SafeNet Authentication Client Integration Guide

Using SafeNet Authentication Client CBA for Office 365



All information herein is either public information or is the property of and owned solely by Gemalto and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2010 - 2017 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Document Number: 007-013412-002, Rev. B Release Date: May 2018

Contents

Third-Party Software Acknowledgement4
Description4
Applicability
Environment5
Audience
CBA Flow using SafeNet Authentication Client
Prerequisites
Supported Tokens and Smart Cards in SafeNet Authentication Client7
Configuring Office 365 and AD FS
Enabling Office 365 Federated Domains8
Configuring the AD FS Certificate Based Authentication Policy9
Running the Solution11
Connecting to Office 36511
Appendix: Connecting to SharePoint in Office 36513
Getting SharePoint URLs13
Connecting to SharePoint15
Appendix: Secure/Multipurpose Internet Mail Extensions (S/MIME) Configuration17
Export to SST file from the trusted Root CA17
Publish Certificate to GAL (Global Address List)21
Enable S/MIME in Office 365 OWA24
Support Contacts

Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Office 365.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

Remote access poses both a security and a compliance challenge to IT organizations. The ability to positively identify users (often remote users) requesting access to resources is a critical consideration in achieving a secure remote access solution. Deploying remote access solution without strong authentication is like putting your sensitive data in a vault (the datacenter), and leaving the key (user password) under the door mat.

A robust user authentication solution is required to screen access and provide proof-positive assurance that only authorized users are allowed access.

PKI is and effective strong authentication solution to the functional, security, and compliance requirements.

SafeNet Authentication Client (SAC) is a public key infrastructure (PKI) middleware that provides a secure method for exchanging information based on public key cryptography, enabling trusted third-party verification of user identities. Gemalto's certificate-based tokens and smart cards provide secure remote access, as well as other advanced functions, in a single token, including digital signing, password management, network logon, and combined physical/logical access.

The tokens come in different form factors, including USB tokens, smart cards, and software tokens. All of these form factors are interfaced using a single middleware client, SafeNet Authentication Client (SAC). The SAC generic integration with CAPI, CNG, and PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications, offering secure web access, secure network logon, PC and data security, and secure email. PKI keys and certificates can be created, stored, and used securely with the hardware or software tokens.

Office 365 from Microsoft is a cloud-based service that is designed to help meet your organization's needs for robust security, reliability, and user productivity.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to Office 365 using Gemalto tokens.

It is assumed that the Office 365 environment is already configured and working with static passwords prior to implementing Gemalto multi-factor authentication.

Office 365 can be configured to support multi-factor authentication in several modes. CBA will be used for the purpose of working with Gemalto products.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to Office 365 using Gemalto's tokens and smart cards.

It is assumed that the Office 365 environment is already configured and working with static passwords prior to implementing Gemalto multi-factor authentication.

Office 365 can be configured to support multi-factor authentication in several modes. CBA will be used for the purpose of working with Gemalto products.

Applicability

The information in this document applies to:

- SafeNet Authentication Client (SAC) Typical installation mode— SafeNet Authentication Client is public key infrastructure (PKI) middleware that manages Gemalto's tokens and smart cards.
- SafeNet Authentication Client (SAC) IDGo800 Compatible mode— IDGo800 Minidriver based package, uses Microsoft Smart Card Base Cryptographic Provider to manage Gemalto IDPrime MD smart cards.

For more details about different SAC installation modes, refer to the Customization section in *SafeNet* Authentication Client Administrator Guide.

• Office 365

Environment

The integration environment used in this document is based on the following software versions:

- SafeNet Authentication Client (SAC) Version 10.5
- Office 365 On Cloud
- AD FS On Windows Server® 2012 R2

Audience

This document is targeted to system administrators who are familiar with Office 365, and are interested in adding certificate based authentication capabilities using SafeNet tokens.

