COBHAM

The most important thing we build is trust



ICED ELECTRONIC SO

AVIATION SERVICES

COMMUNICATIONS AND CON

MISS

CAES Secure Email Guide for External Users

Contents

| Introduction | 2 |
|--|----|
| Organizational Level Secure Email | 2 |
| PGP Global Directory, and PGP Universal Server | 2 |
| Delivery Options | 3 |
| Delivery Option Recommendation | 3 |
| Delivery Options Explained | 4 |
| Getting Started | 5 |
| Enrolling as an External User | 5 |
| Configuring Symantec Encryption Satellite Delivery Option | 7 |
| Uninstalling Symantec Encryption Satellite | |
| Configuring Key or Digital ID/Certificate Delivery Option | 13 |
| Configuring Your Account using a PGP Public Key | 13 |
| Configuring Your Account using an S/MIME (X509) Public Key | 19 |
| Using Your CAES Secure Email Portal | 24 |
| Appendix A | 26 |
| Exporting your S/MIME Certificate | 26 |
| Exporting your PGP Key (from PGP Desktop) | 29 |
| Troubleshooting | |
| All my emails from CAES are "Secure Web Messenger" | |
| I forgot my password for the CAES Secure Web Messenger" | 31 |

Introduction

Managing and securing electronic information has become both a highly visible, and a highly regulated activity. Creating, implementing, and enforcing corporate security policies governing email has become critical to mitigating risk for all organizations. To ensure the security of sensitive email, CAES has implemented a secure email system, powered by Symantec's PGP Universal technology. This document outlines how to set up your email account to work with the CAES Secure Email system.

One of the advantages of the PGP Universal technology is its flexibility. Accordingly, you will need to choose one (1) method of interacting with the CAES Secure Email system. Depending upon the "delivery option" chosen, it may be desirable, or even necessary, to enlist the help of your local IT department to assist with the configurations described in this document.

Organizational Level Secure Email

Organizations that have a company-wide secure email system in place may prefer to configure secure email at the directory server level, rather than at the individual email address level. This higher level configuration would negate the need to perform any of the configurations in this document.

PGP Global Directory, and PGP Universal Server

If you use PGP Desktop software, and have uploaded your PGP key to the PGP Global Directory, you will only need to add the CAES keyserver in your PGP Desktop client (page 13). If you have not uploaded your key to the PGP Global Directory, you will follow the instructions for the Key or Digital ID/Certificate Option (page 12)

If your company uses PGP Universal Server, and has published the LDAP keyserver to the Internet following PGP guidelines, you should not need to perform any of the configurations in this document.

Delivery Options

Delivery Option Recommendation

The table below shows the recommended delivery option based on your current environment. All delivery options are explained in detail in the next section. Please note that your delivery option can be changed in the future.

| 1 – Choose your option below and 2 – Choose your email environment to the right, then find your recommended Delivery Option. | I/My company uses Secure Email technology today and therefore I have a PGP Key or S/MIME certificate | I/My company does NOT use Secure Email technology today |
|--|--|--|
| I can install programs on my computer | Key or Digital ID/Certificate | Symantec Encryption |
| AND I want to configure my computer | Other possible options: | Satellite |
| to integrate fully with CAES Secure Email | Symantec Web Email Protection, Regular Email | Other possible options: |
| | | Symantec Web Email Protection, Regular Email |
| | Key or Digital ID/Certificate | Regular Email |
| I can install programs on my computer however, I DO NOT want to configure | Other possible options: | Other possible options: |
| anything on my computer | Symantec Web Email Protection, Regular Email | Symantec Web Email Protection |
| | | |
| | Key or Digital ID/Certificate | Regular Email |
| I cannot install programs on my | Other possible options: | Other possible options: |
| computer | Symantec Web Email Protection, Regular Email | Symantec Web Email Protection |
| | | |

Delivery Options Explained

The delivery options dictate how you will interact with the CAES Secure Email system. They are listed in the same order here as they are listed on the website when you are asked to choose:

• Symantec Web Email Protection

CAES will create a secure webmail account on our Secure Email servers for you. You will need to log
into the secure website ONLY for secure emails received from CAES. You will continue to receive nonsecure email from CAES in your normal mail application. Sending a secure email to CAES requires
logging in to the secure website.

• <u>Symantec Encryption Satellite</u>

 Symantec Encryption Satellite is a Windows application that can be installed (if you are allowed) on your computer. You will not need to log into the secure website to send or receive secure email with CAES. This option may require additional configuration of your email client and/or assistance from your IT department.

• Key or Digital ID/Certificate

 This option is for users/companies that already use Secure Email technology. CAES supports both S/MIME (X509) Certificates and PGP keypairs. After uploading your public key to the CAES servers, you will use your mail client to exchange secure email with CAES just as you have previously with other email recipients.

<u>Regular Email</u>

This option is recommended for users that are unsure of what to choose. CAES will create a secure webmail account on our Secure Email servers for you. You will need to log into the secure website ONLY for secure emails received from CAES. *You will continue to receive non-secure email from CAES in your normal mail application.* Sending a secure email to CAES requires logging in to the secure website.

