Project 25 Update for IACP
Communications and Technology Committee

Presented by:
Jim Holthaus, Vice Chairman
Project 25 Technology Interest Group (PTIG)
www.project25.org
PTIG P25 Update

- Project 25 Eco System Today
- Project 25 Standards Update And Future Roadmap
- New P25 Security Standards and Updates
  - Link Layer Encryption
  - Encryption Key Fill Device (KFD) Updates
  - P25 Authentication
- What is P25 Compliance????
- PTIG Update and New P25 Resource Documents Available
- P25 New Products and Services Trends
The Project 25 Eco-System Today

Established Base of over 2250 Project 25 Systems on the air today

Including 37 Statewide P25 Systems, numerous region wide, county wide, municipality, campus, and individual facility 25 systems.

Examples: Michigan 90,000 users 1,665 Agencies 12 Million PTT /mo.

  Miami/Dade 30,000 users, 110 Agencies, 7 million PTT/mo.

A Competitive Market-place with 40 Project 25 Product and Service providers

offering a diverse range of P25 solutions at multiple price points and P25 is the preferred technology for Federal Grants

Independent Testing through the DHS CAP Program and a number of certified independent testing Labs.

A Live, Active, Evolving Technology that continues to evolve, developing new capabilities, upgrades, and test standards
2018 P25 Standard Documents approved for Ballot or Publication:

- Trunking Control Channel Messages addendum, Conventional Interoperability test revision, Improved P25 performance Modeling, ISSI suplementary data addendum, ISSI/CSSI Interoperability Test & compliance tests, Security Services Overview revision, Tier 2 Location services revision.

2018 P25 Work in Progress:

- Definition of Link Layer Encryption, Addendum to the Key-fill interface, Definition of Interworking between MCPTT Broad band Data standards and P25, High Signal Strength Intermod test, Revision for Intrinsic Safe radio spec, Revision of Trunking Control Messages, Group/Re-Grouping for the ISSI/CSSI interface, Interoperability test Standard for ISSI Supplementary data.
New P25 Link Layer Encryption (LLE)
Problem Statement

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

<table>
<thead>
<tr>
<th>Standard Number (TIA-102.x)</th>
<th>Title</th>
<th>Effect</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBD</td>
<td>Link Layer Encryption Overview</td>
<td></td>
<td>Ready to move to TR8.3</td>
</tr>
<tr>
<td>AABB-B</td>
<td>Trunking Control Channel Formats</td>
<td>Modification of formats for LLE control channel TSBKs and MBTs.</td>
<td>Not started</td>
</tr>
<tr>
<td>AABB-D</td>
<td>Trunking Control Channel Messages</td>
<td>Addition of ISPs and OSPs in support of LLE operations and LLE key management.</td>
<td>Not started</td>
</tr>
<tr>
<td>AABD</td>
<td>Trunking Procedures</td>
<td>Addition of procedures for LLE key management.</td>
<td>Not started</td>
</tr>
<tr>
<td>BAAD</td>
<td>Conventional Procedures</td>
<td></td>
<td>Not started</td>
</tr>
<tr>
<td>BBAC</td>
<td>Phase 2 Two-Slot TDMA Media Access Control Layer Description</td>
<td>Modification of formats and descriptions of LLE operations.</td>
<td>Ready to move to TR8.3</td>
</tr>
<tr>
<td>BAAA-A</td>
<td>FDMA Common Air Interface</td>
<td></td>
<td>Not started</td>
</tr>
<tr>
<td>BACB</td>
<td>FDMA Common Air Interface</td>
<td></td>
<td>Not started</td>
</tr>
<tr>
<td>BABA-A</td>
<td>OTAR Protocol</td>
<td>Addition of messaging and procedures for LLE key management.</td>
<td>In-Progress – Covered Later</td>
</tr>
<tr>
<td>BACA-B</td>
<td>ISSI Messages and Procedures</td>
<td>Addition of messaging and procedures for LLE key management.</td>
<td>Not started</td>
</tr>
<tr>
<td>BAHA</td>
<td>Fixed Station Interface</td>
<td>Addition of messaging and procedures for LLE key management.</td>
<td>Not started</td>
</tr>
</tbody>
</table>

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.
P25 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.
P25 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:
  o A Key Management Facility (KMF)
  o An Authentication Facility (AF)
  o A Link Encryption Facility (LEF)
  o Another KFD
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 P25 Standards 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 Security for the P25 System Operator:

• 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 1038 Key Values
  - FIPS-140-2 Approved
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)
- DHS CAP Program defines test requirements, monitors P25 Testing in CAP approved laboratories and publishes results.
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](http://www.project25.org)
PTIG Update

New Documents on www.project25.org

- P25 State-wide Systems List with 38 States
- P25 New Products and Services PPT from 20 PTIG members (August-2018)
- “Why so many agencies choose P25 for PTT” from the recent IWCE WEBINAR.

