



S/MIME

Secure/Multipurpose Internet Mail Extensions

A Zimbra Collaboration Whitepaper

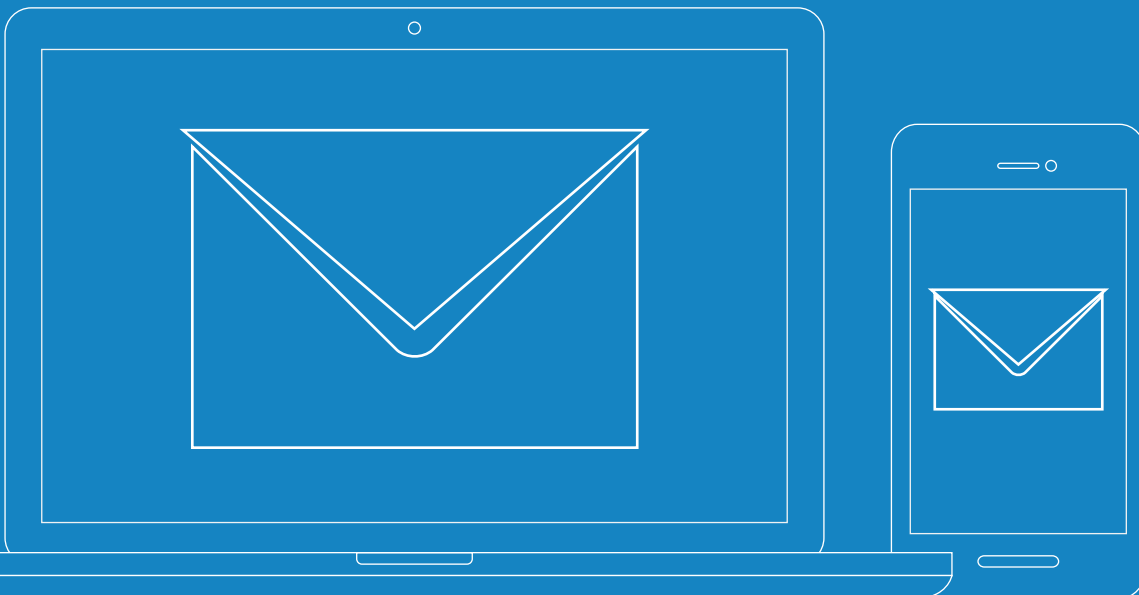


Table of Contents

<u>Introduction</u>	<u>3</u>
<u>How Does S/MIME Work</u>	<u>3</u>
<u>Main Security Components of an Email</u>	
<u>Encryption Certificate</u>	<u>5</u>
<u>Key Benefits of Using an Email Encryption</u>	
<u>Certificate</u>	<u>5</u>
<u>How Does This All Work?</u>	<u>6</u>
<u>Sign Emails on iOS</u>	<u>7</u>
<u>Set Up an S/MIME Certificate on an iPhone</u>	<u>10</u>
<u>Sign Emails on Outlook</u>	<u>10</u>
<u>Install Your Certificate in Outlook</u>	<u>11</u>
<u>Sign Emails on Zimbra Desktop</u>	<u>12</u>
<u>Sending 'Signed' Emails</u>	<u>13</u>
<u>Bibliography</u>	<u>14</u>

Introduction

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for encryption and signing email.

S/MIME uses (asymmetric) encryption so that only the intended recipients can read the contents of email messages and attachments. S/MIME also digitally signs email and attachments. The digital signature allows the recipient to verify the message integrity, or in other words, make it so that the content can not be altered by third parties without the recipient getting a warning.

When used correctly, S/MIME offers both in-transit and at-rest encryption. To get started with S/MIME, a user needs to obtain an S/MIME certificate from a certificate authority. [WP]

S/MIME is on the IETF standards track and defined in a number of documents, most importantly RFC 3369, 3370, 3850 and 3851.

S/MIME encrypts and digitally signs emails, ensuring the email is authentic and has not been altered in any way.

How Does S/MIME Work?

