

Power LogOn® GOV-COA

Certificate-based Offline Authentication

Government Version

Certificate-based authentication for
offline computers



Enables Offline Computer Authentication

Power LogOn GOV-COA solution provides secure login authentication for offline (standalone) computers using your existing digital certificate's smartcard ID credential.

Power LogOn GOV-COA works out-of-the-box with most certificates as found on PIV/PIV-I/CAC/ CIV credentials that have been issued a certificate to facilitate secure login to Windows and applications.



Power LogOn COA works with existing certificate ID badge

Typical Customer

PIV/PIV-I/CAC/CIV and PKI credentials are typically used by government entities and private organizations that handle security-sensitive information. Often, these organizations have highly secure divisions that are not allowed to be linked to a network.

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

PIV-I: Personal Identity Verification-Interoperable

CAC: Common Access Card

CIV: Commercial Identity Verification

PKI: Public Key Infrastructure

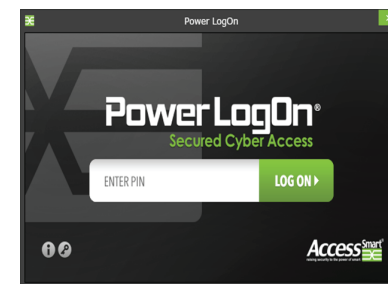
Ready for Immediate Use

- ✓ The user presents their certificate credential to their reader and Power LogOn GOV-COA displays a list of available certificates on user's card.
- ✓ Power LogOn GOV-COA registers the selected certificate for use with the Power LogOn functionality.
- ✓ The user self-enrolls once by entering their identification information and Windows logon credentials.
- ✓ All following user logins, user presents their credential to their reader and enters their PIN.
- ✓ Power LogOn GOV-COA automatically authenticates the user, card, and access rights.

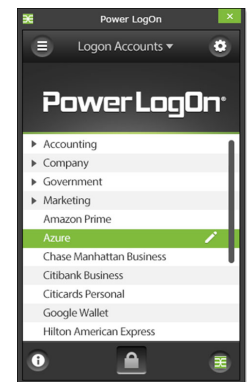
Environment

Ideally suited for computer systems that are isolated from an organization's network and require a high level of security.

- ✓ Works with any credential with a valid X509 certificate.
- ✓ Does not require any PKI infrastructure, other than default Windows settings.
- ✓ FIPS 140-2 verified, FIPS 201, HIPAA, CJIS, NIST 800-171 & 800-63b-AAL3 Compliant



Windows Login Screen



Account Access Screen

Fast, Easy and Affordable

Users don't need multiple credentials. Power LogOn GOV-COA is versatile in that 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!

Power LogOn® GOV-COA

Certificate-based Offline Authentication

Government Version



General Information:

- ✓ **Primary Application:** Enables certificate-based cards for offline workstations Windows and applications login
- ✓ **Secondary Application:** Card-secured logon to computers, and applications, websites, RDP and VPN sessions
- ✓ **Operating System:** Windows 10 (32/64-bit), and Win 7 (32/64)
- ✓ **Network:** Not dependent on a network connection or any outside PKI system components.
- ✓ **Browsers:** Auto launch IE, Firefox, and Chrome browsers
- ✓ **Authentication factors:** Possession, Knowledge, Encryption Keys, CUID, and Challenge/Response

Authentication & Security:

- ✓ FIPS 140-2 Verified by InfoGard®
- ✓ Up to 500 Character Length Passwords
- ✓ Identity, Keylogger, and Social Engineering Protection
- ✓ Phishing and Pharming E-mail Protections
- ✓ Unlimited number of accounts stored in Active Directory
- ✓ Password Generator and Configurator
- ✓ Change Password Reminder
- ✓ Works with PIV, PIV-I, CAC, CIV and other contact smartcards
- ✓ Card Removal Actions: User Log Off, Computer Lock Down, Computer Shut Down, Nothing, or Custom
- ✓ Uses the existing credential's PKI PIN
- ✓ Secure Card Data Printout
- ✓ Card Storage Data Encryption: AES 256, SHA-256
- ✓ The certificate's private key is secured by the smart card
- ✓ Key Diversification
- ✓ Challenge / Response for Card/Server Authentication

Full Featured:

- ✓ FIPS 201 compliant
- ✓ X.509 digital certificates
- ✓ PC/SC compliant card readers
- ✓ Third-Party Software API Integration
- ✓ Multiple Smartcard Compatibility
- ✓ Event logging in records
- ✓ Active Directories supported



Access Security:

- ✓ Windows Bootup Logon
- ✓ Auto Launch Windows Applications
- ✓ Windows Applications Logon
- ✓ Auto User Name & Password Fill and Submit
- ✓ Data Storage Encryption Integration
- ✓ Compatible with most X.509 certificates
- ✓ Multi-function credentials
- ✓ No expensive re-badging required
- ✓ No re-certification of government badges

System Requirements

Stand-alone Computer

Operating System:

Windows® Win10 32/64, Win7 32/64,

Computer:

Pentium® 233 MHz or higher, or compatible;
CD-ROM drive; VGA or higher graphics;
2 GB of RAM; 8 GB Disk Space; and
PC/SC compatible smartcard readers.
Not dependent on a network connection or
any outside PKI system components.



Powered by
Smartcard
Technology®

© 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.