Assignment Question:

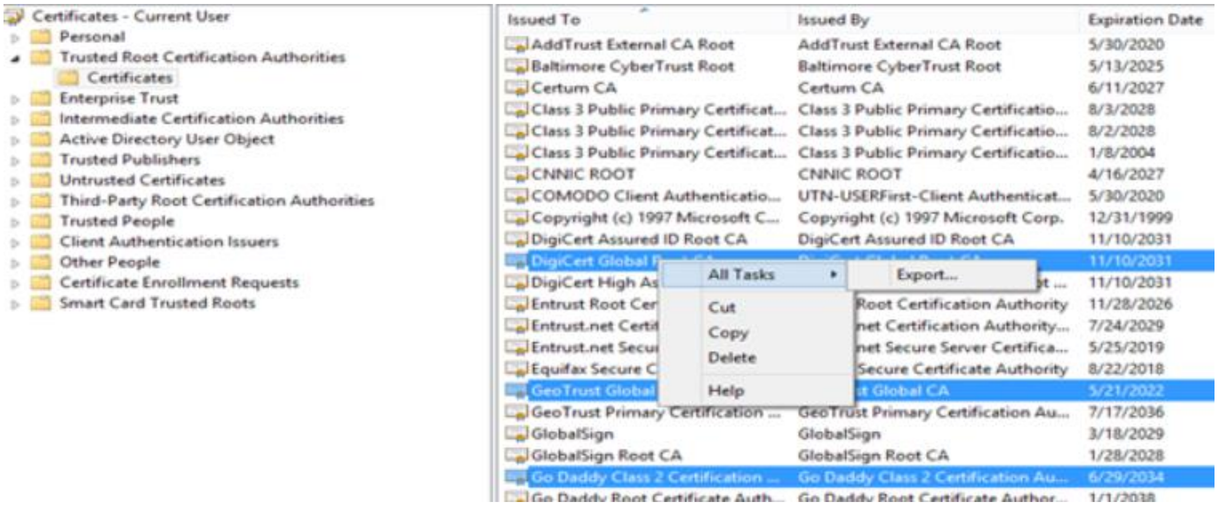
Illustrate the steps for implementation of S/MIME email security through Microsoft® Office Outlook.

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and digital signing of MIME data. Configuring S/MIME in Office 365 is a slightly different procedure than configuring S/MIME on-premises. Configuring S/MIME will allow users to encrypt and/or digitally sign an email. S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity, non-repudiation of origin (using digital signatures), privacy, and data security (using encryption). Further, Office 365 also provides the capability for end users to compose, encrypt, decrypt, read, and digitally sign emails between two users in an organization using Outlook, Outlook Web App (OWA) or Exchange ActiveSync (EAS) clients.

In this scenario, all the users are hosted on cloud and there is no on-premises Exchange organization.
Requirements

1. .SST File (Serialized store): The SST file contains all the root and intermediate certificates that are used when validating the S/MIME message in Office 365. The .SST file is created from certificate store explained below.
2. End user's certificate for signing and encrypting the message issued from Certificate Authorities(CA) either Windows based CA or Third party CA.

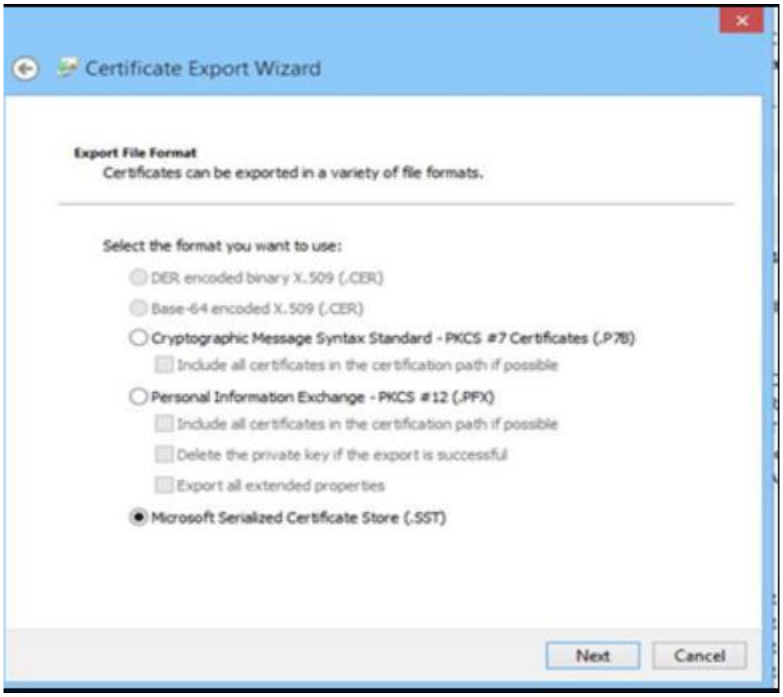
Configuration
Remember that in Exchange Online, only the SST will be used for S/MIME certificate validation. **1. Create a .SST file for the Trusted Root CA / Intermediate CA of the certificate issued to the users:** You can use either Certificate MMC or PowerShellcmdlets to export SST file. I am using Certificate console to export the .SST here: Open **certmgr.msc** snap-in, expand **Trusted Root Certificate Authorities > Certificates** > select the CA Certificates which issued the certificates to end users for S/MIME and right click > **All Tasks** > **Export…**



