Glob@lCerts™

Email Encryption using the GlobalCerts SecureMail Gateway(SMG)

Updated: May 2019

Contents

Introduction

What is secure email?

Secure email is a way to communicate securely between two email clients. Regular emails over the Internet are like a postcard in the mail; anyone can read the message. Secure emails are locked using a digital envelope. A message sent to you is **locked/encrypted with your public key**, creating the envelope, and **can only be unlocked with your private key**. Since only you have your private key, only you can open the envelope. Your private key must be protected and never given to anyone else, while your public key is openly available to anyone wishing to send you a secure message. Your public key is contained in something called a certificate, which binds your name and email address to your public key.

You can also digitally sign a message with these keys. A message is **signed with your private key**, your certificate is then sent along with the message, so that the recipient can check the signature using your public key.

How Do I Send Secure Email?

Sending a secure email is as simple as typing [**secure**] as the first characters in the Subject line of your email and sending the email as usual (signing an email can be accomplished with the **[sign]** keyword). However, there are two ways to send a secure email through the SecureMail Gateway:

1. You and the external party can first **exchange encryption keys**. This allows both of you to send and receive secure emails from this party. This option is useful if you will be regularly exchanging emails with a particular party and if that party uses a secure email system or certificate. See “Sending Secure Email by First Exchanging Encryption Keys” on the next page for more information.

2. Or, you can send a secure email to the external party through the SecureMail Gateway’s **SecureMessenger^{TM} web portal**. SecureMessenger does not require an exchange of encryption keys. Instead, the external party will receive a message directing them to a web page. The recipient accesses your secure email message by clicking on the link in their email message, and entering a passphrase that is related to a hint you have provided. See “Sending Secure Email Without First Exchanging Encryption Keys” on the next page for more information.

Sending Secure Email By First Exchanging Encryption Keys

To exchange encryption keys with another party, all you have to do is receive a digitally signed email from the external party and then send them a secure email in return. The SecureMail Gateway will automatically harvest public keys from digitally signed inbound emails, create your public and private keys, and sign your email.

To exchange encryption keys, the external party must:

- Have a secure email client installed on their desktop. Most of the commonly used email clients (Outlook, Thunderbird, etc.) have this capability.
- Have a private key and public key installed in their email client.
- Send at least one email to you that is digitally signed.

When you receive the digitally signed email, the SecureMail Gateway automatically harvests the external party's public key that is imbedded in the email. It is actually stored in a certificate, which is attached to the secure email message.

Now that the SecureMail Gateway knows the external party's public key, you can send encrypted messages to them. The first time the external party receives your encrypted email; their client will harvest your public key, as well as using their private key to decrypt the email you sent them.

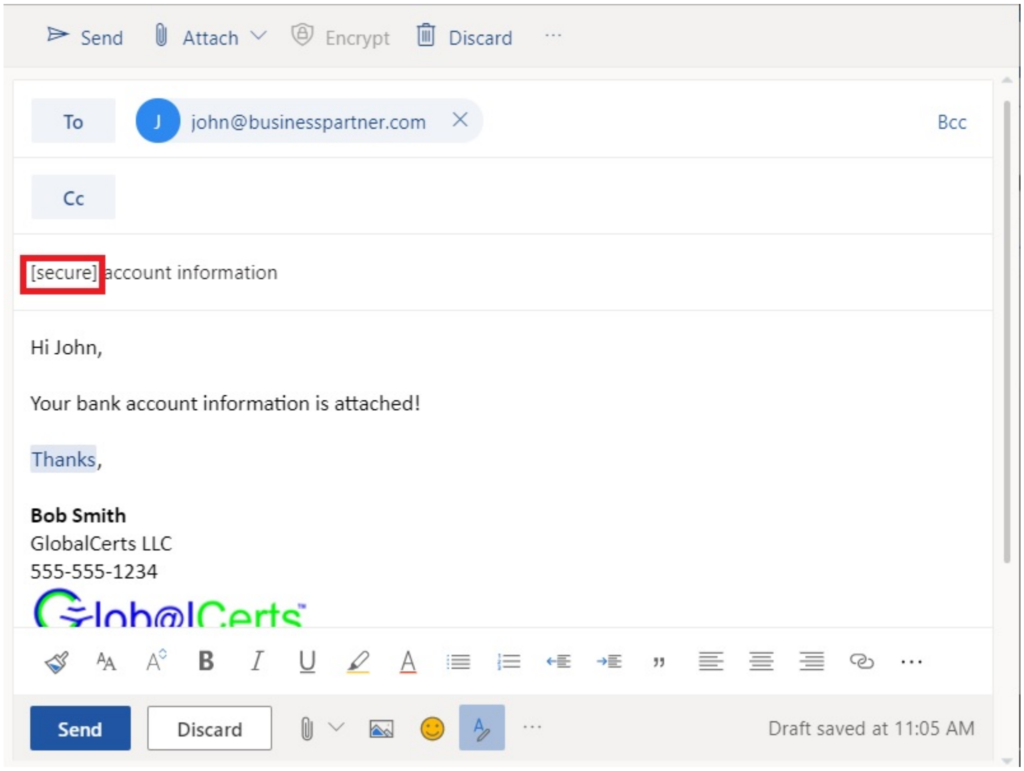
Once keys have been exchanged, either party can send a secure message to the other. All you have to do to send a secure message is to type **[secure]** (including the brackets) to the Subject line of your email message as shown in Figure 1 on the next page.

