Status Update for DTrade PKI/SHA-256 Digital Certificate Upgrade

Industry Notice: *DTrade PKI/SHA-256 Digital Certificates*

DDTC is upgrading the DTrade system to ensure compliance with the use of Access Certificates for Electronic Services (ACES) SHA-256 ("SHA-256") digital certificates by December 31, 2013, as required by federal mandate. As a result, all DTrade users must purchase and register a new SHA-256 certificate by the end of this calendar year for continued use of DTrade.

Whereas the federal mandate requires compliance by December 31, 2013, DDTC will begin allowing users to access DTrade using a SHA-256 certificate on **November 25, 2013.** This effort will allow DTrade users to use either their existing ACES SHA-1 ("SHA-1") certificate or new SHA-256 certificate.   However, after December 31, 2013, only SHA-256 digital certificates will be accepted for DTrade use.

Key Dates:

November 22, 2013 – DTrade will be taken offline at 5:00 pm in order to upgrade the system to accepted SHA-256 certificates. Specific information regarding this outage and transition will be emailed to industry super users (or appointed contacts) as well as posted on the DDTC website.

November 25 - December 31, 2013 – DTrade will accept both SHA-1 and SHA-256 certificates. During this time:

- Users can gain access to DTrade using either certificate type;
  Users must purchase a SHA-256 certificate from one of the authorized ACES certificate vendors (IdenTrust or ORC); and
- Users must register their SHA-256 certificate with DTrade based on established guidelines.

January 1, 2014 – Only users who have purchased and registered their SHA-256 certificates will have access to DTrade. SHA-1 certificates will no longer be accepted.

For further information visit the DTRADE Information Page. (09.24.2013)

Public Key Infrastructure/Secure Hash Algorithm (SHA)-256 Digital Certificate Transition Frequently Asked Questions (FAQ)

1. **Q: Why is DDTC upgrading DTrade?**
   A: The current digital **ce**rtificates used with DTrade are Access Certificates for Electronic Services (ACES) SHA-1 ("SHA-1") based certificates. The National Institute of Standards and Technology (NIST) issued a mandate which requires federal agencies to stop using SHA-1 certificates, effective January 1, 2014.

2. **Q: Why do I have to buy a new certificate?**
   A: In accordance with NIST guidelines, SHA-1 certificates are not authorized for use on government systems after December 31, 2013. Therefore, as of January 1, 2014, SHA-1 certificates will not be accepted for access to the DTrade system.

3. **Q: Who must purchase a new SHA-256 certificate?**
   A: All DTrade users (including those who sign, submit, and check the status of DSP forms (DSP 5, 6, 61, 62, 73, 74)) must purchase and register a SHA-256 certificate with DTrade by December 31, 2013.

4. **Q: What do I do once I purchase a SHA-256 certificate**?
   A: After November 25, 2013, log on to DTrade and register your certificate. For detailed instructions on registering your certificate, please review Getting Started with DTrade.

5. **Q: My current certificate expires December 31, 2013. What do I need to do?**
   A: Purchase a SHA-256 certificate and register it with DTrade between November 25, 2013 and December 31, 2013. For detailed instructions on registering your certificate, please review Getting Started with DTrade.

6. **Q: I already have a SHA-256 certificate. May I use it now?**
   A: No, the current DTrade system only accepts SHA-1 certificates. After November 25, 2013, you may register and use your SHA-256 certificate to access DTrade.

7. **Q: My current certificate expires before November 25, 2013. What must I do to retain access to DTrade?**
   A: If your current SHA-1 certificate expires before November 25, 2013, you will need to purchase a new SHA-1 certificate to retain access to DTrade. Contact your ACES certificate vendor (IdenTrust or ORC) for further guidance on purchasing a DTrade SHA-1 certificate. Please note, DTrade will not accept SHA-1 certificates after December 31, 2013. Users will be required to purchase and register a SHA-256 certificate to access DTrade after December 31, 2013.

8. **Q: My current SHA-1 certificate is valid beyond December 31, 2013. Will I be able to continue to use it with DTrade until its expiration?**
   A: No, SHA-1 certificates will not be accepted for DTrade use after December 31, 2013, regardless of the expiration date.

9. **Q: How long will it take to receive Super Users status once the request is sent to the DTrade Help Desk?**

A: Super User requests will be processed on a first-come-first serve basis. DDTC anticipates a high-volume of super user requests beginning November 25, 2013 and will have additional staff available for assistance. Super Users are encouraged to submit their requests well in advance of the December 31, 2013 deadline to avoid delays.

10. **Q: What changes can I expect with DTrade due to the certificate upgrades?**

A: DTrade functionality will not change; however, users will be required to purchase and register a SHA-256 digital certificate as well as download the new DSP forms and forms viewer (i.e., IBM Forms Viewer v8.0.1). The new versions of the DSP forms and forms viewer are only operational with the SHA-256 certificate; therefore, DTrade users must have a SHA-256 certificate installed on their workstation prior to downloading the new forms and forms viewer. The new DSP forms and forms viewer will be available via DDTC website on the DTrade Information Page closer to the November 25, 2013 deployment date.