Certificates - Current User
- Personal
- Trusted Root Certification Authorities
  - Certificates
- Enterprise Trust
- Intermediate Certification Authorities
- Active Directory User Object
- Trusted Publishers
- Untrusted Certificates
- Third-Party Root Certification Authorities
- Trusted People
- Client Authentication Issuers
- Other People
- Certificate Enrollment Requests
- Smart Card Trusted Roots

Issued To	Issued By	Expiration Date
AddTrust External CA Root	AddTrust External CA Root	5/30/2020
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/13/2025
Certum CA	Certum CA	6/11/2027
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/3/2028
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/2/2028
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	1/8/2004
CNNIC ROOT	CNNIC ROOT	4/16/2027
COMODO Client Authenticatio...	UTN-USERFirst-Client Authenticat...	5/30/2020
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/31/1999
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/10/2031
DigiCert Global		11/10/2031
DigiCert High As	t ...	11/10/2031
Entrust Root Cer	Root Certification Authority	11/28/2026
Entrust.net Certi	net Certification Authority...	7/24/2029
Entrust.net Secu	net Secure Server Certifica...	5/25/2019
Equifax Secure C	Secure Certificate Authority	8/22/2018
GeoTrust Global	t Global CA	5/21/2022
GeoTrust Primary Certification ...	GeoTrust Primary Certification Au...	7/17/2036
GlobalSign	GlobalSign	3/18/2029
GlobalSign Root CA	GlobalSign Root CA	1/28/2028
Go Daddy Class 2 Certification ...	Go Daddy Class 2 Certification Au...	6/29/2034
Go Daddy Root Certificate Auth...	Go Daddy Root Certificate Author...	1/1/2038

2. Select **Microsoft Serialized Certificate Store(.SST) > Click Next and save the SST file:**



Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

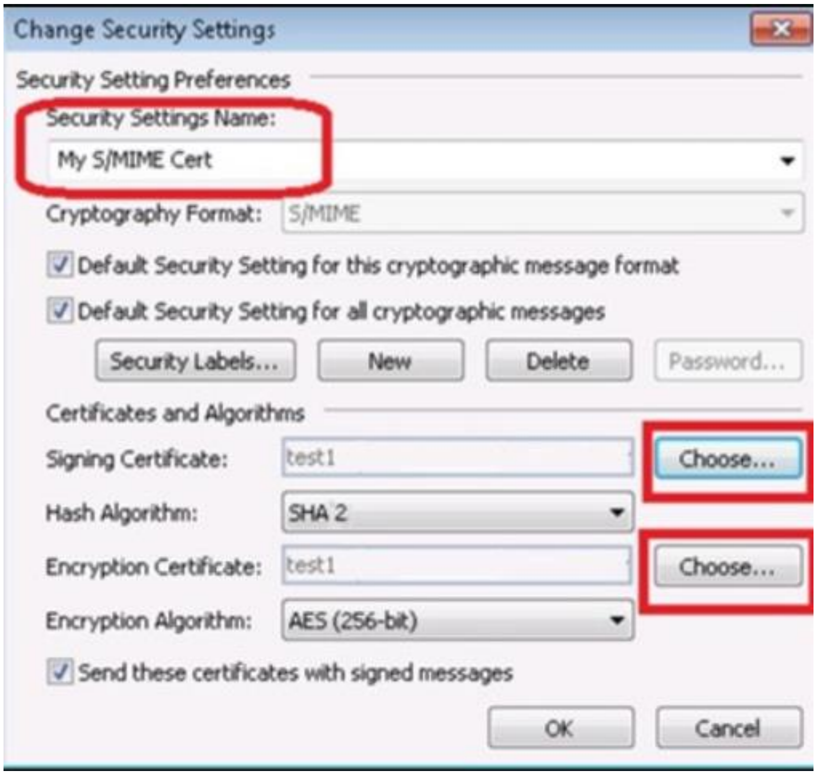
● Microsoft Serialized Certificate Store (.SST)

