How to become CJIS compliant
From planning to implementation

Tom Flynn
Vice President Security

John Bailey
Technical Sales Manager
Advanced Authentication for CJIS Compliance

Tom Flynn
Vice President
Online Banking & Authentication
Gemalto’s Secure Personal Devices
...are in the hands of billions of individuals worldwide

- **12 billion secure devices** –
  Produced and personalized in 2011
- **200 million citizens** –
  Received a Gemalto produced e-Passport
- **500 million people** –
  Carry a Gemalto produced credit card
- **450 mobile operators** –
  Connecting over 2 billion subscribers
- **20 million people** –
  Use Gemalto eBanking solutions
- **30 years experience** –
  Designing/producing digital security solutions
- **Large Enterprise Customers** –
  Microsoft, Exxon, U.S. DOD, BASF, Boeing..
Gemalto: The World Leader in Digital Security

❖ Strong Growing Global Company
   • $2.6B in 2011 revenue
   • 10k employees
   • 87 sales & marketing offices
   • 18 production sites
   • 13 R&D centers

❖ Extensive portfolio of strong authentication solutions & services
   • Secure physical and online identity solutions
   • Versatile authentication software platforms
   • Full professional services offerings

❖ Securing access for top brands and governments for more than 30 years
What is CJIS?

Policy Highlights

- Mandate from FBI's Criminal Justice Information Systems (CJIS)
- Requires Advanced Authentication for anyone accessing CJIS database
- Mandate covers law enforcement, public safety, judicial, and correctional institutions
- Deadline—September 2013
Criminal Justice Information System (CJIS)

Why the Mandate

- Issuance of laptop and mobile devices on the rise among police departments
- CJIS database holds critical, personal information such as fingerprint records, criminal histories, and sex offender registrations
- Security risks associated with weak password-based authentication
Mobility and Security

Wireless 4G LAN is changing the game

- 4G networks are extending the access to secure data to the street, allowing direct CJIS access by an officer on patrol. This results in greater efficiencies and enhances officer security.

- CJIS Policy is designed to help police departments benefit from the technology changes without jeopardizing the security and overall integrity of the system.
CJIS Policy Authentication Requirements

Policy Highlights

- Each user accessing CJIS must have a unique identifier
  - Generic system/Windows logon does not meet the requirement
  - Officers sharing cars & tough books will need unique way to digitally identify themselves
- Non-secure locations (car/remote access) require Advanced Authentication
CJIS Security Policy Requirements

Policy Highlights (cont.)

- Data in transmission and at rest must be encrypted
  - VPN & disk encryption using FIPS certified cryptography
- Planned implementation must be reviewed and approved by regional CSO
- Multiple technologies are allowed

So How Do You Chose?
Options for Advanced Authentication

- **Hardware tokens**
  - One-time password token linked to users’ identity
  - Can be implemented quickly and does not require changes to existing end-user device

- **Certificate-based smart cards (used by DOD)**
  - Microprocessor embedded in card
  - Unique set of keys associated with user provides basis for secure online identification
  - Identity can be used for multiple functions including physical access and identification—driving down overall cost for implementation
Police Department Requirements

- The solution needs to be easy to use by all personnel
  - Require minimum data entry
  - Portable and ruggedized
  - Integrated in the logon process…

- The authentication service must run 24/7
  - High availability back-end architecture

- Integrate with existing infrastructure
  - Windows OS,
  - NetMotion VPN
  - Wireless Network

- Easy to deploy and cost effective to manage
  - No hardware change on the end points
  - Server appliance for the server
OTP: A Good First Move

- One-Time password is intuitive and proven
- Multiple form factor to support your end users
- Ease of deployment with appliances
- Infrastructure ready
  - Windows 7 & 8 logon ready
  - NetMotion approved
Certificate Based Identity Solutions

Optimized and Future Proof

- **Leverages the Microsoft architecture (AD, CA)**
  - Built in high availability architecture with AD

- **Single Sign On from Windows logon to application access**
  - userID is part of the credential—User does not have to type in User ID
  - Card + PIN at windows logon => VPN => application

- **Ease of deployment with IDAdmin 200**

- **Can extend to other applications**
  - Secure messaging
  - Digital signatures
Some Considerations

Selecting and Deploying by September 2013

❖ Understand your options
  - What type of advanced authentication will you deploy?

