Advanced Authentication Methods
Determining the Best Fit for Your Agency

Agenda

- About 2FA
- CJIS Security Policy 5.1 – Advanced Authentication
- Encryption, Secure Connectivity (VPN), and Authentication
- Advanced Authentication – Methods
- Advanced Authentication – Common Challenges
- Recommendations
- Panel Discussion
- Questions

About Us

2FA, Inc.

- Strong authentication software product & services company
- Founded in 2006
- Veteran Owned
- Headquartered in Austin, Texas
- Target industries: Public Safety & Healthcare
- Product name: 2FA ONE
- Over 1,000,000 licenses sold
- Advanced authentication hedgehogs
- Member of NetMotion's Advanced Authentication Alliance

Awards

- Info Security 2013 – Gold award for best authentication product
- Info Security 2013 – Gold award for best security solution for government

The CJIS Advanced Authentication Policy

CJIS Security Policy 5.1

5.6.2.2 Advanced Authentication

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.

* software-based OTP tokens currently under development.

Green = Methods supported by 2FA ONE

Mythbusters & Rumor Control

Go-to-People

- Contact the CJIS Technical Audit Team at TX DPS, they have up-to-date information on the policy and potential changes.
- http://www.txdps.state.tx.us/SecurityReview/index.htm

Updates

- The "exemption" extending to police vehicles was extended until September 30, 2014. Another extension was proposed, but has not been approved.
- The APB has proposed exemptions to agency procured mobile phones that will make it easier to use Apple products. MDM will be required.
- Expect more changes.

When do you need to comply with AA?

CJIS Security Policy 5.1

5.6.2.2.1 Advanced Authentication Policy and Rationale

For interim compliance, users accessing CJI from devices associated with, and located within, a police vehicle are exempt from the AA requirement until September 30th 2014* if the information system being used has not been procured or upgraded anytime after September 30th, 2005.

- Exemption does not cover new or upgraded technology.
- Exemption does not cover systems in privately owned vehicles.
- Exemption does not cover systems not in a Controlled Area.

* Contact CJIS Technical Audit Team @ TX DPS with questions.

Advanced Authentication Methods

1. Biometric systems
2. User-based public key infrastructure (PKI)
3. Smart cards
4. Software tokens
5. Hardware tokens
6. Paper (inert) tokens
7. Risk-Based Authentication

Two other commonly used and approved options

1. DL Swipe - magnetic stripe & 2d barcode
2. RFID badges commonly used for building access

Biometrics

Fingerprint biometrics are the only viable solution.

- **Workflow:** User swipes or places finger on a sensor. A PIN may or may not be required.
- **Authentication:** Authentication can occur at OS logon or application level such as VPN or CAD/RMS etc.
- **Security Level:** High
- **Cost:** Medium/High. Readers $15 to $150+. Software $40+.
- **Reader required:** Yes, but embedded options are available.
- **Pro's:** Nothing extra to carry, lose, forget.
- **Con's:** Does not work for everyone. Does not work with gloves. Inconvenient if users are frequently exposed to dirt, dust, or other contaminants. Readers must be cleaned frequently. According to policy authentication must take place on the server – not a stand alone client. Lighting conditions will affect readability. OS logon will require domain accounts.
- **Recommendation:** Worth considering in temperate climates if readers are embedded in MDT's.

Ease of use: Easy (90% of the time)

Feedback from the field: Like it when it works. Hate it when it doesn't.

User based Public Key Infrastructure

Leverage Microsoft Certificate Services as opposed to third-party certificates.

- **Workflow:** User logs on to MDT with user name and password that resides in Active Directory. Their local account profile is loaded. User launches an application that leverages certificate-based authentication.
- **Authentication:** Application level such as VPN or CAD/RMS etc.
- **Security Level:** Low.
- **Cost:** Low.
- **Reader required:** No.
- **Pro's:** Nothing to carry, nothing to lose, nothing to forget. No environmental issues.
- **Con's:** Low security. Requires users to logon with Active Directory user names and passwords. Requires third-party applications to leverage certificates. According to policy a CP and CPS (documentation) must be created and managed. Requires a higher level of technical expertise to deploy and maintain.
- **Recommendation:** Worth considering if your users logon with assigned user names and passwords to Active Directory and your IT technical staff has the time and knowledge to deploy and maintain the added infrastructure. Check with your third-party application providers to ensure their applications support user-based certificates.