CBA Flow using SafeNet Authentication Client

The diagram below illustrates the flow of certificate-based authentication:



- 1. A user attempts to connect to Office 365. The user is redirected to AD FS proxy server (WAP) for authentication.
- 2. After successful authentication, the user is redirected to SafeNet Authentication Client (SAC) for a secondary authentication. The user uses the SafeNet token on which his certificate resides, and, when prompted, enters the token password.
- 3. The SAC authentication reply is sent back to AD FS, which returns a response to Office 365, accepting or rejecting the user's authentication request.
- 4. The user is granted or denied access to Office 365.

Prerequisites

This section describes the prerequisites that must be installed and configured before implementing certificatebased authentication for Office 365 using Gemalto tokens and smart cards:

- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. In general, any CA can be used. In this guide, integration is demonstrated using Microsoft CA.
- If SAM is used to manage the tokens, Token Policy Object (TPO) should be configured with MS CA Connector. For further details, refer to the section "Connector for Microsoft CA" in the SafeNet Authentication Manager Administrator's Guide.
- Users must have a Gemalto token or smart card enrolled with an appropriate certificate.
- SafeNet Authentication Client (10.5) should be installed on all client machines.

Supported Tokens and Smart Cards in SafeNet Authentication Client

SafeNet Authentication Client (10.5) supports the following tokens and smart cards:

Certificate-based USB tokens

- SafeNet eToken 5110 GA
- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 CC

Smart Cards

- Gemalto IDPrime MD 830 B
- Gemalto IDPrime MD 840 B
- Gemalto IDCore 30B eToken

For all supported devices please refer to SafeNet Authentication Client Customer Release Notes.

Configuring Office 365 and AD FS

Configuring Office 365 and AD FS requires the following:

- Enabling Office 365 Federated Domains, page 8.
- Configuring the AD FS Authentication Policy, page 9.

Enabling Office 365 Federated Domains

- 1. Log in to the AD FS server machine as a domain administrator.
- 2. Open Windows Azure AD Module for Windows PowerShell.
- 3. At the command prompt, type Connect-MsolService, and then click Enter.
- 4. In the Enter Credentials window, enter your Azure AD administrator username and password, and then click OK.

	Enter Credentials	? X	
S		522	
A 10		11 M	
Please entr	er credentials		
Diser Harrie		<u> </u>	
Easword.			

- 5. At the command prompt, perform the following steps:
 - a. Type Set-MsoIADFSContext -Computer <AD FS machine name>, and then click Enter.
 - b. Type **Convert-MsolDomainToFederated –DomainName <your domain name>**, and then click **Enter**.

🖉 Administrator: Windows Azure Active Directory M	todule for Windows PowerShell
PS C:\Users\administrator.SFNTDEMO\Desktop> PS C:\Users\administrator.SFNTDEMO\Desktop> tdemo.com	Connect-MsolService Set-MsolADFSContext -Computer ad.sfn _ ≡
PS C:\Users\administrator.SFNTDEMO\Desktop> NAme sfntdemo.com Successfully updated 'sfntdemo.com' domain. PS C:\Users\administrator.SFNTDEMO\Desktop>	Convert-MsolDomainToFederated -Domai

- 6. Open the AD FS Management Console.
- 7. In the left pane, under **Console Root**, click **AD FS > Trust Relationships > Relying Party Trusts**. In the right pane, Microsoft Office 365 Identity Platform should be listed as a trust.

AD FS	Relying Party Trusts			
Service Trust Relationships	Display Name	Enabled	Туре	Identifier
Claims Provider Trusts Claims Provider Trusts Relying Party Trusts Attribute Stores Authentication Policies	Microsoft Office 365 Identity Platform Device Registration Service	Yes Yes	WS-T WS-T	https://login.microsoftonline.com/ext um:ms-drs:2012-adfs.sactests.com

Configuring the AD FS Certificate Based Authentication Policy

- 1. On the AD FS Management console, in the left pane, under AD FS, click Authentication Policies.
- 2. In the right pane, click Edit Global Primary Authentication.



3. On the Edit Global Authentication Policy window, on the Primary tab, ensure that Certificate Authentication is selected for both Extranet and Intranet.

