T**. For example:

Signature Details	?	×		
Recoverable Signature - The signer's certificate can't be verified, please try again later or check your network connection.				
X John Doe				
John Doe				
Signed by: f4d9cfb4-1132-41ab-91fe-ee96e45d120c				
<u>C</u> ommitment Type:				
Purpose for signing this document:				
Signing as: f4d9cfb4-1132-41ab-91fe-ee96e45d120c	<u>V</u> iew.			
Issued by: MIS-Organization-Access				
See the additional signing See information about	C			
information that was the signer	C	056		
collected				

Chapter 4. Troubleshooting

The following table provides troubleshooting guidelines.

Problem	Cause	Resolution
When attempting to sign a document, the Get a Digital ID dialog appears instead of the Sign dialog.	The Microsoft Office registry entries have not been changed correctly.	Follow setup steps again.
When attempting to sign a document, the following error appears:	Network issue.	Attempt to re-sign the document.
Signing cannot be completed due to problems applying the required timestamp. Check your network connection.		