Advanced Authentication for Mobile Devices

Background:

The concept of Advanced Authentication (AA) has caused some confusion amongst law enforcement agencies in North Carolina and their IT providers; specifically, at what level AA should be implemented (device or application). This notice is intended to provide clarification so AA can be implemented prior to the May 2013 audit by the FBI.

The North Carolina Department of Justice Information Technology Division (ITD) and the SBI have been in contact with the major mobile vendors in North Carolina in an effort to provide guidance to help facilitate this process. This notice may be provided to agency IT providers to help them understand the AA requirement.

In North Carolina, users access the Division of Criminal Information Network’s (DCIN) CJIS application by one of two methods. The first is through Omnixx. The SBI will be releasing an update to Omnixx later this year that will make it compliant with the FBI’s AA requirements. Local agencies need only install and start using the updated Omnixx application in order to meet the AA requirement. Regardless of the location where Omnixx is used, AA will be required.

The second method of accessing DCIN is through a CAD or mobile application. This application can either be purchased from a vendor or written by a local agency. Usually, CAD terminals are located inside a physically secured location (as defined by the CJIS Security Policy) within a law enforcement building where technical security controls have been met, and therefore AA is not required (as long as the physical and technical criteria are met). For mobile devices, one key to understanding how AA should be implemented is the concept of a physically secure location. (See section 5.9.1 of the CJIS Security Policy) Until Sept. 30, 2013 mobile devices inside a police car are considered to be in a physically secure location, but after that date AA rules will apply. (See section 5.6.2.2.1 CJIS Security Policy).

What This Means:

Since terminals running Omnixx will automatically be updated for AA requirements and most CAD terminals are located in physically secured locations, this notice will focus on mobile devices. Below are three scenarios provided by the FBI’s Information Security Officer (ISO) Office that help clarify when AA is and is not needed at the application level. All three scenarios start the same way: a mobile device located in a location not physically secured (as defined by the CJIS Security Policy) has logged into a network with an AA method.

1. Even though AA was used at the network login, the mobile application does not know the AA requirement has been met, therefore the user must log in to the mobile application using AA.
2. The mobile application knows AA has been successfully completed at the network level, so it does not have to use AA.

3. After a successful login to the network using AA, the user’s profile controls access to specific applications based on roles. For example, after login a menu is displayed based on the user’s profile. One of the menu choices is the mobile application. Here the mobile application does not have to use AA.

For more information on each scenario, please see the following pages.

Please note, merely logging on to a local computer or device using AA is not compliant with CJIS requirements.

Questions:

Questions regarding AA implementation should be directed to the North Carolina ISO, Mark Lang, at 919-773-7900.
Scenario 1 – Mobile device network connection (remote access – general)

1. A user initiates a connection to the local agency network from a remote location via an agency-issued mobile device.

2. The user authenticates by providing:
   i. Identification (username)
   ii. 1st authentication factor (password)
   iii. 2nd authentication factor (example: One-Time password from hardware token)

3. The local agency validates the received combination of identification, 1st authentication factor, and 2nd authentication factor.
   i. The requirement for AA has been satisfied.
   ii. The user is granted access to the local agency network.

4. The user (remotely connected to the local agency network) manually launches an application to access CJi. As there are no means established that will assert, or send, the positively authentication identity of the user to the application, the user is required to login to the application using AA.

5. The user authenticates by providing:
   i. Identification (username)
   ii. 1st authentication factor (password)
   iii. 2nd authentication factor (example: One-Time password from hardware token)

6. The application validates the received combination of identification, 1st authentication factor, and 2nd authentication factor.
   i. The requirement for AA has been satisfied.
   ii. The user is granted access to the application.

[Related sections of the CSPs: 5.6.2 Authentication Policy and Procedures, 5.6.2.1 Standard Authentication (Password), 5.6.2.2 Advanced Authentication, 5.6.2.2.1 Advanced Authentication Policy and Rationale]

Scenario 2 – Mobile device network connection (remote access - assertions)

1. A user initiates a connection to the local agency network from a remote location via an agency-issued mobile device.

2. The user authenticates by providing:
   i. Identification (username)
   ii. 1st authentication factor (password)
   iii. 2nd authentication factor (example: One-Time password from hardware token)
3. The local agency utilizes an authentication management server as an identity provider that will validate the received combination of identification, 1st authentication factor, and 2nd authentication factor as provided by the user and assert the individual’s identity to those services connected to this authentication management server to determine the user’s authorized access level.
   i. The requirement for AA has been satisfied.
   ii. The user is granted access to the local agency network.
   iii. The user is granted access to additional services and applications that the user is approved access to via the connection to this authentication management server following the validation and assertion of the user’s asserted credentials.

4. The user (remotely connected to the local agency network) launches an application to access CJI.

5. The authentication management server has properly asserted the user’s identity to the CJI-accessing application, so access is granted for a maximum of 12 hours when the assertion will expire.

[Related section of the CSP: 5.6.2 Authentication Policy and Procedures, 5.6.2.1 Standard Authentication (Password), 5.6.2.2 Advanced Authentication, 5.6.2.2.1 Advanced Authentication Policy and Rationale, 5.6.4 Assertions]

Scenario 3 – Mobile device network connection (remote access - role-based access control mechanisms)

1. A user initiates a connection to the local agency network from a remote location via an agency-issued mobile device.

2. The user authenticates by providing:
   i. Identification (username)
   ii. 1st authentication factor (password)
   iii. 2nd authentication factor (example: One-Time password from hardware token)

3. The local agency validates the received combination of identification, 1st authentication factor, and 2nd authentication factor.
   i. The requirement for AA has been satisfied.
   ii. The user is granted access to the local agency network.
   iii. The user is assigned a specific role or profile that allows access to applications based on that particular profile (i.e., role-based access control).
   iv. The user is granted access to pre-defined applications based on the user’s profile.

4. The user (remotely connected to the local agency network) launches an application to access CJI.

5. Access is granted because the system enforced a role-based access control based on the profile of the user.

[Related sections of the CSP: 5.6.2 Authentication Policy and Procedures, 5.6.2.1 Standard Authentication (Password), 5.6.2.2 Advanced Authentication, 5.6.2.2.1 Advanced Authentication Policy and Rationale, 5.5.2 Access Enforcement, 5.5.2.1 Least Privilege, 5.5.2.2 System Access Control, 5.5.2.3 Access Control Criteria, 5.5.2.4 Access Control Mechanisms]