		Edit Global Au	uthentication	Policy	×
Primary	Multifactor				
Select users to If Integ authen	authentication o have a choic rated Windows tication method	methods. By selecting i s of what method to au authentication method I on browsers that supp	more than one auth thenticate with at s I is specified, it app port Integrated Wind	entication method, ign in. ears as the default dows authentication	you enable 1.
	oms Authentio	ation			
	Certificate Auth	entication			
	et oma Authenio Nindows Authe Certificate Auth	ation ntication entication			
Ena	ible device aut	hentication			
			ОК	Cancel	Apply

4. Click OK.

Running the Solution

Connecting to Office 365

- 1. Open the following URL in a web browser: https://login.microsoftonline.com
- 2. On the Office 365 login window, enter your AD user name (for example, Bob@sactests.com), and then click Next.



3. You will be redirected to your organization's login page. Select the user certificate and click OK.



4. On the **SafeNet Authentication Client Token Logon** window, enter the token password, and then click **OK**.

SafeNet Authenti	cation Client gemal	0
Enter the Token Password		
Token Name:	My Token	
Token Password:	I	
	Current Language: EN	
This is no unliggered on	v for evaluation use only	

5. After successful authentication, you are granted access to the **Office 365** dashboard.

Good a	fternoo	n				٩	Search apps, do	ocuments, people	, and sites	
Apps								In	stall Office apps 🔗	
02	4	w	x	P	N	S	TB	y≑	D	
Outlook	OneDrive	Word	Excel	PowerPoint	OneNote	SharePoint	Teams	Yammer	Dynamics 365	
_										
Flow										
Explore all your	$apps \rightarrow$									
Documen	ts						Ť	Upload and Op	en New 🗠	
Recent Pin	ned Shared	with me D	scover							

Appendix: Connecting to SharePoint in Office 365

Users can connect to SharePoint in Office 365 using their AD credentials and smartcards. Administrator will provide SharePoint URLs to users.

Connecting to SharePoint in Office 365 requires:

- Getting SharePoint URLs, Page 13
- Connecting to SharePoint, Page 15

Getting SharePoint URLs

1. Log in to Office 365 admin center as an administrator.

Good afternoon			21		
Apps				Install Office	e apps \vee
📴 Outlook 🛛 🏠 OneDrive	Word	Excel	PowerPoint	OneNote	
SharePoint TB Teams	Y ≑ Yammer	Dynamics 365	Flow	Admin	
Compliance					
Explore all your apps $ ightarrow$					
Documents			Ť∪	pload and Open	New ~
Recent Pinned Shared with me Disc	over				⊞
		A series of the series of the series of	# selides		

2. Click Admin. You will be redirected to the Admin Center page.

	Office 365 Admin center			Q	@ ?	8
>	Home 🖉 Customize your home					Gemalto
ŵ	Search users groups settings or tasks		٥			
8	man a sold 3 other sounds of other					
RR						
堛	Office 365 Enter	prise E3 setup is 50% complete. G Get apps	et someone to help you.			
	Go to setup	•				
e						
<u>ين</u>	DirSung Stature	Q. Active upper >	Pilling \			
P		X Active users >				
L2	last synced more than 3 days ago	+ Add a user	Total balance: \$0.00			
Ş	no recent synchronization	Edit a user Recet a percurate	 View my bill 			
4 3		- Reset a password				
		. B	1	@ Ne	eed help?	Feedback

3. In the left pane select Admin centers > SharePoint.

	Office 365 Admin center		¢ @ ?	8
>	Home 🖉 Customize your h	iome		Gemalto
ඛ	Search users around settings	or tasks		
R	bearen esers, groups, settings	01.000K3 Z*		
я ^р	Admin contere			
-6	Exchange Df	65 Enterprise E3 setup is 50% complete. Get someone to help you. Get apps		
	Skype for Business ⊡*	to setup		
្	SharePoint 🗅			
0	OneDrive II Open SharePoint ac	min center in a new tab		
P	Yammer ⊡'	Active users > Billing >		
<u>ل</u> د	PowerApps 😅	+ Add a user Total balance: \$0.0	00	
æ	Flow C	Delete a user D Update payment i D Edit a user View mv bill	details	
() }	Security & Compliance Cf	Q Reset a password		