Getting Started

Enrolling as an External User

In order to choose your delivery option, you must enroll with the CAES PGP Universal server as an external user. This process is performed only once and begins when you receive your first "Secure Email" from CAES. This is actually a notification from CAES that you have received a secure email and it is waiting for you on your newly created secure mailbox on the CAES PGP servers. The notification will look as follows:

From: "Doe, John (SSA R4)" <john.doe@cobhamaes.com> Date: March 17, 2020 at 10:33:25 AM EDT To: Jane Smith <janesmith@gmail.com> Subject: PGP Universal Secured Message from the CAES Secure Email system

| You have received a PGP Universal Secured Message from: | | Click here to |
|--|------------|---|
| Doe, John (SSA R4) <john.doe@cobhamaes.com></john.doe@cobhamaes.com> | | enroll as an external user |
| | | external user |
| To read this message securely, please click this link: | K | |
| https://keys.cobhamna.com/b/b.e?r=janesmith%40gmail.com&n=JIcm1ZqBZXFbXin7shohbA%3D% | <u>%3D</u> | |

• The link will bring you to the CAES Secure Email servers where you will be asked to create a passphrase for your account. Please read and follow the recommendations for protecting your passphrase. Enter your chosen password twice, and click CONTINUE.

| COBHAM | Symantec. |
|--|-----------|
| You have received an encrypted message from Cobham | |
| Please create a passphrase to secure future messages delivered to you. This server requires your passphrase to meet the following requirements: They must be at least 8 characters long. It must include an uppercase letter, a lowercase letter, a digit and a punctuation mark. | |
| For example, "kittycat" is not a valid passphrase, but "k1ttYc@t" is a valid passphrase. Here are some recommendations for protecting your passphrase: Use an easy to remember passphrase that you don't need to write down. Don't use obvious passphrases that can be easily guessed. Don't make your passphrase a single word. Don't use famous quotations. | |
| Passphrase: Confirm Passphrase: | Continue |

Copyright © 2014 Symantec Corporation. All Rights Reserved.

 You will now be prompted to select your Delivery Option. Please refer to the "<u>Delivery Options</u>" section of this document for a more detailed explanation. This selection can be changed later from your CAES Secure Email settings page:



- If you selected <u>Symantec Web Email Protection</u> or <u>Regular Email</u>:
 - **YOU ARE FINISHED**. You will be brought to your CAES Secure Webmail Inbox. Proceed to the "Using Your CAES Secure Email Portal" section for more information.
- If you selected **Symantec Encryption Satellite** or **Key or Digital ID/Certificate**:
 - Proceed to the next section(s) in this document to continue your configuration.
 - NOTE: If you selected Key or Digital ID/Certificate, you will need to have your public key available. Please see Appendix A for assistance if necessary

| | 😝 Settings 🛛 🔞 Help 🛛 😧 Logout |
|---|--------------------------------|
| COBHAM | Symantec. |
| Configuration Confirmation | |
| Thank you. Your delivery preference has now been set. | |
| | ОК |

Copyright © 2014 Symantec Corporation. All Rights Reserved.

Configuring Symantec Encryption Satellite Delivery Option

• After selecting the Symantec Encryption Satellite option, you are presented with the PGP End User License Agreement. Please read it and click I AGREE

| | 😑 Settings 🔞 Help 🕻 |) Log | out |
|---|--|-------|-----|
| | COBHRM | ec. | |
| s | ymantec Encryption Satellite Software Agreement | | |
| | NO WARRANTY | | |
| | 11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. | | |
| | 12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. | | |
| | END OF TERMS AND CONDITIONS | | |
| | LAgree Disagree | ~ | |
| | Please read the license agreement over carefully and click either the "I Agree" or "I Disagree" button at the end of the document. | nt | |

Copyright © 2014 Symantec Corporation. All Rights Reserved.

• You will now be given a choice of downloads. Choose the correct version for your system and click CONTINUE



• While the application is downloading, click CONTINUE. You will now be brought to your CAES Secure Email inbox to view the message that began this process.

| COBHA | m | | 😑 Settings 🔞 He | ymantec |
|---------|-----------------------------|-------------------|----------------------------|----------------|
| Compose | @gmail.com's Secure Int | box | 0% 0 | r 100 MB |
| | | | | |
| 🔄 Inbox | ODelete Resend All Messages | Messag | e 1-1 of 1 First Previo | us Next La |
| | | Messag Subject | e 1-1 of 1 First Previor | us Next La |
| Inbox | | | | Size |

This is the actual secure message that CAES sent you. Right now it is in your CAES Secure Email account on the CAES servers, however, once you complete the Symantec Encryption Satellite configuration, you will be able to re-send this message to your normal email client.

• Run the installer file for Symantec Encryption Satellite. Select not to display the Release Notes and click NEXT:



• After the installation is complete, you will be asked to reboot. Please do so:



- When your computer boots back up, the PGP Universal software will prompt you to enter your CAES Secure Email passphrase that you set in the Getting Started section.
 - Enter your password, click "REMEMBER THIS PASSPHRASE", and then click OK

| PGP Universal | | × |
|---|-----------------------|--------|
| Enter Web Messenger <u>p</u> assphrase for keys.aeroflex.com (external @gmail.com) : | | |
| | Show Keystr | okes 🗖 |
| | | |
| Remember this passphrase | <u>O</u> K <u>C</u> a | ncel |

• The software will now enroll with the CAES servers.

| 뗽 PGP Universal | × |
|---|---|
| Retrieving policy from keys.aeroflex.com | |
| | |
| | |

- Upon successful completion, you will see the following screen
 - NOTE: If you have issues enrolling, make sure your computer can communicate outbound over the Internet to keys.cobhamna.com on Port 443 (HTTPS). You may need to contact your local IT department to enable this communication.



