International Wireless and Communications Expo
Orlando, Florida
NPSTC Meeting, March 9, 2018

Project 25 Update for NPSTC

New Standards, Applications, and Interoperability

Presented by:
PTIG - The Project 25 Technology Interest Group

www.project25.org

PTIG P25 Update

- New P25 Security Standards and Updates
  - Link Layer Encryption
  - Encryption Key Fill Device (KFD) Updates
  - P25 Authentication
- P25 Standards Update: TIA TR-8 meetings, Feb 6-8 2018
- What is P25 Compliance????
- PTIG Update
  - New P25 Statewide Systems List
  - New White Papers: P25 Authentication, P25 Trunking Control Channels
  - New P25 Benefits Docs:
    - P25 Top 10 Benefits for non technologist Users
    - P25 Value Proposition for Agency Administrators, procurement managers

Link Layer Encryption (LLE) Problem Statement

- P25 Link Layer Encryption helps ensure the following:
  - Integrity – How can you know the message has not been altered in some way?
    - Specifically Replay Protection ensures that a message cannot be resent later by an untrusted source.
  - Confidentiality – How can you be sure that the message is only received by the intended parties
  - Key Distribution - Do the initiating and receiving parties have the means to securely communicate?

LLE Problem Statement

- P25 End-to-End Encryption for voice calls and packet data protects the contents of the transmission
- End-to-End Encryption by itself does NOT protect against intercepting the identities of the parties involved in a call
  - Initiator of a Call (Typically a User ID)
  - Target of a Call (Typically a Group ID but may be a Supergroup or another User ID)

From: Jeremy
To: Bill
Message: Q@#$
%DFG%^&

LLE Affected Standards

Standard Number (TIA-102.x)	Title	Effect	Status
TBD	Link Layer Encryption Overvie		Ready to move to TR8.3
AABB-B	Trunking	mats for LLE control BKs and MBTs.	Not started
AA		Addition of ISPs and OSPs in support of LLE operations and LLE key management	
	ocedures	Addition of procedures f	
	Conventional Procedures	Addition	
BBAC	Phase 2 Two-Slot TDMA Medi Access Control Layer P		
BAAA-A	FDMA C		
BA		on in nt.	Not started
		aging and procedures for anagement.	Not started
		Addition of messaging and procedures for LLE key management.	In-Progress – Covered Later
AA	tocol	Addition of messaging and procedures for LLE key management.	Not started

LLE standardization is a major effort with many impacts on existing P25 standards.

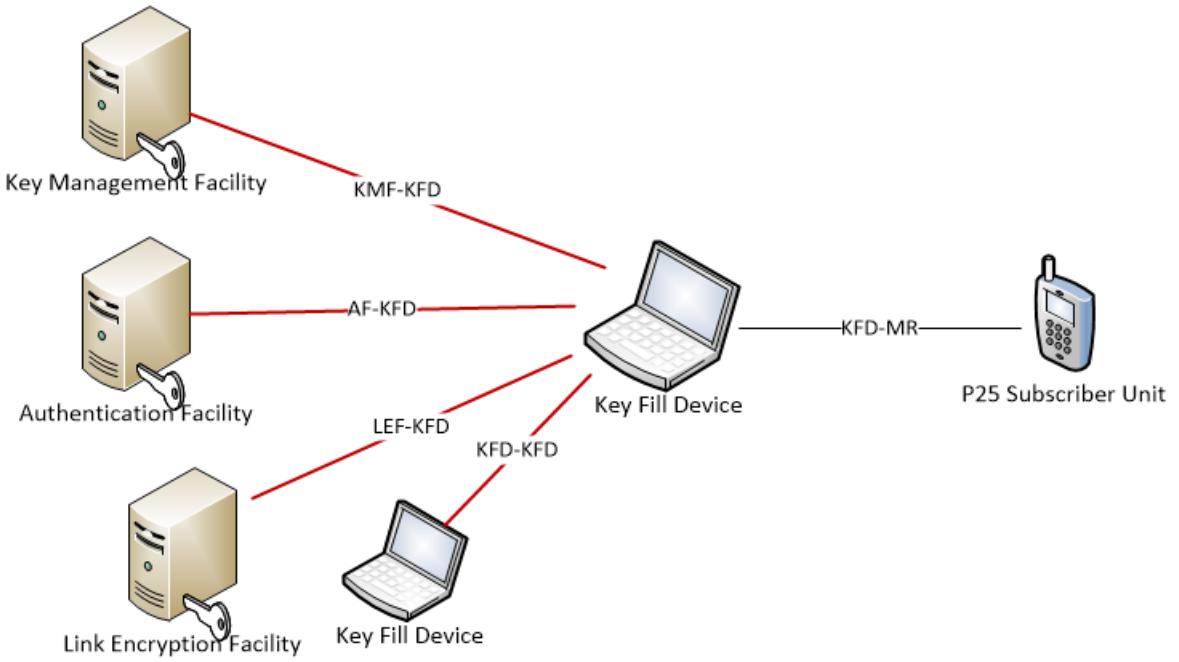
The LLE Overview document establishes the architecture; including the interfaces, published standards, and new standards that are needed.