Sending Secure Email To Someone With No Certificate

If an external party does not have encryption keys installed, you can still send them secure email using the **SecureMessenger** web portal feature.

To send a secure email to an external party with whom you have not or cannot exchange keys:

1. Prepare the email and enter **[secure]** (including the brackets) as the first characters of your Subject line as shown in figure 1 on the next page.



To: john@businesspartner.com

Cc

[secure] account information

Hi John,

Your bank account information is attached!

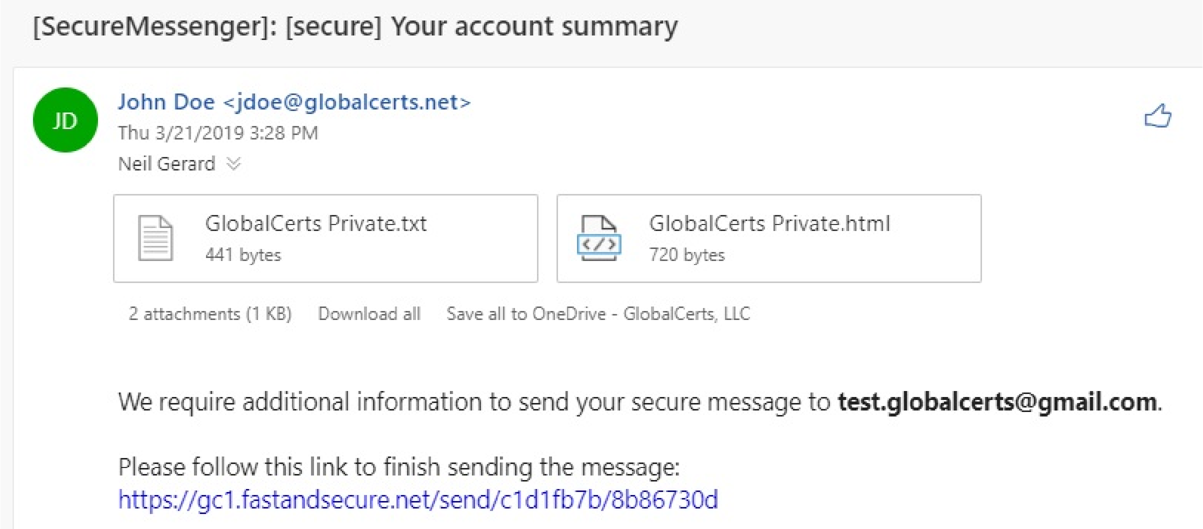
Thanks,

Bob Smith
GlobalCerts LLC
555-555-1234

Figure 1: Using the [secure] flag to ensure encryption

2. Send the email as usual. The SecureMail Gateway will recognize that there is no public key for the recipient, then **looks for a Secure Messenger Template** for the intended recipient. If it finds a template it will send the message encrypting it with the template passphrase.

3. If the gateway cannot find a template for the recipient, it will send you a "bounce back" message similar to the one shown in figure 2 below. If you do not receive a bounce, your system may be set to invite the recipient to create the template, and you do not need to do anything further.



