Prior to issuing a CAC
- Ensure the customer has a valid e-mail address
- If the customer is changing affiliation (e.g., going from Active Duty to Civilian or Contractor status, etc.) and still needs access to previous encrypted email, they should return to their computer (before getting the new CAC) and recover their current encryption key and save it to a CD, so they can import it after being issued the new CAC. (NOTE: once a person changes affiliation, they CANNOT recover the previous e-mail encryption key).

While Issuing the CAC
Advise/brief the customer on the following after getting a new CAC:
- Follow the guidance at the AF PKI Website (web address is on the blue card handout):
- Reboot: Upon getting the new CAC, the customer may need to reboot their computer before logging on. If they don’t reboot, they may not be able to unlock the computer if they left it logged on (and locked) because it may be looking for the CAC they no longer have.
- Do NOT Publish-to-GAL: Advise the customer they should NOT have to publish their certificate to the Global Address List (GAL) unless absolutely necessary. Publishing to the GAL is automatic, but can take up to 24 hours in some instances. IF, after waiting 24 hours, the certificate is still not published, then follow the PTG instructions (posted at the link above).
- Key Recovery: The customer may need to recover the previous CAC encryption key to be able to open previous encrypted email. To do that, advise them to follow the instructions on the following web page:

Please see Reverse Side for More information Regarding Smart Card Logon
Brief the CAC customer on the following “logon” information. Now that PIV certificates are automatically activated at the time of CAC issuance, users may be confused on their first logon attempt after receiving a new CAC.

**Which Certificate to Choose for Smart Card Logon?**
The logon screen will display three certificates: the Email Signing Certificate, PIV Certificate, and DoD Identity Certificate. Continue to select the Email Signing Certificate to log on...it’s on the left. Notice from the image below that the certificate icons look identical. Select the certificate on the left.

If the PIV Certificate (in the center) is mistakenly selected, it will have a 16-digit EDIPI-number. To reselect the correct certificate, simply click “Switch User” and select the Email Signing Certificate (the certificate on the left). . . which is used to log on to the primary account.

After the first logon with a new CAC, you should normally not be asked to choose a certificate on subsequent logons.

**Note:** Users who log on to the same computer as others will have to select the correct certificate every time. Also — users with an additional account that uses the PIV Certificate for authentication (primarily System Administrators) will need to select the PIV Certificate when they log on.

**Dual CAC Holders:** (Primarily ANG and Reserve personnel) Users who have more than one CAC may need to update their CAC with a Personnel Category Code (PCC). For more information about Dual CAC Holders and how to update the CAC, go to the following link:


**For More Information:**
Visit us online today!
AF PKI Web Site
https://afpki.lackland.af.mil