ASTRO SYSTEMS AUTHENTICATION SOLUTIONS

PROTECTING AGAINST DISRUPTION TO YOUR CRITICAL COMMUNICATIONS

MOTOROLA SOLUTIONS

PROTECTING AGAINST CLONED OR STOLEN RADIOS

One of the most important challenges ASTRO system managers face — and unfortunately one of the most common — is unauthorized radios which cannot be verified before gaining access to the system. Whether a radio has been cloned, stolen, or simply lost by the user, restricting network traffic to authorized devices only is critical. ASTRO systems include several authentication and encryption tools to help you in this effort.

Radio Authentication uses a unique authentication key assigned to each radio that is also stored in the authentication center (AuC). The authentication key cannot be read from the radio and then cloned into another device. The correct key must be present in order for the radio to gain access to the ASTRO system. This provides an additional level of control for system owners and prevents unauthorized radios from joining the system.

Encryption Key Management is critical to protecting the integrity of communications on the ASTRO system and overall cyber resiliency. Our secure management ecosystem ensures your radio communications are secured with encryption keys that can be update over-the-air (OTAR). This rekeying option provides the convenience of not having users bring their devices into the shop for manual rekeying, while saving the associated costs.

RADIO AUTHENTICATION: OPERATIONAL FLEXIBILITY

The challenge and response authentication procedure, between the system and a P25 radio, conforms to the authentication service as defined by the P25 Authentication standard TIA 102.AACE and ISSI 8000/CSSI 8000 feature. Each subscriber radio has a different authentication key with session information to prevent exposure to the authentication key. The systems administrator has the flexibility to gradually implement Radio Authentication, using one of the following modes:

- **Selective Authentication** — The system authenticates only radios that have been set up for system access verification
- **Authentication Required** — Once all radios have been programmed with an authentication key, the system can be set up for full authentication
- **No Authentication** — Ability to disable authentication entirely if required

With the ISSI 8000/CSSI 8000 feature, radio authentication can be applied to foreign subscribers (those subscribers "foreign" to your ASTRO system) and the System will support authentication of foreign subscribers. Radio's automatically roam to a foreign system while maintaining its home ID and authenticates with its home system.

AUTHENTICATION

The subscriber will be authenticated on power-up registration. If the subscriber fails the authentication challenge, it will be unable to register on the system and therefore unable to transmit or receive on the system.

RADIO AUTHENTICATION: SOLUTION COMPONENTS

RADIO AUTHENTICATION CENTER

The Radio Authentication Center is a central database that stores the authentication keys for all radios in the system.

KEY VARIABLE LOADER - 5000 (KVL)

The KVL 5000 allows programmers to generate, transport, and fill encryption keys (voice and data), securely and efficiently into secure communication products thereby enabling encrypted communications. Packaged in an easy to use one-handed design with an intuitive UI, the KVL 5000 integrates with Motorola's Key Management Facility (KMF) which provisions radios via Over The Air Rekeying (OTAR). The purpose-built KVL 5000 delivers a quick start and response for easy and efficient key loading on a remote basis - without interrupting the rest of their workflow. The only keyloader that can protect keys with hardware protected keystore, the KVL 5000 provides users with the highest level of secure programming.

AUTHENTICATION KEY

A unique 128 bit AES key, defined by the P25 standard, is required for the authentication key. It is generated by the KVL 5000 and stored in the AuC. To maximize security, the authentication key is never sent over the air and it cannot be read from the radio.

SUMMARY

Radio Authentication allows administrators to protect against potential threats such as cloned or unauthorized radios by restricting system access. A cloned or illegitimate radio can interrupt or listen in on sensitive or classified information which could jeopardize mission-critical communications.

BENEFITS

- Prevent illegal use of cloned radios
- Protect the integrity of the system
- APX family and most XTL/XTS radios are supported
- Radios that access multiple ASTRO systems can authenticate with multiple systems
- Compliant with the P25 TIA102.AACE Link Layer Authentication standard
- Enables Zero Trust Architecture (ZTA)

CORE AUTHENTICATION: ACCESS CONTROL AND DATA INTEGRITY

ACCESS CONTROL

Two-Factor Authentication (2FA optional feature)
Two-factor authentication requires a second form of identity verification before a user is able to log into ASTRO applications or system management tools.

Centralized Authentication: Active Directory (AD) & Remote Authorization Dial-In User Services (RADIUS)
Centralized Authentication is built upon the Active Directory (AD) and Remote Authorization Dial-In User Services (RADIUS) and provides one control point for identification, authentication, and authorization services. The centralized authority defines what functions and operations users can perform, and on what devices.Centralized Authentication also addresses identity management through a centralized user credentials database which enables the customer to manage system access and perform audits.

Centralized Authentication Subsystems
A Centralized Authentication subsystem consists of a group of computers, which uses or offers services to organizational units for the purpose of administrative and policy management. Each element within the system is differentiated based on administrative authority, security policy, configuration, or other operational considerations. Centralized authentication also supports the following functionality:

- Consolidated, consistent and maintainable identity management across diverse platforms and Operating Systems (OS)
- Access enforcement through a central location for administration and assignment of authority
- Single sign-on (SSO) where users can gain access to the operating system and multiple applications using the same account

CORE DATA INTEGRITY

The **Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP)** authentication options provide authentication between peer routers by means of shared Secure Shell keys (SSH). SSH protects the integrity of the keys during installation and automated routine scripts, with one shared key per protocol (OSPF and BGP). If customers require unique keys for the OSPF areas or BGP peers, this may be achieved by manual key configuration on the affected routers. Once the OSPF and BGP Authentication options have been configured, the routers authenticate their peers. Customers are encouraged to change keys periodically.

To learn more, visit:
www.motorolasolutions.com/astrosystem/authenticationsolution

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. © 2022 Motorola Solutions, Inc. All rights reserved. 11-2022 [JP6]