[SecureMessenger]: [secure] Your account summary

John Doe <jdoe@globalcerts.net>
Thu 3/21/2019 3:28 PM
Neil Gerard

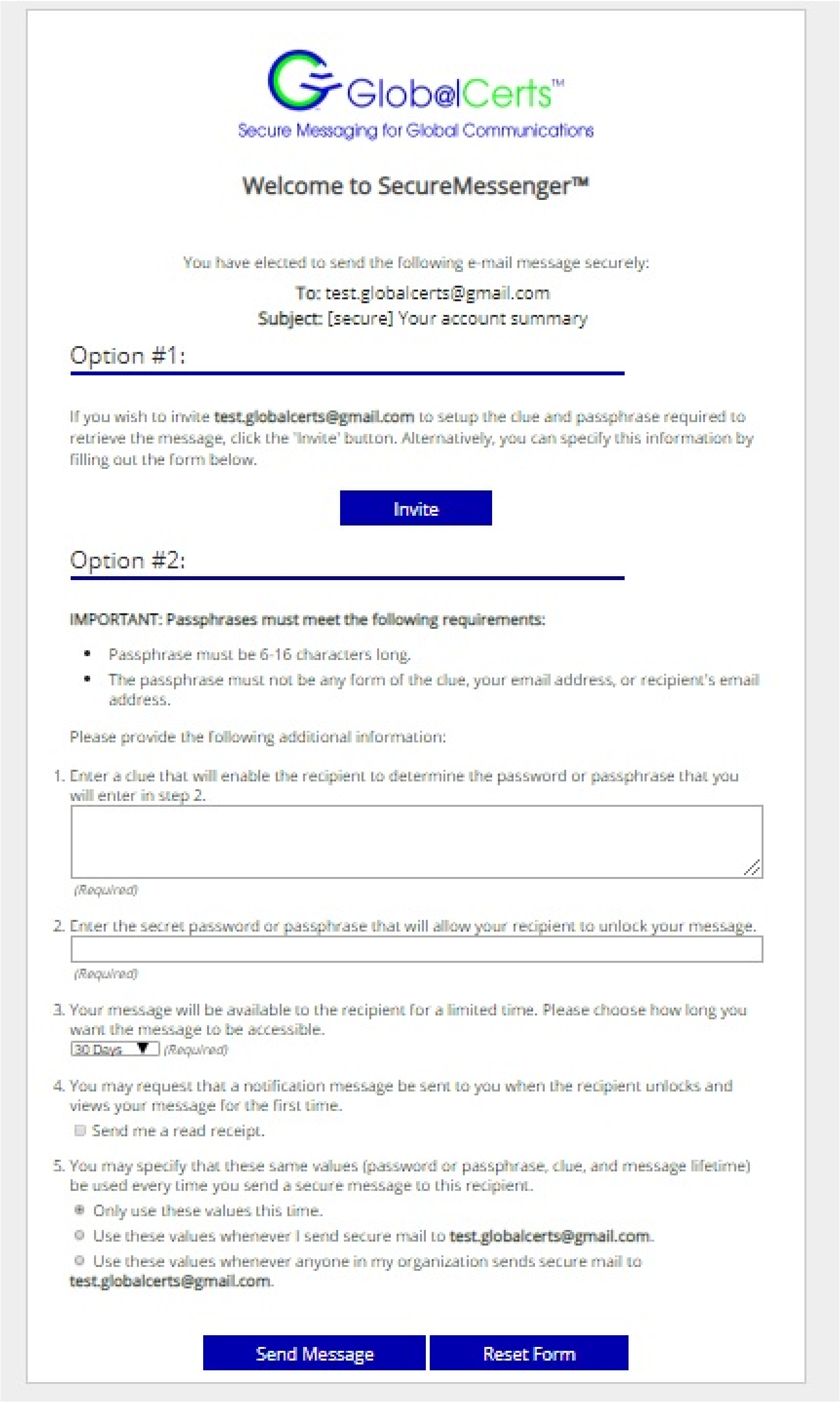
GlobalCerts Private.txt
441 bytes

GlobalCerts Private.html
720 bytes

We require additional information to send your secure message to **test.globalcerts@gmail.com**.

Please follow this link to finish sending the message:
https://gc1.fastandsecure.net/send/c1d1fb7b/8b86730d

1. Click on the link and you will be taken to a secure web page on the SecureMail Gateway. You will see a form like the one shown below (Figure 3).



Welcome to SecureMessenger™

You have elected to send the following e-mail message securely:

To: test.globalcerts@gmail.com
Subject: [secure] Your account summary

Option #1:

If you wish to invite **test.globalcerts@gmail.com** to setup the clue and passphrase required to retrieve the message, click the 'Invite' button. Alternatively, you can specify this information by filling out the form below.