In the right pane, the Office 365 SharePoint URLs are listed.

te collections	Site Collections		
fopath er profiles	New Decte Properties Owners Straining Baye Storage	e Recycle	
5	Search by URL.	1.00 TB available of 1.00 TB	1200 resources available
rm store		STORAGE USED (GB)	SERVER RESOURCE QUOTA
cords management	https://testgemalto.sharepoint.com	0.00	300
arch	https://testgemalto.sharepoint.com/portals/hub	0.00	0
	https://testgemalto.sharepoint.com/search	0.03	0
cure store	https://testgemalto-my.sharepoint.com	0.00	0
ops			
aring			
ttings			
nfigure hybrid			
ress control			

4. Share any or all of the SharePoint URLs with other users.

Connecting to SharePoint

- 1. In a web browser, open any of the Office 365 SharePoint URLs received from the administrator.
- 2. On the Office 365 login window, enter your AD user name (for example, Bob@sactests.com), and then click Next.

MC -		
and the second	Microsoft	-
	Sign in	Charles of Contraction of Contraction
	bob@sactests.com	
	Back Next	at Section
the standard and the	Can't access your account?	
		The second second second second
TAR ATRACT		
Tex Alter Ark	地名美国豪尔特	
The same of the set		
A CASE OF		
		©2018 Microsoft Terms of use Privacy & cookies · ·

3. You will be redirected to your organization's login page. Confirm the certificate and click OK.

	SAC Select a certificate that you want to use for authentication. If you cancel the operation, please cloge your browser and thy again.
Windows Security	
Confirm Certificate Confirm This certificate by clicking OK. If this is not the correct cert click Cancel.	ance
	© 2013 Microsoft

4. On the SafeNet Authentication Client login window, enter the token password, and then click OK

SafeNet Authent	cation Client	gemalto
Enter the Token Password		
Token Name:	My Token	
Token Password:	1	
This is an unlicensed co	Current Language: EN by for evaluation use only.	
	·····	OK Cancel

After successful authentication, the Office 365 SharePoint console is displayed.

Office 365			\$?		
BROWSE PAGE			Q SHARE	/ EDIT	34
s>	Safenet Team Site	Search this sit	e .	v	Q
Home Notebook Documents Site Contents Recycle Bin	Get started with your site reasons this Share your site. Share your site.				
	Documents Tree Control Control Control By Traditic - April 16, 2003 - yarivas Drag files here to uplaad				

Appendix: Secure/Multipurpose Internet Mail Extensions (S/MIME) Configuration

Office 365 uses encryption in two ways: in the service and as customer control. S/MIME allows the user to encrypt email messages.

S/MIME protects your emails from unwanted access.

In order to configure S/MIME with Office 365 the user needs an Enterprise E3 license, in order to upload the certificate via the outlook email client.

Prerequisites:

- 1. Login as Windows Administrator.
- 2. Install MS KB as follows:

X86: Windows6.1-KB2819745-x86.msu

x64: Windows6.1-KB2819745-x64-MultiPkg.msu

Export to SST file from the trusted Root CA

1. On the CA computer, open the certificate manager, and select Run > certmgr.msc.



2. Expand Trusted Root Certification Authorities > Certificates.

🛏 🔿 🙍 🛅 🗂 🖬 🖬 🖬				
Certificates - Current User Certificates - Current User Certificates - Current User Certificates Certificate	Issued To AddTrust External CA Root EddTrust External CA Root EddTrust External CA Root Comparison CyberTrust Root Comparison Comparison DigiCet High Assurance EV Ro Entrust Root Certification Auth Equifax Secure Certification Auth Equifax Secure Certificate Auth EddbalSign GliobalSign Root CA EddbalSign GliobalSign Root CA EddbalSign GliobalSign Root CA EddbalSign Comparison EddbalSign Comparison EddbalSign Eddba	Issued By Issued By AddTrust External CA Root Baltimore CyberTrust Root Class 3 Public Primary Certificatio Copyright (c) 1997 Microsoft Corp. DigiCett High Assurance EV Root Entrust Root Certificate Authority GeoTrust Global CA Go Daddy Class 2 Certificate Authorit. Microsoft Root Certificate Authori Microsoft Root Certific	Expiration Date 5/30/2020 5/13/2025 8/2/2028 12/31/1999 11/10/2031 11/10/2031 11/27/2026 8/22/2018 5/21/2022 3/18/2029 1/28/2028 6/29/2034 1/1/2020 12/31/2020 6/24/2035 3/23/2036 1/8/2004 8/31/2022 8/31/2022 8/31/2022 6/29/2034 7/17/2036	Intended Purpos Server Authentic Server Server Authentic Server Authentic Server Authentic Server Authentic Server Authentic Server Authentic Server Authentic Server Authentic Server Authentic Server Authentic

3. Right click on the certificate which you bought for your business email (in our lab we used a self-signed CA, therefore we will use the Root CA certificate), then select **All Tasks > Export.**

🦀 certmgr - [Certific	ates - Current U	ser\Trusted Root	Certification Authorities\Certi	ficates]	_ 🗆 X
File Action View Help					
🗢 🔿 🙍 📷 🔏 🖬 🗙 🗟 🖬					
Certificates - Current User Personal Certificates - Current User Personal Certificates Cilient Authentication Issuers Cilient Authentication Issuers Certificate Envolument Requests Certificate Roots	Issued To Gropyight (c) Gropyight (c) Gropyight (c) Gropyight (c) Groppight	1997 Microsoft C al Root CA Assurance EV Ro Certification Auth to Certification Auth bal CA sot CA sot CA sot CA sot CA sot CA thenticode(Im) Ro ot Certificate Auth ot Certificate Auth ot Certificate Auth ACCEPTED, (c)97 All Tasks Cut	Issued By Copyright (c) 1997 Microsoft Corp. DigiCert Global Root CA DigiCert Global Root CA DigiCert Global Root CA GlobalSign Certification Authority GeoTrust Global CA GlobalSign Root CA Go Daddy Root Certificate Authoriu. Microsoft Authenticode(tm) Root Microsoft Root Certificate Authoriu. Microsoft Root Certificate Authoriu. No LIABILITY ACCEPTED, (c)97 V	Expiration Date 12/31/1999 11/10/2031 11/27/2026 8/22/2018 5/21/2022 3/18/2029 11/28/2028 6/29/2034 1/1/2038 1/1/2020 6/29/2034 1/1/2020 8/31/2022 8/31/2022 8/31/2022 8/31/2022 8/31/2022	Intended Purpos ~ Time Stamping Server Authentic Server Authentic <ali><ali> <ali> <ali><ali> Server Authentic <ali><ali><ali> Server Authentic <ali><ali><ali> Server Authentic <ali><ali><ali> Server Authentic <ali><ali><ali> Server Authentic Server Authentic Serve</ali></ali></ali></ali></ali></ali></ali></ali></ali></ali></ali></ali></ali></ali></ali></ali></ali>
	Thavte Pri	Copy Delete Help	tarriela Class 2 Certification Autr hawte Primary Root CA hawte Timestamping CA 	6/29/2034 7/17/2036 1/1/2021 7/9/2019 7/17/2036	Server Autnentic Server Authentic Time Stamping Encrypting File S Server Authentic
Contains actions that can be performed on the item.	<		1		>



NOTE: If you select one certificate, the export .sst option is greyed out, so you must select at least 2 certificates (For example, personal and intermediate certificates).

