CONTINUITY OF OPERATIONS

ASTRO® 25 SYSTEMS RADIO AUTHENTICATION SOLUTION

ASTRO 25 voice and data systems provide Project 25 standards-based mission critical communications for public safety agencies around the world. Since first responders rely on these systems, many features are built into the system to protect the integrity of the communications from over-the-air encryption to network security to programs that verify and control devices on the system.

One of the key issues a system manager must address is minimizing the use of unauthorized radios, whether they have been lost or stolen, or have been cloned illegitimately.

The Radio Authentication solution provides an extra level of verification, every time a radio registers to the system.

Over our years of serving public safety, we have built many different tools into the ASTRO 25 system to support and maintain continuity of operations.

PROTECT RESOURCES

The most common method of protection involves closing the system so that only the radios provisioned on the system database have access. An advanced system key can also be used to prevent unauthorized programming of ASTRO 25 radios; the system manager defines who is authorized to program radio IDs into subscribers.

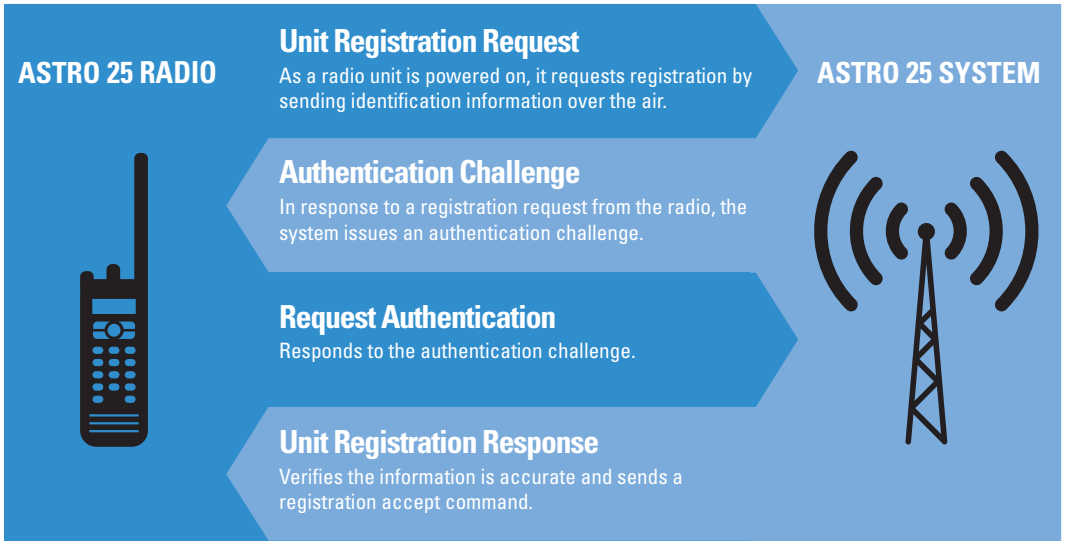
SECURE INFORMATION IN TRANSIT

Protect over-the-air conversations from unwanted eavesdropping using software or hardware encryption.

CONTROL NETWORK ACCESS

In addition to closing a system, Radio Authentication provides an additional layer of protection. Any unauthorized radio, without the correct key, will be denied access to the system and an alert will be sent to the system manager.

PROJECT 25 STANDARDS-BASED
Radio authentication utilizes the Project 25 TIA102.AACE Link Layer Authentication standard. It is over-the-air compatible with other P25 manufacturer's equipment that incorporates the Link Layer standard.



AUTHENTICATION

The subscriber will be authenticated on power-up registration and commanded 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.

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 TIA102.AACE. Each subscriber has a different authentication key with session authentication information passed around the system to prevent exposure to the authentication key. The systems administrator has the flexibility to gradually implement Radio Authentication, which is important for large systems where it takes more time to implement. One of the following modes can be chosen.

- Selective Authentication – the system authenticates only radios that have been set up for authentication.
- 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.

BENEFITS

- Restrict unauthorized system access
- Prevent illegal use of cloned radios
- Protect the integrity of 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. The Radio Authentication client can be deployed on an existing network management PC or a dedicated PC.

KEY VARIABLE LOADER (KVL)

The KVL 4000 generates a unique authentication key for each radio and synchronizes the authentication key information with the ASTRO 25 system remotely over a secure Virtual Private Network (VPN) connection without requiring the operator to travel to the ASTRO 25 core location. The KVL 4000 device can also be used to load voice encryption keys into the radio using a different operation.

AUTHENTICATION KEY

A unique 128 bit AES key, defined by the Project 25 standard, is required for the authentication key. It is generated by the KVL 4000 and stored in the Authentication Center (AuC). To maximize integrity, the authentication key is never sent over the air and it cannot be read from the radio.

IMPLEMENTATION CONSIDERATIONS

The system must be at a minimum ASTRO 25 Release 7.9 with the Radio Authentication feature purchased at the system and individual radios. Many existing XTL and XTS radios, along with the APX family of radios, can be software upgraded to enable the Radio Authentication feature, allowing systems with large fleets to take advantage of this solution. In addition, radios that access multiple ASTRO 25 systems can authenticate with multiple systems if the feature is available on each system.

Motorola Solutions, Inc. 1301 E. Algonquin Road, Schaumburg, Illinois 60196 U.S.A. **motorola.com/ASTRO25**

MOTOROLA