- ***NOTE: If you DO NOT receive the message below, YOU ARE COMPLETE. Proceed to Page 10.
- After completing the enrollment, the software will detect your mail client settings. Depending on those settings, you **MAY** see a screen similar to the following:



This screen indicates that further action is necessary to configure your computer. Symantec Encryption Satellite needs to perform the SSL/TLS to your mail server instead of your mail client.

Simply click OK to this message and then go into your mail client to perform the configuration.

- The following screens show how to make these changes in Microsoft Outlook. For other mail clients, please refer to your user manual
 - o Open Outlook and Go to "ACCOUNT SETTINGS"
 - Outlook 2007
 - Click the TOOLS menu and select ACCOUNT SETTINGS
 - Outlook 2010

- Click the FILE menu and select ACCOUNT SETTINGS
- Select your email account and click CHANGE

| New Bepair | |
|---|------|
| ате Туре | uit) |
| | ult) |
| external @gmall.com IMAP/SMTP (send from this account by defa | ult) |
| | |
| | |
| lected e-mail account delivers new e-mail messages to the following location: | |
| external.@gmail.com\Inbox | |
| in data file F:\Documents and Settings\\Outl external @gmail.com-00000002.pst | |
| | C |

Ensure the correct email account is selected and click CHANGE

• Click the MORE SETTINGS button

| hange E-mail Account | | X |
|--|--|---|
| Internet E-mail Settings Each of these settings a | re required to get your e-mail account | : working. |
| User Information | | Test Account Settings |
| Your Name: | External User | After filling out the information on this screen, we recommend you test your account by clicking the |
| E-mail Address: | XXXXX@gmail.com | button below. (Requires network connection) |
| Server Information | | Test Account Settings |
| Account Type: | IMAP 👻 | Test Account bettings |
| Incoming mail server: | imap.gmail.com | |
| Outgoing mail server (SMTP): | smtp.gmail.com | |
| Logon Information | | |
| User Name: | 200000 | |
| Password: | ***** | |
| v | Remember password | \frown |
| Reguire logon using Securi | e Password Authentication (SPA) | More Settings |
| | | < Back Next > Cancel |

• Select the ADVANCED tab and make sure that the encryption field is set to NONE in both directions



- Click OK
- Click NEXT on the CHANGE EMAIL ACCOUNT screen, then Click FINISH

| Change E-mail Account | Change E-mail Account |
|---|--|
| Internet E-mail Settings Each of these settings are required to get your e-mail account working. | Congratulations! |
| User Information Test Account Settings Your Name: Issemed User E-mail Address: 000000@gmail.com Server Information Issemed User Account Your Account Notice Settings Issemed User Account Your Settings Issemed User Qutgoing mail server: Imp.gmail.com Uger Name: > Bassnort: ********** Image Description ********** Image Description ********** Image Description *************** Image Description ************************************ | You have successfully entered all the information required to setup your account. To close the weard, click Finish. |
| < goods to Cancel | < Back Finish |

- Close Outlook and then Re-Open Outlook
 - You should not receive the SSL/TLS Connection detected notification any longer.
- At this point, you have completed the configuration and can continue to use your email program normally as you always have.
- All emails from CAES that were secured PRIOR to you completing this configuration are still located in your CAES Secure Email portal.
 - Now that you have finished your configuration, you can re-send these emails through the new configuration to your normal email client.
- Log into the CAES Secure Email portal at https://keys.cobhamna.com

| совнат | Symantec. |
|--|---|
| CAES Secure Email Portal In order to gain access to your account and messages you must first enter your email and passphrase associated with this account. | Please login to access your secure inbox: Email Address: Passphrase: I lost my passphrase Login |

Copyright @ 2014 Symantec Corporation. All Rights Reserved.

• Click on INBOX on the left hand side (if not selected already)

| COBHA | m | | ⊘ s | ymanted |
|---------|--------------------------------|--------|--|------------------------|
| Compose | @gmail.com's Secure Inbox | | 0% of | f 100 MB |
| 10 | @ginamoon o coodi o insox | | | |
| Inbox | Delete Resend All Messages | | e 1-1 of 1 First Previou | us Next La |
| Inbox | | | e 1-1 of 1 First Previou Received V | us Next La Size |
| | O Delete | Messag | | Size |

• The message(s) that were secured BEFORE you completed the configuration will be shown here. Click the RESEND ALL MESSAGES button.