New P25 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

<table>
<thead>
<tr>
<th>P25 Statewide Systems (38)</th>
<th>Louisiana LWIN</th>
<th>Phase 1 700</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alabama 1st Responders</td>
<td>Maine MSCS</td>
<td>Phase 1 VHF</td>
</tr>
<tr>
<td>Alaska ALMR</td>
<td>Maryland FRIRIS</td>
<td>Phase 2 700</td>
</tr>
<tr>
<td>Arkansas AWIN</td>
<td>Massachusetts CMS</td>
<td>Phase 2 700/800</td>
</tr>
<tr>
<td>Colorado DTRS</td>
<td>Michigan MPSCS</td>
<td>Phase 1 700/800</td>
</tr>
<tr>
<td>Connecticut CSP</td>
<td>Minnesota ARMER</td>
<td>Phase 1 800</td>
</tr>
<tr>
<td></td>
<td>Mississippi MWIN</td>
<td>Phase 2 700/800</td>
</tr>
<tr>
<td></td>
<td>Missouri MSWIN</td>
<td>Phase 2 700/800</td>
</tr>
<tr>
<td></td>
<td>Montana MSIRS</td>
<td>Phase 1 VHF</td>
</tr>
<tr>
<td></td>
<td>Nebraska NSRS</td>
<td>Phase 1 VHF</td>
</tr>
<tr>
<td></td>
<td>New Hampshire</td>
<td>Phase 1 VHF</td>
</tr>
<tr>
<td></td>
<td>New Jersey NJICS</td>
<td>Phase 2 700</td>
</tr>
<tr>
<td></td>
<td>North Carolina VIPER</td>
<td>Phase 1 700/800</td>
</tr>
<tr>
<td></td>
<td>Ohio MARCS-IP</td>
<td>Phase 2 800</td>
</tr>
<tr>
<td></td>
<td>Oklahoma OWIN</td>
<td>Phase 1 800</td>
</tr>
<tr>
<td></td>
<td>Oregon SRP</td>
<td>Phase 2 700</td>
</tr>
<tr>
<td></td>
<td>Rhode Island SCN</td>
<td>Phase 1 800</td>
</tr>
<tr>
<td></td>
<td>South Carolina PALMETTO</td>
<td>Phase 1 700/800</td>
</tr>
<tr>
<td></td>
<td>South Dakota SRS</td>
<td>Phase 1 VHF</td>
</tr>
<tr>
<td></td>
<td>Tennessee ACN</td>
<td>Phase 2 700/800</td>
</tr>
<tr>
<td></td>
<td>Virginia STARS</td>
<td>Phase 1 VHF/800</td>
</tr>
<tr>
<td></td>
<td>Washington State Police</td>
<td>Phase 2 700</td>
</tr>
<tr>
<td></td>
<td>West Virginia SIRN</td>
<td>Phase 1 UHF Lo</td>
</tr>
<tr>
<td></td>
<td>Wisconsin WIS</td>
<td>Phase 1 VHF/800</td>
</tr>
<tr>
<td></td>
<td>Wyoming WYOLINK</td>
<td>Phase 1 VHF/800</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Responders</th>
<th>Phase 2 700/800</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delaware DPS</td>
<td>Phase 1 800</td>
</tr>
<tr>
<td>Florida SLERS</td>
<td>Phase 1 700</td>
</tr>
<tr>
<td>Hawaii HIR</td>
<td>Phase 1 700</td>
</tr>
<tr>
<td>Idaho ICAWIN</td>
<td>Phase 1 700</td>
</tr>
<tr>
<td>Illinois STARCOM</td>
<td>Phase 2 700/800</td>
</tr>
<tr>
<td>Indiana SAFE-T</td>
<td>Phase 1 800</td>
</tr>
<tr>
<td>Iowa ISICS</td>
<td>Phase 2 700</td>
</tr>
<tr>
<td>Kansas KSICS</td>
<td>Phase 1 700/800</td>
</tr>
<tr>
<td>Kansas KSICS</td>
<td>Phase 1 700/800</td>
</tr>
</tbody>
</table>
Project 25: Top 10 Benefits

- Superior Security using 256 bit AES with OTAR
- A User-Driven Technology with support at numerous frequency bands
- The reliable, de-facto, choice for mission critical communications during Natural Disasters and critical events
- Superior Audio volume and clarity combined with high performance radio designs for Public Safety environments
- Independent testing for performance and interoperability
- Public Safety Grade Reliability and Performance
- Mature, well defined, Air and Wireline Standardized Interfaces
- A Large Installed Base of over 2250 Systems
- A vibrant market-place with more than 3 dozen suppliers and the preferred technology for Federal Grants
- A live, active, technology that continues to evolve with new capabilities, upgrades, and test standards

Project 25 Technology Interest Group
P25 New Product Trends

- **P25 LMR Interoperability with LTE Broadband Data**
  - Multi mode P25/LTE smart phones
  - Mobile P25 radio with Wi-Fi and LTE connectivity
  - New P25 Consoles connect P25 and LTE technologies

- Voice recording in radios
- Mobile radio with simultaneous P25 TX/RX (4 bands)
- New products are P25 Phase 1 and Phase 2 capable

A detailed PPT describing New P25 Products and Services is available on the PTIG website

P25 New Product Trends

- Deployable, mixed-mode, P25 repeaters for Emergency Operations
- Scalable, Configurable, P25 Airborne Radios
- P25 Antenna Site Monitoring
- “Over the Air” radio maintenance for P25 Systems
- “Cloud based” Asset management for P25 Systems
- New P25 Location Services
- P25 enhanced Vocoder Software
Project 25 Update for IACP
Communications and Technology Committee