3. Upload .SST to office 365 server: Update the SST on office 365 exchange server by executing the following commands using remote PowerShell.
$sst = Get-Content <sst file copied from the box>.sst -Encoding Byte

(Example: $sst = Get-Content TenantRoot.sst -Encoding Byte)
Set-SmimeConfig -SMIMECertificateIssuingCA $sst

4. Publish user's certificate to the Exchange Online GAL (Global Address List) using Outlook. If not published, users will not be able to exchange S/MIME encrypted messages.

- On the **File** menu in Outlook 2013, click **Options**.
- On the **Outlook Options** window, click **Trust Center**, click **Trust Center Settings**..., and then click **Email Security**.
- In the **Trust Center window**, click **Settings**... (Here, you need to choose certificate issued by the CA you are going to use for S/MIME).
- In the Change Security Settings window, type the Security Settings Name (you can name it anything) and choose Signing and Encryption certificate. Select the appropriate certificate assigned in previous steps, leave the Algorithm default and click OK.



Change Security Settings

Security Setting Preferences

Security Settings Name: My S/MIME Cert

Cryptography Format: S/MIME

☑ Default Security Setting for this cryptographic message format

☑ Default Security Setting for all cryptographic messages

Certificates and Algorithms

Signing Certificate: test1

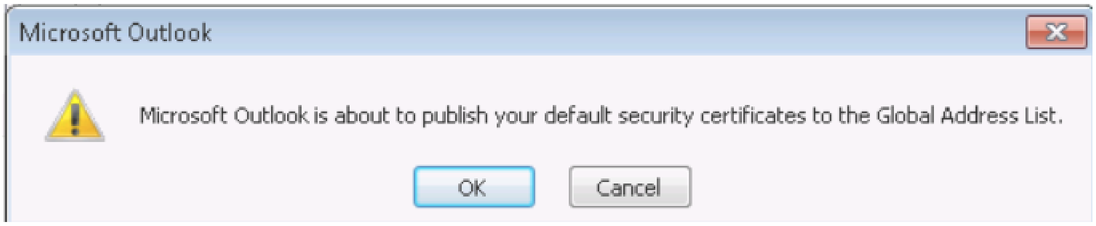
Hash Algorithm: SHA 2

Encryption Certificate: test1

Encryption Algorithm: AES (256-bit)

☑ Send these certificates with signed messages

- Once the information is selected, you will notice the Default Setting is populated with Security Settings Name. Now you can click the Publish to GAL button. To publish the certificate to the GAL, click OK.

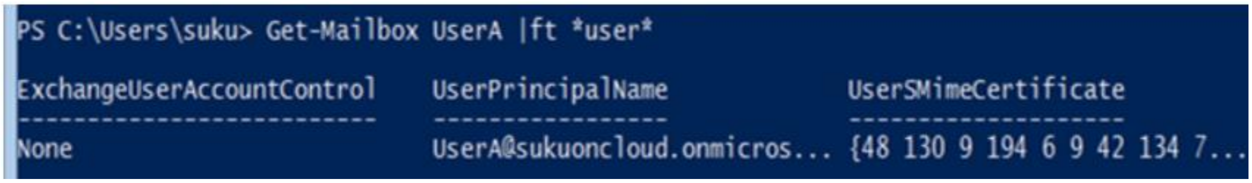


Microsoft Outlook

Microsoft Outlook is about to publish your default security certificates to the Global Address List.

5. To confirm the certificate is published in AAD (Azure Active Directory), connect to Exchange Online using remote PowerShelland run following command. Check to make sure that the UserSMimeCertificate attribute is populated with the certificate information. If not, return to step 4.

Get-Mailbox <user> | FL or FT *user*



```
PS C:\Users\suku> Get-Mailbox UserA |ft *user*

ExchangeUserAccountControl    UserPrincipalName              UserSMimeCertificate
--------------------------    -----------------              --------------------
None                          UserA@sukuoncloud.onmicros... {48 130 9 194 6 9 42 134 7...
```

6. Once you confirm the end user has the certificate on their machine under **certificates > personal** store and also published in AAD, the users can use Outlook, OWA, or EAS to send and receive S/MIME messages.