Ben wants to send an email to his friend Jerry but doesn't want anyone else on the internet to read or modify it. Ben encrypts the email with Jerry's public key. Jerry gives his public key to anyone he wants in a variety of ways, including email (sending a message signed with your private key also sends your public key to the recipient), text or via a key server. Now, Ben or anyone else with Jerry's public key can encrypt the message to Jerry. Only Jerry has his private key, so only he can decrypt and read the email. It is safe from intruders on the internet.

You can get an S/MIME certificate from a trusted certificate authority (CA) and use this to digitally sign your outgoing messages and to decrypt your incoming messages.



Figure 1. Public Key - Private Key [SS]

The way this works is as follows:

- An S/MIME certificate has a key pair: a private key and a public key.
- Both the sender and the recipient must have an S/MIME certificate.
- Senders use the public key (provided by the recipient) to encrypt and send email to the recipient (owner of the key pair).
- The recipient verifies the identity of the sender and the integrity of the email with the public key.
- The recipient uses the private key to decrypt incoming emails.
- The private key is also used by the sender to digitally sign outbound email.

S/MIME provides the following cryptographic security services for electronic messaging applications:

- Authentication
- Message integrity
- Non-repudiation of origin (using digital signatures)
- Privacy
- Data security (using encryption)

S/MIME specifies the MIME type `application/pkcs7-mime[2]` (smime-type “enveloped-data”) for data enveloping (encrypting) where the whole (prepared) MIME entity to be enveloped is encrypted and packed into an object which subsequently is inserted into an `application/pkcs7-mime` MIME entity.



S/MIME Summary

- Certificate
- Private Key
- Public Key
- Digital Signature

Main Security Components of an Email Encryption Certificate

These are the three security pillars of an email encryption certificate:

- 1. Identity Assurance:** An email encryption certificate allows you as the sender to insert a cryptographic digital signature on all outgoing emails. This digital signature can't be modified, deleted, or manipulated by any other person. This gives your recipients assurance about your identity and helps them trust that the message came from you.
- 2. Privacy:** An email encryption certificate encrypts the email content before you hit send and provides in-transit and at-rest data protection. Encryption scrambles the plain text data using a mathematical algorithm to make it incomprehensible. This means that no one can eavesdrop, read, interpret, or steal the content while the email is in transit and while it sits on the intended recipient's server, waiting to be decrypted.
- 3. Integrity:** An email encryption certificate uses principles of the public key infrastructure (PKI) and hashes the entire content of the email, attachments, and the digital signature. An intact hash value is proof of the integrity of the email. This means that if anyone tries to tamper with the email after it's been sent, the hash value changes, which informs the recipients that the email's integrity has been compromised.

Key Benefits of Using an Email Encryption Certificate

These are the main benefits of an email encryption certificate.

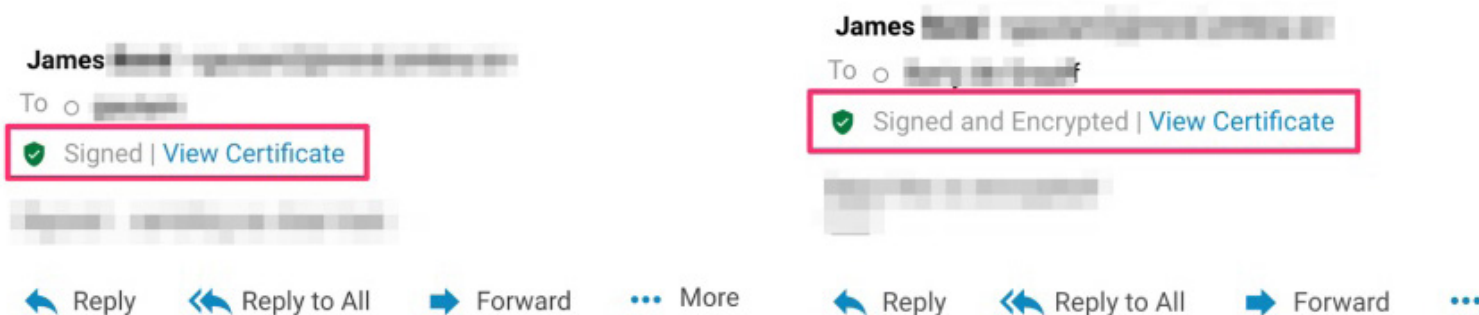
- Protects users from email spoofing scams.
- Prevents any alteration in the email contents after it has been sent.
- Helps people differentiate between phishing and authentic emails.
- Prevents data leaks, data theft, and data loss in transit.
- Protects the business's confidential data from eavesdropping.
- Provides end-to-end encryption if both the parties have installed an email encryption certificate. This means the email remains encrypted not only in transit but also when it is stored (at rest) on the server.

