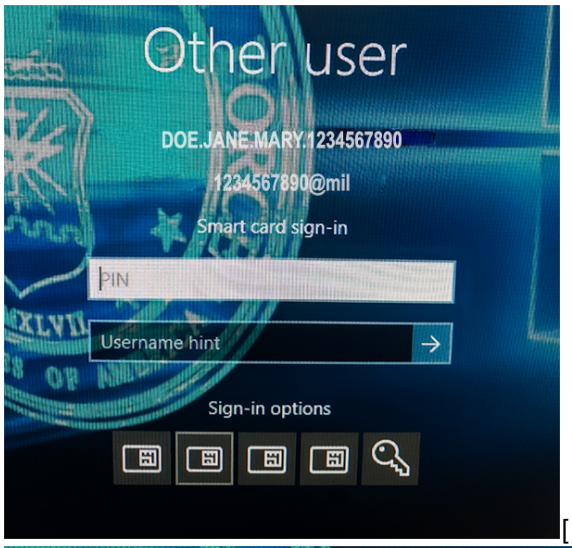
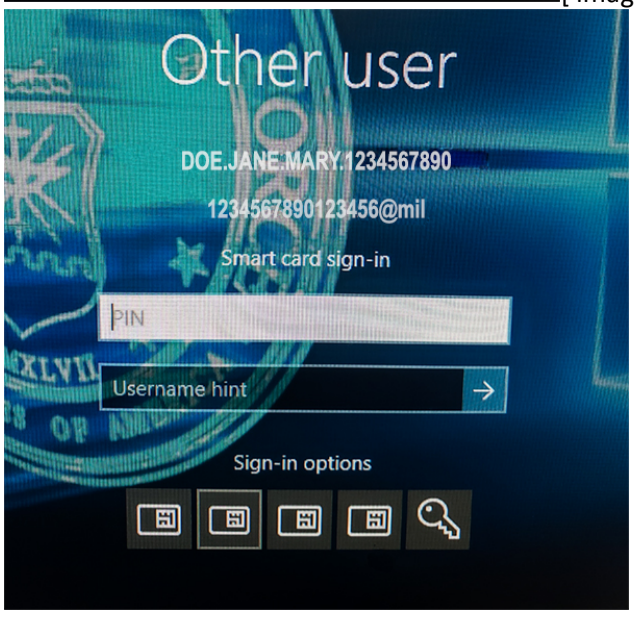
Personal Identity Verification (PIV) Certificate Logon Instructions: The Defense Manpower Data Center (DMDC) is updating the CAC and it affects every Airman, Government Civilian and Contractor who uses their CAC to log onto Air Force unclassified networks, systems, applications, websites, and portals. New CACs will be issued with fewer public key infrastructure (PKI) certificates encoded on the microchip; outwardly, the CAC's appearance will remain the same. CACs with the current configuration will be issued through attrition (e.g., upon expiration of current CAC or change in identification information or status); you will not be issued a new CAC until your current CAC expires.

A summary of changes includes eliminating the Identity Certificate, which leaves the PIV-Authentication (PIV-Auth) Certificate as the only certificate for authentication, reconfiguring attributes in the Email Signature Certificate so that it is used only for digitally signing email and documents, and not authenticating into workstations or applications. The Email Encryption Certificate is not affected by this effort.

With the current CAC/Smart Card Logon, you select the Email Signature Certificate, 10-digit edipi@mil, (image 1) to log onto the DEN network and to most applications, systems and websites that require authentication by PKI certificates. Your user account will be reconfigured to accept the PIV-Auth Certificate, 16 digit edipi+6@mil, for authentication (image 2), after which you will select the PIV-Auth Certificate instead of the Email Signature Certificate.

