Entrust®
Securing Digital Identities & Information

EntrustSecurity
@Entrust

Integrating Advanced Authentication Solutions for CJIS Compliance

Detailed integration scenarios using NetMotion Mobile VPN and Entrust IdentityGuard

Get this White Paper

Entrust.com
1-888-690-2424
Entrust@Entrust.com

Entrust®
Securing Digital Identities & Information

Table of Contents

Accessing CJIS Database

Law enforcement agencies require timely and secure access to services that provide data — wherever and whenever — for stopping and reducing crime.

In response to these needs, the Advisory Policy Board (APB) recommended to the Federal Bureau of Investigation (FBI) that the Criminal Justice Information Services (CJIS) Division authorize the expansion of the existing security management structure in 1998.

Administered through a shared management philosophy, the CJIS Security Policy contains information security requirements, guidelines and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage and generation of Criminal Justice Information (CJI).[1]

The CJIS Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for the access to the FBI's CJIS division systems and information and to protect and safeguard Criminal Justice Information (CJI).[2]

The FBI's CJIS Security Policy, Version 5.1, requires organizations to implement advanced authentication (Section 5.6.2.2) controls to securely and properly access the CJIS database from non-secure locations, including police cruisers.

Entrust's comprehensive suite of identity-based security solutions are designed, in part, to help law enforcement comply with requirements mandated by the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Division.

Entrust identified a number of scenarios in which Entrust products may be used to comply with section 5.6.2.2 of the security policy requiring advanced authentication.

Please Note: Implementation of the solutions, as defined in these use cases, does not ensure CJIS compliance. Only through a formal submission to the appropriate local FBI CJIS representative based on your final implementation may you be given final approval as meeting FBI requirements for advanced authentication.

> *"The CJIS Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for the access to the FBI's CJIS division systems and information and to protect and safeguard Criminal Justice Information (CJI)."*

[1] Criminal Justice Information Services (CJIS) Security Policy, Version 5.1
[2] Ibid.

Accessing the CJIS Network from a Non-Secure Location

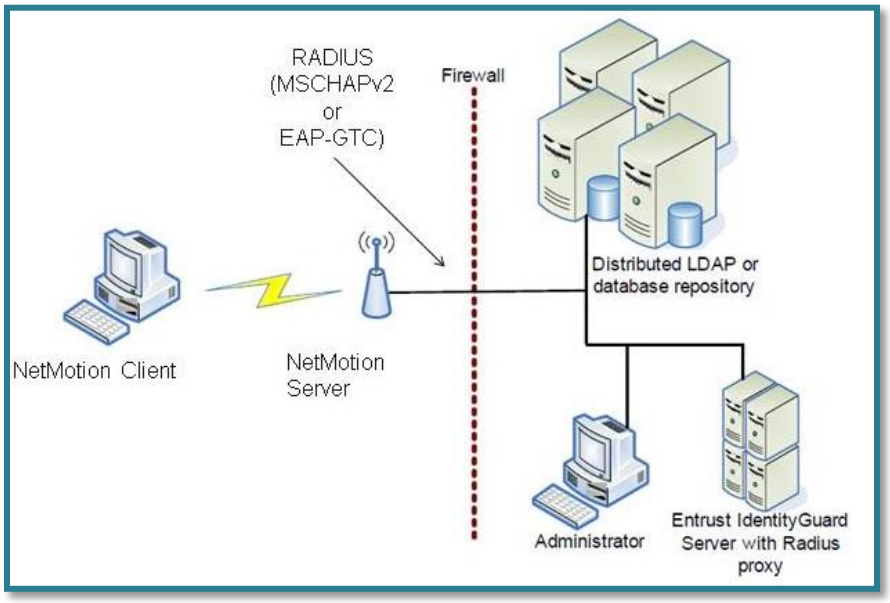
Description

In this scenario, a user is accessing the CJIS database from a non-secure location (e.g., police cruiser) from a mobile Computer Aided Dispatch/Records Management System (CAD/RMS) on a department-issued, Windows-based computer or Mobile Data Terminal (MDT).

Access to the network is established using the NetMotion Mobile VPN. A FIPS 140-2-certified VPN termination point, NetMotion Mobile VPN is configured to require the user to verify their identity via advanced authentication, in addition to their Windows domain username and password, prior establishing the VPN connection that enables access to CJIS data.

The following diagram provides a basic network architecture that shows the relationship between Entrust IdentityGuard and the NetMotion Mobile VPN product.

