

Power LogOn[®] COA

for Government (Offline)

UEI: X4CCM6HULMX6
CAGE: 5AU22
DUNS: 829366660

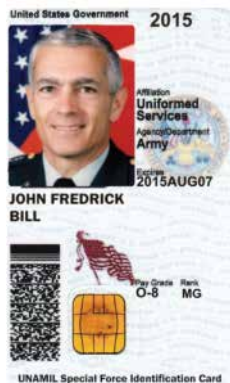


COTS Certificate-based Offline MFA Solution

Enables Offline Computer Authentication

Power LogOn COA is a COTS solution. COA provides secure login authentication for offline (standalone) computer workstations using existing Smart ID credentials with digital certificates..

Power LogOn COA works out-of-the-box with most certificates as found on PIV/PIV-I/CAC/CIV credentials to facilitate secure authentication, authorization, verification, and non-repudiation for



Power LogOn GOV-COA works with existing Government Issued Badges

Ready for Immediate Use

- ✓ User presents their credential to an online enrollment station running Power LogOn COA.
- ✓ The certificate is verified against a revocation list, and adds approved users to an enrollment file.
- ✓ The enrollment file is transferred to offline workstations.
- ✓ The user inserts their credential at offline workstation and types their PIN.
- ✓ Card's private key verifies user's information.
- ✓ Auto-fills Windows Username and Password login. Rejects non-approved users.

Environment

Ideally suited for computer workstations isolated from an organization's network that require certificate-based multifactor authentication.

- ✓ Works with any credential with a valid X509 certificate.
- ✓ Does not require any additional hardware infrastructure.
- ✓ COTS, Self Evaluation to comply to FIPS 140-3, FIPS 201, HIPAA, CJIS, NIST 800-171 & 800-63b-AAL3, and STIGs

Typical Customer

PIV/PIV-I/CAC/CIV and x.509 credentials are typically used by government entities and private organizations that handle security-sensitive information. Often, these organizations have highly secure workstations that must be isolated from the internet.

Power LogOn COA solves that problem, enabling these organizations to take advantage of the high level of security offered by their card, even in a non-networked setting.

PIV: Personal Identity Verification

PIV-I: Personal Identity Verification-Interoperable

CAC: Common Access Card

CIV: Commercial Identity Verification

"There is no other commercial-off-the-self (COTS) product that can do all that Power LogOn COA does."

~ USAF Project Manager

Fast, Easy and Affordable

Users don't need multiple credentials. Power LogOn COA is versatile because the same certificate credential can also be used on workstations and computers that are connected to a network.

Login data for additional login locations, such as local websites or applications, can also easily be entered into Power LogOn COA, enabling card-secured login for those sites.

Administrators can also opt to enroll multiple users at a central workstation. Power LogOn COA creates an enrollment file for each credential, which the administrator then transfers to the target workstations.

Implement secure MFA, identity management, and certificate authentication with Power LogOn COA!

Implement cybersecurity identity and access management with Power LogOn

Power LogOn® COA

Certificate-based Offline Authentication



General Information:

- ✓ Primary Application: Enables MFA digital certificate protected authentication for offline workstation
- ✓ Secondary Application: Auto-fill Username and Passwords into Windows' logon
- ✓ Operating System: Windows 11, Win 10, and Win 7
- ✓ Network: Not dependent on a network connection or any outside PKI system components
- ✓ Enrollment: Online enrollment station file creation tool for revocation verification
- ✓ Authentication factors: Possession, Knowledge, Digital certificate, CUID, and Challenge/Response(Optional)

Authentication & Security:

- ✓ FIPS 140-2 Verified by InfoGard®
- ✓ Up to 500 Character Length Passwords
- ✓ Identity, Keylogger, and Social Engineering Protection
- ✓ No sharing of logon password
- ✓ Unlimited number of enrollment accounts
- ✓ Works with PIV, PIV-I, CAC, CIV & other contact smartcards
- ✓ Card Removal Actions: User Log Off, Computer Lock Down, Computer Shut Down, Nothing, or Custom
- ✓ Uses the existing credential's PIN
- ✓ Secure Card Data Printout
- ✓ Data Encryption: AES 256, SHA-256
- ✓ The certificate's private key is secured by the smart card
- ✓ Key Diversification
- ✓ Optional Challenge/Response for Card/Workstation Authentication

Compliance:

Self-evaluation for compliance:

- ✓ FIPS 140-3
- ✓ FIPS 201
- ✓ NIST 800-53, 63B, 171
- ✓ X.509 digital certificates
- ✓ PC/SC compliant card readers
- ✓ Penetration testing 5-star rating
- ✓ Passed USAF STIGs review



Access Security:

- ✓ Existing digital certificates
- ✓ Credential PIN
- ✓ Auto-fill Windows Username and Password Logon
- ✓ Auto Launch Windows Applications
- ✓ Windows Applications Logon
- ✓ Auto-fill and submit logon forms
- ✓ Data Storage Encryption Integration
- ✓ Compatible with most X.509 certificates
- ✓ Multi-function credentials
- ✓ No expensive re-badging required
- ✓ No re-certification of government badges
- ✓ No expensive hardware updates or modifications

System Requirements

Stand-alone Computer

Operating System:

Windows® Win11, Win10, Win7

Computer:

Windows 7/11 compatible processor; DirectX 9 or later compatible graphics; 2 GB of RAM; 32 GB Disk Space; and PC/SC compatible smartcard reader.

PC/SC compatible smartcard readers.

Not dependent on a network connection or any outside PKI system components.

© ALL INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED "AS IS" ; Access Smart ASSUMES NO RESPONSIBILITY FOR ITS ACCURACY AND/OR COMPLETENESS. Power LogOn, Access Smart, and Powered by Smartcard Technology are registered trademarks licensed by Access Smart, LLC. All other trademarks and trade names are the properties of their respective companies. In no event will Access Smart be liable for damages arising directly or indirectly from any use of the information contained in this document.