IDENTIV SOLUTIONS BRIEF

Authentication Solutions for Criminal Justice Information Services

uTrust FIDO2 NFC Security Keys protect critical network infrastructure and keep law enforcement agencies and citizens safe with mandated MFA cybersecurity.

All U.S. federal and state law enforcement personnel need to follow the Criminal Justice Information Services (CJIS) mandate to access specific information. Identiv's logical access products, including contact/contactless smart card readers, tokens and FIDO2 security keys, can be used with MFA/PKI solutions as part of the authentication process to meet the CJIS requirement.

FBI's Criminal Justice Information Services (CJIS) Mandate

Law enforcement agencies need timely, secure access to systems that provide information from anywhere at any time to prevent and decrease cyber crime.

In response to these needs, the Federal Bureau of Investigation (FBI) introduced the Criminal Justice Information Services (CJIS) mandate that integrates presidential directives, federal laws, FBI directives, and the criminal justice community's decisions. Presented at both strategic and tactical levels, this policy is periodically updated to reflect the security requirements of evolving business models.

On a technical level, the CJIS mandate requires strong, two-factor authentication when accessing the criminal justice database. Strong security is essential irrespective of where access to the data occurs, whether on mobile devices or desktops at law enforcement agencies and headquarters.

Identification and Authentication Under the CJIS Mandate

The CJIS policy obligates law enforcement agencies to identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a criterion for allowing access to agency information systems or services.

Each individual's identity has to be authenticated at either the local agency, CSA, SIB, or Channeler level. The authentication strategy should be part of the agency's audit for policy compliance. The FBI CJIS Division also identifies and authenticates all individuals who establish direct web-based interactive sessions with FBI CJIS Services.

Standard Authenticators

Authenticators are part of the identification and authentication process. Examples of standard authenticators include:

- **Passwords**
- **Hard or soft tokens**
- **Biometrics**
- **One-time passwords (OTP)**
- **Personal identification numbers (PIN)**

For security reasons, users are not allowed to repeat the same password or PIN in the same login sequence.

Advanced Authentication

Advanced Authentication (AA) provides additional security to the typical user identification and authentication of login ID and password. It includes:Standard Authenticators Authenticators are part of the identification and authentication process. Examples of standard authenticators include:

- **Passwords**
- **Hard or soft tokens**
- **Biometrics**
- **One-time passwords (OTP)**
- **Personal identification numbers (PIN)**

For security reasons, users are not allowed to repeat the same password or PIN in the same login sequence.
Advanced Authentication
Advanced Authentication (AA) provides additional security to the typical user identification and authentication of login ID and password. It includes:

- **Biometric systems**
- **User-based digital certificates, such as public key infrastructure (PKI)**
- **Smart cards**
- **Software and hardware tokens**
- **FIDO U2F or FIDO2 security keys**
- **Paper (inert) tokens**

- **Out-of-band authenticators retrieved via a separate communication service channel. For example, an authenticator sent on demand via text message, phone call, etc.**

It also includes risk-based authentication with 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**
- **High-risk challenge/response questions**

As criminals and conspirators are effective at duping people into divulging their credentials (what they know), an effective way to increase security is to leverage what they have (such as a FIDO U2F or FIDO2 device) or who they are (such as a biometric reader).

AA allows a central place for all authentication policies to be managed. This approach is necessary because organizations are usually forced to administer and maintain multiple infrastructures. Not only are multiple authentication infrastructures complicated to manage, but they are also less secure. A single, two-factor or multi-factor authentication framework for all devices and methods is the most secure option.

What Is CJIS Compliance?

CJIS compliance is what keeps professionals in criminal justice and law enforcement (at local, state, and federal levels) in agreement about standards for data security and encryption.

CJIS databases contain all necessary information for detaining criminals, performing background checks, and tracking criminal activity. According to the FBI's Advanced Authentication Requirement, organizations are obligated to use multi-factor authentication (MFA) if employees are accessing criminal justice information systems. This is similar to using a debit or credit card that requires PIN input.

A recurrent strategy for MFA is to use software applications or physical devices that generate unique, one-time passwords with time limits. Multi-factor authentication is a key policy area that should be on every business' CJIS checklist along with data encryption.

MFA Use Cases for CJIS Compliance

Law Enforcement Officers:
Field police officers are always on the move in their squad cars. These field officers need immediate access to the criminal justice information systems in order to verify an individual's identity or a driver's record.

An MFA solution with support for multiple authentication methods helps police departments satisfy the CJIS requirement. Law enforcement officers are prompted for a second-factor authentication (2FA) when logging into their mobile data terminals (MDTs). The officer uses their smart card or a hardware token to fulfill the 2FA, allowing access to the CJI database.

Justice Department Officials:

Prosecutors from the office of the District Attorney often visit a correctional facility and need to access their email, which contains CJIS information. When the prosecutor uses a secure terminal to access their email, MFA software detects that the user is logging in from a new device and prompts for second-factor authentication.

Many MFA solutions also capture the device information and maintain a comprehensive audit trail. They can integrate with complementary CJI data sharing solutions to provide advanced authentication capabilities for secure access.