Entrust IdentityGuard
Wireless Architecture



Authentication Use Cases

The following use cases provide the step-by-step process for implementing advanced authentication via a number of Entrust authentication options.

Use Case 1: Authentication using Entrust Hardware or Mobile Soft Tokens

Products

> Entrust Hardware or Mobile Soft Token

> NetMotion Mobile VPN

Entrust's OATH- and time-based hardware and soft tokens generate a random eight-digit code every 30 seconds. The authentication server may be configured to ask the user for the eight-digit code on their token or the eight-digit code in addition to a four-digit personal verification number (PVN).

The PVN is a unique number associated with the user that provides additional verification of the user's identity.

Step 1

The user executes a simple "*Control+Alt+Delete*" function to log in to their Windows computer with their regular domain credentials.

Step 2

The user enters their username and password.

Step 3

Upon successful verification, the NetMotion Mobile VPN client is launched. Typically, this is automatically launched immediately after Windows logon and prior to the user seeing the desktop.

The NetMotion VPN client prompts the user for their advanced authentication credentials:

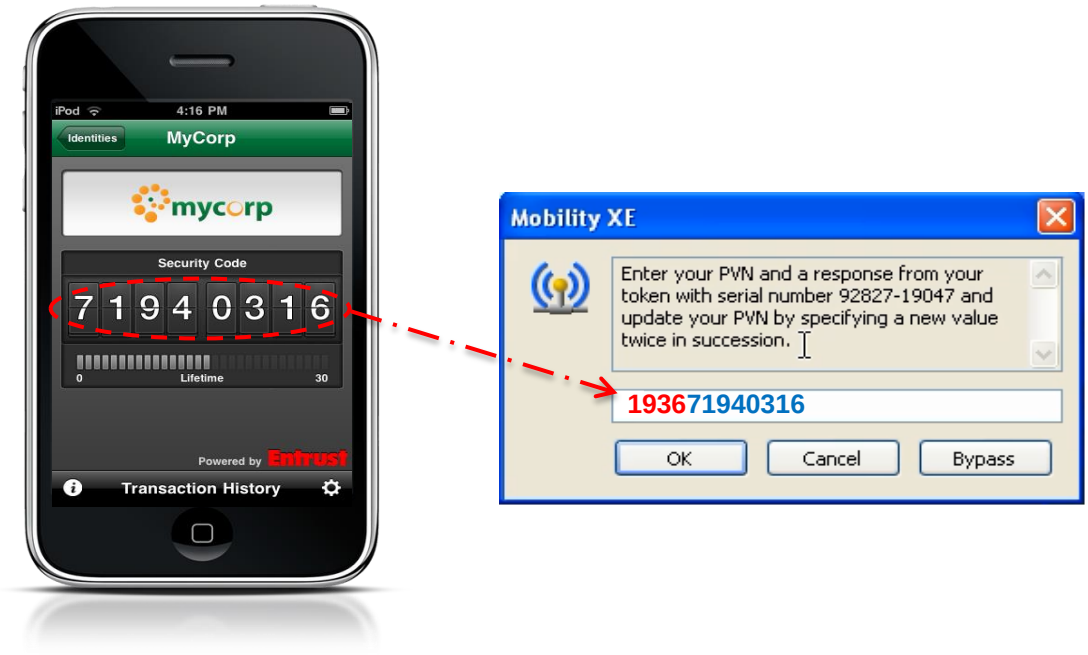
1. Their Entrust IdentityGuard username, which is typically the same as their Windows login username.

   Note: *In some configurations the user will be prompted for their username a second time if it is different than their Windows username.*

2. The eight-digit number from their token.

3. Optionally**,** the user may be prompted for their Personal Verification Number (PVN)**,** if established.

In the example below, the user provides their four-digit PVN (e.g., 1936, illustrated in **red**) in addition to their eight-digit token number (illustrated in **blue**).



Step 4

Upon successful verification of the unique eight-digit code and the PVN (if applicable), the user is authenticated and the NetMotion VPN tunnel is established.

The NetMotion VPN termination point applies the policy/profile/access control filter that permits the network traffic required to execute a CJI query.

Only advanced authenticated users in the appropriate group, with the appropriate profile/policy/access controls applied at the VPN termination point (e.g., Cisco, Microsoft, NetMotion servers), are technically able to execute CJI queries.

As a control layer control, network traffic is blocked for users not in the group allowed to access CJIS on the VPN termination point.

