



# Security Triad for P25 LMR: Encryption, Access, Cyber IDs

Presented by:  
PTIG - The Project 25 Technology Interest Group  
[www.project25.org](http://www.project25.org)

# Agenda



<b>Steve Nichols, PTIG</b>	<b>Introductions, Agenda, PTIG Members, Education Resources, P25 Benefits and Eco-system</b>
<b>Jeremy Elder, L3Harris</b>	<b>P25 Security Services Triad overview. Link Layer Encryption transition.</b>
<b>Scott Wright, State of Connecticut</b>	<b>Multi Agency deployment of AES Voice and Data Security in the State of Connecticut. Agency benefits and best practices for sharing.</b>
<b>Hermina Koshinski, Commonwealth of Pennsylvania</b>	<b>P25 Authentication requirements for P25 in Pennsylvania. Agency benefits and lessons learned.</b>



# Who is PTIG?

- **The Project 25 Technology Interest Group (PTIG)** is a group of individuals and organizations who share the mutual interest of advancing the development, deployment, and applications of Project 25 industry standards.
- PTIG offers a P25 information forum for users and manufacturers with education and training on Project 25 Standards and their applications.
- PTIG members include:
  - **Radio communications subject matter experts**
  - **Public safety and Government professionals**
  - **Equipment manufacturers and LMR engineers**
  - **Service providers and consultants.**



[www.project25.org](http://www.project25.org)



THE LATEST NEWS

- > New Whitepaper:  
Patching and  
Dynamic  
Regrouping over

## Welcome to the Project 25 Technology Interest Group

The Project 25 Technology Interest Group (PTIG) brings you this web site to provide information on all topics concerning Project 25.

Please register on the site for access to additional information. If you previously registered prior to

List of  
P25  
Trunking  
Systems

P25  
Frequently

P25 ISSI/CSSI  
Interoperability

List of P25  
Conventional  
Systems



## P25 Resources available on [www.project25.org](http://www.project25.org)

- P25 System Lists: Trunking and Conventional
- P25 Latest Standards Update Report & List of Standards Documents
- Links to P25 Libraries of Special Interest
  - P25 Security and Encryption Links to DHS Library
  - ISSI/CSSI Interoperability Links to DHS Library and Informal Testing Data
  - P25 CAP Testing Program: Links to DHS CAP approved equipment Lists.
- P25 New Products and Services
- PTIG Conference Panel Presentations PPT Slides
- P25 Frequently Asked Questions (FAQ)
- PTIG Commercial Member listing Primary P25 Contact information and company Website link

# Benefits of Project 25

*P25 is a well established Suite of Standards  
with a User Driven, Evolving Technology*



- **A Public Safety Grade Technology** with High Availability through Redundant and Resilient Configurations in VHF, UHF, 700/800/900 MHz.
- **Direct Mode Communications** when Infrastructure is not available
- **Enabling Interoperability** for Multi Agency Sharing of Voice/Data/Location
- **Secure** AES 256 bit Encrypted Communications
- **Ongoing Standards Development** and upgrades with forward and backward compatibility based on User Priorities
- **Large Nationwide Installed Base of P25 Systems:** 3600+including 42+ State-wide.
- **P25 Sharing = Cost Savings & Improved Coverage for Users**
- **Multi-Vendor Sourcing** from 40 Project 25 Product and Service providers