4. Click Next on the first **Certificate Export Wizard** screen, then select Microsoft Serialized Certificate Store (.sst)

File Action View Help	Cortificate Evenet Wizard	X	
🐺 Certificates - Current User	Certificate Export Wizard	ation Date	Intended Purpos
Personal		/1999	Time Stamping
⊿ Constant A Contraction		0/2031	Server Authentio
Certificates	Export File Format	0/2031	Server Authentio
Enterprise Trust	Certificates can be exported in a variety of file formats.	7/2026	Server Authentie
Intermediate Certification	10	2018	Secure Email, Se
Active Directory User Obj		2022	Server Authentie
Irusted Publishers	Select the format you want to use:	2029	Server Authentie
Untrusted Certificates	O DER encoded binary X.509 (.CER)	2028	Server Authenti
Inird-Party Root Certifica	Base-64 encoded X.509 (.CER)	2034	Server Authenti
Client Authentication Issue	Cruptographic Magazon Suptay Standard - BKCS #7 Cortificator (1779)	038	Server Authenti
Other People		000	Secure Email, C
McAfee Trust	Include all certificates in the certification path if possible	/2020	<all></all>
Certificate Enrollment Rec	Personal Information Exchange - PKCS #12 (.PFX)	2021	<all></all>
Smart Card Trusted Roots	Include all certificates in the certification path if possible	2035	<all></all>
	Delete the private key if the export is successful	2036	<all></all>
		004	Time Stamping
	Export all extended properties	2022	<all></all>
	Microsoft Serialized Certificate Store (.SST)	2022	<all></all>
		2034	Server Authenti
		2036	Server Authenti
		021	Time Stamping
		019	Encrypting File S
	Next Cance	2036	Server Authenti
			>

- 5. Click **Next**, then click **Browse** and select the location and file name where the .sst file will be saved.
- 6. Click Next, Save and then Finish.

Upload .sst file to Exchange Online

- 1. Open windows **PowerShell** (run as administrator).
- 2. Connect to the Office 365 admin account by running the command: **\$UserCredential = Get-Credential.**
- 3. The Windows PowerShell credential request window opens. Enter the admin user name and password. Click **OK**.

	Administrator: Windows PowerShell	_ 🗆 X
Windows PowerShell Copyright (C) 2014 Microsoft Corpo	oration. All rights reserved.	_
PS C:\Users\Administrator> \$UserCr	redential = Get-Credential	
cmdlet Get-Credential at command p Supply values for the following pa Credential	oipeline position 1 rameters:	
	Windows PowerShell credential req ? X	
	Enter your credentials.	
	User name:	
	Password:	
	OK Cancel	

- Enter the following command in order to open a session with Exchange online: \$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential \$UserCredential -Authentication Basic – AllowRedirection
- 5. Enter the following command to remove restrictions for uploading the .sst file: **Set-ExecutionPolicy Unrestricted –force**
- 6. Import the session: Import-PSSession \$Session
- 7. Change the path to where the .sst file was saved (for example, cd c:\)
- Upload the .sst file to Office 365:
 \$sst = Get-Content <SST file> -Encoding Byte
- 9. Configure the sst file to be used for S/MIME: Set-SmimeConfig -SMIMECertificateIssuingCA \$sst
- 10. Close the session: Remove-PSSession \$Session

Publish Certificate to GAL (Global Address List)

To encrypt emails with S/MIME we need to upload the user certificate to the GAL.

- 1. Open Outlook.
- 2. Select File > Options.

間 ? ·		Inbox - bob@sactests.com - Outlook			
File Home Send / Receive		Outlook Options >	×	And the second s	
New New Selumination	General Mail	General options for working with Outlook.	*	Search People	Store
New Delete	Calendar Groups	User Interface options Show Mini Toolbar on selection		Find	Add-ins 🔺
Inbox Sent Items	People Tasks	Enable Live Preview ① ScreenTip style: Show feature descriptions in ScreenTips *			
Drafts Deleted Items	Search Language	Personalize your copy of Microsoft Office User name bob			
 bob@sactests.com Inbox 	Ease of Access Advanced	Initials: b			
Drafts Sent Items	Customize Ribbon Quick Access Toolbar	Office Background: Circles and Stripes * Office Themes Colorful *			
Deleted Items	Add-ins	Office intelligent services			
Conversation History Junk Email	Trust Center	Intelligent services bring the power of the cloud to the Office apps to help save you time and produce better results. To provide these envices, Microsoft needs to be able to collect your search terms and document content. Enable services About intelligent services			
RSS Feeds		Start up options			
Search Folders		Make Qutlook the default program for Email, Contacts, and Calendar Default Programs			
b Groups		Attachment options For files I choose from OneDrive			
■ == ±± 12 ····		For files I choses from OneDrive & Ask me how I want to attach them every time Aways attach them as cloud files OK Cancel			

