Secure Email Communication (DigitalSignature)

IT is beginning the process of sending **S/MIME** digitally signed email messages from automated systems that need to send email to users.

This will allow you to verify the authenticity of the email message and know that it did indeed come from Rice and is not some phishing or hacking attempt.

Currently, only messages from **no-reply@rice.edu** are going to be digitally signed. These messages will appear to be from the user **Automated Email** and the certificate will be issued by **InCommon Standard Assurance Client CA**.

The full certificate chain will look like this:

- AddTrust External CA Root
    - UTN-USERFirst-Client Authentication and Email
        - InCommon Standard Assurance Client CA
            - Automated Email

What is S/MIME?

S/MIME stands for Secure/Multipurpose Internet Mail Extensions and is a standard for public key encryption and signing of MIME data (an email message). What it allows you to do is two things:

1. Ensure to your email recipients that YOU actually sent the email
2. Allows the possibility of sending and/or receiving email encrypted

What does this mean?

When you receive an email from the email address **no-reply@rice.edu**, if it has been digitally signed, you can be assured that it was sent from Rice. If you receive mail from the address **no-reply@rice.edu**, but it is not digitally signed, it could be a fake, forgery or phishing attempt.

How do you know that the message is digitally signed?

This varies by the mail client that you are using, though every mail client will do it similarly. In general, they will all put some indicator in or around the header of the mail message to indicate that the message has been digitally signed and that the signature is valid or invalid.

Various mail clients:

- Google Mail (Gmail)
- Mac Mail
- Webmail
- iOS Mail
- Windows Thunderbird

Other mail clients also allow you to verify the signature but it is slightly different for each one. Please contact your DivRep or the IT Help Desk to learn how to verify this signature in your mail client.

In Google Mail (Gmail)

Currently there is no way to verify a digital signature in Google Mail. Please use Webmail or real mail client to verify the authenticity of the digitally signed messages. We are investigating options with Gmail.

In Mac Mail

In Mac Mail, the digital signature is indicated by the **Security** header of the message and the presence of the **check mark** and the word **Signed**.
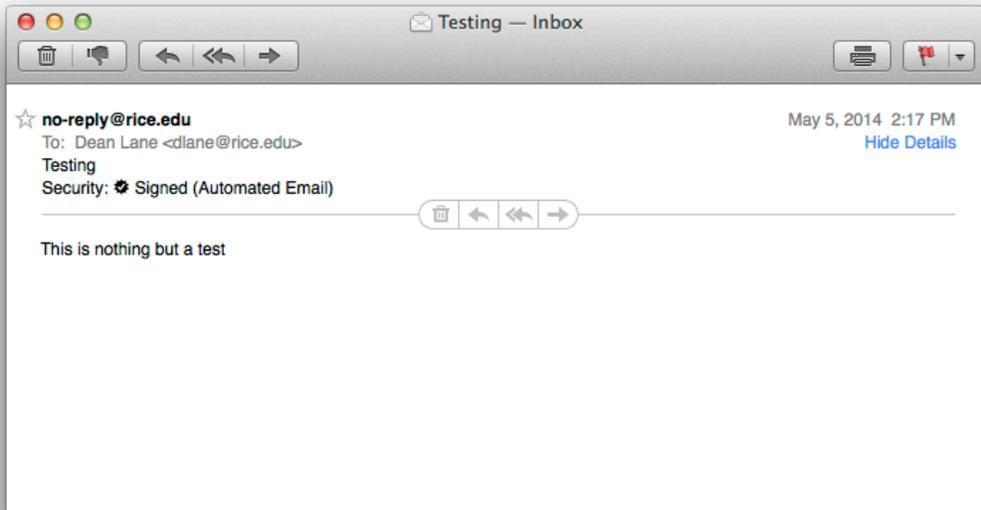
If you click on the **check mark**, you can get more information about the digital signature.
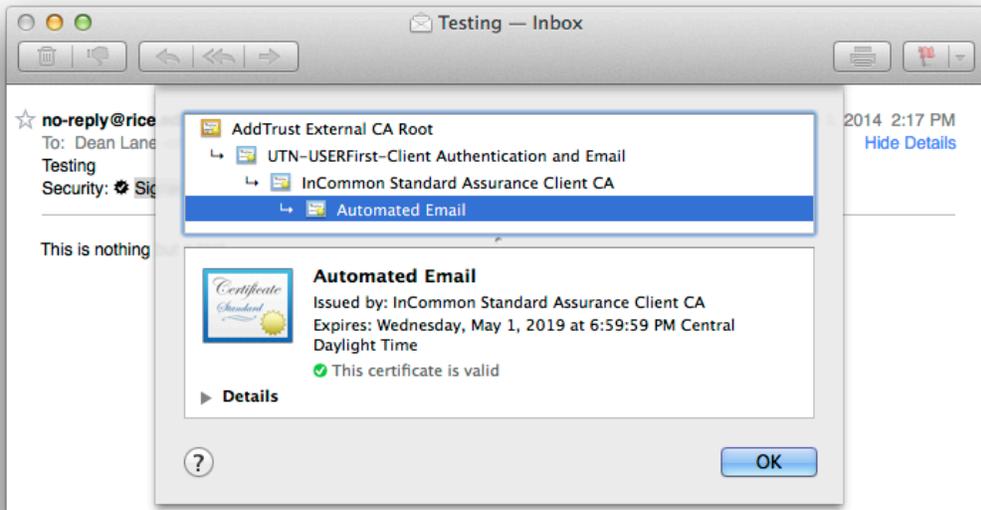
Notice the certificate chain is the same that is printed at the top of this page, that the Expiration date of the certificate has not passed and that there is a green check mark indicating that this certificate is valid.

