White Paper – Secure P25 Radio

Seal SQ
Secure Interoperability

FIPS140 Certification using the SEAL SQ VaultIC Secure Element for the Cryptographic Module in P25 Radios

A State-of-the-art example of a FIPS140 certified cryptographic module for P25 secure radios. Implemented by SEAL SQ with over 20 years of certified secure hardware and PKI experience.

Abstract

The Project 25 (P25) standard has been instrumental in providing communication security since it was developed to encrypt communication. P25 has also allowed for interoperability of communication between cooperating agencies. See P25 description section.

When the P25 radio is certified to Federal Information Processing Standard (FIPS) 140 standards or FIPS140 2(3) Levels 2&3, a higher level of security can be achieved. Since the Land Mobile Radios (LMRs) are mobile, the keys that they store are subject to physical attacks, this motivates the Level 3, hardware protection requirement. Increasingly, agencies are requiring this higher certification, thereby ensuring the highest level of security.

Designing and certifying a cryptographic module for FIPS140 is challenging, time consuming and expensive. In many cases the certification can take up to or over 2 years

We will show how using the off the shelf VaultIC Secure Element as a P25 cryptographic module, the radio achieves FIPS140 certification. We will also show how this design approach is an ideal solution to expand radio manufacturers' Total Available Market into FIPS140 Levels 2&3 opportunities. Using this design architecture, there is a shorter time to market since the VaultIC is pre certified. Having a pre certified cryptographic module eliminates the time it takes for certification.

The VaultIC Secure Element provides a simple, short release cycle, and less-expensive design for FIPS140 certified radios.

Project 25 (P25)

In the event of natural disaster or emergencies, the response needs to be a coordinated effort from all first responders. The coordination depends on reliable and secure communication between the various public safety agencies that are responding to the event. The APCO-P25 standard was developed for interoperable and encrypted digital communication between two-way radio products. When the P25 standard is adopted by agencies such as police, fire, ambulance, military, and emergency rescue service, they are able to communicate reliably and securely.

Many agencies now require NIST FIPS 140-2(3) Level 3 certification to provide tamper proof storage of the encryption keys.

As communication upgrades are implemented in the United States, the Department of Homeland Security frequently requires migrating to P25 to ensure interoperability and security. Other countries worldwide including Australia, New Zealand, Brazil, Canada, India and Russia have also adopted the P25 standard.

Radio Security Architectures

When deciding on an architecture for a radio that will be FIPS140 certified, the designer needs to consider the complexity of the firmware that the compliance labs will certify. Obviously, a simple cryptographic module is easier to certify than a complex one.

Typical Cryptographic Module Architecture

A typical architecture of a cryptographic module for use in a P25 radio will provide high level functions specific to P25 requirements. These high level functions will use the core cryptographic algorithms and secure key storage to implement the non cryptographic P25 API. Figure 1 shows the firmware stack of a typical cryptographic module.

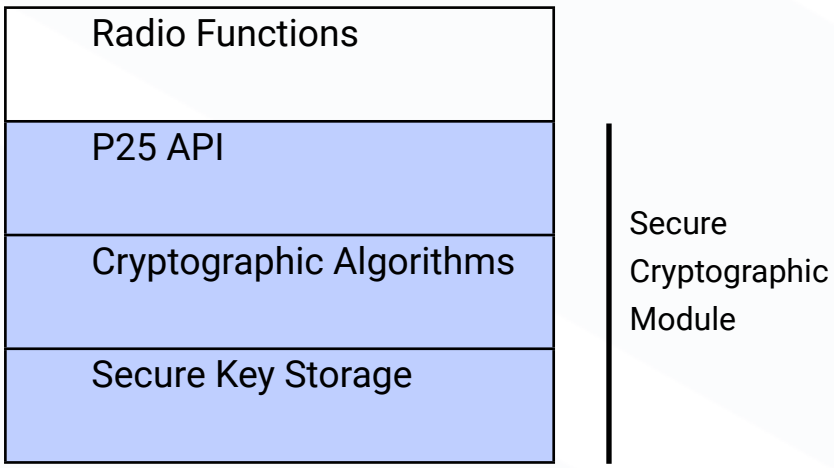


Figure 1. Typical Cryptographic Module Firmware Stack

Notice that in a typical cryptographic module implementation, the complexity of the non cryptographic P25 API is included in the secure portion. This means that the non cryptographic P25 API needs to be certified along with the core cryptographic algorithms and the secure key storage. This added complexity adds both time and expense.