Ease of use: Easy

Feedback from the field: Difficult to manage. Only a handful of vendors support certificates. Users do not logon to domain.

Smart Cards

Leverage Microsoft Certificate Services as opposed to third-party certificates.

- **Workflow:** User inserts card into smart card reader or inserts a token into a USB slot at OS logon, OS recognizes certificate stored on device, user enters PIN, OS logon occurs.
- **Authentication:** OS logon and application level such as VPN or CAD/RMS etc.
- **Security Level:** High
- **Cost:** High. Readers $15 to $50+. Cards $15 to $50+. Software $40+.
- **Reader required:** Yes, but embedded options are available.
- **Pro's:** High security. Used by USG (FBI, DoD, etc.). Mature technology. No environmental issues. Portable. Multi-use – physical and logical access. Facilitates pre-boot and full-disk encryption.
- **Con's:** High cost. Requires users to logon with Active Directory accounts. According to policy a CP and CPS (documentation) must be created and managed. Requires a higher level of technical expertise to deploy and maintain.
- **Recommendation:** Worth considering in if MDTs have embedded readers. Best when used for both physical and logical access on one card.

Ease of use: Easy

Feedback from the field: Users forget card in reader. Infrastructure is complex to deploy.

Software Tokens (OTP)

Soft token generator not approved for use on MDTs.

- **Workflow:** User opens VPN or other application that uses OTP. User generates OTP code within soft token generator, user inputs user name and OTP code, in some cases a PIN and/or password is also required, to authenticate.
- **Authentication:** Application level such as VPN or CAD/RMS etc.
- **Security Level:** Medium.
- **Cost:** Medium. Software $40+.
- **Reader required:** No, but requires a smart phone.
- **Pro's:** Does not require the user to carry something extra if they already have a smart phone. Backlit phone best suited for OTP use in public safety.
- **Con's:** Loss of power. User may not have or be willing to use person phone if not issued by the agency. Soft token generator cannot be used on the MDT. Requires a proprietary authentication server or Microsoft RADIUS backend. Cannot be used for OS logon.
- **Recommendation:** Worth considering if agency issues smart phones and third-party applications support OTP.

Ease of use: Easy.

Feedback from the field: Power loss issues.

Hardware Tokens (OTP)

- **Workflow:** User opens VPN or other application that uses OTP. User retrieves OTP from device. User inputs user name and OTP code, in some cases a PIN and/or password is also required, to authenticate.
- **Authentication:** Application level such as VPN or CAD/RMS etc.
- **Security Level:** Medium.
- **Cost:** Medium/High. Tokens $30+
- **Reader required:** No, but requires a token.
- **Pro's:** Well suited for remote access.
- **Con's:** Users cannot read in low light. The token will eventually run out of battery power. Requires something extra for the user to carry. Not ideal for OS Logon and unlock.
- **Recommendation:** Worth considering if agency supports a lot of remote users.

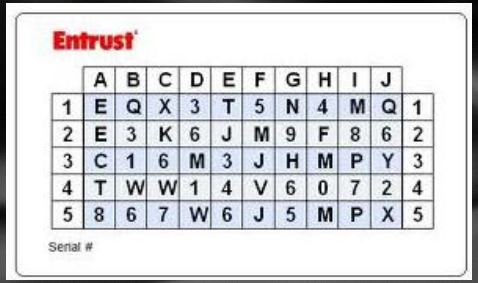
Ease of use: Hard.

Feedback from the field: Hard to read at night. Users lose and break the tokens.

Paper (or inert) Tokens

Entrust IdentityGuard is the only real option due to patent. Be wary of clones.

- **Workflow:** User opens VPN or other application that uses OTP. User inputs user name and OTP code, in some cases a PIN and/or password is also required, to authenticate.
- **Authentication:** Application level such as VPN or CAD/RMS etc.
- **Security Level:** Medium.
- **Cost:** Medium. Token $5+/-. Software $50+/-.
- **Reader required:** No, but requires a paper token.
- **Pro's:** Well suited for remote access and in high user populations that do not authenticate on a daily basis. No environmental issues.
- **Con's:** Users cannot read in low light. Requires something extra for the user to carry. Does not work for OS Logon.
- **Recommendation:** Worth considering if agency supports a lot of remote users.



