



ASTRO 25

CAC / PIV MULTI-FACTOR AUTHENTICATION

Identity management and authentication for computers and mobile devices is an ever-present concern for US Federal Government agencies.

US FEDERAL GOVERNMENT MANDATE

The US Federal Government has mandated Homeland Security Presidential Directive 12 ([HSPD#12](#)) compliance as a means to enhance security for federal buildings and information systems. The directive establishes a government-wide standard for secure and reliable forms of identification issued to its employees and contractors. Government-issued smart cards support the directive and enforce Multi-Factor Authentication (MFA) to network elements for privileged and non-privileged accounts.

The smart card uses a 2-Factor Authentication mechanism by combining a credential (something you have) with a PIN (something you know). It can be used by many Commercial Off-the-shelf (COTS) network operating systems and applications that use Public Key Infrastructure (PKI) certificates for authentication. The PKI-based user authentication feature utilizes smart card authentication certificates to perform digital signature / encryption operations through the private key associated with the certificate. This means the system performing the authentication can verify the signature while also validating the certificate itself.

CAC (Common Access Card) and PIV (Personal Identity Verification) cards are common security tokens used in the federal government space.

SAFEGUARD YOUR ASTRO 25 RADIO SYSTEM

CAC / PIV authentication is available on ASTRO® 25 radio systems with release 7.17.3 or selected releases in the future, enabling smart card authentication for the following ASTRO 25 components: Windows (physical / virtual), RHEL (virtual), Hypervisor (ESXi virtual servers) and Embedded OS platform-based network devices (routers, firewalls, switches, site products, etc.).

CAC / PIV adds security to your ASTRO 25 radio system, providing secure data access to computers at multiple classification levels. Built-in functionality blocks access to the infrastructure when the user employs an invalid smart card or smart card that is not provisioned for access to a particular system. A centralized Active Directory tracks CAC / PIV authorization attempts, provides for efficient monitoring of new equipment, certificate expiry and login failures.

Flexible service packages available for CAC / PIV allow you to manage risk and responsibility of your network performance and security.



MISSION CRITICAL SECURITY SOLUTIONS

CAC / PIV authorization utilizes a FIPS 140-2 Level 3 Hardware Security Module (HSM), which offers the highest level of security and performance for protected key storage, high-speed signature and hardware key generation. HSM backup devices offer secure disaster recovery of the most important keys in the system.

SPANNING THE MISSION-CRITICAL ECOSYSTEM

CAC / PIV authentication and authorization is one element of our total security story. To ensure your system is fully secure, look to Motorola Solutions to provide a holistic set of capabilities that can cater to all your needs. Today's environment demands a range of uniquely delivered products and services that span the entire mission-critical ecosystem — from infrastructure and devices to software and video.

MANAGED AND SUPPORT SERVICES

CAC / PIV product is covered under Essential Plus, Advanced Plus and A La Carte Services. CAC / PIV SUS / RSUS is a prerequisite for all CAC / PIV implementations. CAC / PIV SUA will cover all the yearly CAC / PIV software renewals and hardware support of critical components.

Essential Plus

- 24/7/365 Remote Technical Support
- Network Hardware Repair
- Standard On-site Infrastructure Response with Dispatch
- Annual Preventive Maintenance
- Self-Installed Security Patches (SUS)
- CAC / PIV Software Update Service**
- CAC / PIV SUA**

Advanced Plus

- 24/7/365 Remote Technical Support
- Network Hardware Repair
- Standard On-site Infrastructure Response with Dispatch
- Annual Preventive Maintenance
- Network Event Monitoring
- Self-Installed Security Patches (SUS)
- Remote Security Patches (RSUS)
- Network Updates / SUA
- Security Monitoring*
- CAC / PIV Software Update Service**
- CAC / PIV SUA**

A La Carte Services

- 24/7/365 Remote Technical Support
- Network Hardware Repair
- Standard On-site Infrastructure Response with Dispatch
- Annual Preventive Maintenance
- Network Event Monitoring
- Self-Installed Security Patches (SUS)
- Remote Security Patches (RSUS)
- Network Updates / System Upgrade Agreement (SUA)
- CAC / PIV Software Update Service**
- CAC / PIV SUA**

*Optional | **Mandatory

Learn more at
www.motorolasolutions.com/astro-security



MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. motorolasolutions.com

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2020 Motorola Solutions, Inc. All rights reserved. 07-2020



COMPLIANCE

- Compliant with FIPS 201, AAL 2 / 3
- Common criteria (EAL4+), GSA and DoD JITC certified
- GSA-approved product hardware / middleware software
- Encryption key storage in FIPS 140-2 Level 3 HSM hardware