Use Case 2:
Authentication using Entrust Grid Card

Products > Entrust IdentityGuard Grid Card
> NetMotion Mobile VPN

	A	B	C	D	E	F	G	H	I	J	
1	A3	11	C5	S3	57	K1	M9	FQ	G7	XD	1
2	T6	O7	Q5	29	F3	1K	PE	CZ	N4	K2	2
3	29	ET	B7	M3	AZ	H7	YJ	V8	L0	48	3
4	QK	XR	HR	U6	18	N3	AB	LU	76	X8	4
5	P7	D3	14	LV	Y5	G6	Z9	AW	72	S9	5

Entrust's patented grid card is a credit card-sized authenticator consisting of numbers and/or characters in a row-column format.

Upon login, users are presented with a random coordinate challenge and must respond with the information in the corresponding cells from the unique grid card they possess. Entrust grid cards may be issued as a plastic card or in soft form on a mobile device.

Step 1

The user executes a simple "*Control+Alt+Delete*" function to log in to their Windows computer with their regular domain credentials.

Step 2

The user enters their username and password.

Step 3

Upon successful verification, the NetMotion Mobile VPN client is launched. Typically, this is automatically launched immediately after Windows logon and prior to the user seeing the desktop.

The NetMotion VPN client prompts the user for their advanced authentication credentials:

1. Their Entrust IdentityGuard username, which is typically the same as their Windows login username.

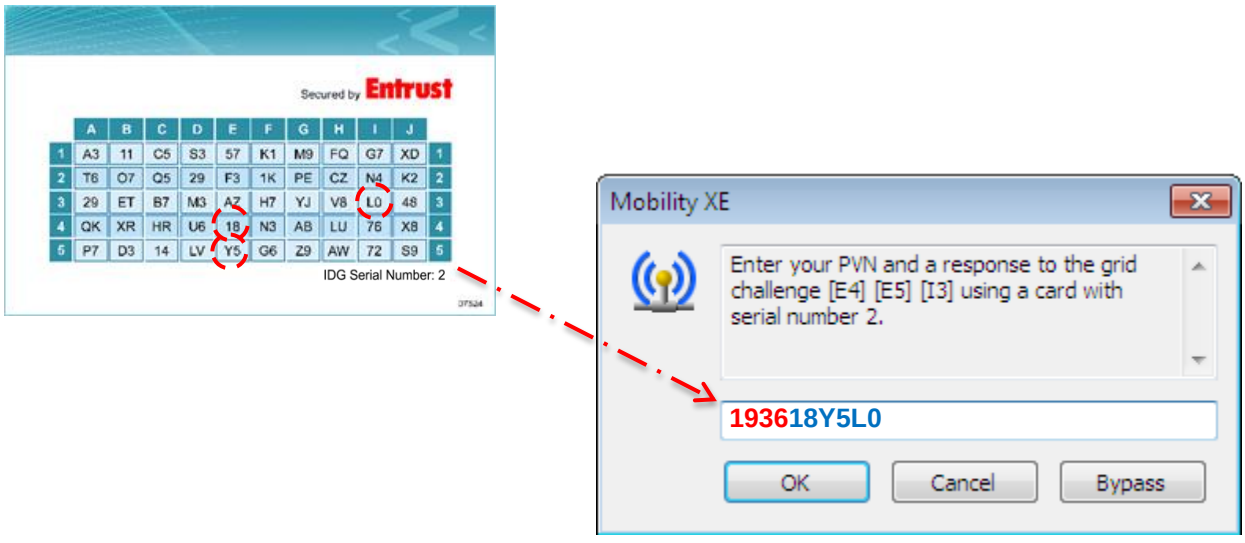
   Note: *In some configurations the user will be prompted for their username a second time if it is different than their Windows username.*

2. The user is presented a random coordinate challenge for information contained in specific cells of their unique grid card. The user refers to their unique grid card to provide the information from the requested cells.

   In the example below, the user is challenged for the information in cells: **E4, E5** and **I3**. The user responds with: **18, Y5** and **L0.**

3. Optionally, the user may be prompted for their Personal Verification Number (PVN), if established.

In the example below, the user first provides their four-digit PVN (e.g., 1936, illustrated in **red**) in addition to the alphanumeric information (illustrated in **blue**) from required grid card cells.



Step 4

Upon successful verification of the correct responses to the grid challenge, the user is authenticated and the NetMotion VPN tunnel is established.