This allows you to know that this message did come from Rice University IT and is something that you should probably pay attention too.

In Webmail

In Webmail, the digital signature is indicated in the body of the message by the **Pad Lock**, the word **Signed** and the yellow box below it.
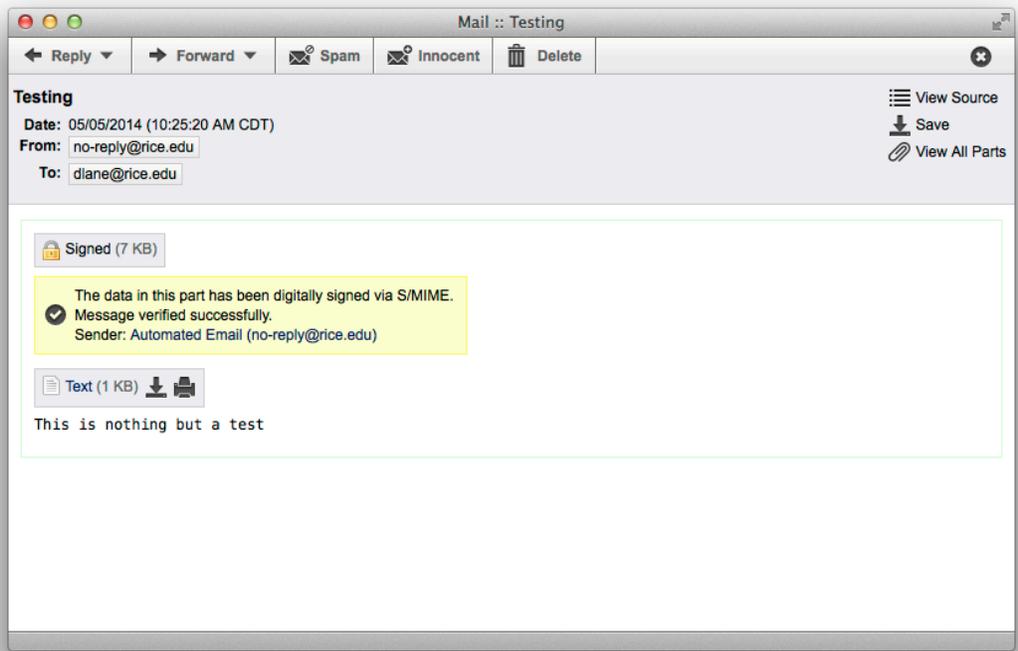
Clicking on the link "Automated Email (no-reply@rice.edu)" in the yellow box will display information about the signature.

```
●  ○  ○      https://webmail.rice.edu/imp/view.php?...C_FnNmKwoKpejj4p9g1&uniq=1399398626470    ⤢

Certificate Owner:
  *postalCode: 77251-1892
  Organisation: Information Technology
  Street Address:
    PO Box 1892
    MS 119
  State or Province: Texas
  Location: Houston
  Country: US
  Common Name: Automated Email
  Email Address: no-reply@rice.edu

Issuer:
  Country: US
  Organisation: Internet2
  Organisational Unit: InCommon
  Common Name: InCommon Standard Assurance Client CA

Validity:
  Not Before: 04/30/2014 07:00:00 PM
  Not After: 05/01/2019 06:59:59 PM

X509v3 extensions:
  *authorityKeyIdentifier:
    keyid:E8:D7:BD:96:AA:DD:D0:08:EF:A1:33:9E:5E:59:98:3C:12:B7:9B:91
  X509v3 Subject Key Identifier:
    3B:7D:44:C8:7B:68:19:27:AA:32:8C:9E:24:6B:8A:8C:A5:31:39:10
  Key Usage:
    Digital Signature, Key Encipherment
  X509v3 Basic Constraints:
    CA:FALSE
  *extendedKeyUsage:
    TLS Web Client Authentication, E-mail Protection
  Certificate Policies:
    Policy: 1.3.6.1.4.1.5923.1.4.3.3.0.1
  CPS: https://www.incommon.org/cert/repository/cps_standard_client.pdf
  CRL Distribution Points:
    Full Name:
  URI:http://crl.incommon.org/InCommonStandardAssuranceClientCA.crl
  *authorityInfoAccess:
    CA Issuers - URI:http://cert.incommon.org/InCommonStandardAssuranceClientCA.crt
OCSP - URI:http://ocsp.incommon.org
  X509v3 Subject Alternative Name:
    email:no-reply@rice.edu

Certificate Details:
  Version: 2
  Serial Number: 9223372036854775807
```