Three security pillars of an email encryption certificate:

- Identity Assurance
 - Privacy
 - Integrity

How Does this All Work?

How do you know that your emails are secure? As shown below, a security indicator communicates when an email is encrypted and secure, and a checkmark verifies if the email was digitally signed.



The way the digital signature works is as follows:

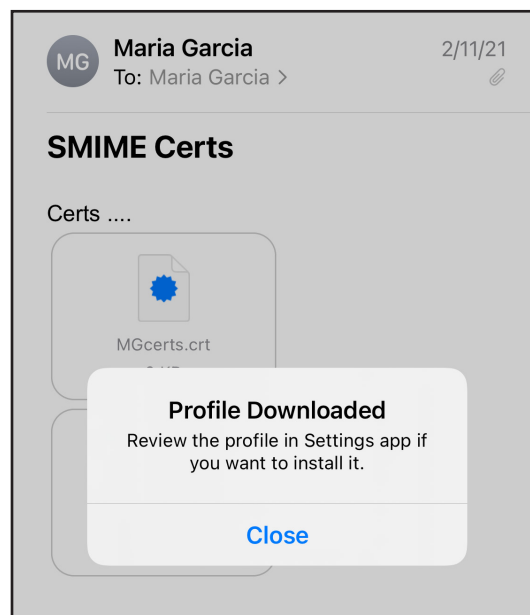
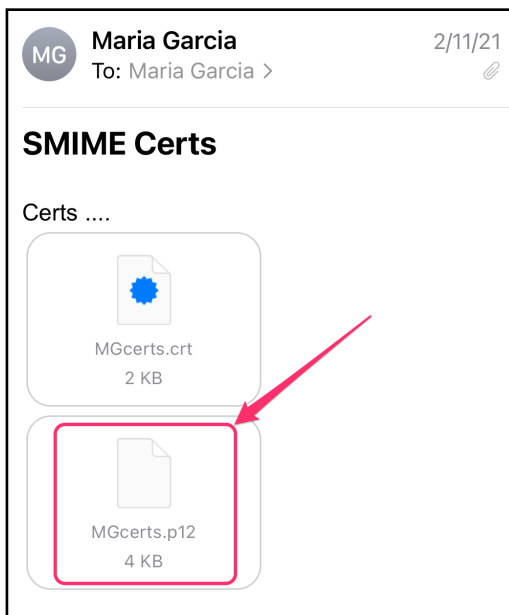
- A digital signature is generated using a private key and authenticated using a public key.
- The public key is sent with the S/MIME protected email — this verifies your identity when the recipient opens the email. Your private key applies your unique digital signature to each email and repeats the process.
- The second component of S/MIME (encryption) encrypts your email data — MIME data — before it transmits from point A to point B (to/from a web server and email client).

Sign Emails on iOS

If you're an Apple iPhone user, you can install an S/MIME certificate on your device to secure your email communications. Once the certificate is generated, send that certificate to your device.

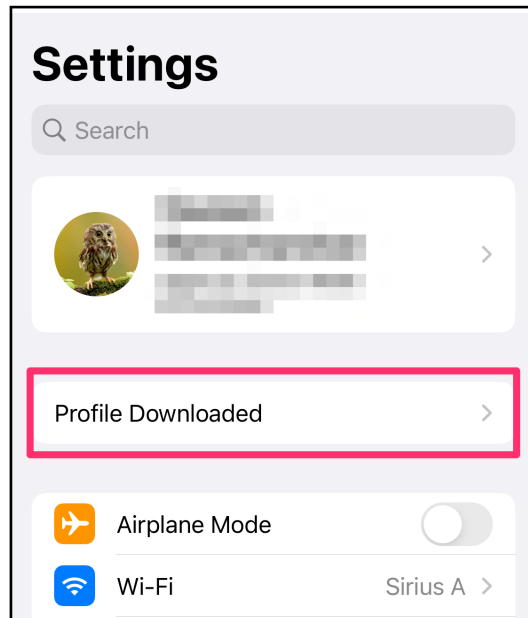
Here's how to install an S/MIME certificate on your iPhone:

1. On your iPhone, open the email that has the certificate files and click on the PKCS#12 (.p12) file.
2. The profile will be added to your settings.

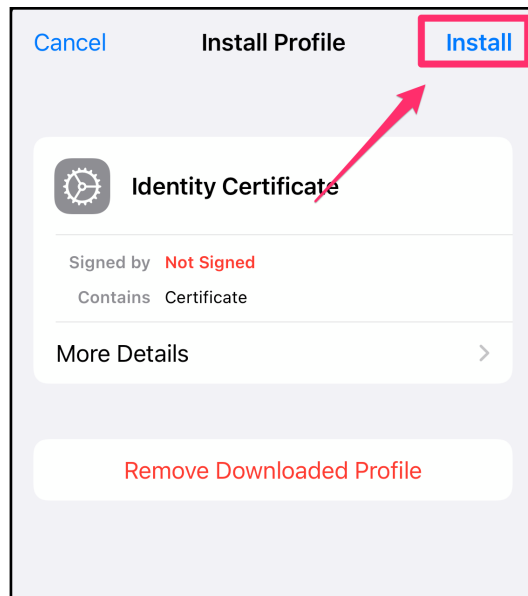


3. Navigate to your settings and click the downloaded profile.
4. Follow the on-screen instructions to install this profile (you will need your device and certificate passwords).
5. WARNING: The profile may not be signed or verified as the CA may not be available.

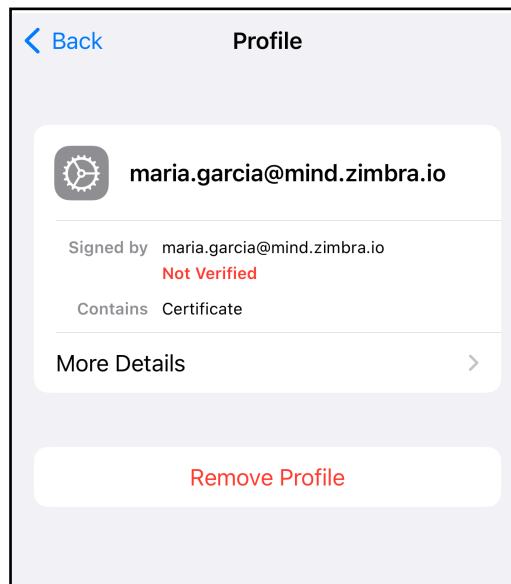
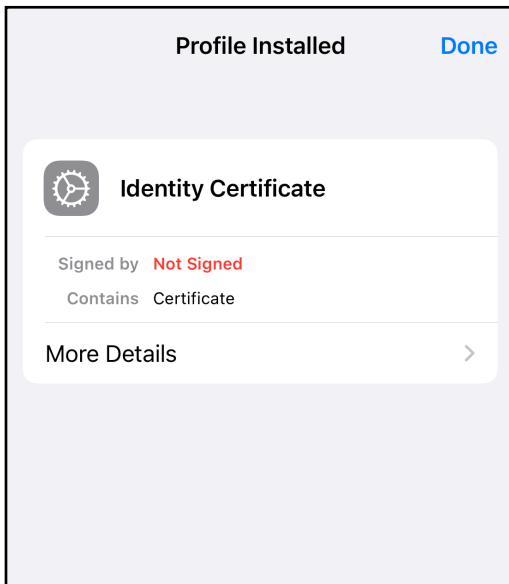
3. Navigate to your settings and click the downloaded profile.



