WHITE PAPER

CDW·G PEOPLE WHO GET IT™

TWO-FACTOR AUTHENTICATION

Combining multiple authentication mechanisms for a higher degree of security

Over the past decade, the demands on government agencies to share information across the federal, state and local levels have increased greatly. This information sharing creates new security requirements that transcend agencies and require them to certify confidence in the identity of the individuals accessing sensitive information.

To meet these new requirements, many agencies at all levels of government are turning to a strategy known as two-factor authentication. This approach supplements traditional user name and password authentication with alternative forms of verification based on a user's physical characteristics (such as a fingerprint or iris scan) or an object in the user's possession (such as a smart card or token).

By requiring an additional authentication factor, the agency gains an added degree of confidence that the users of its systems and information are who they claim to be.

Government agencies considering the implementation of two-factor authentication must understand this approach's requirements and should follow best practices to make it work. Authentication generally relies on three major factors: what you know, what you have and what you are. Systems integrating these factors provide a high-security environment suitable for the sharing of sensitive government information.

TWEET THIS!

Table of Contents

Authenticating Access to Criminal Justice Information Services

Government agencies often adopt advanced-authentication capabilities to accommodate their law enforcement responsibilities. In an effort to increase the security of sensitive law enforcement data, the FBI's Criminal Justice Information Services (CJIS) Division has established stringent requirements for all organizations connecting to its systems. In addition to these federal requirements, many states are now adopting the same requirements for access to state-level criminal-justice systems.

The CJIS security policy contains a detailed list of security requirements covering everything from personnel background checks to encryption key lengths. Among these requirements are several that directly affect authentication to systems handling CJIS information.

The first is that anyone authorized to store, process or transmit CJIS data must be authenticated by a user ID and a password that meets strength requirements that include:

- Having a minimum length of eight characters
- Not being a dictionary word or proper name
- Not being the same as the user ID
- Expiring within 90 days
- Not being identical to any of the user's previous 10 passwords
- Not being displayed when entered by the user

The password-complexity requirement applies to all situations that involve users accessing CJIS data electronically. Although these requirements apply only to CJIS systems, they can serve as best practices for all password-based authentication mechanisms.

When a user is accessing data from an agency-managed device within a secure facility, the CJIS security policy considers this a sufficient level of authentication. However, a second requirement applies to authentication requests that originate outside a secure facility or through a device not managed by the law enforcement agency. In these cases, the agency must also implement advanced authentication as defined by the CJIS policy:

"Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based public key infrastructure (PKI), smart cards, software tokens, hardware tokens, paper (inert) tokens, or

'Risk-based Authentication' that 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."

This policy allows for a wide variety of authentication mechanisms that accommodate the varying needs and capabilities of law enforcement agencies. In every case, the technique chosen must meet the basic requirements of two-factor authentication described in this white paper.

One important exception written into the CJIS policy covers police vehicles: Users accessing CJIS data from a police vehicle on a system that was not purchased or upgraded after Sept. 30, 2005, are exempt from advanced-authentication requirements until Sept. 30, 2013. Users of these systems will have to comply with the advanced-authentication requirements as of October 2013.

CJIS Remote-access Scenario

Here is a scenario of how a law enforcement officer can access CJIS data remotely:

An investigator with a county sheriff's department is travelling while conducting a criminal investigation. While on the road, the investigator develops a lead and wants to gather information on the source's criminal background. The officer wants to use a notebook PC to connect to a department system that contains CJIS data via a coffee shop's wireless network.

After ensuring that other patrons are unable to view the material on the computer screen, the investigator powers up the notebook and connects to the county law enforcement virtual private network (VPN). The officer is prompted to enter a user name and password.

After typing the issued user name, the officer pulls out a keychain, presses a button on a security key fob and reads a string of eight characters. The investigator's personal identification number (PIN) is added to that string and entered as the password. The computer successfully completes the VPN connection.