In iOS Mail

In iOS Mail, the digital signature is indicated by the presence of the **check mark** beside the **From** address.

If you click on the **From** address , you can get more information about the digital signature.
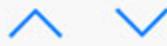
no-reply@rice.edu
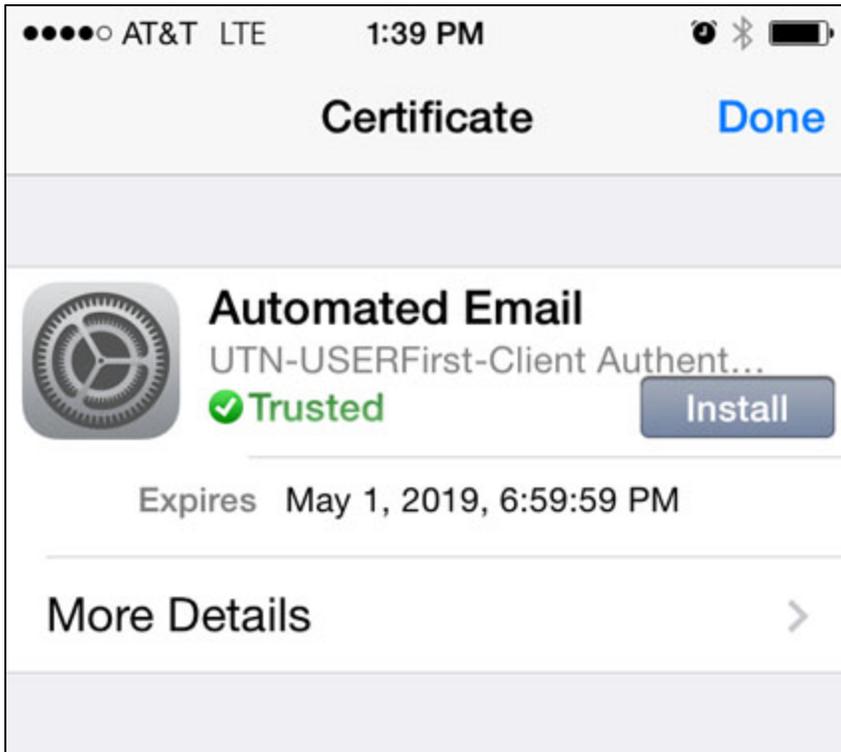
✔ Signed

The sender signed this message with a
trusted certificate.

View Certificate

Add to VIP

Create New Contact

Add to Existing Contact

And then clicking on verify certificate will show you this:

In Thunderbird for Windows mail, the digital signature is indicated by the presence of an **envelope icon** with a red seal beside the **Date** stamp.

Click on the **envelope icon** to display the certificate message.

From no-reply@rice.edu

Subject **Testing**

To Carlyn Chatfield

5/6/2014 1:08 PM

Other Actions ▾

Hell
This

Your
Your
Your

(c)

This   dating this
sign

Message Security   ☒

Message Is Signed

This message includes a valid digital signature. The message has not been altered since it was sent.

Signed by: Automated Email

Email address: no-reply@rice.edu

Certificate issued by: InCommon Standard Assurance Client CA

[View Signature Certificate]

Message Not Encrypted

This message was not encrypted before it was sent. Information sent over the Internet without encryption can be seen by other people while in transit.