LLE Important User Considerations

- Update to P25 standards for LLE will have no impact on users that don't require LLE.
- LLE will support interoperability with legacy subscriber units that don't support LLE and subscriber units that support LLE on the same network.
  - For example in P25T, the standards will support a mix of protected & unprotected groups operating on the same site.
- Key management is designed to be as seamless as possible – supporting distribution of future keys before they take affect.
- Protection of the RLEK (& derived CLEK) is very important.
- There is still some time until the standard is published and equipment that conforms to the standard is typically available 12-18 months after publication of a standard.

Key Fill Device (KFD) Addendum Scope

- Enhances interoperability for P25 encryption by providing standards-based interfaces between a Key Fill Device (KFD) and the following:
  - A Key Management Facility (KMF)
  - An Authentication Facility (AF)
  - A Link Encryption Facility (LEF)
  - Another KFD



KFD Addendum User Considerations

- TODAY: Interfaces between KMF, AF, and KFD and the KFD are proprietary. This presents challenges for interoperability between different P25 manufacturers.
- There is no impact on the interface between the KMF and SU with this change. Should allow support for legacy devices with new/updated KFDs.
- There is still some time until the standard is published and equipment that conforms to the standard is typically available 12-18 months after publication of a standard.

P25 Authentication Problem Statement

- P25 Authentication Helps Ensure:
  - Only Authorized Radios Obtain Service on a Trunking System
  - Reduces the Risk to Public Safety Communication Systems Arising From Pirated System Keys or Programming Software
  - Reduces the Possibility of Duplicate Radio IDs
  - Improves Protection From Lost or Stolen Radios

P25 Link Layer Authentication User Considerations

- P25 LLA User Considerations:
  - Multiple Trunking Systems Can Be Supported
    - Unique Authentication Key For Each System and Radio ID
  - Authentication Is Usually Part of Registration, But Can Occur at Anytime
  - Disabling the Key In the Authentication Server Will Prevent an Unaccounted for Radio From Gaining System Access
  - Utilizes 128 Bit AES Encryption
    - 3.4 X 10^{38} Key Values
    - FIPS-140-2 Approved

P25 Standards Update: 2017 Publications

Air Interfaces

- **A revision to the FDMA Common Air Interface Standard** was published.

  This revision addresses errata that have been collected since the last publication.

- **A revision to the FDMA Common Air Interface Reserved Values document** was published.

  This revision addresses errata that have been collected since the last publication.

- **A revision to the Trunking Interoperability Test Standard** was published.

  This revision merges the FDMA and TDMA material and addresses an error in a call pre-emption test procedure.

- **A new Standard for a TDMA Control Channel** Media Access Control (MAC) Layer was published.

  This standard describes the messages and procedures for a single slot (or "dual slot") TDMA control channel. A single slot control channel in combination with a single slot voice traffic channel allows single (12.5 kHz) channel trunking sites.

- **An addendum to the Trunking Control Channel Messages** standard was approved for publication.

  This addendum introduces a "Vehicle Sensed Emergency" flag to the Emergency Alarm message.

- **An addendum to the Trunking Control Channel Messages** standard was approved for ballot.

  This addendum introduces an "Accessory Sensed Emergency" flag to the Emergency Alarm message.

P25 Standards Update: 2017 Publications

Wireline Interfaces

- **A revision to the Fixed Station Interface Standard** was published.

  This revision adds additional capabilities the most significant of which is Packet Data.

- **An addendum to the ISSI Messages and Procedures for Supplementary Data** was published.

  This addendum expands the existing emergency alarm request message to indicate that the emergency alarm request has been generated by conditions other than depression of the emergency alarm button

- **An addendum to the ISSI Messages and Procedures for Supplementary Data** was approved for ballot.

  This addendum introduces the messages and procedures for Individual Regrouping control across an ISSI/ CSSI.

Data

- **A revision of the Location Services Overview bulletin** was approved for publication.

  This revision aligns the content of the Overview document with the content of the Tier 1 and Tier 2 Location Service Specifications.

Broadband

- **An addendum to TSB-88.3** was published.

  This addendum adds new broadband-to-narrowband interference scenarios.