• The servers will send all messages back through the system with your new PGP Satellite configuration (encrypted to your new PGP key)

• To verify that the configuration is working, go back to your email client and look at the new message(s) that have arrived. The email should look as follows:

| First Message to a Non-Aeroflex user | | |
|---|---|-------------------|
| User, Aeroflex&eroflexUser@aeroflex.com] | | |
| Sent: Thu 7/12/2012 3:39 PM | | |
| To: External@gmail.com | | |
| | -Notice the "PGP Decrypted" message and the blue border (annotation | on) |
| * PGP Decrypted Message | Notice the Tor Deciypted message and the blac border (annotation | 511) |
| Hello: | | |
| This is my first secure email to you. | CONFIGURATION AND TESTING IS NOW COMPLETE. | |
| | • If the newly arrived email looks as follows, then it is not wor | [.] king |
| | First Message to a Non-Aeroflex user | |
| | User, Aeroflex [AeroflexUser@aer of]ex.com] | |
| | Sent: Thu 7/12/2012 3:39 PM | |
| correctly: | To: External @qmail.com | |
| concerty. | 🖂 Message 📄 Version.bt (131 B) 💿 Message.pgp (3 KB) | |
| Please reboot your computer at this point an | d | try |
| to resend all messages again. If that fails, | | |
| to reserve an messages dgdill. If that falls, | | |

Uninstalling Symantec Encryption Satellite

please contact CAES at PGP.Admins@Cobhamaes.com

- If for any reason you wish to uninstall Symantec Encryption Satellite (such as switching delivery options), you must un-enroll from the CAES Secure Email servers, otherwise you may continue to receive secure email from CAES that you would not be able to read.
 - Uninstalling Symantec Encryption Satellite will not have any effect on the already decrypted email in your client. You will still be able to read previously sent secure emails from CAES that were sent while you had Symantec Encryption Satellite selected as your delivery option.
- Uninstall Symantec Encryption Satellite as you would any other application
 - CONTROL PANEL > PROGRAMS AND FEATURES
- When you select to uninstall, it will prompt you to un-enroll



• After contacting the CAES Secure Email servers, you will receive the following notice:

| PGP Universal X |
|---|
| Until you 'unenroll' from an External PGP Universal Server, it can continue to send you encrypted email messages. If you do not unenroll, you may receive future messages which you cannot decrypt. |
| Successfully unenrolled from keys.aeroflex.com |
| Unenroll Done |

- The program will continue to be uninstalled and you will be asked to reboot when you are finished.
- NOTE: If you performed the changes on the top of page 9 when you installed Symantec Encryption Satellite, be sure to set them back to their original values.

Configuring Key or Digital ID/Certificate Delivery Option

• After selecting the Key or Digital ID/Certificate option, you are presented with a screen asking you for the "public" portion of your PGP Key/Digital Certificate.



• The next screen you are presented with depends on what type (PGP or S/MIME) of public key you just uploaded. Please proceed to the appropriate section for the type of key you uploaded.

Configuring Your Account using a PGP Public Key

• After uploading your public PGP key, you are presented with the following screen and must configure a few things on your PGP Desktop software. PGP Desktop software is the only CAES supported PGP client.

| | nel User | |
|--|---|--|
| 1000 • Y | 0x357E70A1 3772 DFC6 1F46 0A78 8698 | E C |
| | 06EB E30D 91EE 357E 70A1 | |
| | o Total Signatures | |
| | | |
| | ges should be made to you and to encrypt your replies. | ur PGP Desktop configuration in order to decrypt and verify messages you receive from |
| ways records com | and to encrypt your repores: | |
| 1. Add Keys | erver | |
| Add this keys | erver to your list of keyserve | ers in the PGP Desidop options. You will need the following pieces of information in order to |
| do this: | | 1 |
| Name Port |); keys.aeroflex.com | |
| | vin: aeroflex.com | |
| 1 | 1.1.22 | |
| 2. Add Orga | nization Key | |
| First, downlo | ad the Organization Key. | |
| | ownhant Organization Kny | < |
| -100 | ewonan organization Key | |
| | | |
| Then, import | | up keyring. If the Validity column in PGP keys does not indicate the key is valid, sign the key d in the Key Properties window. |

-The uploaded PGP key information is displayed here. Verify it is correct

This information for CAES's PGP keyserver is needed so that you do not need to exchange public keys with CAES users. Configuring this allows PGP Desktop to search for, and find, the public keys of CAES users.

Click the DOWNLOAD button.

You must download CAES's organization PGP key so that you can verify and trust all CAES PGP keys for encryption with PGP Desktop.

• Save the CAES organization key to a location on your computer.

| File Download 🛛 🛛 🗙 | | Save As | | | | | ? × |
|--|---------------|-----------------------------|---|-----------------------------|-------|-------|--------------|
| Do you want to open or save this file? | | | SYSTEM (F:) | | • 3 🕫 | • 🖭 🏷 | |
| Name: key0xB83D53EE304F000A.asc Type: PGP Armored File, 5.87KB | | | Documents and | Settings | | | |
| Type: PGP Armored File, 5.87KB | | My Recent Documents | i I386 | | | | |
| From: keys.aeroflex.com | | 1 | MSOCache | | | | |
| Open Save Cancel | | Desktop | Constraint Program Files Quarantine WINDOWS | | | | |
| While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. <u>What's the risk?</u> | \rightarrow | My Documents My Computer | | | | | |
| | | S | | | | | |
| | | My Network | File <u>n</u> ame: | aeroflex_organization_key.a | asc | • | <u>S</u> ave |
| | | Places | Save as type: | PGP Armored File | | • | Cancel |