# Founding Members



**L3HARRIS**<sup>®</sup>  
FAST. FORWARD.



**MOTOROLA**  
SOLUTIONS



**taii**  
communications

**ZETRON**

# Sustaining Members



**CTA**

**ICOM**<sup>®</sup>



**etherstack**  
wireless software

EF Johnson Technologies, Inc.  
a **JVCKENWOOD** Company

**JVCKENWOOD**

# Project 25 Technology Interest Group



## Corporate and Professional Members





# P25 Security Triad

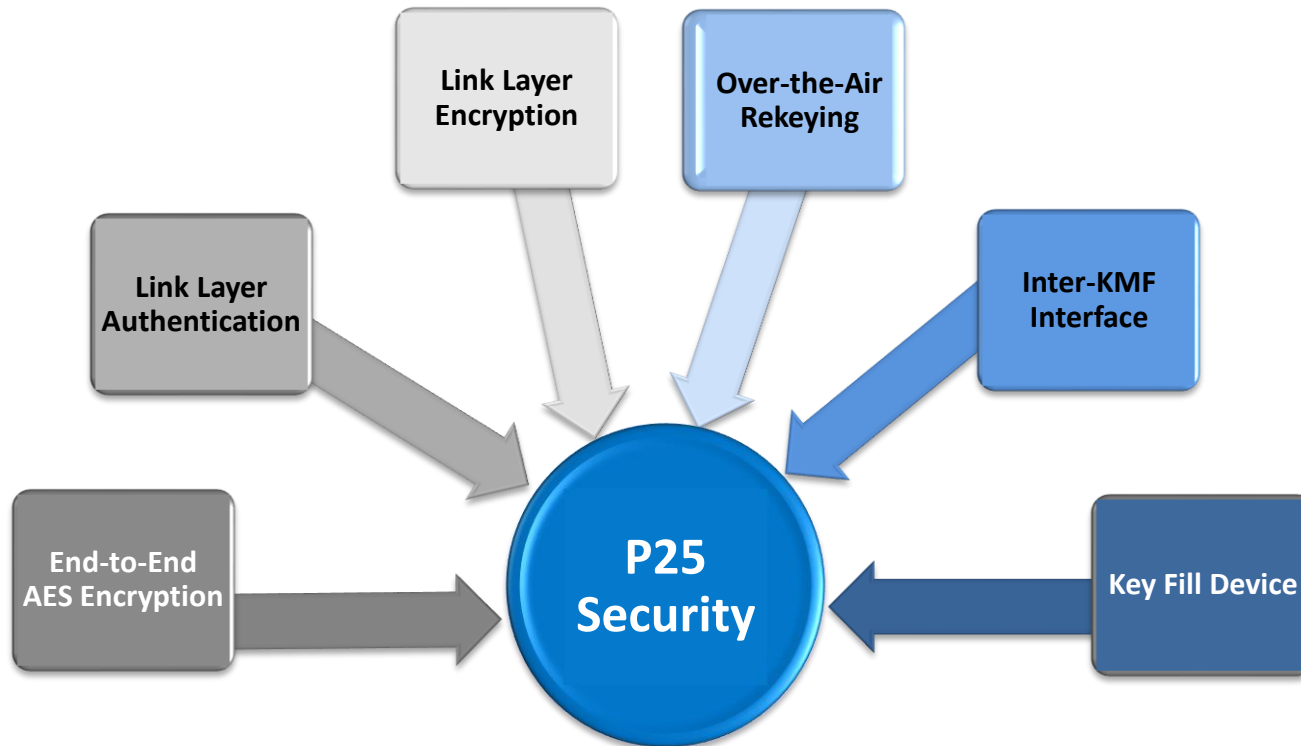
## P25 Security Services Overview and Link Layer Encryption Transition.

**Jeremy Elder**

Director of Product Experience Technology for L3Harris  
Technologies, Inc.

# P25 Security Concepts

P25 offers **Defense-in-depth** through multiple layers of security services



Security Service	User Benefit/Protection	Avail?
End-to-end AES encryption	Secure, interoperable exchange of voice and data	✓
Link Layer Authentication (LLA)	Authenticate subscriber units (SUs) and Infrastructure to ensure they are legitimate	✓
Link Layer Encryption (LLE)	Protect over-the-air signaling from interception	Not yet
Over-the-air-Rekeying (OTAR)	Stage new key material over P25 common air interface	✓
Inter-KMF-Interface (IKI)	Transfer key material online or offline between separate systems/KMFs	✓
Key Fill Device (KFD)	Transfer key material securely from portable key fill to P25 SU	✓

