ARE YOU CJIS READY?

4 CONSIDERATIONS FOR CHOOSING THE RIGHT AUTHENTICATION SOLUTION

WHO NEEDS IT?

Who Needs to Implement Advanced Authentication in order to comply with CJIS?

All local, state, and federal agencies that access and handle Criminal Justice Information through its lifecycle - from creation through dissemination, whether at rest or in transit.

What is Advanced Authentication?

Advanced Authentication (also known as multi-factor authentication) ensures that a user is who they claim to be. The more factors used to determine a person's identity, the greater the trust of authenticity.

Multi-factor authentication can be achieved using a combination of the following factors:

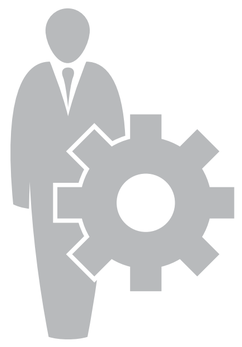
- Something You Know – password or PIN
- Something You Have – token or smart card (two-factor authentication)
- Something You Are – biometrics, such as a fingerprint (three-factor authentication)

1 CHOICE OF STRONG AUTHENTICATION

An authentication solution that offes a range of authentication methods and form factors allows agencies to address different levels of assurance with different authentication types and offers law enforcement officers a choice of form factors – depending on their user preferences.

2 EASY TO SETUP

Service-based solutions that do not require extensive infrastructure investments allow agencies to shorten time to deployment considerably.



3 MEETS BUDGET EXPECTATIONS

Several factors can lower implementation and running costs of an authentication solution:

- Automated provisioning, and workflows require lower management overhead which translates into lower administration costs.
- Self-service portals lower helpdesk costs by allowing users to manage most authentication administration tasks by themselves.
- Service-based authentication solutions eliminate infrastructure investments and ongoing maintenance costs, significantly lowering Total Cost of Operations and Ownership.
- Authentication solutions that offer a wide range of methods – including software tokens, phone tokens and context-based authentication – allow you to lower costs around token provisioning and life cycle management.

SAFENET AUTHENTICATION SOLUTIONS

SafeNet's Next Generation Authentication Solutions protect identities and ensure that individuals are who they claim to be. Delivered in the cloud, or on-premises, SafeNet's solutions support numerous use cases, and assurance levels.

Benefits

- Fully automated workflows reduce management and administration overheads
- Native identity federation lets you protect cloud based applications
- Widest token choice - Hardware, software, SMS, OOB and tokenless solutions maximize risk mitigation and use convenience

4 DESIGNED FOR GROWTH

Solutions that offer flexible pricing models and automated workflows allow you to easily add users as needed.

SEPTEMBER 2014 IS YOUR DEADLINE

TIME IS RUNNING OUT...

SafeNet® THE DATA PROTECTION COMPANY