• Open your PGP Desktop software by right clicking the lock icon in your system tray



• Select the TOOLS menu and select EDIT KEYSERVERS



Select ADD

| Server Address | Туре | Trusted |
|-------------------|---------------------------|---------|
| keyserver.pgp.com | PGP Global Directory LDAP | Yes |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | Add Edit | Remove |
| | | |

• Fill out the new keyserver information as follows and then click OK:

| Edit Server | × |
|-----------------------------|--------------------------|
| Туре: | PGP Keyserver LDAPS |
| Address: | keys.aeroflex.com |
| Port: | Default (636) Custom |
| Base DN: | |
| Authentication Certificate: | |
| | <u>QK</u> <u>Cancel</u> |

- Verify your Keyserver list now includes the keys.CobhamNA.com server
 - You may have more servers than shown here

| Server Address | Туре | Trusted |
|--|--|-----------------|
| keyserver.pgp.com keys.aeroflex.com | PGP Global Directory LDAP PGP Keyserver LDAPS | Yes |
| | | |
| | Add Edit | Re <u>m</u> ove |

• Select the FILE menu and select IMPORT



• Browse to the CAES organization key you saved earlier and select OPEN:



• At the Select Key screen, click IMPORT:



• Right-click the key in PGP Desktop and select SIGN



• Confirm that you want to sign the key by clicking OK (you may be asked for your personal PGP key passphrase)

| PGP Sign Key | | × |
|---|--|---------|
| By signing the selected user ID(s), you are key(s) and attached user ID(s) actually belo | certifying based on your own direct first-hand knowledge that th ong to the identified user(s). | he |
| Before signing, make sure the $\mbox{key}(s)$ were q fingerprint with the owner. | given to you in a secure manner by the owner or you have verifi | ied the |
| Key/User Name | Fingerprint | |
| aeroflex.com | 2884 DEE6 410B 30FB 745D A2EF BB3D 53EE 304F 000A | |
| aeroflex.com <pgp.admins@aerofl< td=""><td>2884 DEE6 410B 30FB 745D A2EF BB3D 53EE 304F 000A</td><td></td></pgp.admins@aerofl<> | 2884 DEE6 410B 30FB 745D A2EF BB3D 53EE 304F 000A | |
| • | | F |
| Allow signature to be exported. Ot | hers may rely upon your signature. | |
| More Choices | <u>OK</u> <u>Cancel</u> <u>H</u> el | p |
| | \downarrow | |
| PGP Enter Passphrase for Selecte | ed Key 🔀 | |
| <u>S</u> igning key : | | |
| External User < External User @gmail. | com> (RSA/2048) | |
| | Show Keystrokes | |
| Passphrase of signing key: | | NOTE |
| | t | he C |
| | | scree |
| | | |
| | <u>QK</u> <u>Cancel</u> | |

NOTE: This is asking for your personal PGP key passphrase, NOT the CAES Secure Email portal passphrase. You will only see this screen if your passphrase is not cached.

• You should now see the CAES organization key as verified



- You have completed the configuration.
- All emails from CAES that were secured PRIOR to you completing this configuration are still located in your CAES Secure Email portal.
 - Now that you have finished your configuration, you can re-send these emails through the new configuration to your normal email client.
- Log into the CAES Secure Email portal at <u>https://keys.cobhamna.com</u>

| совнят | Symantec. |
|--|---|
| CAES Secure Email Portal In order to gain access to your account and messages you must first enter your email and passphrase associated with this account. | Please login to access your secure inbox: Email Address: Passphrase: I lost my passphrase Login |

Copyright © 2014 Symantec Corporation. All Rights Reserved.

• Click on INBOX on the left hand side (if not selected already)

| COBHA | m | | 😑 Settings 😔 H | elp 设 Lo |
|---------|---------------------------|---------------------|-----------------------------|--------------|
| Compose | @gmail.com's Secure Inbox | | 0%10 | f 100 MB |
| Nbox 🔤 | O Delete All Messages | - | e 1-1 of 1 First Previo | - |
| sent 🖌 | | Subject PGP Test | Received ▼ Today 1:29 PM | Size 6 KB |
| | | | | |

- The message(s) that were secured BEFORE you completed the configuration will be shown here. Click the RESEND ALL MESSAGES button.
- The servers will send all messages back through the system, this time encrypting to your PGP key

Configuring Your Account using an S/MIME (X509) Public Key

• After uploading your public S/MIME key, you are presented with the following screen and must configure a few things on your computer.

| hank you fi | r uploading your certificate. This server will now encrypt messages to you using your certificate. |
|-------------|---|
| | ation Certificate must be installed properly in your environment in order to decrypt and verify messages you receive from and to encrypt your replies: |
| 1. Dow | nload the Organization Certificate |
| . | |
| | Download Organization Certificate |
| | |
| -2. Insta | II The Certificate Into Your Mail Client |
| • 01 | llook / Outlook Express |
| | ou use Microsoft Outlook, open Internet Explorer, open Internet Options from the Tools menu, select Certificates from the ntent panel, and then Import the Organization Certificate as a Trusted Root Certification Authority. |
| • Ot | er Email Clients |
| | ase refer to your email client documentation for information on how to install a Trusted Root CA Certificate. |
| Pl | |
| | hese steps will allow you to trust the certificates from senders signed by the Organization Certificate, and encrypt your replies |

Click the DOWNLOAD button.