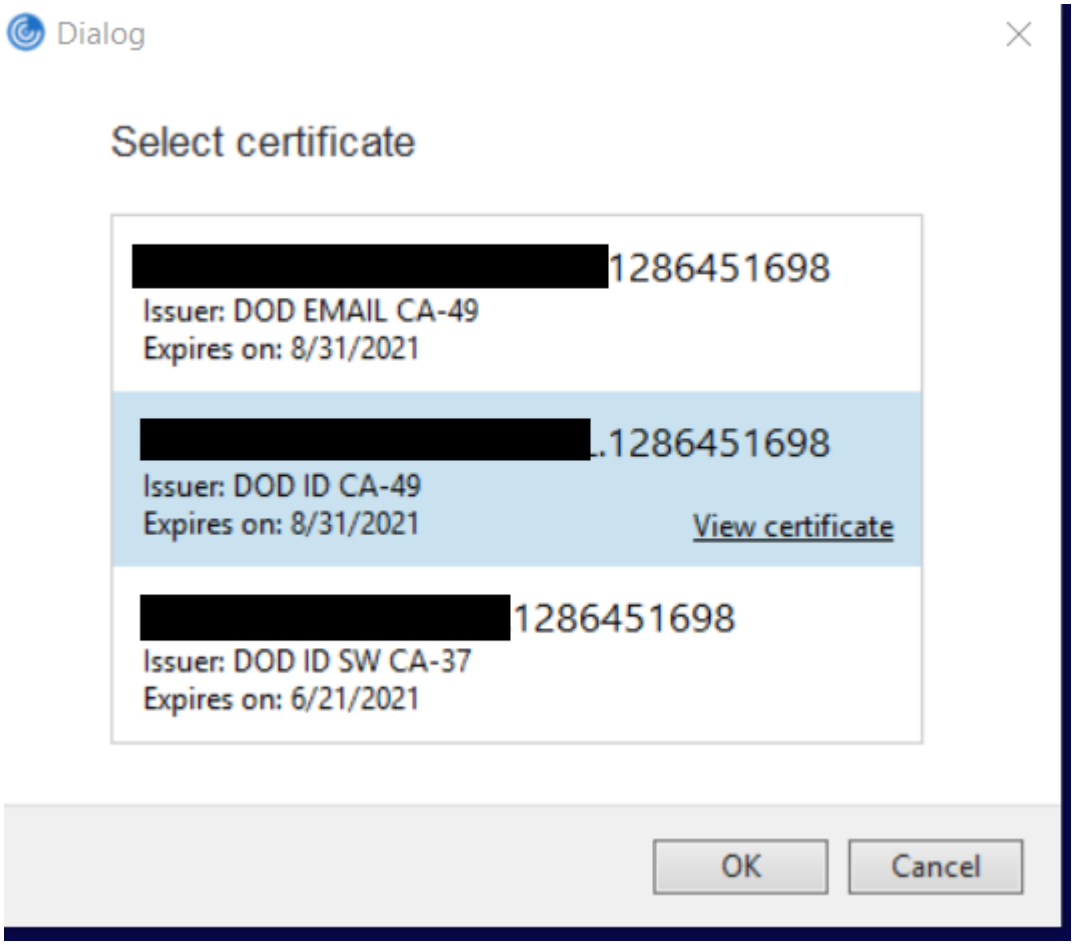


[image 1]

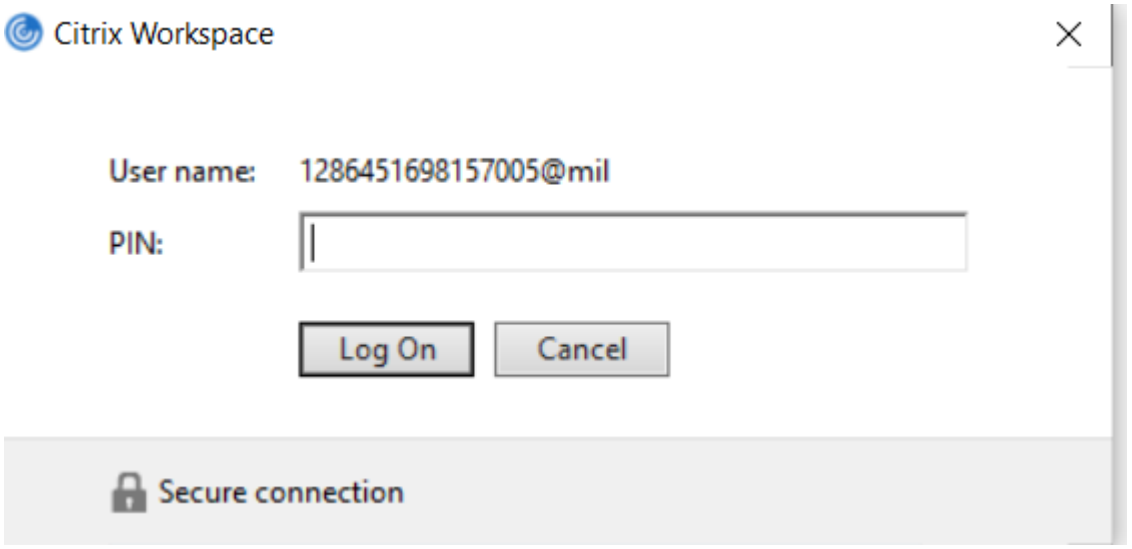


(image 2)

