Data Sheet

9 Things to Know About CJIS

Are you ready to meet the latest CJIS Security Policy requirements?

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

1. What is the CJIS Security Policy?

The Criminal Justice Information Services (CJIS) Security Policy outlines security precautions that law enforcement agencies need to take to safeguard sensitive information such as fingerprints and criminal backgrounds. The policy covers best practices in wireless networking, remote access, data encryption and multi-factor authentication (MFA).

2. What are the requirements?

To comply, law enforcement agencies at local, state and federal levels need to implement advanced authentication methods for cases where the risk of unauthorized access is high. All data must be protected and encrypted whether the data is at rest, in transit, or in use by October 2024.

3. How does MFA fit into the CJIS Security Policy requirements?

Recently, the Criminal Justice Information Service agency began revamping its access policies to align with President Joe Biden's Executive Order 14028 on Improving the Nation's Cybersecurity. This Executive order calls for more stringent security standards to be put in place for all federal agencies, such as implementing "advanced authentication" methods.

These advanced authentication methods mean taking a multi-layered approach to verifying the identity of users accessing a system or sensitive data. These methods must also be phishing-resistant, so hackers and attackers cannot gain access.

In the latest version of this security policy, CSP 5.9.2, multi-factor authentication (MFA) will be required every time a user seeks to access criminal justice information.

4. What methods are not accepted as MFA?

Thales aligns with NIST and the general consensus in the security industry – weaker authentication methods are discouraged or disallowed.

- Email
- SMS text messages
- Phone calls

5. What considerations should I take into account when deciding which approach to take?

Given that 90% of hacks start with compromised credentials, you may be in one of the many organizations looking for ways to deploy MFA across your entire SaaS estate.

In today's enterprise reality, users have diverse authentication needs. Some users will have inconsistent mobile coverage. Many will use multiple devices. All will need to securely access dozens of apps.

To maintain optimal security and ensure a convenient login experience, IT leaders should look for a solution that can:

- Meet users' expectations about being able to log into law enforcement portals and other apps, whatever the context, on any device, with an MFA experience that suits them
- Address the needs of IT teams who have to support and onboard thousands of users remotely and securely with minimal involvement
- Support multiple business units across the globe and offer a local language experience
- Deliver an audit trail of all access and authentication events and remain compliant

6. How can Thales help my organization meet the CJIS requirement?

With its wizard-based template for hundreds of enterprise apps, Thales SafeNet Trusted Access lets you enable a policy in a couple of minutes — we make it easy and fast to meet the CJIS Oct 2024 deadline.

SafeNet Trusted Access enables organizations to protect enterprise applications and scale securely in the cloud with a broad range of authentication capabilities, while ensuring security with Smart SSO and policy-driven access controls.

> "Enable a policy in a couple of minutes"

Thales SafeNet Trusted Access

Universal authentication methods

OTP Push

FIDO

Biometric

Hardware

Pattern Based

PKI

Passwordless

3rd Party

Google Authenticator

Password

Voice

eMail

SMS

- Deploy secure access quickly & efficiently
- Avoid vendor lock-in & keep control of your access security
- Prevent breaches and avoid financial liability and penalties
- Meet budget and business goals

a. In addition to expanding the MFA options, SafeNet Trusted Access simplifies implementation, management, and governance.

SafeNet Trusted Access provides Smart Single Sign-On (Smart SSO, also known as "Secure SSO") – the ability to seamlessly evaluate each access attempt and enforce the right authentication method for your user.

Smart SSO offers the optimal balance of convenience and security, and helps organizations achieve Zero Trust security by evaluating access security continuously and stepping up authentication measures when the access attempt does not match what you have configured as acceptable. Unlike regular SSO, Smart SSO eliminates the scenario in which a user's credentials can become a single point of failure.

b. Thales can support all of your users' diverse authentication needs and help you achieve "authentication everywhere" by offering the largest selection of authentication methods with different form factors and certifications to support a spectrum of users and work environments. Our focus is:

1. **Risk-appropriate authentication**
2. **End-to-end security**
3. **Low-friction and superior user experience**
4. **Minimum number of authentication methods/ user**
5. **Audit trail and certifications to meet compliance regulations**

7. How does Thales meet NIST security categorizations?

Thales offers authentication methods for every NIST Assurance Level, with software and hardware solutions including: OTP + PIN + Password, mobile push + biometrics, FIDO devices, and a pattern-based option. This means you can deploy multiple authentication methods to your users – or deploy different authentication methods to groups of users – and enforce the right method depending on their needs, security constraints and the login context.

8. Overview of Thales Authentication

Thales' SafeNet Trusted Access provides authentication and access management, including Smart SSO, other cloud services and on-prem apps. SafeNet Trusted Access simplifies implementation, management and governance, allowing you to meet the diverse authentication needs of your users and ensure optimal access security for all apps. Smart SSO improves security and user experience, increases productivity and decreases help desk costs.

Authentication

Offering the broadest range of authentication methods and form factors, SafeNet Trusted Access authentication solutions allow customers to address numerous use cases, assurance levels, and threat vectors with unified, centrally-managed policies — managed from one authentication backend delivered in the cloud or on-premises.

Supported authentication methods include context-based authentication combined with step-up capabilities, One-Time Password (OTP), FIDO, X.509 certificate-based solutions, and OOB. All authentication methods are available in numerous form factors, including mobile authenticator app and pattern-based software authenticators, and smart card, USB security key/token hardware authenticators.

Physical Access

Thales offers a range of FIDO devices and smart cards with dual physical and logical access capabilities, including contact cards with a wide choice of card body options and contactless technologies, and interface cards compatible with NFC. Use case examples include: Building access, printing, computer log in, email encryption, and document signing. This allows users to have a single authentication device for logging into CJIS and other cloud services, and accessing physical premises and devices.

Strong Authentication for Privileged Access

SafeNet Trusted Access supports policy-based access with the ability to apply and enforce different methods of authentication and session management rules depending on the role of the user and the sensitivity of the resource.

9. Why Thales?

Thales offers the only complete portfolio of Authentication and Access Management solutions, including Cloud Access Management, FIDO, PKI, Certificate-Based Authentication (CBA), One-Time Password (OTP) authentication, identity federation, complete lifecycle management and auditing tools.

Thales also has data protection and encryption solutions that work together with our Authentication and Access Management solutions to provide persistent protection and management of sensitive data.

Make sure you meet the latest CJIS Security Policy requirements with Thales.