The NetMotion VPN termination point applies the policy/profile/access control filter that permits the network traffic required to execute a CJI query. Only advanced authenticated users in the appropriate group, with the appropriate profile/policy/access controls applied at the VPN termination point (e.g., Cisco, Microsoft, NetMotion servers), are technically able to execute CJI queries.

As a control layer control, network traffic is blocked for users not in the group allowed to access CJIS on the VPN termination point.

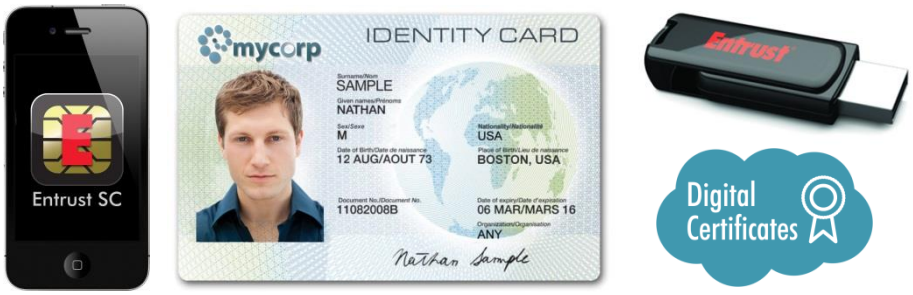
The advanced authentication server is not connected to, nor asserting, credentials to the CJI application (i.e., OSSI MCT), but is only used to validate the establishment of VPN for this particular user.

Use Case 3: Authentication using Entrust Smartcard

Products

> Entrust PKI Certificates on Smartcard, USB or Mobile Device

> NetMotion Mobile VPN



Leveraging Entrust's award-winning public key infrastructure (PKI) for certificate issuance and management — which offers in-house or managed service models — credentials may be stored on a variety of formats, including mobile devices, contact and contactless smartcards, USB tokens and cloud-based options.

Upon login, the user is presented with a challenge for their certificate. The user unlocks access to the stored credential to complete the user authentication.

Step 1

The user executes a simple "*Control+Alt+Delete*" function to log in to their Windows computer with their regular domain credentials.

Step 2

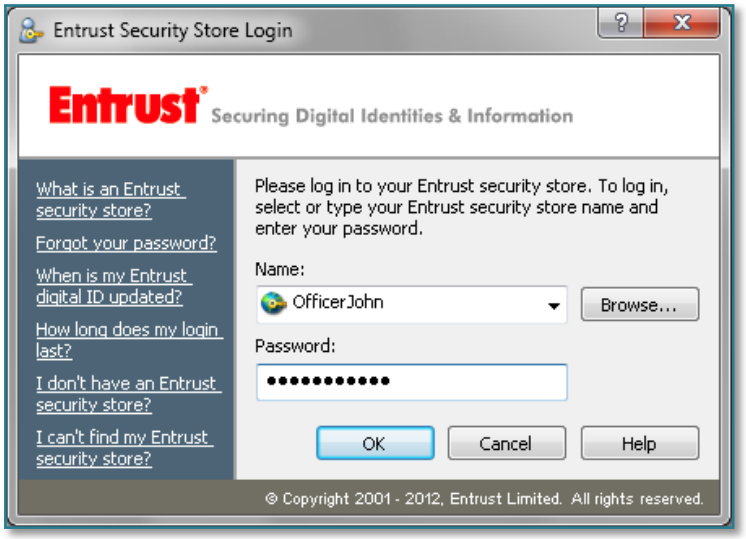
The user enters their username and password.

Step 3

Upon successful verification, the NetMotion Mobile VPN client is launched. Typically, this is automatically launched immediately after Windows logon and prior to the user seeing the desktop.

The NetMotion VPN client prompts the user for their advanced authentication credentials:

1. Upon acceptance of the username and password, the user is asked for their digital certificate.
2. The user provides their password that unlocks access to their digital certificate. The certificate is authenticated as currently valid and belonging to the user.



Step 4

Upon successful verification of the digital certificate, the user is authenticated and the NetMotion VPN tunnel is established.

The NetMotion VPN termination point applies the policy/profile/access control filter that permits the network traffic required to execute a CJI query.

Only advanced authenticated users in the appropriate group, with the appropriate profile/policy/access controls applied at the VPN termination point (e.g., Cisco, Microsoft, NetMotion servers), are technically able to execute CJI queries.

As a control layer control, network traffic is blocked for users not in the group allowed to access CJIS on the VPN termination point.

The advanced authentication server is not connected to, nor asserting, credentials to the CJI application (i.e., OSSI MCT), but is only used to validate the establishment of VPN for this particular user.