VaultIC Secure Element as a Cryptographic Module

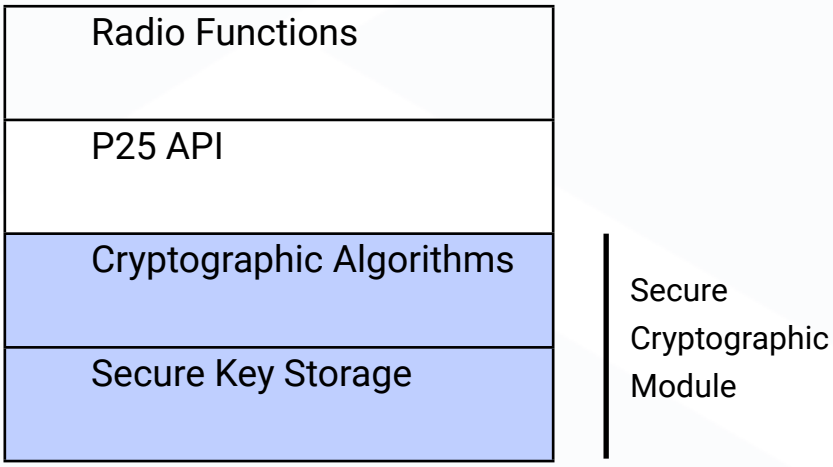


Figure 2. Cryptographic Module Firmware Stack with the VaultIC

The VaultIC is designed for secure cryptographic operations and secure key storage. The secret keys are used on chip so they are never compromised in the cryptographic calculations. This simple architecture allows the cryptographic capabilities of the VaultIC to be certified independently from the radio functions and the non cryptographic P25 API.

Cryptographic Module Challenges

Costly Development

The development of a FIPS140 certified P25 cryptographic module for a Land Mobile Radio (LMR) has multiple challenges. First, the cryptographic requirements for FIPS certification needs to be meticulously followed. Second, there is the extra expense to secure the keys from physical and side channel attacks. These two factors add cost to the BOM and time to the development.

Time Consuming FIPS Certification

Once the cryptographic module is functional, it must go through testing at a compliance lab and the results submitted to NIST for certification. Between the lab and NIST, the process can take 1 or 2 years. Level 3 certification is particularly difficult since the keys must be physically shielded to achieve the security. This makes the certification process both costly and time consuming.

Not Optimized

There are many factors influencing the performance of a cryptographic module. The design must include a secure MCU, side channel resistant cryptographic algorithms, and tamperproof memory for the keys. When designing a cryptographic module using discrete components, it is difficult to optimize for speed, power, and secret key protection.

Smaller Available Market

This is more of a market challenge than a technical challenge. However, a radio that is not FIPS140 certified for all levels of operation has a Total Available Market that is smaller than a radio that is certified. Customers are increasingly requiring FIPS140 security and if the radio is not certified, it cannot be used in their applications.

Certified Secure Element as Cryptographic Module

FIPS140 Certification

To achieve a radio that is FIPS140 certified, it is not the radio itself that is certified but only the FIPS140 certified Cryptographic Module in the radio.

This is an important point that allows the VaultIC Secure Element to be certified independently, and then every radio that uses it can be certified.

Here is an overview of the FIPS140 certifications:

- FIPS140-2

  The FIPS140-2 is a U.S. government computer security standard used to approve cryptographic modules. The title is Security Requirements for Cryptographic Modules. Initial publication was on May 25, 2001, and the last day to certify is March 31, 2022.

