Power LogOn® GOV-COA

for Government (Offline)

COTS Certificate-based Offline MFA Solution

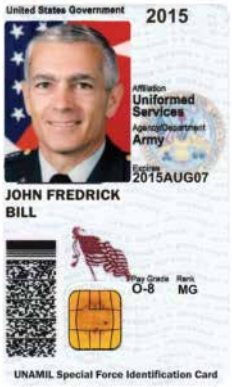
UEI: **X4CCM6HULMX6**
CAGE: **5AU22**
DUNS: **829366660**



Enables Offline Computer Authentication

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

Power LogOn GOV-COA works out-of-the-box with most certificates as found on PIV & CAC credentials to facilitate secure authentication, authorization, and non-repudiation for Windows logon.



Power LogOn GOV-COA works with existing Government Issued Badges

Typical Customer

PIV, CAC 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 GOV-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
CAC: Common Access Card

Ready for Immediate Use

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

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

Environment

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

- ✓ Works with PIV and CAC credentials with valid X509 certificate.
- ✓ Does not require any additional hardware infrastructure.
- ✓ COTS, Self-evaluation to support FIPS 140-3, FIPS 201, HIPAA, CJIS, NIST 800-171 & 800-63B-AAL3, NIST 800-53, STIGs, and others.

Fast, Easy and Affordable

Users don't need multiple credentials.
Power LogOn GOV-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 GOV-COA, enabling card-secured login for those sites.

Administrators can also opt to enroll multiple users at a central workstation. Power LogOn GOV-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 GOV-COA!

Implement cybersecurity identity and access management with Power LogOn

Power LogOn® GOV-COA

Certificate-based Offline Authentication



General Information:

- ✓ Primary Application: Enables MFA digital certificate-protected authentication for offline workstations
- ✓ Secondary Application: Auto-fill Username and Passwords into Windows' logon
- ✓ Operating System: Windows 11 & 10
- ✓ Network: Not dependent on a network connection or any outside PKI system components
- ✓ Enrollment: Online enrollment station file creation tool for revocation verification
- ✓ Key Diversification >> Challenge-response-based encryption key derivation

Authentication & Security:

- ✓ FIPS 140-3 self-evaluated
- ✓ 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 and CAC credentials with valid X.509 certificates
- ✓ Card Removal Actions: User Log Off
- ✓ Uses the existing credential's PIN
- ✓ Secure Card Data Printout
- ✓ Data Encryption: AES-256, SHA-256, and Uses the Microsoft cryptographic services provided by the Windows operating system.
- ✓ The certificate's private key is secured by the smart card
- ✓ Key Diversification
- ✓ Auto-fill Windows Username and Password Logon >> Secure transmission of username and password information to Windows logon process

Specification Review:

Self-evaluations, designed to support:

- ✓ FIPS 140-3, and 201, CJIS,
- ✓ CMMC-L1, DISA STIGs,
- ✓ NIST 800-53, -63B, -171
- ✓ HSPD-12, FAR/DFARS, CISA,
- ✓ FedRAMP, Zero Trust, & HIPAA
- ✓ Penetration testing 5-star rating in 2021
- ✓ USAF accepted our DISA 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® 11 & 10

Computer:
Windows 11 & 10 compatible processor; PC/SC compatible smartcard reader.

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.

4049 Northwood Pl • The Villages • FL • 32163 • Phone: (949) 218-8754