Software-Based Authentication: Entrust IdentityGuard

Entrust's flagship authentication solution, Entrust IdentityGuard, continues to lead the industry as one of the most robust software authentication platforms, delivering scalability, reliability and the most diverse set of authenticators supported on the market today.

Entrust IdentityGuard serves as organizations' single comprehensive software-based authentication platform, while concurrently bridging them to emerging technologies for strong mobility, cloud and credentialing offerings.

Physical & Logical Access

Entrust IdentityGuard provides a new standard for physical and logical access control for effective enterprise authentication. This integrated platform approach simplifies the issuance and management of smartcards and certificates, leveraging industry standards such as PIV — all from a single trusted vendor.

Mobile Smart Credentials

Entrust IdentityGuard Mobile Smart Credentials transform a mobile device into a virtual smartcard, eliminating the need for physical smartcards or hardware-based one-time passcodes (OTP).

The mobile smart credential is more convenient, easier to use, less expensive to deploy and provides support for a number of authentication and information protection needs within an organization.

Entrust Mobile Smart Credentials may be leveraged to solve a wide array of use-cases:

- Physical access to facilities
- Logical access to computers, networks and applications
- Digital-signing of forms, documents and emails
- Encryption of email and information

More Authentication Choices

The software authentication platform enables organizations to layer security — according to access requirements or risk — across diverse users and applications.

Entrust's authentication capabilities include smartcards and USB tokens, soft tokens, grid cards and eGrids, IP-geolocation, questions and answers, mobile smart credentials, out-of-band one-time passcode (delivered via voice, SMS or email), and a range of one-time-passcode tokens.

Easy Integration

Entrust’s open API architecture allows for tight integration with today's leading mobile device management (MDM), identity access management (IAM) and public key infrastructure (PKI) vendors.

This enables Entrust IdentityGuard to work with new and existing enterprise implementations, plus adds the ability to integrate in-house or managed service-based digital certificates.

Industry Standards & Support

Entrust IdentityGuard supports more than a dozen types of popular and innovation authenticators. Centralized policy allows the controlled co-existence and transition between authenticators from a single management console.

Entrust IdentityGuard also supports the latest industry standards, FIPS-201 and Desfire, along with older technologies to enable a smooth transition.

While Entrust does provide the entire solution to save customers the pain of individual product integration, our standards-use allows for components to be swapped out as desired.

Entrust IdentityGuard provides an optional module, ID-SYNC, that will automatically instruct the physical access control system when a card is issued or deleted. The solution will replicate this information to all systems the enterprise is using worldwide.

Conclusion

The FBI's CJIS Security Policy, Version 5.1, requires organizations to implement advanced authentication (Section 5.6.2.2) controls to securely and properly access the CJIS database from non-secure locations by **September 30, 2013.**

Entrust's comprehensive suite of identity-based security solutions are designed, in part, to help law enforcement comply with requirements mandated by the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Division.

Entrust is able to provide all of the authentication options outlined in the CJIS Security Policy for access the CJI data. The use cases outlined within this document provide examples from a number of Entrust's popular advanced authentication options.

Please Note: Implementation of the solutions, as defined in these use cases, does not ensure CJIS compliance. Only through a formal submission to the appropriate local FBI CJIS representative based on your final implementation may you be given final approval as meeting FBI requirements for advanced authentication.

Entrust & You

More than ever, Entrust understands your organization's security pain points. Whether it's the protection of information, securing online customers, regulatory compliance or large-scale government projects, Entrust provides identity-based security solutions that are not only proven in real-world environments, but cost-effective in today's uncertain economic climate.

A trusted provider of identity-based security solutions, Entrust empowers governments, enterprises and financial institutions in more than 5,000 organizations spanning 85 countries.

Entrust's award-winning software authentication platforms manage today's most secure identity credentials, addressing customer pain points for cloud and mobile security, physical and logical access, citizen eID initiatives, certificate management and SSL.

For more information on Entrust solutions for CJIS compliance, please contact the Entrust sales representative in your area, call **1-888-690-2424** or visit **entrust.com/cjis**.

Company Facts

Website: www.entrust.com
Employees: 359
Customers: 5,000
Offices: 10 Globally

Headquarters

Three Lincoln Centre
5430 LBJ Freeway, Suite 1250
Dallas, Texas 75240

Sales

North America: 1-888-690-2424
EMEA: +44 (0) 118 953 3000
Email: entrust@entrust.com

follow us on twitter tweet