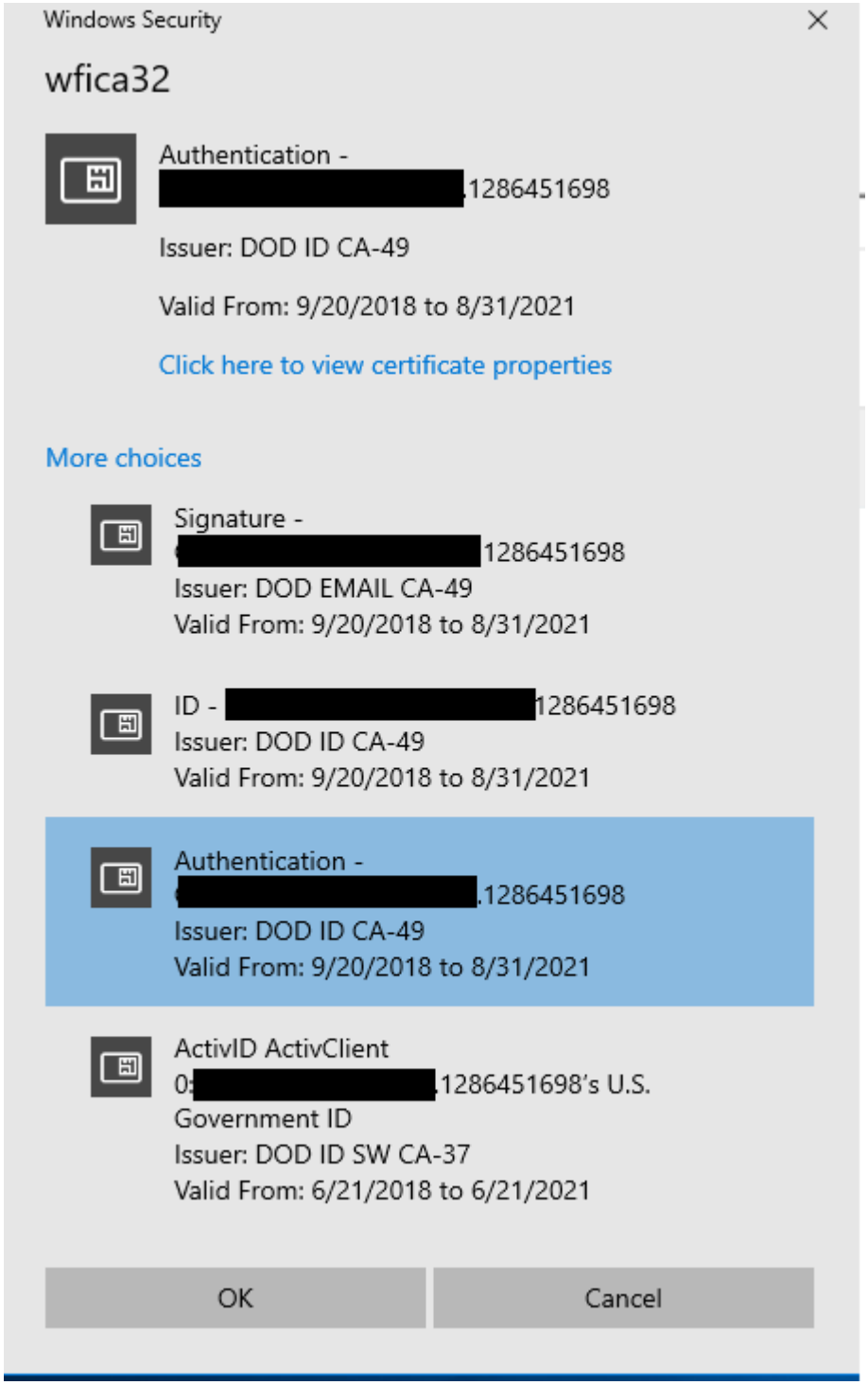
Changes to the Citrix log in. User will now select their DOD ID cert instead of the DOD Email cert