The investigator then opens a web browser and accesses the intranet page for the department's law enforcement information system. This presents a login screen where the user name and password are entered to gain access to CJIS data.

In this scenario, the investigator meets both the advanced authentication and encryption requirements of the CJIS security policy. A hardware token is used to access the departmental VPN and a standard user name and password to gain access to the website.

These two technologies combine to satisfy the advanced authentication requirement. Provided that the department is using a VPN that is certified as meeting FIPS 140-2, the officer's use of the departmental VPN meets the encryption requirements.

In addition to the advanced-authentication requirements, all connections to CJIS systems from nonsecure locations must be protected by encryption technology using a minimum key length of 128 bits.

CJIS policy further mandates that these systems be certified by the government as meeting the requirements outlined by the National Institute of Standards and Technology (NIST) in Federal Information Processing Standard (FIPS) Publication 140-2. This certification is issued on a version-by-version basis and must be updated when the cryptographic technology changes.

The easiest way for law enforcement agencies to meet the encryption requirement for traveling users is with a virtual private network (VPN), as described later in this white paper.

Securing Access with Multifactor Authentication

Controlling access to information systems requires two distinct activities: determining the identity of the end user (the identification phase) and proving that the end user is who he or she claims to be (the authentication phase).

In most cases, identification is very straightforward: Information systems simply ask the user to provide his or her identity in the form of a unique user name. Security is added to the process through the authentication phase, when the user is asked to provide proof of the claimed identity.

Authentication techniques rely on a variety of mechanisms to prove claims of identity, but all of these techniques may be grouped into three categories:

- **Something the user knows:** This authentication mechanism relies on secret information that only the user and the authentication system know. The most common implementation of this approach is the secret password. Other examples of knowledge-based authentication include PINs, pass phrases and the answers to challenge questions (for example, "What is your mother's maiden name?").
- **Something the user has:** In this approach, the authentication mechanism verifies that the user possesses something that proves identity. This often involves a token that requires the user to press a button to receive a code to be entered into the authentication system.

The system will use a mathematical algorithm to validate that the code came from the user's token, establishing possession. Other examples of devices that this authentication approach might use include smart cards and physical keys.

- **Something the user is:** Biometric authentication relies on a physical characteristic of the user to verify his or her identity. These mechanisms measure some unique trait, such as fingerprints, hand geometry, palm veins, facial patterns or iris/retinal patterns. The system compares the characteristics of the user seeking access with information stored in the authentication database to determine whether the identity claim is legitimate.

Each type of authentication mechanism has its advantages and drawbacks. Knowledge-based authentication mechanisms are inexpensive, easy to implement and familiar to end users. However, if an attacker is able to learn the password or other secret information used to verify a user's identity, there is no way for the system to determine the impostor from the legitimate user.

Password-security Best Practices

Users of password-based authentication mechanisms often complain that the difficulty of remembering complex passwords is compounded by password expiration requirements. Many government agencies address this concern by educating users about how to devise mnemonic phrases to generate and remember passwords that meet the requirements of strict security policies.

Employing password mnemonics not only addresses concerns about the difficulty of remembering passwords, but it also encourages users to create strong, difficult-to-guess passwords that enhance security.

Here are some examples of strong passwords and their corresponding mnemonics:

- Ne14+10s ("Anyone for some tennis?")
- Idw2g4c. ("I don't want to go for a checkup, period")
- Mfs/p50p ("My favorite store slashes prices 50 percent")

Device-based approaches eliminate the risk of an impostor and the legitimate user having access at the same time, because only one person can possess the token or smart card at a time. However, if the authentication device is lost or stolen, anyone in possession of it could impersonate the user until its absence is discovered.

Biometric systems are more difficult to attack, as they rely on a physical trait of the user for authentication. But these systems can be expensive, and some end users may feel the physical aspect involved invades their privacy.

To balance these advantages and disadvantages, agencies seeking a high level of security combine multiple authentication mechanisms to ensure a greater degree of certainty regarding an end user's identity. This approach is known as *multifactor authentication* because it combines techniques from two or more of the identity authentication categories.