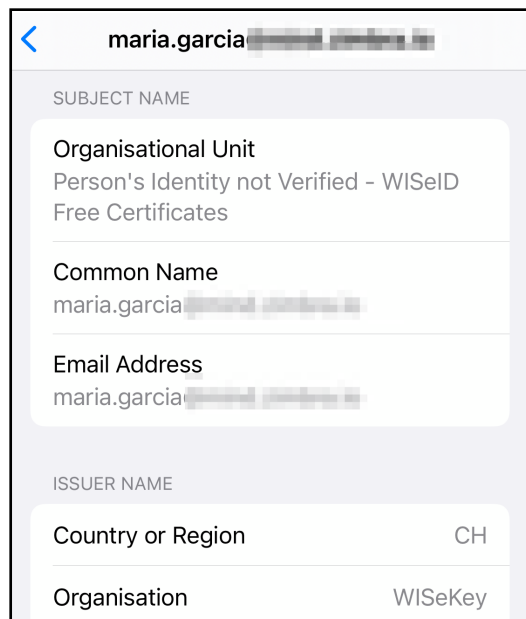
4. Follow the on-screen instructions to install this profile (you will need your device and certificate passwords).



5. WARNING: The profile may not be signed or verified as the CA may not be available.



Now, your certificate is successfully installed on your iPhone.



Set Up an S/MIME Certificate on an iPhone

Once you're done with the certificate installation process, it's time to set up an S/MIME certificate on your iPhone.

1. Go to Settings and select Accounts & Passwords.
2. Select the account that you want to set up.
3. Go to Advanced.
4. Navigate to the S/MIME section and enable S/MIME.
5. Enable the sign toggle and select the S/MIME certificate you installed.

All mails composed and sent using this account will now be signed.

Sign Emails on Outlook

Installing your Outlook encryption certificate and inserting a digital signature into an email are just one-time processes. Once set up correctly, your digital signature will automatically attach to all of your outgoing emails. Plus, you don't have to take any manual steps to encrypt and hash the digital signature. Everything is done automatically by the email encryption certificate.

Follow these steps to digitally sign your emails on Outlook.

Prerequisites

1. Download and save the PKCS#12 file (i.e., your email signing certificate) on your local machine. Remember the file path.
2. Keep the password secure. You will need it for the installation process.

Install Your Certificate in Outlook

Follow the steps below to install an encryption certificate in Outlook:

1. Open 'File', and click 'Options.'
2. In the 'Outlook Options' window, navigate to 'Trust Center' and select 'Trust Center Settings.'
3. In the 'Trust Center' window, navigate to 'Email Security' (left nav-pane).
4. On the right, under the Digital IDs (Certificates) tab, click 'Import/Export.'
5. On the 'Import/Export Digital ID' window, select 'Import existing Digital ID from a file.'
6. Click 'Browse' and navigate to the location on your PC where the file is stored.
7. Click 'Open.' The file path should now be in the 'Import File' field.
8. Enter the password that you used when downloading the file, and click 'OK.'
9. In the dialog box, click 'OK.'
10. Under 'Email Security', select 'Settings.'
11. In the 'Change Security Settings' window, enter the name for your security settings.
12. Under 'Certificates and Algorithms' next to the 'Signing Certificate' field, click 'Choose' to load your certificate and then click 'OK' on the confirm certificate window.
13. Repeat for the 'Encryption Certificate' field. If you have more than one, select the same certificate as you did for the previous step.
14. Click 'OK' and once the 'Change Security Settings' window closes, select the default options you want via the four checkboxes under the 'Encrypted email' tab.
15. Once you click 'OK' to close the 'Trust Center Window', your certificate is installed and ready to use!

Sign Emails on Zimbra Desktop

The Zimbra Desktop app refers to the system location for validating the user's private certificates.

