ASTRO RADIO AUTHENTICATION

PROTECT AGAINST UNAUTHORIZED RADIO ACCESS

OVERVIEW

One of the most important challenges radio system managers face is keeping unauthorized radios off their P25 radio system. Users with cloned or illegally programmed radios can disrupt critical communications, putting the safety of first responders and the public at risk. With Radio Authentication, you can prevent illegitimate radio units from accessing your ASTRO® system.

Radio Authentication provides a mechanism which requires the radio to prove that it is genuine before it is allowed to join the radio system. Verification is done by matching a unique authentication key stored in each radio to a database in the Authentication Center (AuC). The correct key must be present in order for the radio to gain access to the system. Authentication keys can be loaded into the radio via a handheld Key Variable Loader (KVL) and then uploaded to the AuC. Once loaded, the key cannot be read from the radio or cloned into another device.

FEATURES

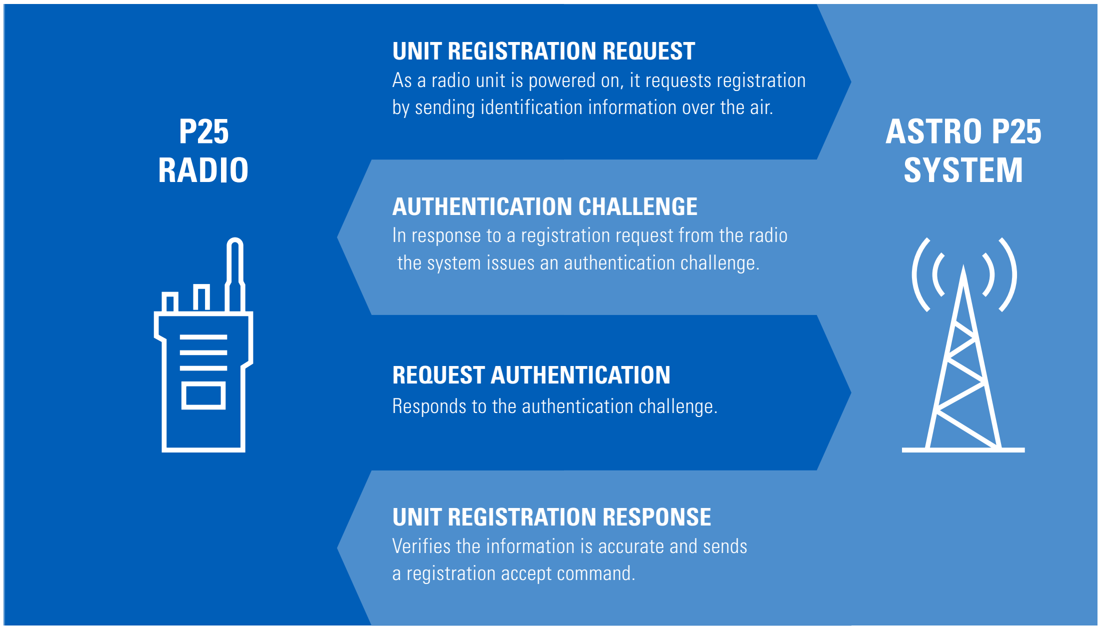
- P25 standards compliant
- Foreign and roaming radio authentication
- ASTRO multi-zone and DSR compatible
- System-wide controls
- Digital Vehicular Repeater System (DVRS) support
- FIPS 140-3 compliant Key Variable Loader (KVL)

BENEFITS

- Protect against cloned and illegal radios
- Preserve system resources for valid radios
- Prevent disruption of critical communication
- Manage authentication rollout to your schedule
- Enable Zero Trust Architecture (ZTA)

SOLUTION COMPONENTS

- Authentication Center (AuC) - Provides centralized key storage and management.
- Key Variable Loader (KVL) - Generates and loads authentication keys (K) into radios. Uploads K-SUID pairs into the AuC.
- ASTRO Zone Controller (ZC) - Enforces radio authentication for enabled units.



P25 RADIO

UNIT REGISTRATION REQUEST
As a radio unit is powered on, it requests registration by sending identification information over the air.

AUTHENTICATION CHALLENGE
In response to a registration request from the radio the system issues an authentication challenge.

REQUEST AUTHENTICATION
Responds to the authentication challenge.

UNIT REGISTRATION RESPONSE
Verifies the information is accurate and sends a registration accept command.

ASTRO P25 SYSTEM

AUTHENTICATION

Radio authentication is inserted into the unit registration process. If the radio fails to authenticate, it will not complete the unit registration process and will be unable to access the system.

HOW IT WORKS

Using AES-128 bit encryption, the KVL generates a random authentication key (K) for each radio (SUID) and programs the keys into the radios. The KVL will upload the K-SUID pairs into the Authentication Center (AuC). The KVL operator never sees a randomly created K. Although a K can be manually entered, for security reasons it should be avoided if possible.

During the radio registration process, the radio unit must demonstrate in its response to the authentication challenge that it possesses a matching K to the SUID. If the radio fails to authenticate, it will not complete the registration process and will be unable to transmit or receive on the system. This challenge and response authentication procedure conforms to the authentication service as defined by the P25 TIA 102.AACE Link Layer Authentication standard.

The authentication procedure can be supported during P25 interoperability over our Critical Connect interoperability solution. Radios from another system can authenticate using their home ID while roaming on your system. Likewise, radios homed on your system can authenticate while roaming on other systems.

System-wide controls allow the administrator to set the authentication mode. These modes enable you to gradually deploy authentication keys across your radio fleet as well as resolve any issues without having to disable authentication for all radios. Modes include:

- Authentication Disabled - No authentication occurs on the system.
- Authentication Enabled - Only radios provisioned with an authentication key must authenticate. This mode is useful if your entire fleet has not yet been provisioned with authentication keys.
- Authentication Required - All radios must be authenticated. Typically set to this mode after all radios have been programmed with an authentication key.

COMPATIBILITY

- ASTRO trunked radio systems 7.9 or later[1]
- Motorola Solutions APX mobile and portable radios
- Most Motorola Solutions XTL mobile and XTS portable radios
- KVL 4000 and KVL 5000

[1] ASTRO Express systems are not supported

For more information, visit motorolasolutions.com/astro-security.

MOTOROLA SOLUTIONS

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