# Encrypted Voice and Data (Security on P25)

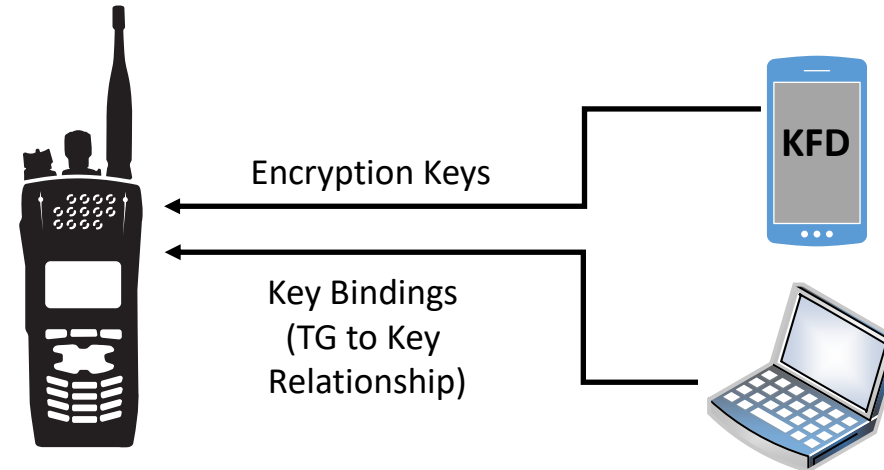


- Voice and data can be encrypted to enable secure operation
- Encryption can be activated via a switch or “bound” to a particular talkgroup
- Successful communication requires use of same Algorithm and Key
  - AES-256 (Advanced Encryption Standard) is the ONLY P25 standardized algorithm
  - DES is deprecated / other proprietary solutions are less secure and not interoperable
  - Single key and multi-key implementations available for subscribers
- Standardized options for manual keyloading and over the air rekeying (OTAR) – **next slide**

# P25 Key Management Techniques

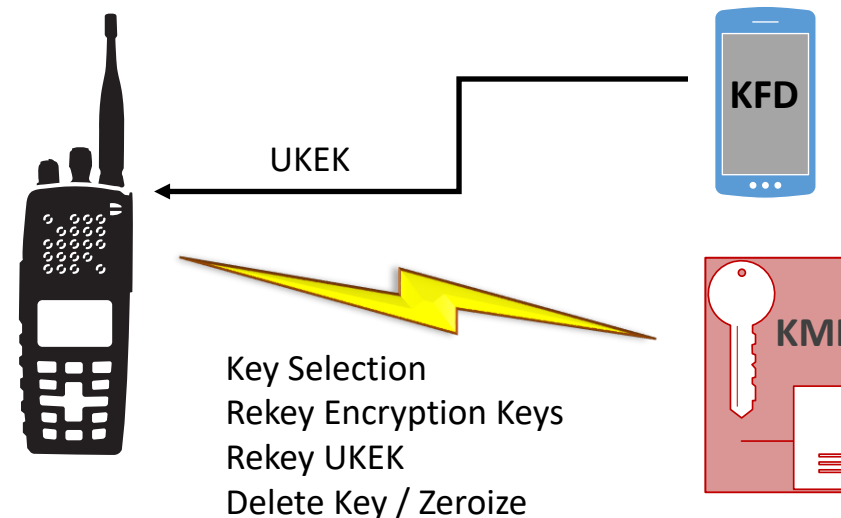
## Key Fill Device (Manual Keying)

- Key Bindings are established in codeplug / radio configuration
- Compromised radio compromises keys; requires rekeying of fleet



## Key Management Facility (OTAR)

- Unique Key Encryption Key (UKEK) initially loaded using KFD
- Key Management Facility (KMF) located in a secure physical location
- Keys rekeyed securely over the air from KMF
- Message Authentication and Encryption employed in message signaling