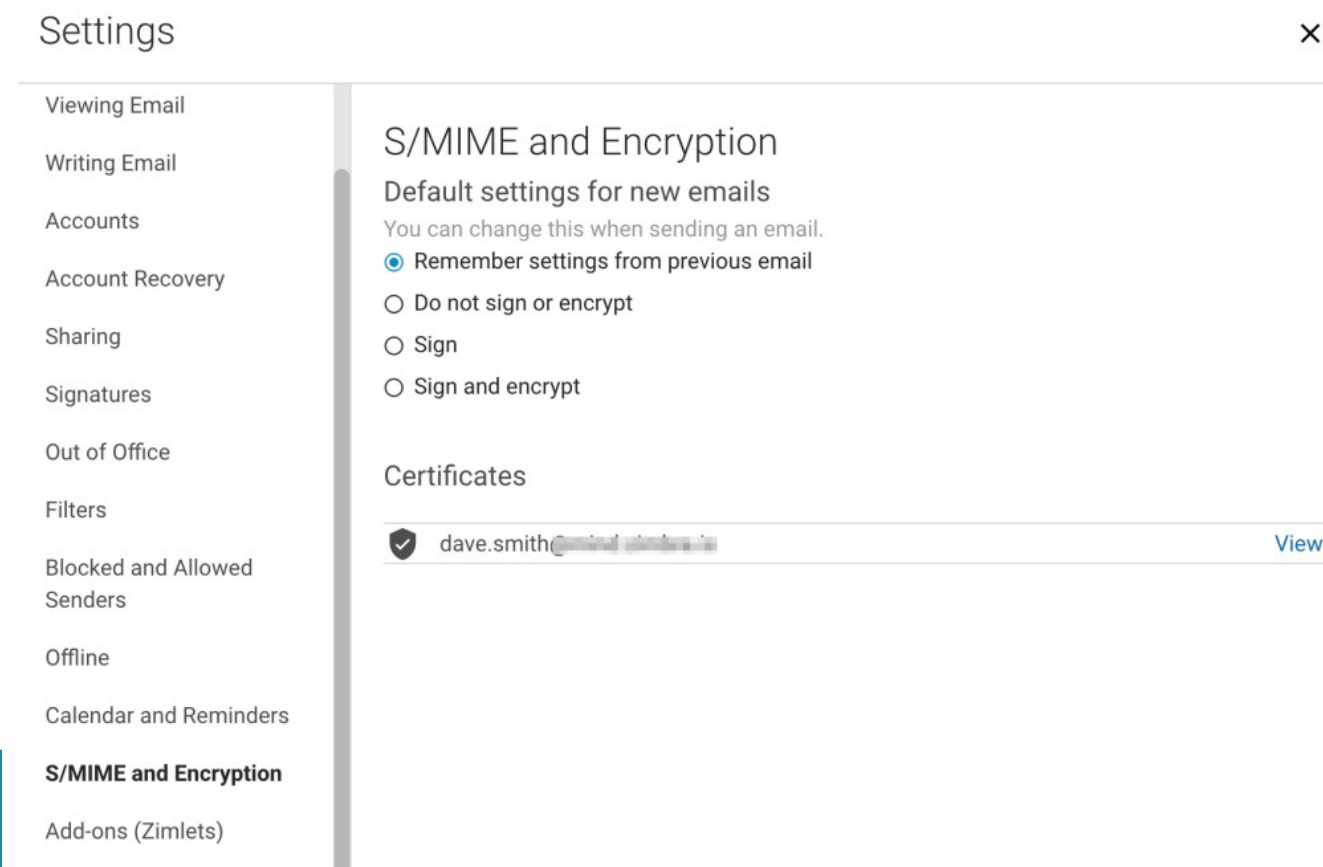
On the Mac, open (or double-click) the certificate file. The Keychain Access will prompt you for the certificate passphrase. Enter the passphrase you created when you requested the certificate.

The certificate will be installed on your Mac and will appear in the "My Certificates" section of Keychain Access. The certificate is now available for Apple Mail, Zimbra Desktop, and other applications that can use client certificates.

Set the trust level of the certificate.