You must download CAES's Organization certificate so that your computer will trust CAES S/MIME certificates for decryption with your mail client.

• Save the CAES Organization certificate to a location on your computer



- Open the Internet Options on the computer
 - CONTROL PANEL > INTERNET OPTIONS > CONTENT tab > CERTIFICATES



• Select the TRUSTED ROOT CERTIFICATE AUTHORITIES tab and then click IMPORT



• At the WELCOME TO THE CERTIFICATE IMPORT WIZARD, click NEXT



• Click BROWSE and select the CAES Organization certificate you saved earlier and then click NEXT



• Ensure the certificate will be placed into the TRUSTED ROOT CERTIFICATION AUTHORITIES and click NEXT



• At the COMPLETING THE CERTIFICATE IMPORT WIZARD, click FINISH



Ensure that you receive a successful confirmation and click OK



• NOTE: If you receive the message below:



• Go back and perform the import again, this time using the OTHER PEOPLE tab:

| Certificates | | | ? × |
|------------------------------|--------------------------|-------------------|----------------------------|
| Intended purpose: | | | T |
| Personal Other People In | rmediate Certification A | uthorities Trus | ted Root Certification • • |
| | | | |
| Issued To | Issued By | Expiratio | Friendly Name |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Import Export | Remove | | Advanced |
| Certificate intended purpose | 15 | | |
| | | | |
| | | | View |
| | | | |
| | | | ⊆lose |

- The following configuration is optional, but recommended. It will let your email client search for CAES S/MIME certificates without you having to exchange signed emails with the CAES user.
 - The following screens show how to make these changes in Microsoft Outlook. For other mail clients, please refer to your user manual
 - Open Outlook and Go to "ACCOUNT SETTINGS"
 - Outlook 2007
 - Click the TOOLS menu and select ACCOUNT SETTINGS
 - Outlook 2010
 - o Click the FILE menu and select ACCOUNT SETTINGS

Select the ADDRESS BOOK tab and then click NEW



Choose INTERNET DIRECTORY SERVICE and click NEXT

| ld New E-mail Account | × |
|---|--------|
| Directory or Address Book Type You can choose the type of directory or address book you'd like to add. | × |
| • Internet Directory Service (LDAP) | |
| Connect to an LDAP server to find and verify e-mail addresses and other information. | |
| C Additional Address Books | |
| Connect to an address book to find and verify e-mail addresses and other information. | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| < Back Next > | Cancel |
| | |

• Enter keys.CobhamNA.com for the server name and then click MORE SETTINGS

| hange E-mail Account | × |
|--|--------|
| Directory Service (LDAP) Settings You can enter the required settings to access information in a directory service. | × |
| Server Information | |
| Type the name of the directory server your Internet service provider or system administrator has given you. | |
| Server Name: keys.aeroflex.com | |
| Logon Information | |
| This server requires me to log on | |
| User Name: | |
| Password: | |
| Regure Secure Password Authentication (SPA) | |
| < <u>Back</u> <u>Ment</u> > | Cancel |

• On the CONNECTION tab, fill out as follows

| Microsoft LDAP Directory | X |
|--|----------------------------|
| Display Name The <u>di</u> splay name as it ap keys.aeroflex.com | opears in the Address Book |
| Connection Details | 636 |
| Use Secure Sockets Layer | v |
| ОК | Cancel Apply |

• On the SEARCH tab, fill out as follows

| Microsoft LDAP Directory |
|--|
| Connection Search |
| Server Settings Search timeout in seconds: 60 Specify the maximum number of entries you want to return after a successful search: 100 |
| Search Base C Use Default C Custom: 0=Users |
| Browsing <u>Enable Browsing (requires server support)</u> |
| OK Cancel Apply |

- Click OK, then click NEXT, then click FINISH, and finally click CLOSE
- Now close Microsoft Outlook and re-open it to make the new address book take effect
- You have completed the configuration.
- All emails from CAES that were secured PRIOR to you completing this configuration are still located in your CAES Secure Email portal.
 - Now that you have finished your configuration, you can re-send these emails through the new configuration to your normal email client.
- Log into the CAES Secure Email portal at <u>https://keys.cobhamna.com</u>

| COBHAM | Symantec. |
|--|---|
| CAES Secure Email Portal In order to gain access to your account and messages you must first enter your email and passphrase associated with this account. | Please login to access your secure inbox: Email Address: Passphrase: I lost my passphrase Login |

Copyright © 2014 Symantec Corporation. All Rights Reserved.

• Click on INBOX on the left hand side (if not selected already)

| OBHRI | | | Symantee. |
|---------|---|---------------------|--|
| Compose | @gmail.com's Secure Inbox | | 0% of 100 MB |
| | | | |
| 🔨 inbox | 🖉 Delete 🛛 🔿 Resend All Mess ges | | Message 1-1 of 1 First Previous Next Last |
| | Delete Resend All Mess bes From | Subject | Message 1-1 of 1 First Previous Next Last Received * Size |
| Sent | | Subject PGP Test | |

• The message(s) that were secured BEFORE you completed the configuration will be shown here. Click the RESEND ALL MESSAGES button.