Option #2:

IMPORTANT: Passphrases must meet the following requirements:

- Passphrase must be 6-16 characters long.
- The passphrase must not be any form of the clue, your email address, or recipient's email address.

Please provide the following additional information:

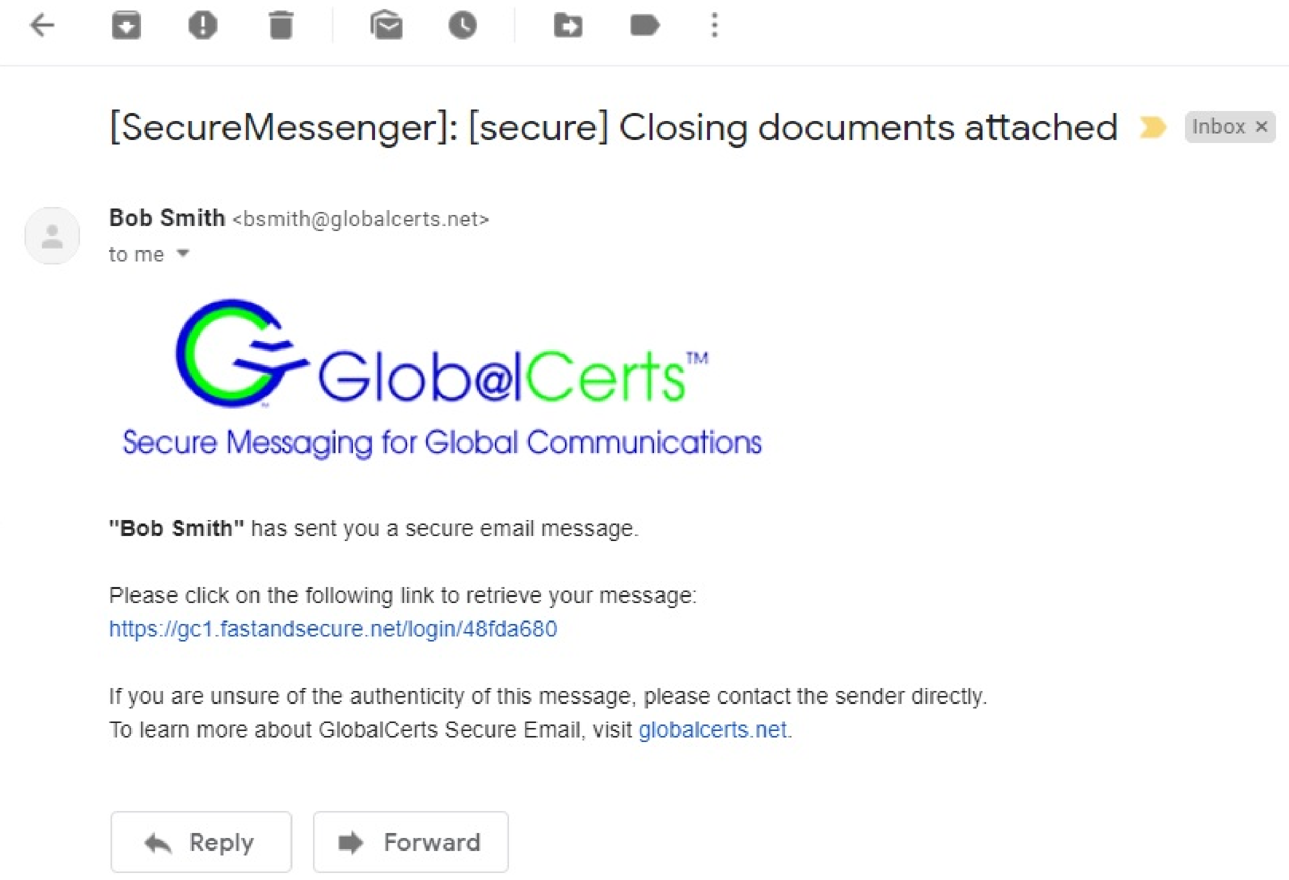
1. Enter a clue that will enable the recipient to determine the password or passphrase that you will enter in step 2.
   (Required)
2. Enter the secret password or passphrase that will allow your recipient to unlock your message.
   (Required)
3. Your message will be available to the recipient for a limited time. Please choose how long you want the message to be accessible.
   30 Days ▼ *(Required)*
4. You may request that a notification message be sent to you when the recipient unlocks and views your message for the first time.
   □ Send me a read receipt.
5. You may specify that these same values (password or passphrase, clue, and message lifetime) be used every time you send a secure message to this recipient.
   ● Only use these values this time.
   ○ Use these values whenever I send secure mail to **test.globalcerts@gmail.com**.
   ○ Use these values whenever anyone in my organization sends secure mail to **test.globalcerts@gmail.com**.

