Using your ECA identity Certificate on DOD PKI-enabled websites * These instructions assume that you have already properly loaded your certificates into

Mozilla Thunderbird.

1) Launch your Mozilla Firefox browser and go to your favorite DoD PKI-enabled website. A window should pop up stating that the website is certified by an unknown certificate. Select the "accept this certificate permanently" and click OK.

Website	Certified by an Unknown Authority	×
	Unable to verify the identity of usn.hq.navy.mil as a trusted site.	
∠₽	Possible reasons for this error:	
	- Your browser does not recognize the Certificate Authority that issued the site's certificate.	
	- The site's certificate is incomplete due to a server misconfiguration.	
	 You are connected to a site pretending to be usn.hq.navy.mil, possibly to obtain your confidential information. 	
	Please notify the site's webmaster about this problem.	
	Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site usn.hq.navy.mil?	
	Accept this certificate permanently	
	O Accept this certificate temporarily for this session	
	\odot Do not accept this certificate and do not connect to this Web site	
	OK Cancel	

2) Please enter your private key password in the **Master Password** prompt, and click **OK**.

Passwor	d Required	×1
3	Please enter the master password for the Software Security Device.	
	OK Cancel	

3) If you entered your private key password correctly, you should see the front page of the DoD PKI-enabled website that you want to access (e.g. https://infosec.navy.mil/PKI/). Please note that some DoD PKI-enabled websites may require registration of your PKI certificate or creation of a separate User ID and password.



Send a Digitally Signed Email from Mozilla Thunderbird.

* These instructions assume that you have already properly loaded your certificates into Mozilla Thunderbird.

1. Click on the WRITE icon from the top menu bar.



2. Click on the down arrow on the right side of the Security icon to view or change the security settings and select "Digitally Sign this message".

🟫 Compose: (no subject)	
<u>File Edit View Insert Format Options Tools Help</u>	
Send Contacts Spell Attach Security Save	
From: Nate Jensen <jensenn@orc.com> • Do Not Encrypt This Message Encrypt This Message</jensenn@orc.com>	<u>_</u>
To: Le Digitally Sign This Message	
View Security Info	
Subject:	

3. Complete and send the message.

Send an Encrypted Email from Mozilla Thunderbird:

* These instructions assume that you have already properly loaded your certificates into Mozilla Thunderbird.

1. Click on the WRITE icon from the top menu bar.

🧟 jensenr	n@orc.co	m - Thunderbir	'd									
<u>Eile E</u> dit	⊻iew	<u>G</u> o <u>M</u> essage	<u>T</u> ools <u>H</u>	elp								1) }
🥌 🗸	Write	Address Book	Reply	Reply All	Forward	Ø∵ Tag	X Delete	Junk	Si + Print	G Back -	erward -	Subject or Sender

2. Click on the down arrow on the right side of the Security icon to view or change the security settings and select "Encrypt This Message".

🗠 Compose: (no subject)	
Eile Edit View Insert Format Options Tools Help	
Send Contacts Spell Attach Security Save	
From: Nate Jensen <jensenn@orc.com> • Do Not Encrypt This Message • To: Encrypt This Message</jensenn@orc.com>	X
To: 🔤 Digitally Sign This Message	
View Security Info	
Subject:	

(= l a d

3. Complete and send this message.

Mozilla Thunderbird Instructions for Identity and Encryption Certificates:

* These instructions assume that you have already properly loaded your certificates into Mozilla Thunderbird.

1. Open your Mozilla Thunderbird inbox.

2. From the top menu bar select Tools->Account Settings



3. Once in the Account Settings window, select Security.

count Settings	
jensenn@orc.com	Security
-Server Settings -Copies & Folders -Composition & Addressing -Offline & Disk Space -Junk Settings -Return Receipts -Security Gmail - natejensen -Server Settings -Copies & Folders -Composition & Addressing -Disk Space -Junk Settings -Return Receipts -Security Local Folders -Disk Space -Junk Settings -Disk Space -Junk Settings Outgoing Server (SMTP)	To send and receive signed or encrypted messages, you should specify both a digital signing certificate and an encryption certificate. Digital Signing Use this certificate to digitally sign messages you send: Jensen.Nathanael.D.ORC1000014776.ID's Select Clear Digitally sign messages (by default) Encryption Use this certificate to encrypt & decrypt messages sent to you: Jensen.Nathanael.D.ORC1000014776.Enc Select Clear Default encryption setting when sending messages: Never (do not use encryption) Required (can't send message unless all recipients have certificates Yiew Certificates Security Devices
<u>A</u> dd Account	
Set as De <u>f</u> ault	
<u>R</u> emove Account	
	OK Cancel

4. From this window, based upon your preferences, you can set it so that every e-mail is digitally signed and encrypted.