3. On the left pane select Trust Center and then on the right pane click Trust Center Settings

III ち +	Inbox - bob@sactests.com - Outlook	- 12	a x
File Home Send / Receive	Outlook Options X	1 million	1.12
New New Final Items* New Verwal Items* New Verwal Items* A Favorites	General Image: Calendar Help keep your documents safe and your computer secure and healthy. Mail Security & more Security & more Groups Visit Office.com to learn more about protecting your privacy and security. People Mensored Transworthy Computing Manual People Manual People	Search People Address Book Filter Email * Find	Store
Sent Items Drafts Deleted Items 4 bob@sactests.com	Tasks Microsoft Outlook Trust Center Search The Trust Center contains security and privacy settings. These settings help keep your computer secure. We recommend that you do not change these settings. Irust Center Settings Ease of Access Access Access Irust Center Settings		
Inbox Drafts Sent Items Deleted Items Archive Conversation History	Customize Ribbon Quick Access Toolbar Add-ins Trust Center		
Junk Email Outbox RSS Feeds Search Folders			
For the second seco		5	
🔤 📰 🕹 😳 ···	OK Cancel		

4. On the left pane select Email Security.

≣ 5 ₹		
File Home Send / Receive	Trust Center X	
Archive Sert Rems Delete Rems	Trutted Publishers Encrypted email Privacy Options Encrypted email Attachment Handing Add digital signature to outgoing messages Automatic Download Macro Settings Macro Settings Encrypted email Digital Do contents and attachments for outgoing messages Encrypted email Digital Do contents and attachments for outgoing messages Digital Do contents that Settings (beb@sactests.com) ▼ Settings. Programmatic Access Digital Do contentificates) Digital Do contentificates Digital Do contentificates Digital IDs (Certificates) Digital IDs (Certificates) Read at Plain Tect Read at Plain tect Secting In plain tect Script in Folders Allow script in shared folders Allow script in Public Folders	Search People ☐ Address Book ▼ Fitter Fmal - Find Add-ins ▲
🖬 🖬 🕹 😥	OK Cancel	J

5. In the Trust Center window click **Settings.** The **Change Security Setting** window opens.

闘 5 ·	Inbox - bob@sactests.com - Outlook		0 //×
File Home Send / Receive	Trust Center X	1 Carrier	
Prove Provide the second	Tudied Publisher: Pricey Options Email Security Attachment Handling Automatic Download Macro Setting: Pregrammatic Access Digital Security Setting: Digital Security Setting: Digital Security Setting: Digital Digital Security Setting: Digital Digital Digital Digital Security Setting: Digital Digital Digital Security Setting: Digital Digital Digital Control Setting for all coptographic message format: Digital Read acceler Society: Hish Algorithm: Digital Security Setting for all coptographic message: Control Non- Control Digital Society: Digital Society: Digital <	Search People	Add-Ins A

6. On the Change Security Settings window, choose Security Setting Name and then click Choose, (to the right of the Signing Certificate field).

闘 ち +	Inbox - bob@sactests.com - Outlook	0 - 0 X
File Home Send / Receive	Trust Center X	
File Home Send / Receive Image: Send / Receive Image: Send / Receive Image: Send / Receive New Image: Send / Receive Image: Send / Receive Image: Send / Receive New Image: Send / Receive Image: Send / R	Tusted Publishers Privacy Options Encrypted email Tusted Fublishers Privacy Options Incrypt contents and attachments for outgoing messages Attachment Handling Automatic Download Macro Settings Incrypt contents and attachments for outgoing messages Options Incrypt contents and attachments for outgoing messages Display Incrypt contents and attachments for outgoing messages Options Incrypt contents and attachments for outgoing messages Options Incrypt contents and attachments for outgoing messages Options Incrypt contents and attachments for outgoing messages Digital Security Setting Preferences Digital Security Setting Preferences Digital Options Security Setting for this cryptographic message format Digital Default Security Setting for this cryptographic message format Digital Security Setting for this cryptographic message format Display for Magnethme Incryption Certificate Bropption Algorithme Incryption for Magnethme Algorithme Incryption for Magnethme Bropption Certificate Incryption for Magnethme Brop	Search People Piker Final Find Add-ins
b Groups Image: Base bit and bit an	OK	

- 7. The **Confirm Certificate** window opens. Select the certificate issued by the CA you are going to use for S/MIME.
- 8. After choosing the certificate, click **OK**.