More specifically, the combination of mechanisms from two categories is known as two-factor authentication and is considered the gold standard in authentication.

There are many ways to implement two-factor authentication, including some that are found in everyday life. A few examples of two-factor authentication scenarios include:

- Withdrawing money from an automated teller machine that requires both an ATM card (something you have) and the account PIN (something you know)
- Logging into a VPN that requires a user name and secret password (something you know), as well as a one-time password from a token (something you have)
- Gaining access to a secure government building that requires presentation of an identification card (something you have) and completion of a retinal scan (something you are)
- Using a telephone-based system that requires a user to speak a pass phrase; the system checks a database to determine that the phrase was correct (something you know) and that the user's voiceprint is a match (something you are)

The most important thing to remember about two-factor authentication is that the factors must come from different categories. A system that asks a user to provide a password and to answer security questions is not two-factor authentication: Both factors are the same — something you know.

Similarly, a building's access system that requires a fingerprint scan, voiceprint and retinal scan would certainly be high-security, but it would not qualify as two-factor authentication because each of these techniques uses biometric mechanisms.

Before Implementation: Plan and Test

Planning and testing are essential for agencies looking to implement a two-factor authentication system. They should conduct planning beforehand and testing once the system is in place to determine what challenges must be overcome before implementation.

It is important during the testing phase to involve the people who ultimately will use the system. However, testing should start with only a few users to keep the process manageable, rather than risk overload by bringing too many on at once.

Cost is also an important factor in choosing a system. Some solutions have low upfront costs, but high back-end costs after the first year or upon license renewal. Some two-factor solutions have five-year licenses, but incur significant renewal costs in the sixth year. An IT department should examine these details closely to avoid unwelcome budget surprises in the future.

Tokens and Smart Cards

The most common way for government agencies to move beyond passwords is by adopting an authentication system that verifies identity with the aid of a hardware device that users keep in their possession. Such devices satisfy the "something you have" requirement.

When used along with a password or PIN in the "something you know" category, the combined measures meet two-factor authentication requirements in an easy, cost-effective manner. These hardware devices can be broken down into two major categories: tokens and smart cards.

Tokens

Tokens are devices that participate in the authentication process by sharing secret information with the system. When attempting to verify his or her identity, the user interacts with the token in some manner (it varies depending on the type of token) to prove possession of the device to the authentication system.

Tokens can be categorized by the three major techniques used to authenticate possession:

- **One-time password tokens:** These generate a password that the user types into the authentication system. To generate the password, both the token and the system use a cryptographic algorithm based on either the current time (in which case the clocks of the token and the system must be synchronized) or the sequence of authentication requests using a counter.

The user typically presses a button on the token to generate the one-time password and enters it into the authentication system. That system then uses the same algorithm to generate the one-time password and compares it to the value received. If they match, the user is determined to possess the token and identity is authenticated.

- **Challenge-response tokens:** The authentication system provides input, called a nonce, to the user, who must enter it into the token. The token then uses a cryptographic algorithm that only it and the authentication system know to generate a response. This response is sent back to the system, which compares it to the known algorithm output to authenticate the user's identity.
- **Out-of-band tokens:** These systems rely on a known secure communication channel, such as a mobile phone, to validate a user's identity. When the user logs on to a system, the authentication system sends a text message to the user's registered mobile phone containing a one-time password that must then be entered to prove possession of the phone.

Such systems have the advantage of typically not requiring additional hardware, because users normally already have mobile phones.

Systems using one of these techniques provide very strong security when used in combination with either knowledge-based or biometric authentication factors.

Pseudo-random Number Generators

One of the biggest challenges regarding one-time password systems is generating the password in the first place. The root of this difficulty concerns creating as random a number as possible using a computer or some external source.

There is simply no way for a computer to generate a truly random number. Instead, cryptographers must rely on technology that generates numbers using an algorithm that approximates true randomness, known as a pseudo-random number generator (PRNG).

