Advanced Authentication

NC CJIN Governing Board

13 October, 2011

George A. White
FBI CJIS ISO

Brief Policy History

- Two year development
- Fully vetted by all state representation
- Criminal and civil
- Requirements and transition documents published
  - Transition dates applied
- Audit cycles incorporate transition

Authentication Changes

- Protect the Criminal Justice Information
- Identifying the user vs. the device
- Knowing where the user is located
  - Technical controls as well as physical and personnel controls
- Advanced authentication

Authentication

Authentication is the process of verifying a claimed identity, determining if the subject is really who he/she claims to be. It is based on at least one of the following three factors:

- something a person *has* (smart card, token, key, swipe card, badge)
- something a person *knows* (password, passphrase, PIN)
- something a person *is* (fingerprint, voice, retina/iris characteristics)

**Strong, or two-factor, authentication contains two out of these three methods.*

Advanced Authentication

A single form of authentication (standard authentication* = password) is not a very secure means of authentication. Therefore, many organizations have introduced into policy a second means, or form of, authenticating a person's identity.

**Standard Authentication (Password) requirements can be found in the CSP in Section 5.6.2.1*

For the purpose of the CJIS Security Policy (CSP), the process of requiring more than a single factor of authentication is most often referred to as Advanced Authentication, or AA.

Policy Definition

"Added security functionality, in addition to the typical user identification and authentication of login ID and password, such as: biometric systems, public key infrastructure (PKI), smart cards, software tokens, hardware tokens, or "Risk-based Authentication" that includes a software token element comprised of a number of factors."

When AA is Required

Advanced Authentication and the CJIS Security Policy

- The requirement to use AA is dependent upon the physical, personnel and technical security controls_associated with the user's location.

- Therefore:
  - AA shall not be required for users requesting access to CJI from within a physically secure location (defined *in Section 5.9*) and when the technical security controls have been met (defined in *Sections 5.5 and 5.10*)

  - AA is required when it can't be determined from where a user is originating, e.g. utilizing wireless or web

- The CSP offers a flow chart, or decision tree, to help agencies determine when AA is required. (*Figure 8 and Figure 9 of Section 5.6.2.2.2)*

Advanced Authentication

Means and Methods of Advanced Authentication

Some means of AA are:

- Biometric systems (fingerprint readers, retina scanners, etc.)
- User-based public key infrastructure (PKI)
- Smart cards
- Software tokens (tokens stored on electronic device, i.e. pin numbers or one-time-passwords)
- Hardware tokens (RSA tokens, etc)
- Paper (inert) tokens (a homemade One-Time Password-styled, e.g. “bingo cards”)
- A “Risk-based Authentication” which includes a software token element comprised of a number of factors, such as network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions

Challenges

- Mobile Environment
  - Type of device doesn’t matter
    - Tablet, Android, iPhone, iPad, etc.
  - It’s how the CJI is accessed or stored

- Technical
  - Assertions
    - From Device
    - Between Applications

- Resources
  - Cost
  - Knowledge

Advanced Authentication

Advanced Authentication Use within Your CJIS Community

- It is important to recognize that the FBI and CJIS does NOT certify/endorse any single vendor product regardless of what any vendor tells you. So, how will the CJIS ISO Program help you?

- The CJIS ISO Program will:

  - Provide an analysis of a proposed solution/product brought to us by an ISO request as it would be implemented within your network to the requirements of the CSP

  - Offer advice and suggestions based off a completed analysis of a proposed solution/product

  - Answer any questions or concerns to add clarity to the AA requirements of the CSP

Questions

Any Questions??