Mobility XE™ and CJIS Security

Meeting Requirements for Advanced Authentication and Encryption

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 Mobility XE mobile VPN from NetMotion Wireless is widely used in law enforcement, and can be used to comply with CJIS requirements for mobile-device access.

CJIS security policy section 7.3 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. Specific deadline information is in the CJIS security policy, which is available on the LEO Web site. An agency's CJIS System Agency Information Security Officer should be able to provide a copy.

Each state is responsible for establishing its own interpretation and implementation of the advanced authentication requirement. Public safety agencies that use Mobility XE have the flexibility to implement any of the advanced authentication methods.

Low-cost, Standards-based Approach

NetMotion has deliberately adopted a low-cost approach for implementing a fully compliant, secure system so that agencies may comply without seeking significant new budget outlays. It is based on widely available, industry-standard infrastructure: RADIUS servers as the front-end for Microsoft's Active Directory Authentication, and PKI (public key infrastructure) for provisioning and exchange of digital certificates. There are multiple, low-cost RADIUS systems available, and PKI support is built into Microsoft server operating systems. Other PKI solutions are supported if they are compatible with X.509v3 user certificates, standard Microsoft CAPI-enabled access to those certificates, and the RADIUS EAP-TLS or EAP-TLS inside PEAP protocol.

Advanced Authentication Methods Supported

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

Smart cards. Mobility XE 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 XE.

Compliance with FIPS 140-2 Encryption Requirements

In addition to strong authentication, CJIS security policy mandates the use of FIPS 140-2 validated encryption. According to sections 7.10 (wireless) and 7.12 (encryption): "… a minimum of 128-bit encryption with NIST or CSE certification of the cryptographic module to ensure it meets FIPS Publication 140-2 for 'Security Requirements for Cryptographic Modules.'"

Mobility XE's use of validated/certified cryptographic libraries (NIST certificate numbers 237, 441 and 493) meets this requirement. Any amibiguity concerning whether an entire product or only an embedded module needs to be certified is clarified in Appendix c.18 of the CJIS security policy.

Public Key Infrastructure (PKI). Mobility XE 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 XE where the biometric function is used in place of a PIN or password to unlock access to the X.509v3 certificates. In addition, Mobility XE 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 XE 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 Mobility XE version 7.x and 8.0 on Windows 2000 Server; Mobility XE version 8.5 and 9.0 on Windows Server 2003; and Mobility XE version 9.2 on Windows Server 2003 and Windows Server 2008 R2.

RSA SecurID

Electronic token devices are another strong authentication method specified in the CJIS policy. Specifically, Mobility XE 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 XE 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 XE 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. Sections 7.13 and 7.15 mandate the use of personal firewalls and antivirus protection. Mobility XE, 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.

Conclusion

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

For more information:
www.netmotionwireless.com