# Project 25 Inter-Key Management Facility Interface (IKI)



## What is the IKI?

**A:** Interface between multiple P25 Key Management Facilities (KMFs), regardless of manufacturer.

## Is there a standard for the IKI?

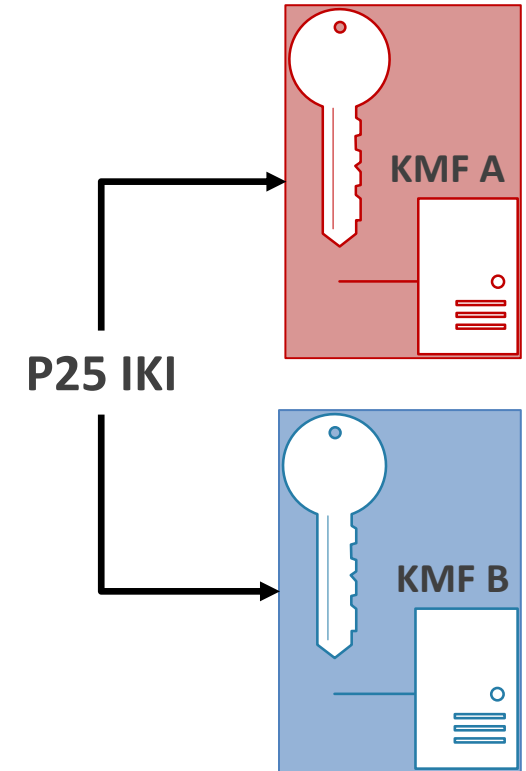
**A:** Yes – the “**Project 25 KMF-to-KMF Interface**” standardized the IKI. A revision with Improved Interoperability for encryption key sharing between Key Management Facilities (KMFs) was published in July 2024

## Does the P25 IKI require an IP network connection between KMFs?

**A:** Not necessarily... the P25 IKI supports an offline (file-based) transfer of keys and an online transfer of keys over a network.

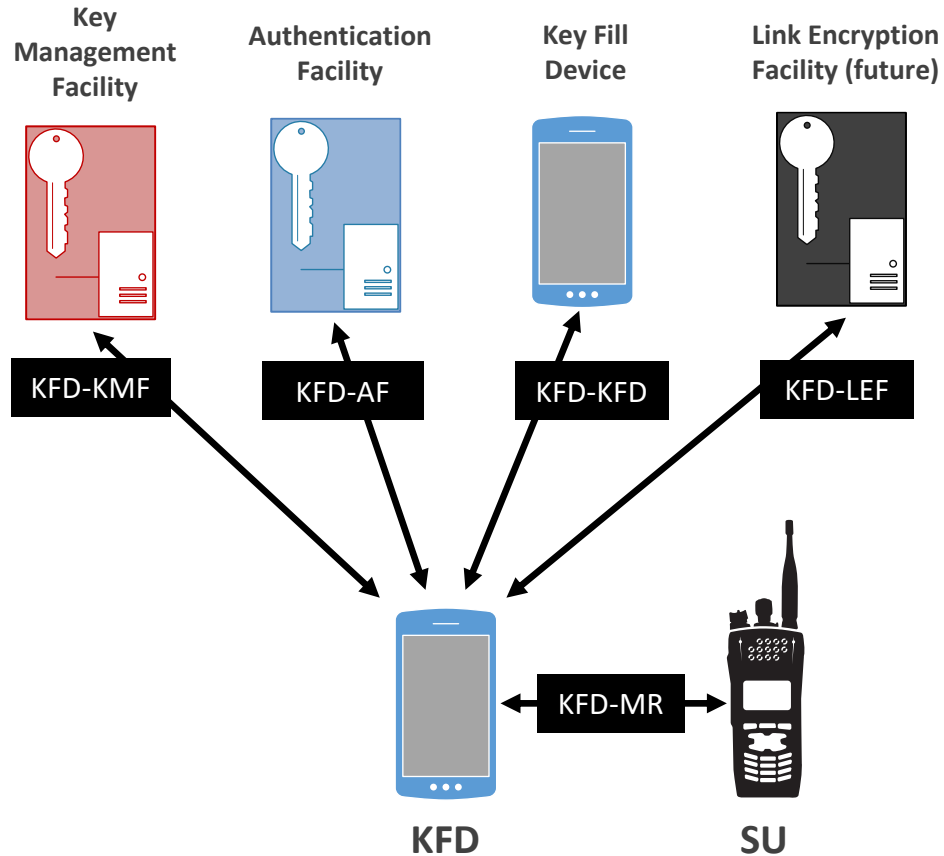
## Why are we just now hearing about the P25 IKI?

