gemalto
security to be free

SOLUTION BRIEF

How to become CJIS Compliant with SafeNet Authentication

Introduction

Cybercrime is recognized by the US federal government as being a major threat to economic and national security. Indeed, numerous cyber attacks carried out in recent years have been aimed at government and state bodies. At the frontline of crime prevention, law enforcement agencies are vulnerable to network vulnerabilities, threats, and events which could undermine their professional abilities.

In order to ensure that law enforcement agents operate in a secure environment, the Criminal Justice Information Services Security Policy (CJIS-SP) defines requirements of timely availability of shared information and data confidentiality. The CJIS-SP must be adhered to by any organization that exchanges criminal records, including 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.

CJIS Authentication Requirements

To become compliant with CJIS-SP, law enforcement agencies need to implement advanced authentication (section 5.6.2.2) for cases where the risk of unauthorized access is high.
In order to successfully pass the triennial compliance and security audits by the FBI CJIS Division, CJIS-SP provides a list of advanced authentication methods that agencies can implement. Below are some guidelines that provide insight into how to select the advanced authentication method that is most appropriate to your agency.

Choosing an Advanced Authentication Solution

Consider a solution that offers a choice of 2FA (two factor authentication methods)
An authentication solution that offers a range of authentication methods and form factors allows addressing different levels of assurance, and offers law enforcement officers a choice, depending on their user preferences and security needs.

Benefits

- **Fully automated -** Reducing the time and cost of provisioning, administration, and management of users and tokens.
- **Widest token choice -** Hardware, software, SMS, and tokenless solutions accommodate multiple use cases and risk levels.
- **Low TCO -** Reducing the total cost of operation compared to traditional strong authentication environments.
- **Scalability –** A comprehensive solution prepared for growth and evolving needs based on the rapid changes in the threat landscape.

Consider a solution that will allow you to meet CJIS schedules in a timely manner
Service-based solutions that do not require extensive infrastructure investments allow agencies to shorten time to deployment considerably. Moreover, service-based solutions offer scalability and flexibility from a budget and user management perspective.

Consider a solution that meets TCO expectations.
There are several factors that lower the overall implementation and running costs of an authentication solution:

- Automated management workflows: Authentication solutions that offer automated provisioning and automated workflows typically require lower management overhead, which translates into lower administration costs.
- **Self-service portals:** Offering comprehensive self-service functions to end users lowers help desk costs by allowing them to manage ongoing administrative tasks themselves.
- **Service-based delivery:** Service-based solutions eliminate infrastructure investments and maintenance costs, significantly lowering the total cost of operations and ownership.
- **Authentication choice:** Solutions that offer a wide range of authentication methods – including software tokens, phone tokens, and context-based authentication – allow organizations to lower costs around token provisioning and lifecycle management.

SafeNet Authentication Solutions for CJIS compliance

SafeNet Authentication Solutions enable law enforcement agencies to meet the CJIS Security Policy for advanced authentication with a fully automated strong authentication solution that can be delivered as a cloud-based service or installed in a local data center.

SafeNet Authentication Solutions address numerous use cases, assurance levels, and threat vectors with unified, centrally managed policies—managed from one authentication back end delivered in the cloud or on-premises.

SafeNet Authentication Solutions offer fully automated provisioning, and user and token administration, significantly reducing management overhead and investments compared to traditional authentication solutions. SafeNet Authentication Solutions support the broadest range of authentication methods and form factors – all of which meet the CJIS requirement for advanced authentication.

SafeNet Authentication Methods and Form Factors

Certificate-based authentication enables secure remote access and other advanced applications in a single USB or smart card authenticator.

One-Time Password (OTP) authenticators generate a dynamic OTP, ensuring that only properly authenticated users are authorized to access critical applications and data. Hardware-based solutions include smart cards that can be bundled with identification badges, badges that allow physical access to the workplace, and/or a variety of USB tokens.

Hardware-based authentication solutions are considered to be the most secure, and SafeNet provides several solutions with validation (such as FIPS 140-2) that they are adequately secure.

Software and phone-based solutions provide the same functionality as hardware solutions but run as a software application, usually on a mobile device (iOS, Android, Mobile Windows, and BlackBerry). The popular perception is that software-based authenticators are less secure than hardware solutions, but, in reality, it depends on the risks this solution tries to mitigate and the threats it faces.

Out-of-Band Push OTP
Single-tap push OTP on mobile devices lets users authenticate with a single tap of a finger on their mobile device.

Out-of-Band via SMS and email
SMS or email delivery of OTPs turns any mobile phone into an authentication token. There's no software to install or hardware to distribute, reducing the acquisition and operating costs of an advanced authentication solution.

Grid Authentication (GrIDsure)
Grid authentication (pattern matching) is based on an nXn grid filled with random numbers, where the user is authenticated by entering the current numbers that appear in a preregistered pattern.

About Gemalto's SafeNet Identity and Data Protection Solutions

Gemalto's portfolio of Identity and Data Protection solutions offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions–from the edge to the core. Gemalto's SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

Contact Us: For all office locations and contact information, please visit www.safenet-inc.com

Follow Us: data-protection.safenet-inc.com

GEMALTO.COM

gemalto
security to be free