File Home Send / Receive	Taut Centre	10 00 77
New New Mew Mew New New I Favorites	Trusted Publishers Encrypted email Póxory Options Encrypt contents and attachments for outgoing messages Add digital signature to outgoing messages Encrypt Settings 	Search People
Indox Sent Items Dealts Dealts Dealted Items Dealts Sent Items Dealts Sent Items Archive Conversation History Junk Email Outbox Sasch Folders Search Folders	Automidad Maco Sattings Programmatic Access Digital Programmatic Access Digital Programmatic Access Digital Read ac Bre Scrufty Stating of this crystographic messages Central Scruft Stating of this crystographic messages Scruft Stating of this crystographic messages Central Scruft Stating of this crystographic messages Encrystion Centralizate and Agorithms Encrystion Centralizate with signed messages Disord Magorithm Af5 (256-bit) Concellence	
🖬 🖬 🖉 ···	OK Ca	ncel

9. In the **Trust Center** window, click **Publish to GAL** in order to publish your certificate to Office 365. Once the certificate is uploaded to GAL, you will receive a confirmation message.

Dia Daniel Brancisco	
File Here Serd / Recive Trust Center Image: Clean Up- New Clean Up- Subscr Detect Prove Center Prove Center New Clean Up- Subscr Detect Prove Center Prove Center Prove Center New Clean Up- Subscr Detect Prove Center Prove Center Prove Center New Detect Prove Center Prove Center Prove Center Prove Center Index Detect Prove Center Prove Center Prove Center Prove Center Index Detect Prove Center Prove Center Prove Center Prove Center Data Detect Berns Programmatic Acces Programmatic Acces Prove Center Prove Center Data Detect Berns Confirm this center Detect Berns Confirm this center Detect Center Detect Berns Conversition Fistory Nuck Email Center Center Center Notices Sis Feeds Search Foldes Center Center Center Center Seruites Center Center Center Center Center	Cancel C

Enable S/MIME in Office 365 OWA

1. Login to Office 365 with the user credentials and click Office 365.

 Office 365				A 🌣 ?	bob 🤷
Good afternoor	n	O Sear	ch online documents	Settings	×
Apps			Install Office apps 🖂	Search all settings	Q
🖸 Mail 🍊	OneDrive	Word	X Excel	Theme Default theme	~
PowerPoint N	OneNote	SharePoint	Teams	Start page Set your start page	~
Y≑ Yammer ►	Dynamics 365	Flow		Notifications On	v
Explore all your apps $ ightarrow$				Password Change your password.	
Documents Recent Pinned Shared v	with me Disco	ver		Your app settings Office 365 Mail Calendar	
		~ *		Yammer	^
			Feedbac	k 🗸	

2. On the right pane select Mail

Good afternoon	O Sear	ch online documents	Settings	
Apps		Install Office apps	Search all settings	
💽 Mail 🍊 OneDrive	Word	Excel	Theme Default theme	
PowerPoint N OneNote	SharePoint	Teams	Start page Set your start page	
Y ← Yammer Dynamics 365	Flow		Notifications On	
Explore all your apps $ ightarrow$			Password Change your password.	
Documents		→ Upload and Open New	Your app settings	
Recent Pinned Shared with me Disc	over		Mail Calendar People	

3. The user's mail settings window opens. On the left pane select S/MIME



4. Check the checkboxes to support S/MIME and click Save.



Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information		
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017 USA		
Phone	United States	1-800-545-6608	
	International	1-410-931-7520	
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.		