Figure 3: SecureMessenger™ Sender's Web Interface.

2. If you wish to set up the clue/passphrase, complete the required fields. The clue (1) should allow the recipient to determine the passphrase. The time limit (3) determines how long the message remains available after the recipient has first read it. The default is two weeks. Checking the receipt notification check box (4) will cause a return receipt email to be sent to the original sender. You may also choose to store the template for future user in item 5.

3. Click on the **“Send Message”** button to send the message.

4. The SecureMail Gateway will send the recipient a message like the one shown below (Figure 4).



[SecureMessenger]: [secure] Closing documents attached

Bob Smith <bsmith@globalcerts.net>
to me

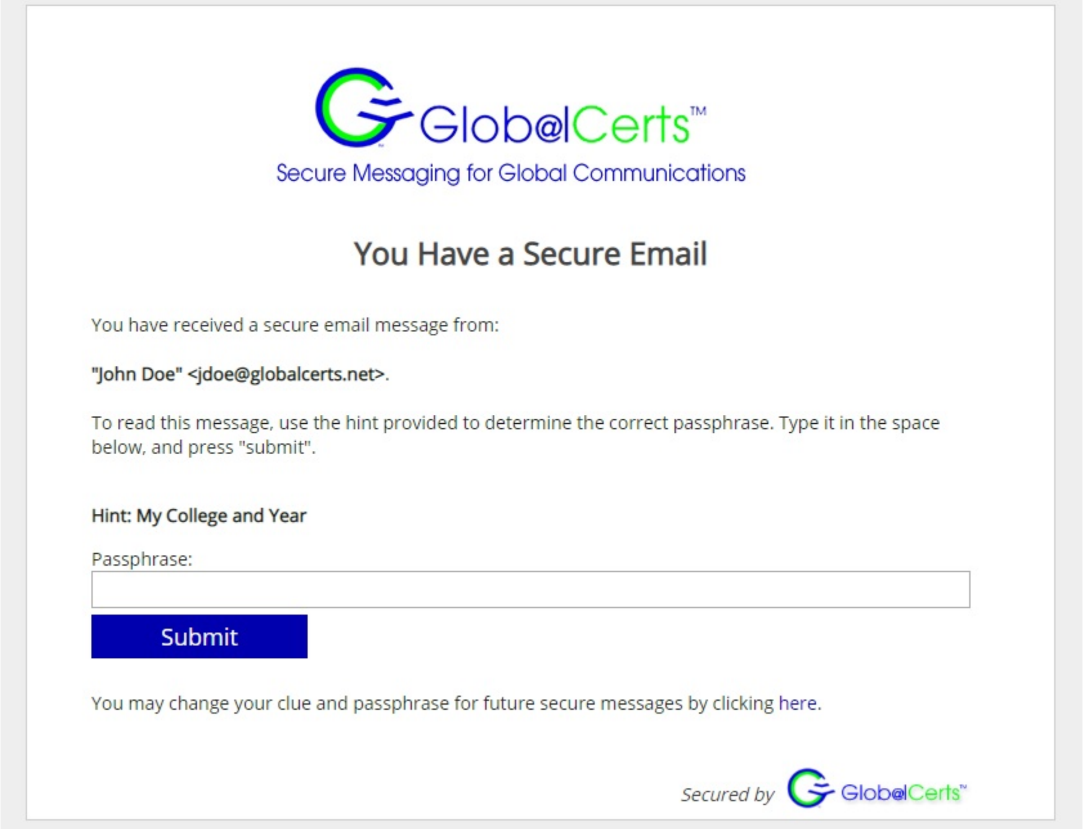
"Bob Smith" has sent you a secure email message.

Please click on the following link to retrieve your message:
https://gc1.fastandsecure.net/login/48fda680

If you are unsure of the authenticity of this message, please contact the sender directly.
To learn more about GlobalCerts Secure Email, visit globalcerts.net.