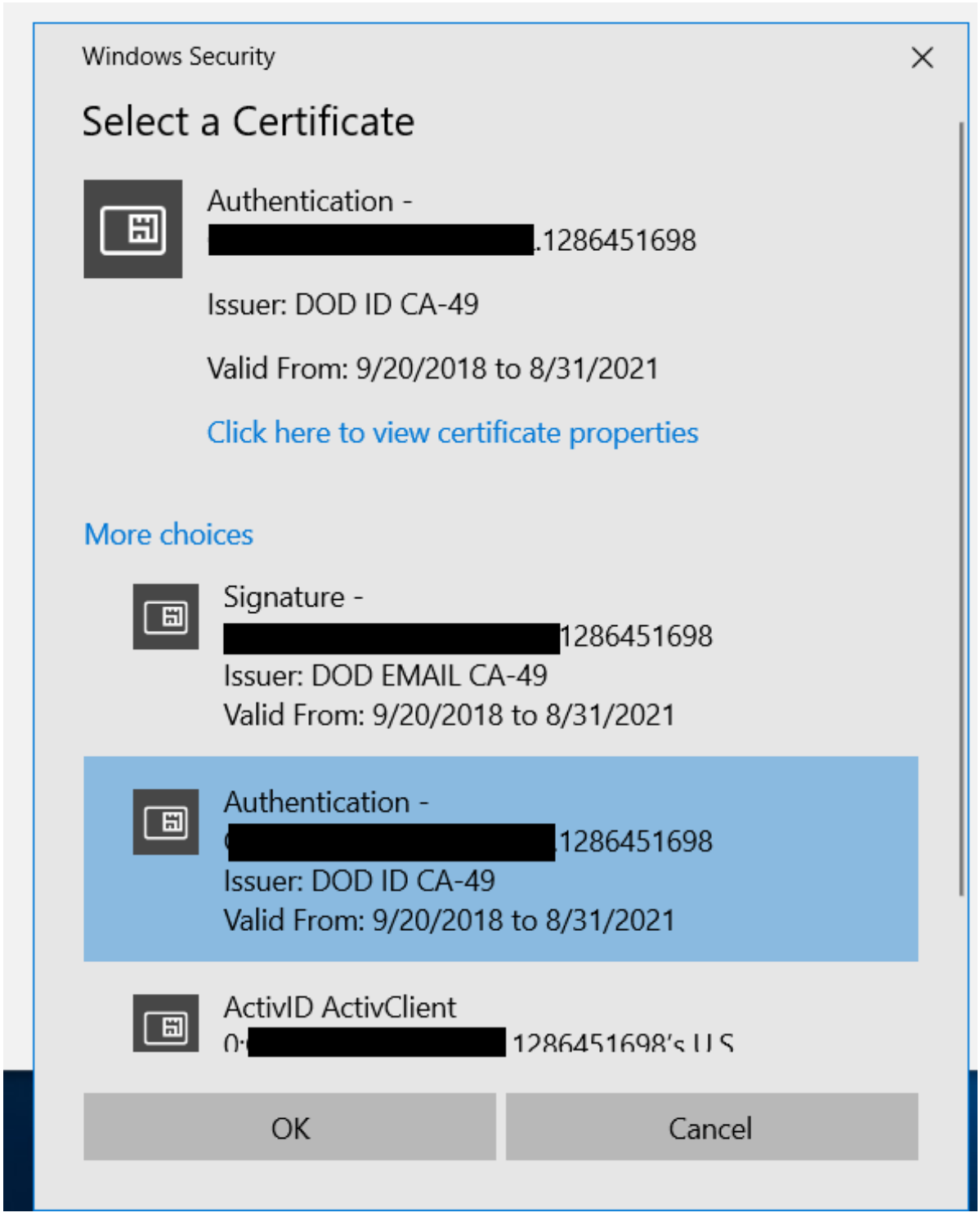
The user name will now have 16 digits instead of 10 digits



When prompted when loading the desktop select the Authentication cert (DOD ID)



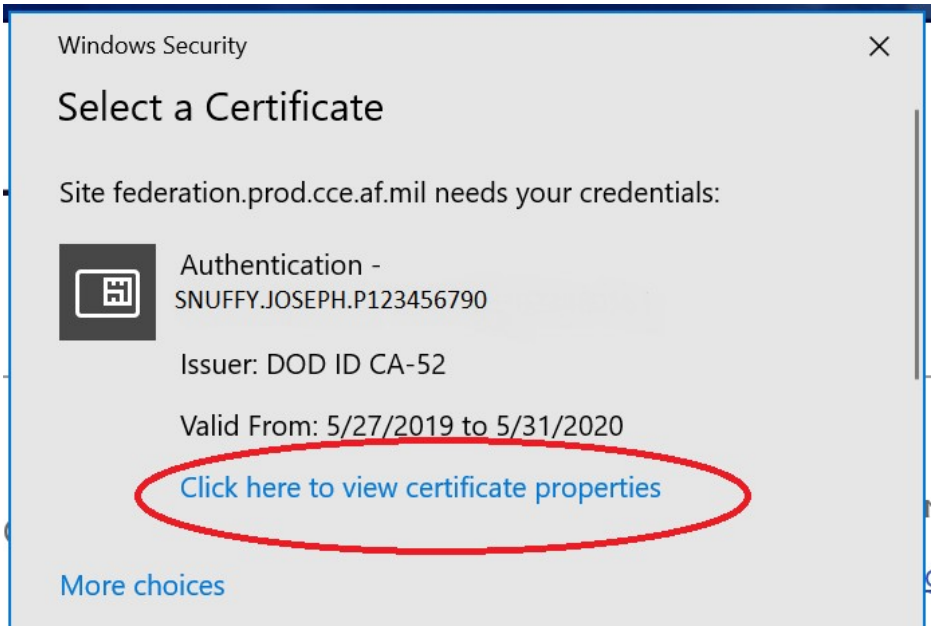
Changes to the Horizon DC3on log in. When prompted users will select their Authentication DOD ID cert

