CASE STUDY

DoD Branch Needed Offline, Cert-Based, MFA for Issued CAC ID's

As an IT representative for one of the DoD armed services, we need to secure our offline, stand-alone, Windows-based workstations using our existing CAC ID's and digital certificates.

Because each workstation is offline, we can't validate the card's certificate through our standard online verification. Plus, each workstation must only allow specific, authorized users, and reject everyone else.

Finally, we must be able to add and remove users easily when conditions change.
Access Smart, can you deliver a solution to meet our needs?

Access Smart's Power LogOn Government Certificate-Based Offline Authentication (Gov-COA) solution fulfills this very specific MFA login requirement for the DoD.

Security Challenges

1. **Use existing issued CAC credential, CAC X.509 Certificates, and CAC PINs**
   We can not rebadge our personnel or issue them a second credential.
2. **Secure Windows Password Login with an IT Centralized Password Manager**
   Each workstation must have strong, unique passwords that the user doesn't know, type, or manage.
3. **Certificate validation done offline**
   An independent certificate validation is required on each offline workstation.
4. **Manage the Certificate Authentication on each workstation**
   IT needs to securely and easily add and remove user's certificates from each workstation.
5. **SEWP Contractors**
   We can only purchase products from DoD approved SEWP Contractors.

The Solution

Already in use: **DoD** CAC IDs, CAC X.509 Certificates, CAC PINs, Offline Windows workstations

Purchase: Power LogOn Gov-COA software that includes both the enrollment software and logon manager, and Power LogOn COA SaaS licensing. No new or replacement hardware is required.

Here are some key Power LogOn Gov-COA highlights that solved their challenges:

1. **Use existing infrastructure**

   Power LogOn is compliant with DoD's smart card infrastructure specification (FIPS 201). Since no new card data is added or existing card data is modified, no CAC re-issuance or re-certification is required.

2. **Government Security Specifications Compliance**

   Power LogOn is compliant with security specifications like: NIST 800-53, 800-63, 800-171, FIPS 140-2 and FIPS 201. Next, Access Smart performed a self-assessment against STIG v5, and found no open Category 1 items. Finally, an ethical hacking firm, Secure Network Technologies, evaluated Power LogOn Gov-COA and awarded it five out of five cybersecurity stars.

3. **True Multi-Factor Authentication**

   The user inserts their CAC ID into an existing CAC smart card reader, and then types their pin. Next, Power LogOn validates the card's certificate against the workstation's enrolled certificates. If approved, the secure Windows login password is automatically filled in and the user is logged on to the workstation. All without the user knowing, or typing, any passwords. This is true MFA because it combines something they have with something they know.

4. **SEWP Contractors**

   Access Smart has over 20 approved SEWP contractors who are authorized to bid and sell Power LogOn Gov-COA.

Customer Feedback

Power LogOn Gov-COA met all our requirements. What we like about Access Smart was how responsive they were to our wants. We had custom requirements that they were able to adapt for us quickly. We recommend this solution to other DoD branches who need CAC enabled MFA security for offline workstations.

Power LogOn Gov-COA Evaluation Kit

Access Smart offers Power LogOn Gov-COA evaluation kits through our approved SEWP resellers. A commercial version of Power LogOn COA is also available. Please contact Access Smart at sales@access-smart.com, or your MSP, to get more information.