Figure 4: SecureMessenger™ Recipient Notification Email

5. The recipient clicks on the supplied link and sees a screen similar to that shown below (Figure 5). They enter the passphrase and click on the “Submit” button.



You Have a Secure Email

You have received a secure email message from:

"John Doe" <jdoe@globalcerts.net>.

To read this message, use the hint provided to determine the correct passphrase. Type it in the space below, and press "submit".

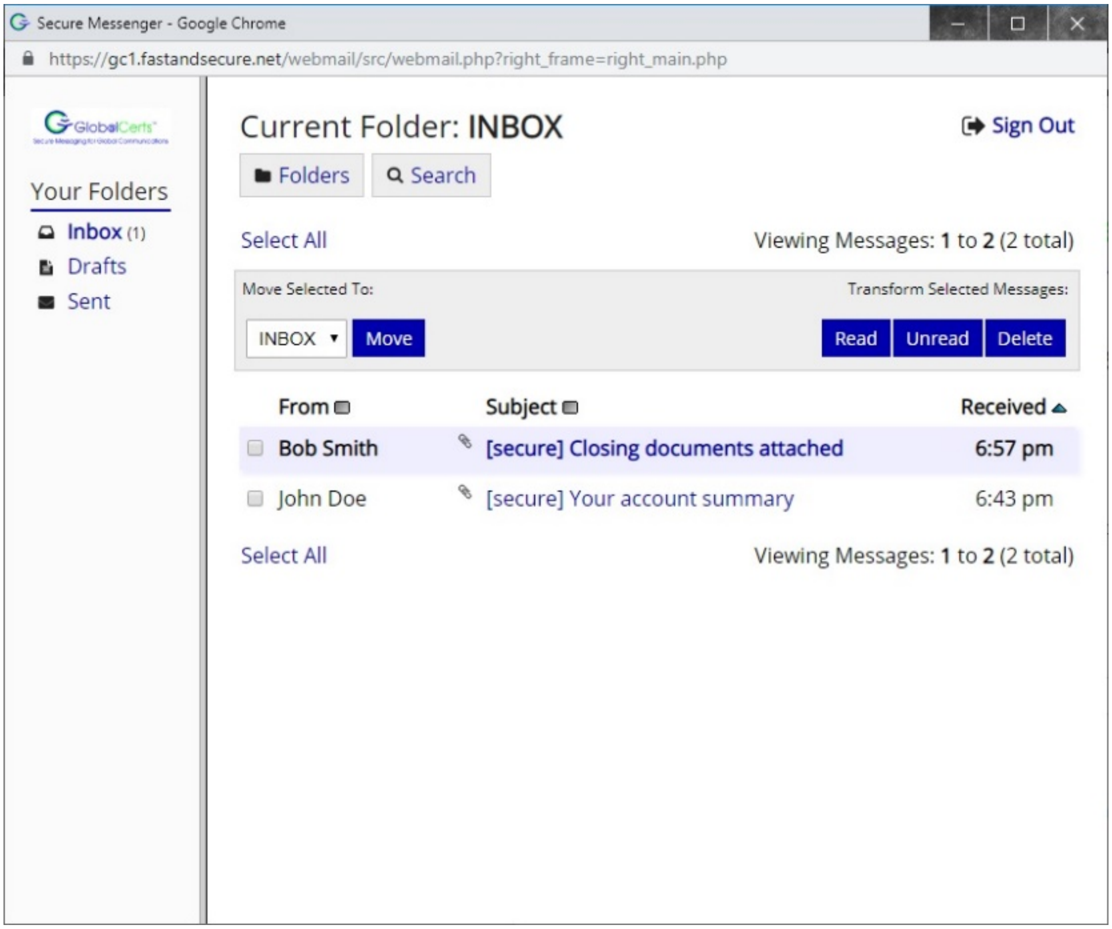
Hint: My College and Year

Passphrase:

You may change your clue and passphrase for future secure messages by clicking here.

Figure 5: SecureMessenger™ Recipient Authentication

6. The recipient is authenticated and able to read the message in its unencrypted format as shown (Figure 6). If the return receipt check box were enabled, then you would receive an email message notifying you that your message had been picked up.



