
CUMBERLAND
COUNTY
NORTH CAROLINA
Meeting the Mandate
CJIS Advanced Authentication

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

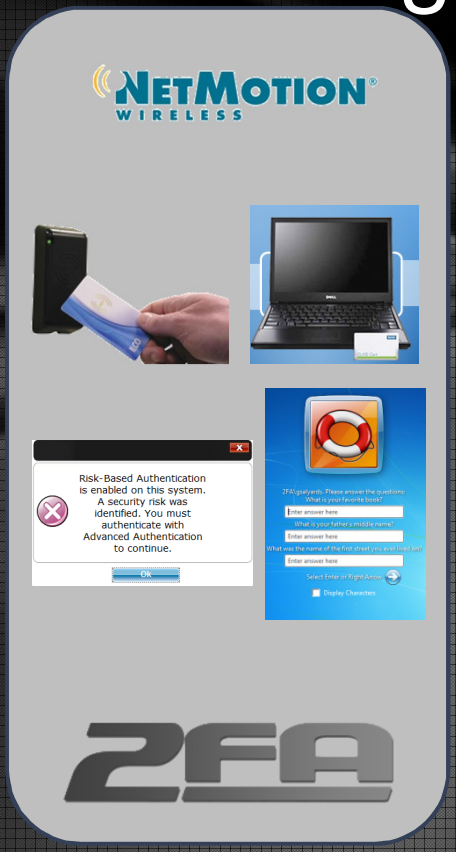
Two other commonly used and approved options

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

Cumberland County's Selected Technology

Selected 2FA ONE from Identity Automation

1. Leveraged what we already had deployed
2. RFID using contactless cards
3. Risk-Based Authentication as a back-up
4. Lots of other options
5. Dell laptops with RFID embedded reader
6. USB connected reader for other systems
7. Seamless integration with NetMotion



Risk-based Authentication

- **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.
- **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 to use and compliant.

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

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+.
- **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. (unless the tablet is Microsoft Windows based)
- **Recommendation:** Worth considering if agency uses proximity technology for building access.

Ease of use: Easy.

Feedback from the field: Users love it.

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. Talk to your vendors about AA (hardware, VPN, CAD, etc.)
6. Prepare yourself for the eventuality of the desktop requiring the same authentication standards.
7. Be prepared to provide more than one AA option.


CUMBERLAND
COUNTY
NORTH CAROLINA
Questions
Stephen Jelinek
Assistant I.T. Director
Cumberland County Sheriff's Office
sjelinek@ccsonc.org