QTSO MEMORANDUM

MEMO NUMBER: **2023-010**

TO: QIES State Coordinators

CC: CMS Central and Regional Office Contacts

FROM: QIES Technical Support Office

DATE: **MARCH 8, 2023**

SUBJECT: **ASE-Q DIGITAL CERTIFICATE UPDATE INFORMATION AND PROCESS**

OVERVIEW

ASPEN's mobile applications, ASE-Q and LTCSP share a common database to store survey information captured during the facility inspection process. This database is Sybase iAnywhere, which provides advanced data encryption based on digital certificate keys. The current digital certificate installed with ASPEN mobile applications is approaching its expiration date on April 4, 2023 and needs to be updated by that date.

The replacement of the certificate must be performed under a Windows user account with Administrator privilege, and therefore this update is not a candidate for deployment through the ASE-Q auto-update process as most end-users do not have such Administrator privilege. Instead, each agency should plan to deploy this update based on your standard procedures for software updates.

Updates may be completed across all affected systems at once, in the case where your agency utilizes automated deployment tools, or updates may be performed on a computer-by- computer basis according to the needs of your agency as long as **all ASE-Q computers in your agency are updated by April 4, 2023**.

WHAT THIS MEANS FOR YOUR AGENCY

CMS Regional Offices (ROs) and Central Office (CO)

For CMS RO and CO users, this update will be coordinated through Leidos and CMS-DQSAS staff, and no CMS RO/CO staff action is necessary.

State Agencies

For states, an ASPEN update patch file, AspenCertUpgrade.zip, is posted to the QTSO website at:
http://star.alpinetg.com/upgrade/ASE/AspenCertUpgrade.zip

When unzipped, this file will yield three separate files needed for the update: AspenCertUpgrade.exe, cert.cer, and identity.pem. There are several options for executing this update for your ASE-Q users, but in all approaches the user or deployment process performing the update must run under a Windows account with **Administrative privilege**.

DEPLOYMENT OPTIONS FOR SAS

Manual Deployment

After downloading and extracting the three update files to any folder on the computer to be upgraded:

1. Launch the AspenCertUpgrade.EXE update program using a Windows account with Administrator privilege.
2. The update will then be applied to the computer.
3. Restart the computer if prompted to do so.

The update process creates a log file, ASPENCertUpgrade.log, in the same folder where the update patch was run. The log file is provided for troubleshooting and is not otherwise needed. Refer to the Testing section below for more information on verifying the update process.

Automated Deployment

To assist in preparing and testing your automated deployment, the AspenCertUpgrade.EXE update program provides several optional switches for controlling the update process. These can be used if your agency deployed the ASE-Q application to other than its default location (C:\ASPEN\ASEQ) and/or if the Windows Service name for SQL Anywhere is not the default name, which is the same as the computer name. The switches also allow you to run the upgrade patch in quiet mode, and to automatically reboot the computer if desired upon completion of the update.

The application supports the following optional command line switches:

*/**h** help*

*/**q** quiet mode (does not display information to screen, but writes to log file)*

*/**certpath**=<path to cert.cer file to be replaced >*

*/**pempath**=<path to identity.pem file to be replaced>*

*/**servicename**=<specify the service name of the SQLAnywhere service>*

*/**r** Automatically reboots the computer*

*Example: AspenCertUpgrade.exe **/q /r /certpath**=c:\apps\common\aspen **/pempath**=c:\apps\ase\data **/serviceName**=aspen.sqldbname*

Custom Deployment

To update the two certificate files - Cert.cer and Identity.pem - directly through a custom process that does not use the AspenCertUpgrade.EXE program, complete the following steps through your deploy tool using an account with Administrator privilege:

1. Copy the new “cert.cer” file to
    i. “C:\Program Files\Common Files\Aspen” (for 32-bit machines)
    ii. “C:\Program Files (x86)\Common Files\Aspen” (for 64-bit machines)
2. Copy the new “identity.pem” file to “C:\ASPEN\ASEQ\data” (default location of ASEQ\data)
3. After both files have been replaced, you must either reboot the computer system, or directly restart the SQL Anywhere service through the Windows Task Manager.

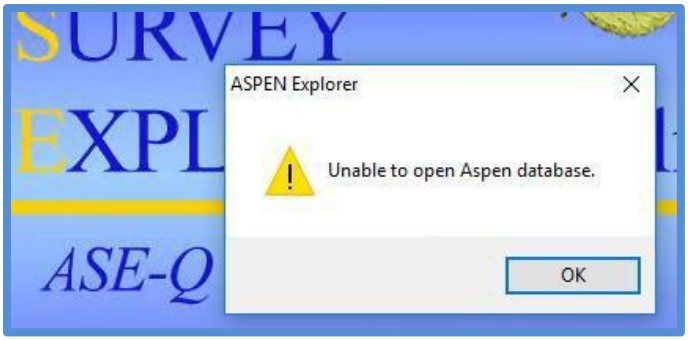
SPECIAL CONSIDERATIONS

For SAs where survey teams have the practice of synchronizing survey information through direct network transfer (cabled or wireless), the source and destination computers must have the same version of the digital certificate – either current or new – for successful survey transfer. Survey transfers via portable media (e.g., USB stick) or through direct connection between ASE-Q (Sybase) and ACO (Oracle) are not affected by the certificate version.

TESTING THE UPDATE

For SAs utilizing an automated approach, verifying your deploy procedures on a few computers before proceeding for general deployment is highly recommended.

You can verify that the update has been successfully deployed to a computer by changing the system clock on that computer to a date after April 4, 2023 and then starting ASE-Q after the update has been applied and the computer restarted. If the update was successful, ASE-Q will start and operate normally. If the update was not successful, you will receive the message below when starting ASE-Q.



ASSISTANCE AND QUESTIONS

If you have any questions concerning this information, please contact the QTSO Help Desk at help@qtso.com or call 1 (888) 477-7876.