Secure Messenger - Google Chrome

https://gc1.fastandsecure.net/webmail/src/webmail.php?right_frame=right_main.php

Current Folder: INBOX

Viewing Messages: 1 to 2 (2 total)

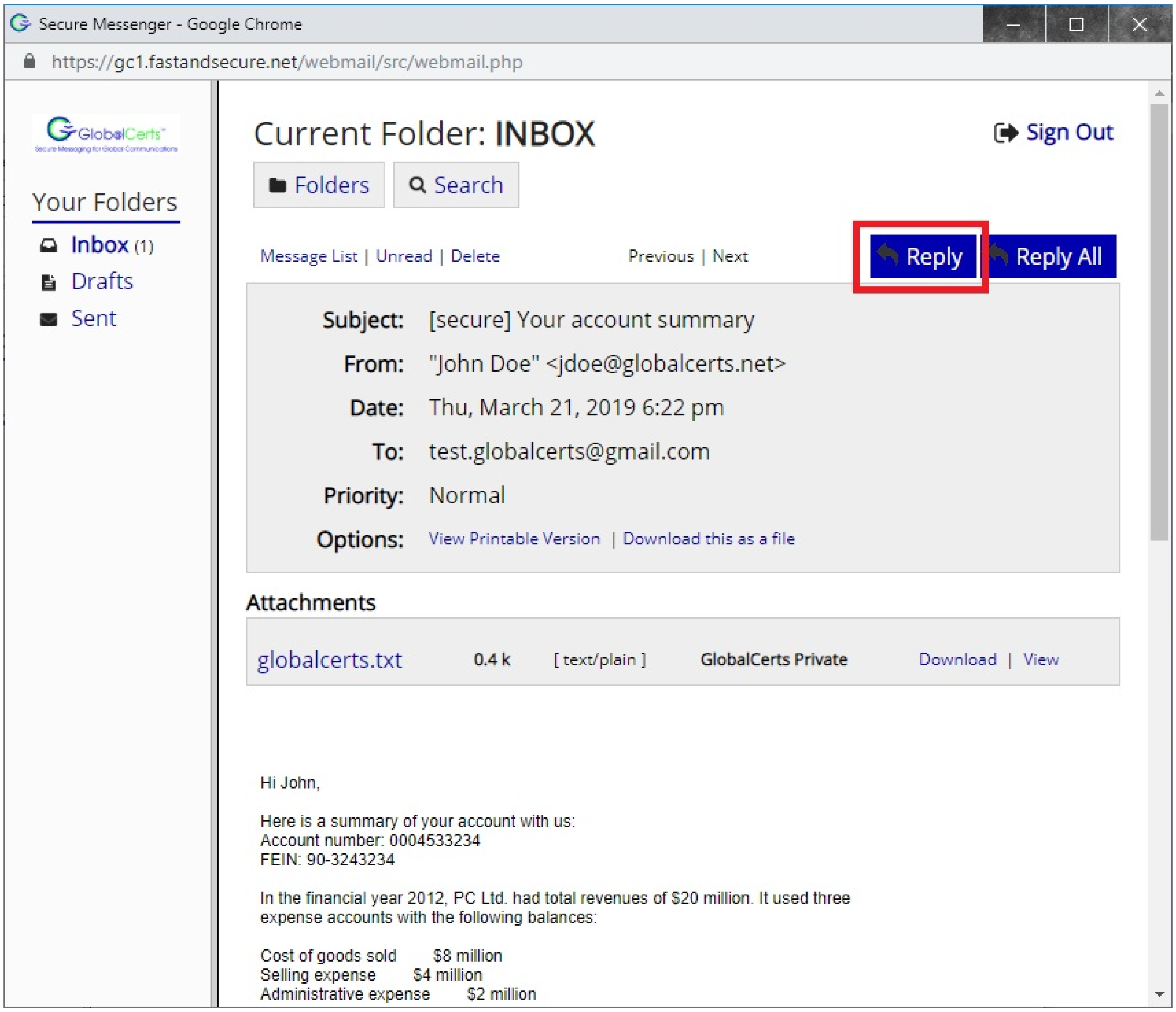
Move Selected To: INBOX

	From		Subject	Received
□	Bob Smith	✎	[secure] Closing documents attached	6:57 pm
□	John Doe	✎	[secure] Your account summary	6:43 pm

Viewing Messages: 1 to 2 (2 total)

Figure 6: SecureMessenger™ Webmail Interface - Received Mail

7. The recipient can securely reply to the original sender using the **"Reply" button**. Clicking on this button will open a reply form similar to the one shown below (Figure 7). The response will be encrypted and signed.