❖ Make an Advanced Authentication choice that:
  - Works with your infrastructure
  - Is easy to use, easy to deploy
  - Anticipates changes in the authentication landscape

❖ User education is key
  - Provide technology that makes authentication easy

❖ Chose a vendor who…
  - Will provide you with options
  - Has experience working with police/defense organizations
Select Reference Customers

❖ Complete Secure Identity Deployments
  • Deployed identity solution for visual, physical and logical access
  
  - U.S. Department of Defense
  - UK Ministry of Defence
  - Qatar National Police
  - U.S. Federal Bureau of Investigation
  - Berlin Police
  - Tokyo Metropolitan Police
  - U.S. Department of Homeland Security
  - Swedish National Police

❖ eCitation & Citizen Card Access
  • Police identity card used to log into mobile terminal for issuing electronic citations and to gain access to citizen identity card information

  - Queensland Police (Australia)
  - French National Police (Gendarmerie)
Thank You

Tom Flynn
Thomas.flynn@gemalto.com

Gemalto.com/identity/solutions/get-ready-for-CJIS.html
John Bailey – Technical Sales Manager
John.bailey@netmotionwireless.com
Company

- Develop security and management software for mobile field workers
- Formed 2001
- 130+ Employees
- 25+ Industry Awards

Customers

- 2,200+ customers
  - 97% maintenance renewal rate
  - 98% satisfaction rate
  - 50% revenue from add-on sales

Locations

- Headquartered in Seattle, WA
- Sales Offices throughout North America and Europe
Over 2,200 Customers in a Variety of Industries

**Government**
- Orange County Sheriff's Office
- Chicago Police Department
- Metropolitan Police Department
- New York Police Department
- Los Angeles Police Department
- Seattle Police Department
- Portland Police Bureau
- Houston Police Department
- Dallas Police Department
- Los Angeles Fire Department

**Utilities**
- Avista Utilities
- Ameren
- Atlanta Gas Light
- APS
- CPS Energy
- Alagasco
- conEdison
- JEA
- Dominion
- Chesapeake
- KeySpan
- PSE&G
- PGW
- PG
dEnergy
- Nevada Power
- Seattle Public Utilities
- Sempra Energy
- Terasen Gas
- NW Natural

**Healthcare**
- UCLA Healthcare
- Providence Health & Services
- Marshfield Clinic
- Advocate Health Care
- Mayo Clinic
- St. Luke's
- Visiting Nurse Service of New York
- St. Jude Medical
- Scott & White Healthcare
- Allina Hospitals & Clinics
- Wichita Clinic

**Insurance**
- Travelers
- Liberty Mutual
- Grange Insurance
- Amica

**Enterprise**
- United Airlines
- Delta Airlines
- Unilever
- Beckman Coulter
- Hertz
- Comcast
- Cox Communications
- Johnson Controls
- Siemens
- Continental
- KCI
- Neopost
Mobility XE – the industry leading Mobile VPN
- Removes common barriers to successful mobile deployments
- Client and server software
- Support for all Microsoft devices

**Productivity**
- Enhances productivity of mobile field workers

**Security**
- Industry standards
- Built with mobile field workers in mind

**Management**
- Centralized control and visibility
Security – Industry Standards

**Encryption**
- **FIPS 140-2 Validated**
- 128, 192 or 256-bit AES Encryption

**Authentication Methods**
- MS Active Directory
- RADIUS
- Smartcards
- Digital Certificates

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 XE’s use of validated/certified cryptographic libraries (NIST certificate numbers 237, 441, 1507, 1328, and 1335) meets this requirement.**

*TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments*
Enhanced Security

» Lock-down clients
  • Ensure traffic is routed through the corporate network
  • Access to & from device ONLY through encrypted tunnel
  • Complimentary to client firewall

» Validate user identity throughout the day
  • Configure periodic user re-authentication without disrupting application sessions

» Verify device identity
  • Stop foreign devices from accessing corporate network

» Machine authentication
  • Users log in from approved machines only
Enhanced Security

- **Quarantine Devices and/or Users**
  - Quarantine NEW Devices – keeps unapproved devices off the network
  - Prevent lost or stolen devices from accessing the enterprise

- **Control application access by user group or device**

- **Keep devices in the field current on patches**
  - Unattended over-the-air management of mobile devices
  - Extend the reach of existing device and patch management utilities.
  - Supports Active Directory scripting & objects

- **Network Access Control**
  - Prevents or allows user connection based on client’s compliance to corporate policies
  - Client evaluates → Server enforces
    - Allow | Warn | Remediate | Disconnect | Quarantine
  - Integrates with Policy Module for ‘smart’ remediation
NetMotion and Gemalto – Deployment Examples

Certificate-based smart card

OTP
NetMotion MXE Server Configuration

Integration Guide Available

**Authentication: User - Protocol**

**Global Setting**

**Protocol:**
- NTLM
- RSA SecurID
- RADIUS - LEAP
- RADIUS - EAP (PEAP and EAP-TLS)

Click here to fill in the default value.

**Protocol** specifies the protocol the Mobility server will use to provide user credentials to the authentication server. All Mobility servers in a server pool must use the same protocol to authenticate all users.

See Configuring Client Authentication.

**RADIUS Server Entry**

- **IP Address:** 10.128.105.12
- **Port:** 1812
- **NAS ID:** netmotion
- **Shared secret:** ************
- **Confirm shared secret:** ************

[OK] [Cancel]
THANK YOU

john.bailey@netmotionwireless.com