• The servers will send all messages back through the system, this time encrypting to your S/MIME key

Using Your CAES Secure Email Portal

• The first screen you will see after selecting the Regular Email or PGP Web Messenger option, will be the original secure email sent by CAES.

| Compose | 🔦 Reply 🛛 🦘 Reply To All 🖉 Delete 🚔 Print | Message 1 of 1 First Previous Next |
|----------------|---|--|
| 🛃 Inbox 🏹 Sent | From: @cobham.com> To: @gmail.com> Subject: PGP Test | 02/20/2018 1.29 F |
| | PGP Test | |
| | | |
| | | |
| | Please consider the environment before printing this email | |
| | Please consider the environment before printing this small This e-mail and any files transmitted with it ("E-mail") is intended solely for the addresses()) and may contain information under applicable like. If you are not the intended addresses(), any disclosure, reproduction, copyreg, distribution or or distributed or copies to foring multion, residing in the United States or advance, which the prior organized of the distributed or copies to foring multion, residing in the United States or advance, which the prior organized of the time that is an an error, plase delete I and deletroys all copies of the E-mail and notify the ander multidative is takeforder the like the known prior any subdatory or difficult or associated conception can be under the bits final acception. | of the E-mail is strictly prohibited. It may also contain data subject to the been transmitted from a United States location, and cannot be disseminated. Department of State or appropriate export licensing authority. If you have receiv- call or return e-mail. Is any lability in respect of the content (including errors and omissions) nor shall th |
| | Please consider the environment before printing this email This e-mail and any first transmitted with 1("E-mail") is intended table for the addressed() and may contain information under applicable like. If you are not the intended addressed(), any disclosure, neproduction, copyrup, distribution or interface and the first in Arm Regulations or United States or abrand, without the prior approval of the U.S. the E-mail in euror, jease date in a defany of a point of the E-mail and endity the under intendent or abrand, without the prior approval of the U.S. the E-mail in euror, jease date in a defany of a point of the E-mail and endity the under intendent or visible to an of the sum of the endity of subpoint or the E-mail in euror, jease date in the defany of a point of the E-mail and endity of the under intendent of the sum of the endity of the subpoint of the U.S. | ther use of the E-mail is strictly prohibited. It may also contain data subject to the been transmitted from a United Statis location, and cannot be dissemitated, . Department of State or appropriate seport licensing authority. If you have recei- all or return e-mail of the context (including errors and onitission) nor shall be say lability in respect of the context (including errors and onitission) nor shall |

REMEMBER: Symantec Web Email: EVERY email you receive from CAES will be a notification from the CAES Secure Email servers, and will contain a link to the corresponding message on the CAES Secure Email portal.

Regular Email: Non-secure emails from CAES will come in to your email program. Secure email's from CAES, however, will continue to be a notification that contains the link to the corresponding message.

- From the email message, you can REPLY, REPLY ALL, DELETE, and PRINT
 - REPLY: Replies securely to the CAES user that sent the message
 - o REPLY ALL: Replies securely to all recipients of the original message
 - NOTE: You cannot add any new recipients to the email unless they have an CobhamAES.com

Settings
The Message Could Not Be Sent
The following addresses were not in the original recipient list and are not managed by this PGP Universal Server:
User@somedomain.com

- o DELETE: Deletes the email message on the portal
- PRINT: Prints the message

email

- → From the navigation bar, you can COMPOSE, go to your INBOX, and go to your SENT items folder
 - COMPOSE: Creates a new email to one or many CobhamAES.com addresses
 - \circ $\;$ INBOX: Brings you to your INBOX view. Click here when finished reading a message.
 - SENT: Brings you to your SENT ITEMS view.

• Your INBOX view is as follows

| 2 | | | 😂 Settings 🔗 Help 🛛 Cogo | SETTINGS: Changes your delivery option |
|---------|--------------------------------|----------------|---|---|
| совня | m | | Symantec. | HELP: Displays PGP Help |
| | | | | LOGOUT: Logs out of the portal |
| Compose | @gmail.com's Secure Inb | ох | 0% of 100 MB | |
| 💐 Inbox | Oelete Resend All Messages | Messag | e 1-1 of 1 First Previous Next Last | [↓] The amount of space your portal is using |
| Sent | Prom | Subject | Received V Size | compared to your total allowed |
| ~ | SSA | PGP Test | Today 1:29 PM 6 KB | compared to your total anowed |
| | 🖉 Delete 🔷 Resend All Messages | Messag | e 1-1 of 1 First Previous Next Last | |
| | | | | You may click either the sender's name, or |
| | | Copyright © 20 | 4 Symantec Corporation. All Rights Reserv | |
| | | | | the subject to open the email |

• The COMPOSE view is as follows

| Compose | - Send Attach X Cancel | |
|---------|------------------------|--|
| Inbox | From: Bgmail.com | |
| Sent | To: | |
| | Ce | |
| | Subject | |
| | Add attachment | |
| | | |
| | | |
| | | |

- From the COMPOSE screen, you can SEND, ATTACH, and CANCEL
 - SEND: Sends the email. Click this when you are finished with the message. You will see:



• ATTACH: Attaches a file to the secure email. Clicking ATTACH bring up the following screen:



• CANCEL: Cancels the email and returns you to your INBOX view

Appendix A

Exporting your S/MIME Certificate

This section describes how to export the public version of your S/MIME certificate from the Windows operating system. If you do not use Microsoft Windows, OR if you do not have Administrative rights on your computer, you will need to contact your local IT department for instructions on how to export your S/MIME public key.

