MOBILITY AND CJIS SECURITY

Meeting Requirements for Advanced Authentication and Encryption

Matching Needs with Solutions

Criminal Justice Information Services (CJIS) security policy mandates minimum security procedures for all law enforcement agencies using wireless technology to connect to the federal system. The NetMotion Mobility® mobile VPN is widely used in law enforcement, and can be used to comply with CJIS requirements for mobile device access.

CJIS security policy version 5.2 section 5.6 calls for the use of advanced authentication methods – authentication based on additional factors beyond simple user name/password authentication. All newly procured or upgraded systems that connect to CJIS via wireless networks, the Internet or dial-up must meet the standards. Existing systems must comply by 2013, although CJIS recommends agencies not delay putting measures in place to meet the requirements as soon as possible. Public safety agencies that use Mobility have the flexibility to implement any of the advanced authentication methods.

Mobility can be used to comply with CJIS requirements for mobile device access.

Low-cost, Standards-based Approach

To assist with complying with the CJIS advanced authentication directive, NetMotion Wireless has created the Advanced Authentication Alliance - certifying interoperability between Mobility and many leading authentication solutions. For more information on the advanced authentication alliance, see http://www.netmotionwireless.com/authentication.aspx,

NetMotion has adopted a low-cost approach for implementing a fully compliant, secure system so that agencies may comply without significant new budget outlays, and it is based on widely available, industry standards.

Advanced Authentication Methods Supported

Mobility versions 8.5 and above support the following methods, which are specifically listed in the CJIS security policy version 5.1.

Smart cards

NetMotion Mobility supports advanced authentication using smart cards, including smart cards that comply with the requirements specified in Homeland Security Presidential Directive 12 (HSPD-12). Smart cards conforming to Federal Information Processing Standards Publication 201 (FIPS 201), Personal Identity Verification (PIV) of Federal Employees and Contractors and NIST Special Publication 800-78-1, Cryptographic Algorithms and Key Sizes for Personal Identity Verification are all supported. PKI Smart cards from vendors that meet Microsoft's smart card mini-driver requirements and from vendors that provide a Microsoft Cryptographic Service Provider (CSP) are compatible and supported for use with Mobility.

Public Key Infrastructure (PKI)

Mobility supports strong user authentication with X.509v3 user certificates stored on the mobile device, in a protected location only accessible to users who successfully complete desktop authentication and who provide the password to access the user certificate.

Biometric Systems

Vendors providing solutions with biometric access to PKI smart cards and/or user certificates are supported by Mobility where the biometric function is used in place of a PIN or password to unlock access to the X.509v3 certificates.

In addition, Mobility supports biometric-based user authentication on the Ubtek and Wave biometric systems, which are commonly installed on Lenovo, Itronix, and Dell portable computers.

Microsoft IPSec

Mobility fully supports the use of PKI X.509v3 certificates and shared secrets on both the Mobility client and server using Microsoft's IPSec transport. Each packet is authenticated using IPSec AH headers, or a defense-in-depth strategy by using ESP encryption and integrity checking. This method is currently supported on all versions of Mobility.

COMPLIANCE WITH FIPS 140-2 ENCRYPTION REQUIREMENTS

In addition to strong authentication, CJIS security policy mandates the use of FIPS 140-2 validated encryption.

Section 5.10.1.2 Encryption explicitly defines acceptable encryption standards:

- **Paragraph 1** - "encryption shall be a minimum of 128-bit."
- **Paragraph 4** - "When encryption is employed the cryptographic module used shall be certified to meet FIPS 140-2 standards."

Mobility's use of validated/certified cryptographic libraries (NIST certificate numbers 237, 441, 493, 1507, 1328, 1335 and 1878) meets this requirement.

2FA

NetMotion Wireless offers both full Advanced Authentication Solution, helping you set up your solution from scratch, and Advanced Authentication Assistance, which reviews your current solution and authentication vendor and helps to ensure you're meeting all of your requirements.

RSA SecurID

Electronic token devices are another strong authentication method specified in the CJIS policy. Specifically, Mobility supports RSA SecurID, which uses an electronic token to generate a one-time password.

Mobility servers communicate directly with the RSA Authentication Manager via Authentication Agent software installed on the Mobility server. Mobility versions 7.x and above are certified as RSA SecurID Ready. They are compatible with RSA SecurID hardware, USB and software tokens on all client operating systems that Mobility supports.

Beyond Current Requirements

While not specifically required under current CJIS policy, the following measures represent an additional layer of protection, and could assist in complying with more stringent requirements in the future.

Device authentication

The current security policy mandates user authentication as opposed to device authentication. However, Mobility also allows individual devices to authenticate independent of the user, with the ability to mandate that users only be allowed to authenticate with specific devices. This provides an additional security factor that exceeds the CJIS requirement.

Enforcement for firewalls and anti-virus

Section 5.10.4 mandates the use of personal firewalls and antivirus protection. Mobility, through its Mobile NAC module, can verify that these measures are in place and enabled, require that antivirus signatures are updated according to organization policy, and even automatically update those signatures through integration with the Policy Management module.

Extensive Platform Support

Mobility has extensive platform support, working on the majority of widely-used mobile operating systems. Mobility supports Android devices running on Android 4.0x to 4.3x, and Windows Pro Tablets as well as devices running Windows XP, 7, and 8. Mobility also offers connectivity for iOS, Mac, and Linux devices.

iOS

Conclusion

NetMotion product development specifically engineers our product to be compliant with applicable portions of CJIS security policy. In addition, Mobility provides extensions and integration with other vendors' products, promoting more streamlined compliance with the policy as a whole.

NETMOTION®
WIRELESS

www.NetMotionWireless.com

FOR MORE INFORMATION, CONTACT US:

United States

Seattle, Washington
Telephone: (206) 691-5500
Toll Free: (866) 262-7626
Sales@NetMotionWireless.com

Europe

Germany and France
CentralEasternEurope@NetMotionWreless.com

United Kingdom
NorthernEurope@NetMotionWireless.com