PRNGs begin with a seed value, provided by the user or an external source, such as the time. This seed value is then manipulated mathematically to generate a stream of numbers with random properties. To be considered cryptographically secure, the PRNG must be constructed in such a way that an attacker who has knowledge of the seed value cannot use it to derive the output stream of random numbers.

If a one-time password algorithm uses a PRNG that is not cryptographically secure, an attacker could monitor the stream of one-time passwords (for example, by generating several with a system token), and then use those to determine the values of future passwords that might be assigned to other users. The attacker who manages to crack the algorithm could use that knowledge to compromise the authentication system.

For this reason, one-time password systems should always rely on a cryptographically secure PRNG that is generally accepted by the security community. These include the PRNGs provided by Microsoft in its Cryptographic Application Programming Interface (CAPI) and the /dev/random devices in Mac OS X and FreeBSD.

Smart Cards

Smart cards fall into a special category of challenge-response tokens. They typically take the form of an organization's traditional identification card but contain an embedded integrated circuit that makes them "smart." This integrated circuit is responsible for participating in the challenge-response process when the card is inserted into a compatible reader.

Smart cards are among the most popular two-factor authentication systems for a number of reasons:

- They typically are the size of a credit card, easily fit in a user's wallet and, therefore, are carried consistently.
- Most organizations already issue staff identification cards and can simply modify the process for issuing them for those who need smart cards.
- They are easy to use: A worker needs only to insert the card in the reader, and the challenge-response process takes place automatically.

Smart cards used in federal agencies or to support federal processes should be manufactured and configured to comply with the NIST standards found in FIPS Publication 201 regarding personal identity verification for federal employees and contractors.

Common Access Cards in the Defense Department

Government agencies are the most prolific users of smart-card technology, with the Department of Defense (DoD) leading the way. The DoD adopted the technology as a replacement for the identification cards previously issued to all users, such as active-duty military personnel, civilian employees, military contractors and members of the Reserves and National Guard.

As of 2008, the DoD had issued more than 17 million of these smart cards, known as Common Access Cards (CACs), and had adopted them as a requirement for accessing many military systems.

To authenticate his or her identity, the user inserts the card into the reader on a CAC-equipped workstation. The user is then prompted to provide the PIN corresponding to the card, completing the two-factor authentication process.

Biometric Measurement Devices

Biometric systems rely on measuring a unique physical characteristic of a user and then comparing subsequent authentication attempts by that user to the stored biometric patterns. Biometric systems can measure a wide range of human characteristics, from fingerprints to facial features to iris patterns in the eye.

Biometric Authentication Options

Authentication via fingerprints is both the oldest and the most common biometric technique in use today. This approach relies on the fact that the ridge patterns on the human fingertip are known to be unique to each individual.

Fingerprint readers may use optical, electrical, thermal or tactile scanning to detect the patterns on the finger of a user.

The system then compares this image to the authentication database to determine whether it is the fingerprint of a known, authorized user and makes an acceptance/rejection decision based on the closeness of the match.

Vein structure is another unique biometric characteristic that authentication systems measure. Readers use infrared scanning to detect the pattern of veins in a user's finger, palm or the back of the hand. These patterns are unique to an individual and are compared to the authentication database entry to determine whether a user should be granted access.

Facial recognition can be used for both biometric authentication and the identification of unknown subjects. These systems capture two- or three-dimensional images of a user's face and compare them to stored images in a database.

The major advantage of facial-recognition systems is that images can often be captured from a distance and without requiring any special behavior on the user's part. These systems also have been used by law enforcement organizations at large athletic events to identify criminal suspects in the crowd. Such uses have raised significant privacy concerns over the surreptitious use of facial-recognition technology on unwitting subjects.

Optical scanners measure unique patterns in the eyes of authentication subjects. Older scanners measured the vein patterns in the retina by shining a bright light directly into the eye. Those systems are rarely used today because people found them both uncomfortable and unnecessarily invasive.

