ASTRO

Smart Card Multi–Factor Authentication

Identity management and authentication for computers and mobile devices is an ever–present concern.

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 MFA solution uses a two-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 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 radio system

Smart card multi-factor authentication is available on ASTRO® radio systems with release A2022.HS or selected releases in the future, enabling smart card authentication for the following ASTRO system components: Windows (physical / virtual), RHEL (virtual), Hypervisor (ESXi virtual servers) and embedded OS platform-based network devices such as routers, firewalls, switches, and site products.

Smart card MFA adds security to your ASTRO 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. Smart card MFA utilizes agency provided PKI services (e.g. certificates, CRLs/OCSP) to authenticate the users in the ASTRO radio system.

Spanning the mission–critical ecosystem

Smart card multi-factor 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.

Compliance

- Compliant with FIPS 201, AAL 2 / 3
- Compliant with NIST: SP 800-53, SP 800-73
- GSA-approved product hardware / middleware software

Learn more, visit:
www.motorolasolutions.com/astro-security

MOTOROLA SOLUTIONS

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