P25 Standards Update: 2018 Publications

Air Interfaces

- **An addendum to the Trunking Control Channel Messages standard** was approved for publication.

  This addendum introduces an "Accessory Sensed Emergency" flag to the Emergency Alarm message.

Wireline Interfaces

- **An addendum to the ISSI Messages and Procedures for Supplementary Data** was approved for publication.

  This addendum introduces the messages and procedures for Individual Regrouping control across an ISSI/ CSSI.

P25 Standards Update: Work in Progress

Air Interfaces

- **A revision to the Conventional Interoperability Test standard** is in progress

  This revision corrects editorial errors and makes clarifications on various test procedures but does not add, remove or technically alter tests.

- **Creation of a High Signal Strength Intermodulation Rejection Test** is in progress.

  This test will measure the ability of a P25 or analog conventional FM receiver to reject an unwanted broadband base station signal, thereby preventing degradation to the reception of a desired signal. Performance specifications are expected to follow completion of the measurement method.

Wireline Interfaces

- **Group Regrouping for the Trunking ISSI/CSSI Standard** is in progress.

  This work will enable dispatch equipment connected to Trunking Infrastructures via the ISSI/CSSI to control group regrouping services. Note the control channel messaging for these services has already been standardized.

- **A revision of the ISSI Recommended Compliance Assessment Tests bulletin** is in progress.

  This revision will add recommended interoperability tests for Trunking CSSI applications and add recommended interoperability tests of TDMA operation of the Trunking ISSI and CSSI.

- **A new Interoperability test standard for Trunked ISSI Supplementary Data Services** is in progress**.**

  This document will provide a standard set of tests for validating interoperability of Supplementary Data Services (Emergency Alarm, Call Alert, etc) operating across a Trunked ISSI.

P25 Standards Update: Work in Progress

Security

- **Definition of a Link Layer Encryption Security Service** is in progress.

  This is the first big new technology upgrade for improved Security for all air interfaces of P25. It protects control channel control messages, and hides group and individual IDs.

- **An addendum to the Key Fill Interface standard** is in progress.

  This will enable Key Fill Device (KVL) interface to a KMF, an Authentication Facility and another Key Fill Device

Data

- **A revision of the Tier 2 Location Service** is in progress**.**

  This revision corrects editorial errors and makes corrections to EXI Encoding examples.

Broadband

- **Definition of 3GPP Mission Critical standard services interworking with TIA Land Mobile Radio standard services** is in progress.

  This document will describe interworking of features (example; group and individual calls) that are common between 3GPP LTE standards and P25 Trunking, P25 Conventional and Analog Conventional FM LMR standards.

What is P25 Compliance ???

"P25 COMPLIANCE" is not strictly defined but most consider "compliance" to mean:

- Adherence to published documentation

P25 SoR drives P25 Standard creation/content

P25 Standards enable interoperability

P25 Standard tests describe consistent methods for testing implementations against a published standard (Performance, Conformance and Interoperability)

Levels of "P25 Compliance"

1. Compliance in the context of the P25 SoR

- P25 SoR is created and maintained by P25 Steering Committee's User Needs Subcommittee (UNS)
- UNS' view of what interfaces, services, features, etc that should be addressed by P25 standards and/or implemented in P25 systems/equipment
- Includes importance ranking (Mandatory, Standard Option, Standard Option-Required)
- P25 SoR is not part of the P25 Standard
- Compliance statements at this level mean the functionality described in the SoR has been implemented
  - P25 SoR contains high level descriptions of functionality that does not enable interoperability
  - Most SoR items trace to published P25 standards, however some do not

Levels of “P25 Compliance”

2. Compliance in the context of the P25 Standards

- Manufacturers selectively implement standard functionality based on the customers they serve
  - P25 Interfaces (Air, Wireline, etc)
  - P25 Services (Data, Security, etc)
  - P25 Features (Group call, Ind call, etc)
- Compliance statements at this level mean some set of functionality covered by the P25 Standard documents has been implemented per the document and is expected to interoperate

P25 Capabilities Guide
Background and Purpose

PTIG's P25 Capabilities Guide was created and is maintained by a Working Group within PTIG

- Manufacturer and User Agency representatives active in P25/ TIA-102 Standards

Intended to be an aid to identify what P25 Interfaces, Services, and Functionality are covered by published P25/TIA-102 Standards

- Assist customers in writing RFP's that meet the P25 standards
- Compare neighboring system functionality for interoperability planning
- Available for Download at **www.project25.org**

Levels of “P25 Compliance”