Retinal scanners have given way to scanners that capture images of the iris without the use of bright lights. Iris scanners can read patterns from a distance, though, presenting many of the same privacy concerns found with facial-recognition systems.

User Acceptance of Biometric Authentication

Acceptability to the system's end users is one of the most important factors to consider when evaluating biometric options. People being scanned often have concerns about the intrusiveness of the systems and may be hesitant to submit to biometric authentication for fear that the stored data may be used for other purposes.

Some also may be unnerved by the prospect of a computer measuring personal characteristics. Others also may have an aversion to fingerprint scanners because of the common linkage between fingerprinting and criminal investigations.

In environments with low acceptance of biometric authentication, security professionals should consider using methods with a lower perceived invasiveness. Most often, these are devices that use characteristics easily visible to the human eye, so system users do not feel that the system is measuring a "private" characteristic. For example, facial-recognition systems may be more readily accepted in many environments than retinal scanners.

Despite these concerns, however, biometric authentication is gaining more popular acceptance as security concerns continue to evolve. For example, Walt Disney World recently began fingerprint authentication at turnstiles for holders of season passes to prevent unauthorized sharing of passes.

Deploying Biometric Authentication

Once an agency has made the decision to use biometric authentication, it should carefully select a system that meets its security requirements and will be widely accepted by users. The IT department should consider holding a series of informational meetings to explain why biometric authentication is being instituted, provide instruction on the use of the system and outline the privacy safeguards that will protect the data collected from staff.

Before deploying the system, the agency should have an enrollment period to register users. During this period, the IT department should ask each user to visit the enrollment station with photographic proof of identity. Upon verifying the user's identity, an enrollment technician should capture the biometric data necessary to identify the end user and then take several test readings to ensure that the user will be properly authenticated when the system is fully deployed.

When biometrics are used to control access to a facility, technicians should be stationed at the entrance to assist users who have difficulty with the system or experience false rejections. When biometrics are used to control access to computer systems, the organization should have staff on call or circulating throughout the building to assist users, especially during the early morning hours when users are first attempting to log on.

Evaluating Biometric Systems

Evaluating the effectiveness of biometric authentication systems can be tricky for two reasons: They may use very different authentication techniques; and it is possible to manipulate many of their performance characteristics. For example, an unscrupulous sales representative could promise a biometric system that will never admit the wrong person and accomplish that by turning up the system's sensitivity so high that it rejects everyone.

There are several performance characteristics used when discussing biometric systems:

- **False acceptance rate (FAR):** This is the probability that the system will mistake an impostor for a legitimate user and provide unauthorized access.
- **False rejection rate (FRR):** This is the probability that the system will mistake a legitimate user for an impostor and prevent legitimate access.

- **Crossover error rate (CER):** This is the point at which the level of false acceptances and false rejections are equal. That point can be achieved by adjusting the sensitivity of the biometric system.

A system's FAR and FRR may be easily manipulated by adjusting its sensitivity. Turning the sensitivity higher increases the FRR and reduces the FAR, while turning the sensitivity lower increases the FAR and reduces the FRR. It is not possible, however, to alter the CER of a system. For this reason, CER is the best measure to compare when evaluating different biometric-authentication solutions.

Virtual Private Networks

Users increasingly require access to agency networks from remote locations. Whether they are travelling for work, checking e-mail while on vacation or simply teleworking, productivity increases when agents and staff are able to access agency systems from home or the road.

VPNs use encryption technology to provide secure connections from remote networks to the agency network. The encryption provided by a VPN protects private information from eavesdroppers who may be monitoring the public networks being used by an agency's workers and provides those users with a secure way to interact with that data outside the traditional boundaries of the network.

VPN Client Access Methods

The first decision to be made when deploying a virtual private network is what technology the end users will employ to access the VPN. An organization has two main choices here: a client-based VPN or a Secure Sockets Layer (SSL) VPN.