Secure Messenger - Google Chrome
https://gc1.fastandsecure.net/webmail/src/webmail.php
GlobalCerts
Your Folders
Inbox (1)
Drafts
Sent
Current Folder: INBOX
Sign Out
Folders
Search
Message List | Unread | Delete
Previous | Next
Reply
Reply All
Options:
View Printable Version | Download this as a file
Attachments
Download | View

Subject: [secure] Your account summary
From: "John Doe" <jdoe@globalcerts.net>
Date: Thu, March 21, 2019 6:22 pm
To: test.globalcerts@gmail.com
Priority: Normal

globalcerts.txt	0.4 k	[text/plain]	GlobalCerts Private

Hi John,

Here is a summary of your account with us:
Account number: 0004533234
FEIN: 90-3243234

In the financial year 2012, PC Ltd. had total revenues of $20 million. It used three expense accounts with the following balances:

Cost of goods sold $8 million
Selling expense $4 million
Administrative expense $2 million

Figure 7: SecureMessenger™ Webmail Reply Interface

How Do I Receive Secure Email?

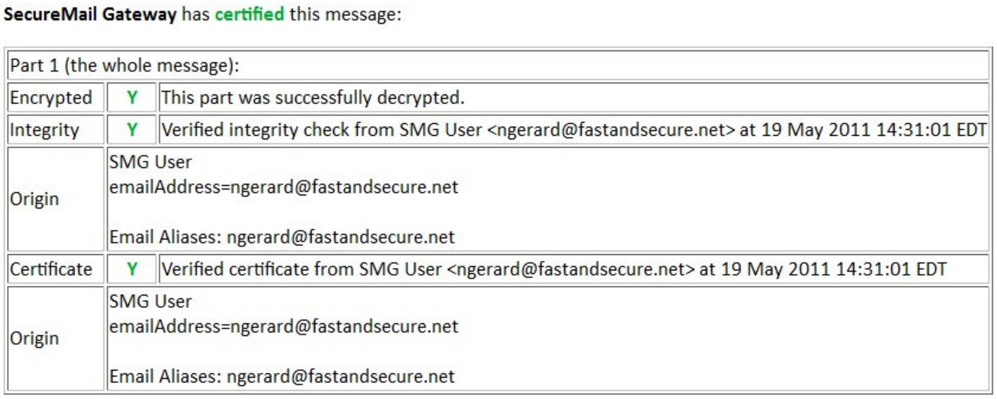
Once encryption keys have been exchanged, receiving an encrypted message is just like receiving a regular email message. The party sending you the email simply has to choose to send the email securely. When you receive a secure email, **it will appear as a regular email; however, there will be a small attachment to the email to show its security status.**

An external party may also send you a secure email by replying to a secure email that you sent through SecureMessenger.

How can I make sure that a message I receive is encrypted?

Because the SMG operates transparently at the gateway level, you can send email with a SecureMail Gateway in place and remain unaware of whether the Gateway found it possible to encrypt your mail. However, the SecureMail Gateway allows you to determine the security of received email. This is done by attachments called **cryptography summaries**.

The cryptography summaries on your emails can indicate three things. The "Encrypted" row contains information about whether the email was encrypted. The "Integrity" row contains information about whether the email included a valid digital signature. The "Certificate" row contains information verifying that the certificate attached to the email is valid, and identifies the email address of the certificate owner. This ensures that the public key you are using to check the signature actually belongs to the email address from which you are receiving email.



SecureMail Gateway has **certified** this message:

Part 1 (the whole message):		
Encrypted	Y	This part was successfully decrypted.
Integrity	Y	Verified integrity check from SMG User <ngerard@fastandsecure.net> at 19 May 2011 14:31:01 EDT
Origin	SMG User emailAddress=ngerard@fastandsecure.net Email Aliases: ngerard@fastandsecure.net	
Certificate	Y	Verified certificate from SMG User <ngerard@fastandsecure.net> at 19 May 2011 14:31:01 EDT
Origin	SMG User emailAddress=ngerard@fastandsecure.net Email Aliases: ngerard@fastandsecure.net	

Figure 8: A typical cryptography summary for an email digitally signed and encrypted.

Summary

Basic email travels back and forth across the Internet unprotected and vulnerable to attack. Email security consists of two fundamental concepts, encryption and signing. Encryption conceals the contents of a message, and a signature ensures the integrity of the message. Without encryption the message can be read by anybody who sees it in transit, without a signature, the message can be altered without the recipient’s knowledge. The SecureMail Gateway ensures that both techniques are used correctly to ensure email security.