- Open the Certificates Manager
 - Windows XP Click your START button and select RUN, then type certmgr.msc , then click OK

| Run | ? X |
|-------|--|
| | Type the name of a program, folder, document, or Internet resource, and Windows will open it for you. |
| Open: | certmgr.msc |
| | OK Cancel Browse |

• Windows 7 – Click your START button and type certmgr.msc in the search bar, then hit ENTER

| 🎾 See ma | ore results | | | |
|----------------|-------------|--------|---|---------|
| certmgr.m | sc | | × | Log off |
| © Start | 5 | \sum | | |

- Select the PERSONAL certificate store and then select the CERTIFICATES folder
 - Find your S/MIME certificate. Right click the certificate and choose ALL TASKS > EXPORT



export wizard, click NEXT



At the Export Private Key screen, select NOT to export the private key and click NEXT •



At the Export File Format screen, choose Base-64 encoded X509 and click NEXT .



At the File to Export screen, click BROWSE. Enter a filename and location, click SAVE. Confirm and click NEXT. .



Cobham Secure Email User Guide (for External Recipients)

• At the Completing the Export screen, confirm the settings and click FINISH



• You will receive the confirmation as follows



NOTE: Upload the generated file when you are asked for your key in the Enrolling as an External User section.

Exporting your PGP Key (from PGP Desktop)

This section describes how to export the public version of your PGP key from the PGP Desktop software only. If you do not use PGP Desktop, you will need to contact your local IT department or software manual for instructions on how to export your PGP public key.

- Open PGP Desktop
 - Right click your icon in the system tray and select Open PGP Desktop



Click PGP KEYS on the left hand side and then right click your PGP key in the right hand pane and select EXPORT



• Select a location for the file and give it a filename. Make sure you DO NOT export the private key.



Troubleshooting

All my emails from CAES are "Secure Web Messenger"

Problem: All my emails from CAES are encrypted or only receive "Secure Web Messenger" email notices, even though the CAES sender did not encrypt the message.

Cause: Your Secure Messaging Settings are set to "Symantec Web Email Protection"

<u>Solution</u>: Log in to the CAES Secure Email Portal at <u>https://keys.cobhamna.com</u> and go to "Settings" and select the option for "Regular Email" and click "Choose Option".

| | V. | |
|---|---|----|
| | 😑 Settings 🛛 Ələp 🔞 Logou | ıt |
| COBHAM | Symantec. | |
| | Copyright © 2014 Symantec Corporation. All Rights Reserved | I. |
| ecure Messaging Settings | | |
| You are currently registered as a Regular Email user. | | |
| Please select how you would like to receive future messages from Cobh O Symantec Web Email Protection (Recommended) | am. | |
| Let me read all my messages from Cobham securely on this | Neb site. | |
| Save a copy of all outgoing messages in my "Sent" mess | ages folder. | |
| Symantec Encryption Satellite | | |
| I want to install a small background service on my computer to | automatically secure messages I exchange with Cobham. | |
| Key or digital ID/certificate (Select this option if you are an adva | nced user.) | |
| | that I want to use to secure messages I exchange with Cobham. | |
| Regular Email | | |
| | | |
| I want to receive as many messages as possible via normal e because of higher security needs. | mail. Some messages may still be delivered via other means | |

I forgot my password for the CAES Secure Web Messenger"

Problem: I forgot my password to the CAES Secure Email Portal or my password has expired.

Solution: Go to the CAES Secure Email Portal at https://keys.cobhamna.com and click "I lost my passphrase"

| COBHAM | Symantec. |
|--|---|
| CAES Secure Email Portal In order to gain access to your account and messages you must first enter your email and passphrase associated with this account. | Please login to access your secure inbox: Email Address: Passphrase: I lost my passphrase Login |

Copyright © 2018 Symantec Corporation. All Rights Reserved.

• Enter the email address you originally registered on the CAES Secure Email Portal and click **Send**:

| COBHAM | Symantec. |
|--|----------------------------|
| Reset Passphrase | |
| Please enter your email address to receive a link where you can safely reset your passphrase. Your current passphrase you enter a new one. | e will remain active until |
| Email Address: | Send |

Copyright © 2018 Symantec Corporation. All Rights Reserved.

- You will receive an email with a link to reset your passphrase. If your account is in the "Locked" state, check your mailbox for the "Symantec Encryption Server Account Unlock" email from Symantec Encryption Server, and follow the instructions in the email to unlock your account
 - Note: if you do not receive the email within 30 minutes please check your SPAM folder and inform your
 IT department to allow emails from "DONOTREPLY@cobhamna.com"