**A:** Manufacturers are beginning to field IKI solutions based on increased customer demand for a secure method to share keys between systems.



**KMFs that support the IKI are entering the market and manufacturers beginning to test implementations in the field.**

# Key Fill Device Enhancement



## Update to enhance P25 key sharing interoperability:

- Adds new standardized interfaces between a P25 Key Fill Device and the following P25 services:

Key Management Facility (KMF)	Authentication Facility (AF)
Another Key Fill Device (KFD)	Link Encryption Facility (LEF) - future

- Includes unassigned keys – to ease sharing interop keys
- Improves key loading for P25 Subscribers by adding:
  - Standardized USB interface
  - Forwarding Key Management Messages (KMMs) from KMF & AF

Standard on-track for publication this year. New products typically follow 12-18 months after publication.

# Link Layer Encryption (LLE) Solution

## LLE will be COMPREHENSIVE

Draft Standard designed to “protect” the over-the-air signaling in all P25 configurations: direct mode and systems; conventional and trunking; traffic channels and control channels



P25C Direct Mode



P25 Trunked and P25Conventional

## LLE will be SECURE

Draft Standard based on sound security principles addressing the three components of the security triad



LLE standard completion is not expected before 2026 – Equipment availability is usually 12-18 months after publication

# LLE Transition Scenarios

The proposed new standard provides compatibility between RFSS and previously deployed radios that do not support LLE

- Interoperability with legacy radios
- Mix of LLE enabled/not enabled SU
- Multiple transition scenarios possible



## Example Transition Approaches

- All SUs LLE enabled from start – for example greenfield implementation
- Agency-by-Agency migration to LLE as SU equipment gets upgraded
- Regional migration to LLE as all SU equipment in an area gets upgraded



**THANK YOU!**



[www.l3harris.com](http://www.l3harris.com)

**Jeremy Elder**

Director of Product Experience Technology for L3Harris  
Technologies, Inc.

[Jeremy.Elder@L3Harris.com](mailto:Jeremy.Elder@L3Harris.com)



# Connecticut Land Mobile Radio Network



Scott Wright  
Sr. Telecommunications Engineer II



# State of Connecticut – P25 System Statistics

2 Zones – each with both on site and geo redundant servers

Frequencies: 150+

IP Consoles: 263

Subscriber units: approximately 35,000

2024 System Statistics:

PTT's: 106,893,019

Seconds: 624,170,072.4

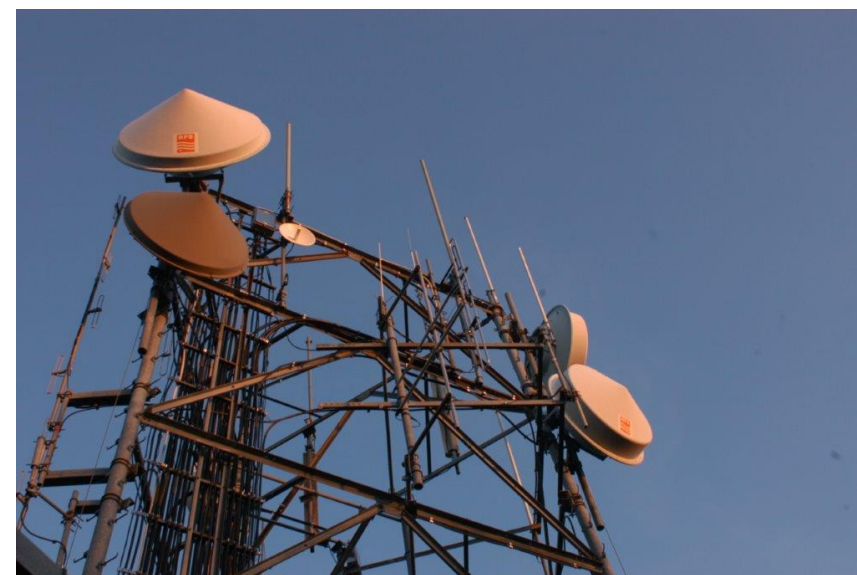
Connectivity:

Private/Shared Microwave

State Fiber Optic

Leased circuits

Satellite/LTE/VPN if necessary





# State of Connecticut – CLMRN

## P25 Encryption – Connecticut's Plan

Interoperable encryption IS possible

Designed from the ground up for interoperability

Common Key Management Facility

Coordinated encryption plan

Statewide OTAR capability

Access to NLECC interoperable encryption

# Encryption



*Best Practices for Encryption in P25 Public Safety Land Mobile Radio Systems*

September 2016



[https://www.cisa.gov/sites/default/files/publications/20160830%20Best%20Practices%20for%20Encryption\\_Final%20Draft508\\_0.pdf](https://www.cisa.gov/sites/default/files/publications/20160830%20Best%20Practices%20for%20Encryption_Final%20Draft508_0.pdf)

# P25 Resource Sharing



## Value in Collaboration

- Statewide, Regional, Multi-State, Federal, etc.

## Value in Planning

- Build appropriately from the start
- All inclusive strategies and response

## Cost

- Chance of reducing parallel costs
- Reduced Operations and Maintenance Costs
- Affordable for more users

## Capacity

- Pooled opportunities equals appropriate resources



# P25 Feds and Encrypted Interoperability

## Federal agencies/departments

- Are obligated to seek FISMA compliance
- In the case of Encryption that means FIPS
  - That means it cannot be DES, or RC4 variants
- So – to promote encrypted interoperability...
  - Please consider using AES
  - Note CAP AP/DHS rules on non-standard encryption
  - Ponder how long DES may remain in P25 Standard?
  - Encrypted Interop with Feds the justification you need?



# National SLN Assignments

SLN	Algorithm	Use	SLN Name	Crypto Period (Annual key changes are completed on the first working Monday of October)
1	DES	Public Safety Interoperable	ALL IO D	Annual
2	DES	Federal Interoperable	FED IO D	Annual
3	AES	Public Safety Interoperable	ALL IO A	Annual
4	AES	Federal Interoperable	FED IO A	Annual
5	DES	National Law Enforcement State and Local Interoperable DES	NLE IO D	Static
6	AES	National Law Enforcement State and Local Interoperable AES	NLE IO A	Static
7	AES	US – Canadian Fed Law Enforcement Interoperability	FED CAN	Static
8	AES	US – Canadian PS Interoperability	USCAN PS	Static
9	DES	National Tactical Event	NTAC D	Single Event Use – Not to exceed 30 Days
10	AES	National Tactical Event	NTAC A	Single Event Use – Not to exceed 30 Days
11	DES	Multiple Public Safety Disciplines	PS IO D	Static
12	AES	Multiple Public Safety Disciplines	PS IO A	Static
13	DES	National Fire/EMS/Rescue	NFER D	Static
14	AES	National Fire/EMS/Rescue	NFER A	Static
15	DES	National Task Force Operations	FED TF D	One time use as needed for Special OPS
16	AES	National Task Force Operations	FED TF A	One time use as needed for Special OPS
17	DES	National Law Enforcement Task Force (one time only operation)	NLE TF D	One time use as needed for Special OPS
18	AES	National Law Enforcement Task Force (one time only operation)	NLE TF A	One time use as needed for Special OPS
19	AES	Federal – International Law Enforcement Interoperability	FED INTL	When needed by operational requirement
20	AES	Public Safety – International Law Enforcement Interoperability	PS INTL	When needed by operational requirement



# Encrypted Interoperability

The best for last - SLN/CKR's

- SLN's are only required for comms between  
KMF and subscriber radio during OTAR  
KMF and keyloader (KFD) or KFD to KFD  
KFD to radio
- SLN's have nothing to do with radios ability to  
decrypt a message (TEK, Key ID, ALGID do matter)
- SLN de-confliction is only relevant within the context of your  
KMF/OTAR/KFD environment.