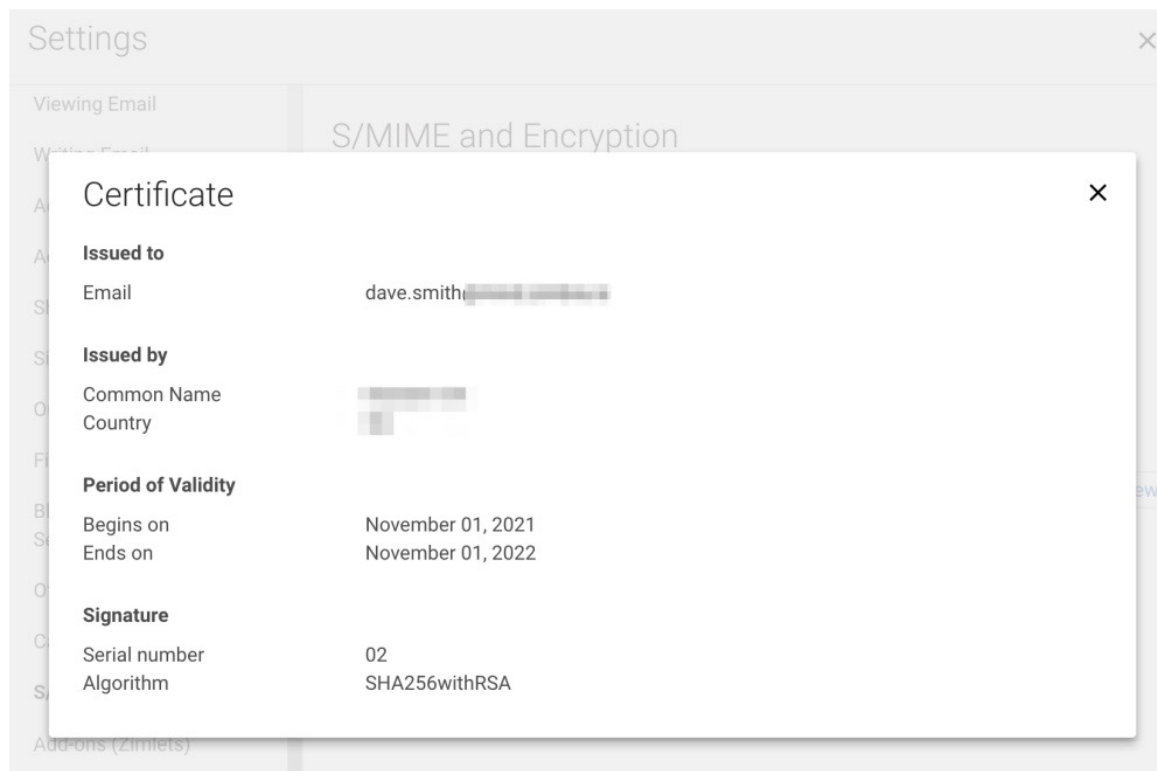
1. Double-click the added certificate in the system folder.
2. Select 'Always trust' in the trust field.
 - Grant Zimbra Desktop app the access to the certificate key - Expand the certificate and click on the certificate key.
3. Go to the Access control tab. Add Zimbra Desktop in the list of apps that have access to the key.

Now you will see the certificate and change the options in your Zimbra Desktop settings (Settings → SMIME and Encryption)



The screenshot shows the 'Settings' window with a sidebar on the left and a main content area on the right. The sidebar lists various settings categories, with 'S/MIME and Encryption' highlighted. The main content area is titled 'S/MIME and Encryption' and contains the following information:

- S/MIME and Encryption**
- Default settings for new emails**
- You can change this when sending an email.
- Remember settings from previous email
- Do not sign or encrypt
- Sign
- Sign and encrypt
- Certificates**
- dave.smith@central.zimbra.com [View](#)



Sending 'Signed' Emails

To send a signed email:

1. Compose a new message.
2. Add a recipient in the To field.
3. Choose an option from the top, right-hand dropdown. 'Do not sign or encrypt' is selected by default.
 - Do not sign or encrypt: Mail is neither signed nor encrypted. This is equivalent of disabling the S/MIME feature.
 - Sign: Send signed message to the recipient.
 - Sign and Encrypt: Send signed and encrypted messages to the recipient.
4. Click Send.

Bibliography

☒ [SS] <https://sectigostore.com/page/email-encryption/>

☒ [WP] <https://en.wikipedia.org/wiki/S/MIME>



Copyright © Synacor, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. ZIMBRA is a trademark of Synacor, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.