





SecurID Keyfob Checklist for External Dual Factor Readiness for Supplier access to HQMS Comport

External access to any Raytheon Proprietary, Competition Sensitive, Company Most Private or Export Controlled data requires dual-factor authentication. The preparation for dual-factor authentication requires multiple actions from the external users and the internal Raytheon points of contact (sponsors). External users who are not dual-factor ready will not be allowed access to the DMZ (Comport) until the dual-factor phases described below are completed. **This document lists all steps required for an external user to complete in order to use a SecurID keyfob for Dual Factor Authentication.** For users with digital certificate or Common Access Card (CAC), please refer to the *Digital Certificate or CAC Checklist* document.

It is the responsibility of the sponsor and the external user to ensure that all tasks listed below are completed (in order) before the external user will be allowed access.

Phase	Description/Task	Additional Help	Estimated Timeframe
I – Directory Services Security Questions and Answers	<p>External user must submit two (2) Security Questions and Answers to DirectoryServices@raytheon.com.</p>  <p>Security Questions & Answers.pdf</p> <p>*Once user receives confirmation email from Directory Services the user may proceed to Phase II</p>	<p>Las Colinas Help Desk: 1-877-844-4712</p>	<p>5 minutes</p> <p>*waiting period</p>
II – Set Directory Services Password	<p>External user calls the Las Colinas Help Desk: 1-877-844-4712 and asks to setup their Directory Services password.</p> <p><i>Note: Sponsor does not have to be on the call if Phase I is complete.</i></p>	<p>Las Colinas Help Desk: 1-877-844-4712</p>	<p>5 minutes</p>
III – Test Directory Services Password	<p>External User should test their SSO username and password here: https://webauth.raytheon.com/test/</p>	<p>Las Colinas Help Desk: 1-877-844-4712</p>	<p>5 minutes</p>
IV – Verify US Citizenship	<p>If the external user has a “us_person_flag” status of “Yes” or “user_type” is “Foreign Person”, skip to the next phase.</p> <p>If the external user has a “us_person_flag” status of “No” and “user_type” is “U.S. Person”, follow the attached instructions</p>  <p>GSS US Proof of Citizenship.pdf</p>	<p>Global Security Services (GSS)</p> <p>May Martinez (520) 794-3591 or Gloria Tipton (520) 545-8479</p>	<p>1 hour – several days</p>

<p>V – Process Raytheon SecurID keyfob Request</p>	<p>Sponsor will request a SecurID keyfob using the Non-Raytheon Person SecurID Request Form: http://securitydb.it.ray.com/nrpRAS</p> <p>Please note: The external user should fill out the attached form and return it to the Sponsor prior to the Sponsor requesting a SecurID keyfob:</p>  <p>External User SecurID form.doc</p> <p><i>Note: If the external user already has a Raytheon SecurID, then proceed to the next phase.</i></p>	<p>Prerequisites:</p> <ul style="list-style-type: none"> • Phase IV above completed • External User completes the ‘External User SecurID form’ • Need A08/E08 approver for the keyfob request (this is what the form refers to as “sponsor”) 	<p>5 - 10 minutes to process 1 – 2 weeks for SecurID to be received</p>
<p>VI - Complete ITAR Training</p>	<p>External user must complete a one (1) hour web-based ITAR training using the attached instructions.</p> <p>Please note: a SecurID keyfob is needed prior to completing this step.</p>  <p>ITAR Training.pdf</p> <p>*Once training is complete, user must wait one day (24 hours) for processing to complete</p>	<p>Las Colinas Help Desk: 1-877-844-4712</p>	<p>1 hour</p> <p>*24 hour waiting period from time of completion</p>


POINT OF CONTACT

Questions on the implementation of this process should be addressed to the Raytheon POC (Sponsor).



Digital Certificate Checklist for External Dual Factor Readiness for Supplier access to HQMS


External access to any Raytheon Proprietary, Competition Sensitive, and Company Most Private or Export Controlled data requires dual-factor authentication. The preparation for dual-factor authentication requires multiple actions from the external users and the internal Raytheon points of contact (sponsors). External users who are not dual-factor ready will not be allowed access to the DMZ (Comport) until the dual-factor phases described below are completed. **This document lists all steps required for an external user to complete in order to use a Digital Certificate or Common Access Card (CAC) for Dual Factor Authentication.** For users with SecurID, please refer to the *SecurID Keyfob Checklist* document.

It is the responsibility of the sponsor and the external user to ensure that all tasks listed below are completed (in order) before the external user will be allowed access.