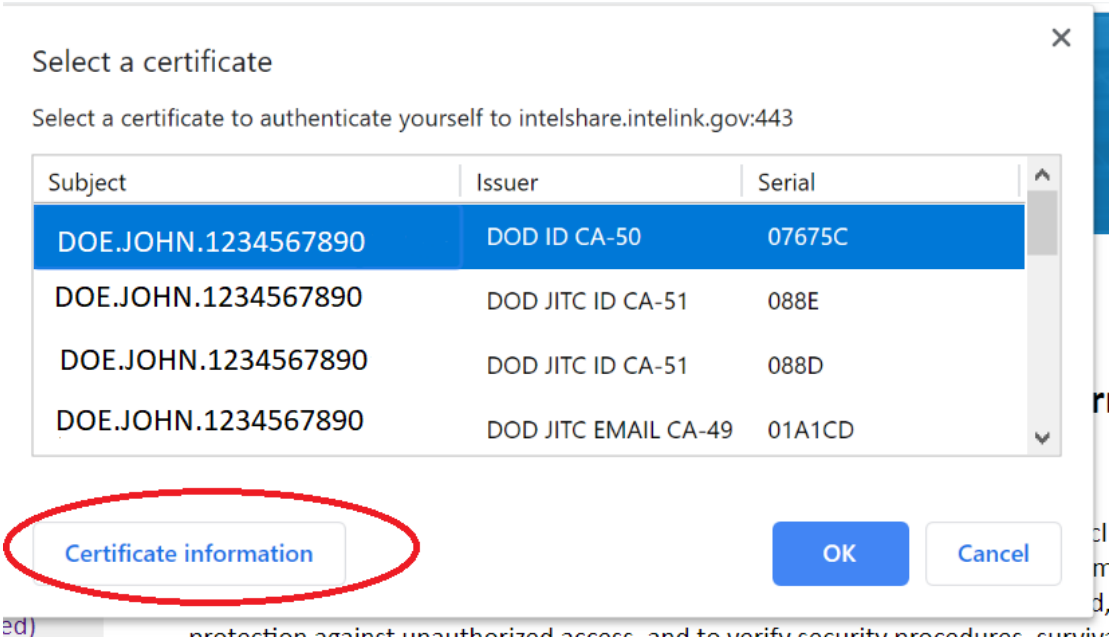


Identifying your PIV Auth Certificate

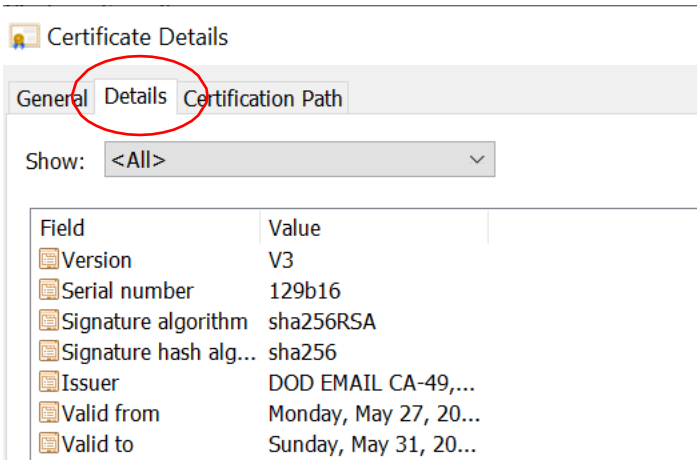
When logging into a system or application you are presented with multiple certificates to select; the PIV Auth certificate can be identified by following the steps below.

From the Windows Security “Select a Certificate” box presented select a certificate and then click on “Click here to view certificate properties”.





Next select the “Details” tab.



From the details menu scroll down to the “Subject Alternative Name” and double click. The Principal Name value identifies the certificate. If there are 10 digits this is NOT your PIV Auth certificate. If there are 16 digits in the Principal Name value, as in the picture below, this IS your PIV Auth certificate.