3. Compliance in the context of the P25 Standard Tests

- Compliance statements at this level mean The implemented functionality produces the specified results under the specified conditions for:
  - Performance: standard measurement methods with associated specifications (primarily applies to RF)
  - Conformance: standard feature operation with proper message sequence and message content
  - Interoperability: standard feature operation between equipment of different manufacturers

Levels of "P25 Compliance"

4. Compliance in the context of the DHS OIC CAP

- Compliance statements at this level mean:

  The functionality has been implemented per the P25 Standard document(s) and will pass the associated P25 Standard Test(s) covered by published CABs and testing has been done in CAP recognized labs and reports have been approved by DHS OIC

- Recommended Compliance Assessment Test Telecommunication Systems Bulletins (RCAT TSBs)
  - Created by the industry and user community TIA members that produce and maintain the P25 Standard documents and P25 Standard Test documents and endorsed by the P25 Steering Committee
  - Provided to the DHS OIC CAP Advisory Panel for consideration when drafting or revising Compliance Assessment Bulletins (CABs)
  - **RCATs** are P25 recommendations for P25 tests appropriate for use when "assessing" P25 standard compliance of a product
  - **CABs** define testing and test result reporting for the DHS OIC Compliance Assessment Program

DHS OIC CAP Testing Resources

One-stop shop website:
www.dhs.gov/science-and-technology/p25-cap

- Lists of P25 CAP compliant equipment along with supporting documentation
  - Summary Test Reports (STR) and Suppliers' Declaration of Compliance (SDOC)
- Participating P25 CAP recognized labs
- Latest Compliance Assessment Bulletins
- P25 CAP Advisory Panel

PTIG Update

New P25 Statewide Systems List

- 38 P25 State-wide Systems

New White Papers

- P25 Authentication,
- P25 Trunking Control Channels

New P25 Benefits Docs:

- P25 Top 10 Benefits for non technologist Users
- P25 Value Proposition for Agency Administrators, procurement managers

New P25 State-wide Systems List

P25 Statewide Systems (38)	
Alabama 1st Responders	Phase 2 700/800
Alaska ALMR	Phase 1 VHF/700
Arkansas AWIN	Phase 1 700/800
Colorado DTRS	Ph 1 to Ph 2 700/800
Connecticut CSP	Ph 1 800 CERN Ph1 700
Delaware DPS	Phase 1 800
Florida SLERS	Phase 1 700
Hawaii HIR	Phase 1 700
Idaho ICAWIN	Phase 1 700
Illinois STARCOM	Phase 2 700/800
Indiana SAFE-T	Phase 1 800
Iowa ISICS	Phase 2 700
Kansas KSICS	Phase 1 700/800
Louisiana LWIN	Phase 1 700
Maine MSCS	Phase 1 VHF
Maryland FRIRS	Phase 2 700
Massachusetts CMS	Phase 2 700/800
Michigan MPSCS	Phase 1 700/800
Minnesota ARMER	Phase 1 800
Mississippi MWIN	Phase 2 700/800
Missouri MSWIN	Phase 2 VHF/700/800
Montana MSIRS	Phase 1 VHF
Nebraska NSRS	Phase 1 VHF
New Hampshire	Phase 1 VHF
New Jersey NJICS	Phase 2 700
North Carolina VIPER	Phase 1 700/800
Ohio MARCS-IP	Phase 2 800
Oklahoma OWIN	Phase 1 800
Oregon SRP	Phase 2 700
Rhode Island SCN	Phase 1 800
South Carolina PALMETTO	Phase 1 700/800
South Dakota SRS	Phase 1 VHF
Tennessee ACN	Phase 2 700/800
Virginia STARS	Phase 1 VHF/800
Washington State Police	Phase 2 700
West Virginia SIRN	Phase 1 UHF Lo
Wisconsin WIS	Phase 1 VHF/800
Wyoming WYOLINK	Phase 1 VHF/800

Project 25: Top 10 Benefits

Public Safety Grade Reliability and Performance

Mature, well defined, Air and Wireline Standardized Interfaces

Superior Security using 256 bit AES with OTAR

A User-Driven Technology with support at numerous frequency bands

A Large Installed Base of over 2250 Systems

The reliable, de-facto, choice for mission critical communications during Natural Disasters and critical events

A vibrant market-place with more than 3 dozen suppliers and the preferred technology for Federal Grants

Superior Audio volume and clarity combined with high performance radio designs for Public Safety environments

Independent testing for performance and interoperability

A live, active, technology that continues to evolve with new capabilities, upgrades, and test standards

WWW.Project25.org

International Wireless and Communications Expo
Orlando, Florida
NPSTC Meeting March 9, 2018

PTIG P25 Update

New Standards, Applications, and Interoperability