# Encrypted Interoperability



REMEMBER:

*If you want to interoperate with a subscriber that gets key from another KMF as long as you have the same TEK, Key ID and ALGID, you will communicate.*



# Thank You

## Scott Wright

Sr. Telecommunications Engineer II  
Deputy Statewide Interoperability Coordinator  
Connecticut Department of Emergency Services and Public Protection  
Division of Statewide Emergency Telecommunications

[scott.wright@ct.gov](mailto:scott.wright@ct.gov)

860-462-9899



# PENNSYLVANIA P25 SYSTEM

## PA-STARNet

**Hermina Koshinski**

PMP, ITIL SS & CSI

Chief, Radio Operations Engineering & Support

P25 System Administrator & Engineer

Pennsylvania State Police - Statewide Radio Network Division



# Commonwealth of PA - P25 Trunked Phase 2 System



2 primary zones both with geo redundant zones fully equipped with the same infrastructure

Sites: 180 mainly stand-alone sites

Frequencies: VHF, UHF, 800 & 700 MHz - 712 plus unique (Part90 PS & BILT, Part80 Maritel, Part22, NTIA)

IP Consoles: 239

Subscribers: Approximately 34,500

Foreign connections: 2 CSSI & 2 ISSI (more in queue)

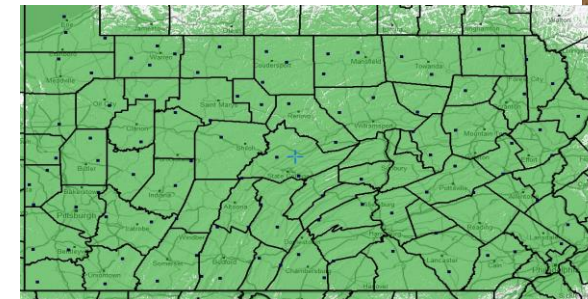
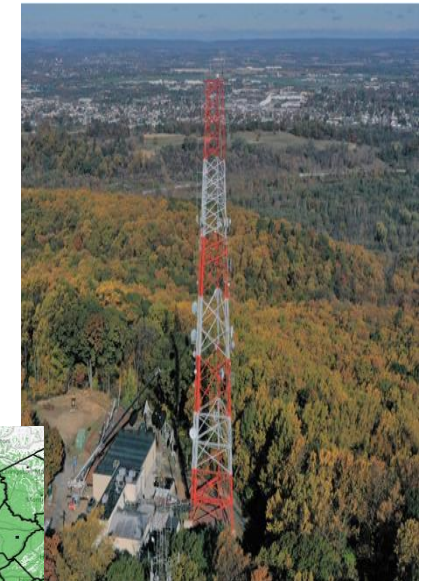
2024 Statistics: PTT's: 58,348,457

Connectivity:

- Resilient Private/Shared IP Microwave
- Leased Circuits
- LTE

Security:

- Advanced Encryption Standard (AES) 256 Encryption
- P25 Link Layer Authentication



PA-STARNET



**pennsylvania**

STATE POLICE  
STATEWIDE RADIO NETWORK DIVISION

# P25 Radio Authentication Things to Know



## P25 Authentication Helps:

- With only allowing authorized subscribers on a P25 trunking systems
- Reduces the Possibility of Duplicate Radio IDs
- Improves Protection From Lost or Stolen Radios

## P25 LLA User Considerations:

- Multiple trunking systems can be supported
  - Unique authentication key for each trunked system and subscriber
- Different manufacturers have different implementations and options
- It is important to understand what the implementation limitations are with the subscribers that are on the system and of the system itself

# P25 Link Layer Authentication Standards



## P25 Link Layer Authentication Standards:

- TIA-102.AACE-A
  - Telecommunications Industry Association (TIA) is a standards body that creates standards to define methods of measurement, performance, and requirements for radio equipment.
- Is a Supplementary Service
- Available Only for Trunking Systems
  - Phase 1 and Phase 2
- Utilizes 128 Bit AES Encryption Key
- Going to be reviewed in near future



# P25 Radio Authentication Overview



P25 Authentication Key Elements that you need to have in place in order to do Radio Authentication:

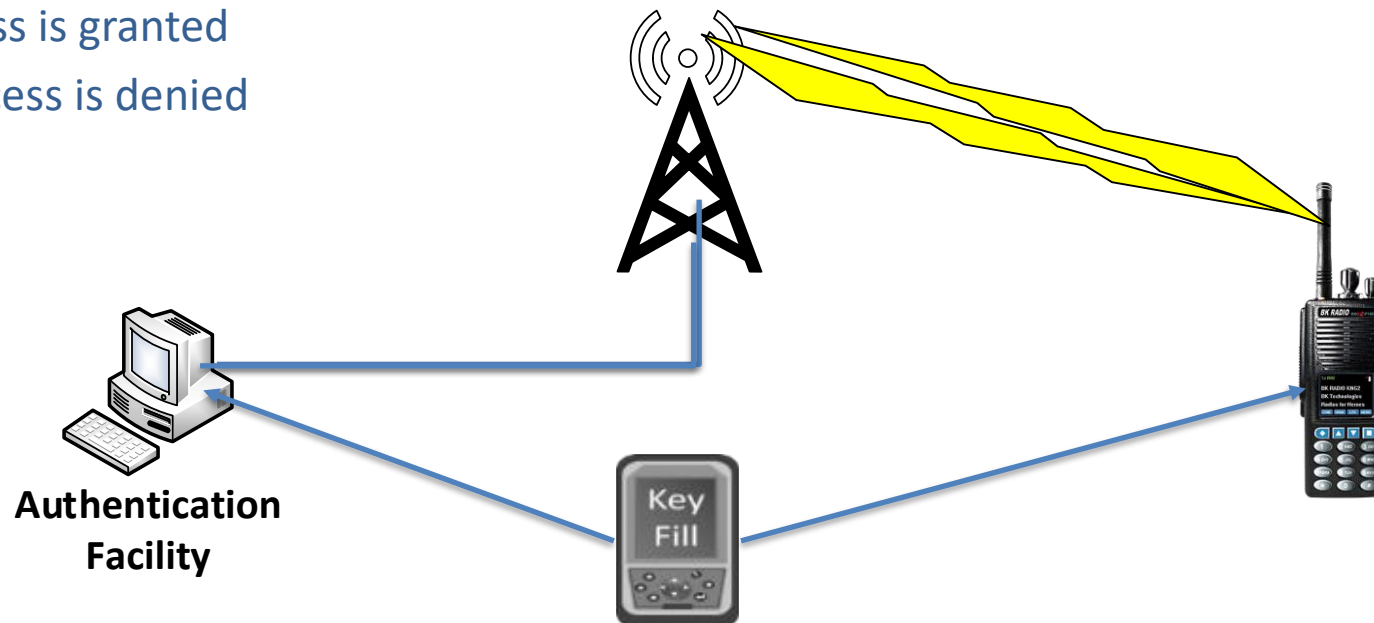
- Authentication Facility
- P25 Trunked Radio System
- P25 Subscriber Radios
- Key Fill Device (KFD)

# P25 Radio Authentication Overview



## P25 Authentication Process:

- Unique authentication key is loaded into Subscriber Unit (SU)/ Authentication Facility (AF) via a P25 Key Fill Device (KFD) or manual entry.
- RFSS sends authentication challenge to SU
- P25 SU sends a responds to the RFSS
- RFSS compares the response to the challenge
  - If correct access is granted
  - If incorrect access is denied



# Interoperability



Multiple interoperability efforts are in the works with various entities. *Only possible since transitioning to a P25 standard based system.*



PA-STARNET



# P25 Radio Authentication Things to Know



It is possible and works as intended, but there is a limited knowledge base on this subject when it comes to implementations and best practices.



# THANK YOU!!

## Hermina Koshinski

PMP, ITIL SS & CSI

Chief, Radio Operations Engineering & Support

P25 System Administrator & Engineer

Pennsylvania State Police - Statewide Radio Network Division



# Security Triad for P25 LMR:

Encryption, Access, Cyber IDs





[www.project25.org](http://www.project25.org)