First Responders:

It is imperative to deploy fast, one-touch authentication for first responders such as police officers and firefighters, as time is of critical importance. First responders need secure, speedy access to machines, VPN, and CJIS systems like criminal databases, license plate databases, and more.

With an MFA solution, first responders get fast and easy access to protected systems and data via reliable hardware security that does not require a battery or network connectivity. It offers strong one-touch security and is much faster than typing in an OTP.

How Identiv Supports MFA Authentication for CJIS Compliance

As police and law enforcement agencies adopt new mobile technologies, the risk of unauthorized access to record databases that store sensitive citizen information, criminal history, fingerprint records, and motor vehicle information grows.

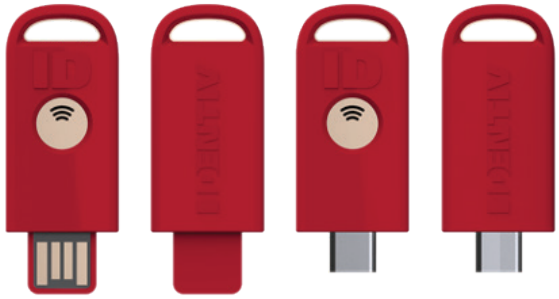
With officers on patrol and at desks, efficient, easy access to these records is critical. Tight budgets and IT resources need scalable solutions to support growing needs. In addition, the CJIS mandate and other security standards require the use of multi-factor and risk-based authentication methods.

Identiv's security solutions help federal, state, and local law enforcement agencies to:

- **Comply with CJIS mandate for two-factor or advanced multi-factor authentication from remote or unsecured locations**
- **Deploy the right authentication factor that meets the needs of each user with mobile access, tokens, or smart cards**
- **Balance security and convenience with a broad selection of authentication methods that allows for both strong information security and frictionless access**

uTrust FIDO2 Security Keys

FIDO2 is the umbrella term for FIDO Alliance's newest set of specifications. It enables users to capitalize on common devices to authenticate online services in both desktop and mobile environments. FIDO2 helps organizations achieve a seamless and passwordless login experience from all devices.



Identiv's uTrust FIDO2 Security Keys are strong near field communication (NFC) MFA devices, providing a simple, strong authentication experience that eliminates the need for passwords. With multi-protocol FIDO U2F, FIDO2, smart card (PIV), OpenPGP, and OTP support, these security keys are resistant to phishing attacks, safeguarding your credentials and accounts.

You can use uTrust FIDO2 Security Keys as credentials for:

- **Government employees or contractors (desktop and mobile)**
- **Citizen access to government services**
- **Public safety and first responders**
- **Emergency communications personnel**

Assembled in the U.S.A,, uTrust FIDO2 Security Keys support both contact (USB A/C) and contactless (NFC) use cases. They provide multi-protocol support for FIDO2,
FIDO U2F, PIV, TOTP, HOTP, and WebAuth enables strong multi-factor authentication and removes the necessity for

passwords. Plus, they are compatible with Windows, Linux, macOS, Android, and iOS.

Based on public-key cryptography, the cryptographic security model of the devices eliminates the risk of phishing, password theft, and replay attacks. The FIDO cryptographic keys are stored on-device and are unique for each website, meaning they cannot be used to track users across sites.

Benefits of uTrust FIDO2 Security Keys for CJIS Compliance

Hardware security keys are increasingly being recognized as the practical and responsible way to solve the CJIS compliance challenge. The best part about this approach is the one-touch authentication process.

For example, when users sign into their email or apps, they enter their password and click "sign in". However, the process does not end there. They are required to provide a second authentication factor to prove their identity and are then authorized to sign in to the account. Next, the user simply inserts their unique, personal key into their device, presses the button, and receives access instantly.

In the background, a challenge-response exercise is initiated using public-key cryptography between the security key and the service provider. This removes the risk of users' accounts being accessed via compromised credentials or a phishing attack.

Here are a few benefits of using Identiv's uTrust FIDO2 Security Keys:

- **Simple and secure as there are no server-side shared secrets to steal**
- **Protects against phishing, man-in-the-middle, and replay attacks**
- **FIDO certified**
- **Cost-effective and user-friendly solutions**
- **Lower development/maintenance costs and little-to-no provisioning costs**

- **Faster time to market and future-proof**
- **Multi-protocol and multiple connectivity support**
- **TAA compliant**

Closing Thoughts

The easiest, most effective option to comply with the CJIS mandate is to invest in hardware-based security keys supporting FIDO2 specifications. The FIDO2 protocols for passwordless authentication allow agencies to harness mobile technology for easier authentication in multiple channels.

Since FIDO2 credentials are cryptographically registered to a user's enrolled device, they cannot be easily shared by users, unlike passwords. Leveraging cryptographic login credentials coupled with biometric strong authentication, fraudulent individuals can be prevented from accessing CJIS data.

Identiv's uTrust FIDO2 NFC and NFC+ Security Keys protect the critical network infrastructure and keep law enforcement agencies and citizens safe with mandated MFA cybersecurity.

Visit identiv.com, request a demo, or call +1.888.809.8880 to learn more.