	A	B	C	D	E	F	G	H	I	J	
1	E	Q	X	3	T	5	N	4	M	Q	1
2	E	3	K	6	J	M	9	F	8	6	2
3	C	1	6	M	3	J	H	M	P	Y	3
4	T	W	W	1	4	V	6	0	7	2	4
5	8	6	7	W	6	J	5	M	P	X	5

Ease of use: Mixed.

Feedback from the field: Does not work in low light. Only several vendors support the technology.

Risk-based Authentication

The least secure AA method.

- **Workflow:** User provides user name to application. Application analyzes risk factors associated with user's profile and end-point , if risk is determined then the user is required to answer one or more security questions prior to submitting password.
- **Authentication:** Application level such as VPN or CAD/RMS etc. 2FA does this at the OS level.
- **Security Level:** Low.
- **Cost:** Low. Software $40+.
- **Reader required:** No.
- **Pro's:** Nothing to carry, nothing to lose. Truly tokenless. Good for high user populations that access data over a browser. No environmental issues.
- **Con's:** Least secure. User's tend to forget answers to their questions. Prone to hacking. If the policy tightens RBA will be the first to go.
- **Recommendation:** Worth considering if your agency has no budget or is looking for a simply method that complies with the policy.

Ease of use: Easy.

Feedback from the field: This doesn't appear to be that secure. Users forget answers.

DL Swipe – Magnetic/2d bar code

Leverage what you already have.

- **Workflow:** User swipes DL or agency issued ID at OS or application logon and enters PIN.
- **Authentication:** OS Logon, application level such as VPN or CAD/RMS etc.
- **Security Level:** Medium.
- **Cost:** Medium. Readers $30+. Software $40+.
- **Reader required:** Yes, but you may already have them in vehicles.
- **Pro's:** Does not require the user to carry something extra. Users understand how to use the technology. Low failure rate. No environmental issues.
- **Con's:** Less secure than other card solutions. Does not work for remote access, such as from a phone or tablet.
- **Recommendation:** Worth considering if agency has magnetic stripe readers in the vehicles.

Ease of use: Easy.

Feedback from the field: Users like it.

Proximity Cards

Leverage what you already have.

- **Workflow:** User taps badge at OS or application logon and enters PIN.
- **Authentication:** OS Logon, application level such as VPN or CAD/RMS etc.
- **Security Level:** Medium/High.
- **Cost:** Medium/High. Readers $40 to $100+. Software $40+.
- **Reader required:** Yes, but embedded options are available.
- **Pro's:** Very easy to use. Does not require the user to carry something extra. Users understand how to use the technology. Low failure rate. No environmental issues.
- **Con's:** Does not work for remote access, such as from a phone or tablet.
- **Recommendation:** Worth considering if agency uses proximity technology for building access.

Ease of use: Easy.

Feedback from the field: Users love it.

Common Challenges

Common challenges heard from agencies:

- One policy, 50 states, 23,000 different opinions.
- No budget.
- Concerned that the policy will change or be pushed back.
- CAD vendor doesn't know about advanced authentication.
- Lack of local expertise.
- No USB ports available.
- MDTs not on domain, not connected to Active Directory.
- Officers log on locally to MDTs.

Recommendations

1. Leverage what you have – no need to reinvent the wheel.
2. Don't forget about logging and auditing – it's important too!
3. Participate in a ride along with one of your officers. Educate them on the policy and ask them what they would prefer.
4. Conduct mini-pilots with your officers.
5. Get to know your State Information Security Officer.
6. Talk to your vendors about AA (hardware, VPN, CAD, etc.)
7. Prepare yourself for the eventuality of the desktop requiring the same authentication standards.
8. Be prepared to provide more than one AA option.

Panel Discussion

Beth Ann Unger, CGCIO
Infrastructure Manager
City of Arlington

Zeis Chen
Project Manager
City of Addison

Jason Waltz
CJIS Compliance Coordinator
Milwaukee Police Department

Questions

2FA Inc.
10713 FM 620, Suite 201
Austin, TX 78726
(512) 918-3200
Sales@2fa.com

Recommendations

1. Leverage what you have – no need to reinvent the wheel.
2. Don't forget about logging and auditing – it's important too!
3. Participate in a ride along with one of your officers. Educate them on the policy and ask them what they would prefer.
4. Conduct mini-pilots with your officers.
5. Know your State Security Officer.
6. Talk to your vendors about AA (hardware, VPN, CAD, etc.)
7. Prepare yourself for the eventuality of the desktop requiring the same authentication standards.
8. Be prepared to provide more than one AA option.