Phase	Description/Task	Additional Help	Estimated Timeframe
I – Directory Services Security Questions and Answers.	<p>External user must submit two (2) Security Questions and Answers to DirectoryServices@raytheon.com.</p>  <p>Security Questions & Answers.pdf</p> <p>*Once user receives confirmation email from Directory Services the user may proceed to Phase II</p>	Las Colinas Help Desk: 1-877-844-4712	5 minutes *waiting period
II – Set Directory Services Password	<p>External user calls the Las Colinas Help Desk: 1-877-844-4712 and asks to setup their Directory Services password.</p> <p><i>Note: Sponsor does not have to be on the call if Phase I is complete.</i></p>	Las Colinas Help Desk: 1-877-844-4712	5 minutes
III – Test Directory Services Password	<p>External User should test their SSO username and password here: https://webauth.raytheon.com/test/</p>	Las Colinas Help Desk: 1-877-844-4712	5 minutes
IV – Verify US Citizenship	<p>If the external user has a “us_person_flag” status of “Yes” or “user_type” is “Foreign Person”, skip to the next phase.</p> <p>If the external user has a “us_person_flag” status of “No” and “user_type” is “U.S. Person”, follow the attached instructions</p>  <p>GSS US Proof of Citizenship.pdf</p>	<p>Global Security Services (GSS)</p> <p>May Martinez (520) 794-3591 or</p> <p>Gloria Tipton (520) 545-8479</p>	1 hour – several days

<p>V – Purchasing Digital Certificate</p>	<p>* If external user is a DoD personnel, proceed to next Phase to register their Common Access Card (CAC)</p> <p>In this phase, the External user will contact one of the three authorized Digital Certificate Authorities listed below to purchase a digital certificate:</p> <ul style="list-style-type: none"> • VeriSign: http://www.verisign.com/authentication/government-authentication/eca-certificates/ • ORC: http://www.eca.orc.com/ • IdenTrust: http://www.identrust.com/certificates/eca/buy_eca.html <p>When purchasing a digital certificate, make sure it is an ECA certificate with the following attributes:</p> <ul style="list-style-type: none"> • Certificate Type: <i>Identity</i> • Assurance Level: <i>Medium Assurance</i> (software-based, stored in the web browser) <p><i>Note: International users who need a dual-factor token should request a Raytheon-issued SecurID keyfob. External users from Australia, Canada, New Zealand, and United Kingdom can use the notarial services provided by U.S. consular offices and embassies for identity proofing purposes but users from any other foreign country (Norway, Germany, Sweden, etc.) cannot. For this reason, international users (especially those not in the four countries mentioned above) who need a dual-factor token, should request a Raytheon-issued SecurID keyfob from their Raytheon Sponsor (see 2a - SecurID Keyfob Checklist.doc).</i></p>	<p>VeriSign Support: https://knowledge.verisign.com/support/eca-support/index.html</p> <p>ORC Support: (1-800-816-5548) http://www.eca.orc.com/instructions.html</p> <p>IdenTrust Support: http://www.identrust.com/support/instructions.html</p>	<p>1 – 2 weeks</p>
---	--	--	--------------------

<p>VI – Configure and Test Digital Certificate</p>	<p>The external user should load their digital certificate into their browser and test it using instructions received from the vendor:</p> <ul style="list-style-type: none"> • VeriSign: https://knowledge.verisign.com/support/eca-support/index?page=content&id=S:SO9629&actp=search&searchid=1227652290329 • ORC: http://www.eca.orc.com/instructions_CertTestMSIE.html • IdenTrust: http://www.identrust.com/support/howto/ht_cert-test.html • Department of Defense (DoD): Go to https://services.onr.navy.mil If you are able to log in and see “Welcome (your name)” on the top-right hand side, then your digital certificate is working properly. <p>If the test is successful, proceed to the next step. If the test fails, please contact your digital certificate vendor to troubleshoot and resolve the error (see vendor support info in the next column).</p>	<p>VeriSign Support: https://knowledge.verisign.com/support/eca-support/index.html</p> <p>ORC Support: (1-800-816-5548) http://www.eca.orc.com/instructions.html</p> <p>IdenTrust Support: http://www.identrust.com/support/instructions.html</p> <p>DoD Support: Please contact your local DoD Help Desk / Computer Support</p>	
<p>VII – Register Digital Certificate with Raytheon</p>	<p>In this phase, the external user should follow the attached instructions to register their digital certificate with Raytheon:</p> <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">  dod_digital_certificate_registration.pdf DoD: </div> <div style="text-align: center;">  non-dod_digital_certificate_registration.pc Non-DoD: </div> </div> <p>* Once completed, user must wait one (1) hour before proceeding to next phase</p>		<p>5 minutes</p> <p>*1 hour waiting period</p>

VIII - Complete ITAR training	<p>External user must complete a one (1) hour web-based ITAR training using the attached instructions.</p> <p>Please note: digital certificate or CAC must be registered with Raytheon prior to completing this step.</p>  <p>ITAR Training.pdf</p> <p>*Once training is complete, user must wait one day (24 hours) for processing to complete</p>	Las Colinas Help Desk: 1-877-844-4712	<p>1 hour</p> <p>*24 hour waiting period from time of completion</p>
-------------------------------	---	---	--

POINT OF CONTACT

Questions on the implementation of this process should be addressed to the Raytheon POC (Sponsor).