Client-based VPNs require end users to either install software on their systems or configure their operating system's built-in VPN client to access the agency VPN. When the user wishes to access the agency network, he or she opens the VPN client software and connects remotely.

This approach uses technologies such as the IP security (IPsec) tunneling protocol to establish a secure tunnel between the end user's computer and the agency's VPN endpoint. All VPN traffic is encrypted at one end of the tunnel and decrypted at the other end. Anyone intercepting the tunnel traffic is unable to read it without access to the secret VPN encryption key.

The client-based approach is effective, but it requires advance configuration and administrative access to the system. This limits the ability of users to connect from personal computers.

SSL-based VPNs use the built-in SSL encryption technology of a user's web browser to establish a secure connection to the agency's network. To access an SSL VPN, the user simply opens a browser and navigates to the agency VPN web page. The web page may then install a small piece of software (such as a Java applet) on the end user's computer to facilitate the connection.

Traffic between the user's computer and the agency network then travels through the web browser's SSL connection. This approach has the advantage of being very simple for the end user, who needs only to remember the URL of the VPN web page.

Securing VPN Endpoints

One of the biggest security concerns surrounding the deployment of VPNs is the security of endpoint computers that will connect to the agency network. The IT department should carefully plan policy and technical controls to ensure that the systems connecting to the agency network remotely will not subject the rest of the computing environment to unnecessary risk. Here are a few best practices to protect the agency network:

- **Deter access for personal devices:** Agencies should consider a policy that prohibits connecting personally owned computing devices to the VPN. Agencies that choose this option should inform users that the VPN is open only to agency-owned systems and that workers needing access from home or while traveling should carry an agency-owned computer with them.
- **Provide security support:** Agencies that choose to allow the use of personally owned devices to connect to the VPN should consider providing staff with free or low-cost access to security software for their personal computers. Makers of antivirus software often provide a "home use" contract option that, for a nominal fee, extends the agency's enterprise antivirus license to cover home use.
- **Utilize network access control:** Agencies should employ NAC software, which allows testing of the security posture of a remote computer device before granting it access to the agency network. NAC tools may be used in conjunction with a VPN to validate that the device is fully patched, has current antivirus software and meets the agency's firewall standards.
- **Quarantine remote access:** Agencies may also wish to place computer systems connecting via VPN into a quarantine network that limits their access. This approach may be used to allow remote users access to many resources while isolating them from the agency's most sensitive systems and data.

Combining these best practices with a common-sense approach to security can provide a safe and secure computing environment for agency workers and contractors who need to work from remote locations.

Deploying VPNs in the Enterprise

Administrators seeking to deploy a VPN must choose a back-end system to support VPN connections. This system will be responsible for listening for incoming VPN connection requests, authenticating users (with either single-factor or multifactor authentication) and creating the secure tunnel between remote endpoints and the agency network.

Agencies with low demand for VPN use may choose to deploy a software-based VPN that simply requires a domain server with VPN software that will perform the encryption and gateway functions required to establish connectivity. The major disadvantage of this approach is that encryption is computationally intensive, and servers are not optimized for performing the millions of calculations per second required to maintain a VPN connection.

An agency that expects a large number of VPN users will likely find it more efficient to use a dedicated VPN concentrator. These appliances contain specialized hardware dedicated to performing the encryption and decryption operations required by a VPN.

They are able to handle a large number of simultaneous users. And they scale in a much more cost-effective manner than trying to build servers to handle similar numbers of concurrent VPN users. Most agencies with more than a few hundred staff typically find that a hardware VPN is the optimal solution for their environments.

TWEET THIS!

The information is provided for informational purposes. It is believed to be accurate but could contain errors. CDW does not intend to make any warranties, express or implied, about the products, services, or information that is discussed. CDW®, CDW·G® and The Right Technology. Right Away® are registered trademarks of CDW LLC. PEOPLE WHO GET IT™ is a trademark of CDW LLC.
All other trademarks and registered trademarks are the sole property of their respective owners.
Together we strive for perfection. ISO 9001:2000 certified