- FIPS140-3

  On March 22, 2019, the United States Secretary of Commerce approved FIPS140-3, Security Requirements for Cryptographic Modules to succeed FIPS140-2. FIPS140-3 became effective on September 22, 2019.

- Devices that are FIPS140 certified have a valid certification for 5 years from validation by NIST.

- FIPS140 Certification Levels

  Level 1:

  The lowest FIPS140 level. It certifies the implementation of cryptographic algorithms, the hardware is “production-grade”, and various egregious kinds of insecurity are absent.

  Keys loaded in the clear.

  Level 2:

  Adds requirements for physical tamper-evidence and role-based authentication.

  Keys loaded in the clear

  Level 3:

  Adds requirements for physical tamper-resistance and identity-based authentication, and for a physical or logical separation between the interfaces by which “critical security parameters” enter and leave the module, and its other interfaces.

  Keys loaded encrypted. Wrapped based on the TIA-102.AACA-A standard.

Since the timeframes for 140-2 and 140-3 overlap, there will be valid certifications for both standard simultaneously.

The motivation to provide both certification levels 2&3 on the single VaultIC Secure Element has to do with balancing the strict FIPS140 Level 3 requirements of loading only encrypted keys and the common practice of loading clear text keys. Providing both levels on the VaultIC allows a single radio board layout while supporting Level 2 and Level 3 radios.

From an interoperability standpoint, Level 3 radios can only interoperate with other Level 3 radios. Level 2 radios can interoperate with all non-Level 3 radios, including radios that are not FIPS certified.

Cryptographic Co-Processor

The VaultIC Secure Element is a specialized semiconductor chip that is specifically designed for secure operation. The VaultIC includes cryptographic co processing features that optimize the speed of execution for cryptographic algorithms. The VaultIC also includes physical protection features of shielding, encrypted memory, encrypted communication, etc. These features are designed to protect against tampering, microprobe attacks, reverse engineering, side channel attacks, timing attacks, fault injection, etc. Furthermore, the FIPS140 certification demonstrates these features in testing labs with state-of-the-art equipment to ensure physical security.

Having the VaultIC as a cryptographic co processor in the radio design, there is the opportunity to secure other general-purpose use cases. A few important use cases are listed below.

- Cryptographic Use Cases:
  - Secure Boot / Trusted Execution
  - Secure Firmware Update
  - Secure Data / Encrypted Memory

Optimized Semiconductor Chip

Since the VaultIC Secure Element is a single chip, it is optimized for speed and power in a way that a cryptographic module that uses discrete elements cannot. The package of the VaultIC is small, conserving both board space and power consumption. Minimizing both the size and the battery life of the radios.

Easy Integration

The VaultIC Secure Elements is shipped with firmware integration libraries that make integration simple. There are both I2C and SPI communication options.
The VaultIC is a commercially available off the shelf part that can be integrated into an existing radio design for a small fraction of the cost for in-house designed cryptographic module.

Faster Time-To-Market

Since the certification process can take up to 2 years, adding the pre certified VaultIC Secure Element to the design eliminates the delay and trouble in certifying an in house designed cryptographic module.

Expanded Available Market

Customers are increasingly requiring FIPS140 security. A radio that is FIPS140 certified for all levels of operation has a Total Available Market that is larger than a radio that is not certified. Additionally, the credibility that is associated with a FIPS140 certified radio adds value to both the radio and the brand.

TIA Requirements

Encryption

The specific details for the encryption protocol are defined in the TIA 102.AAAD Project 25 standard document. This document defines the protocols for key selection, encryption bit order, block encryption system, clock schedule, etc. For details on the encryption scheme required, please refer to the TIA standard document. The VaultIC Secure Element supports the highest standard for P25 encryption, the Advanced Encryption Standard algorithm using 256-bit keys (AES 256) described in Annex C. The VaultIC also supports the specific modes for encryption / decryption of Output Feedback (OFB) defined in the TIA P25 standard.

Key Loading

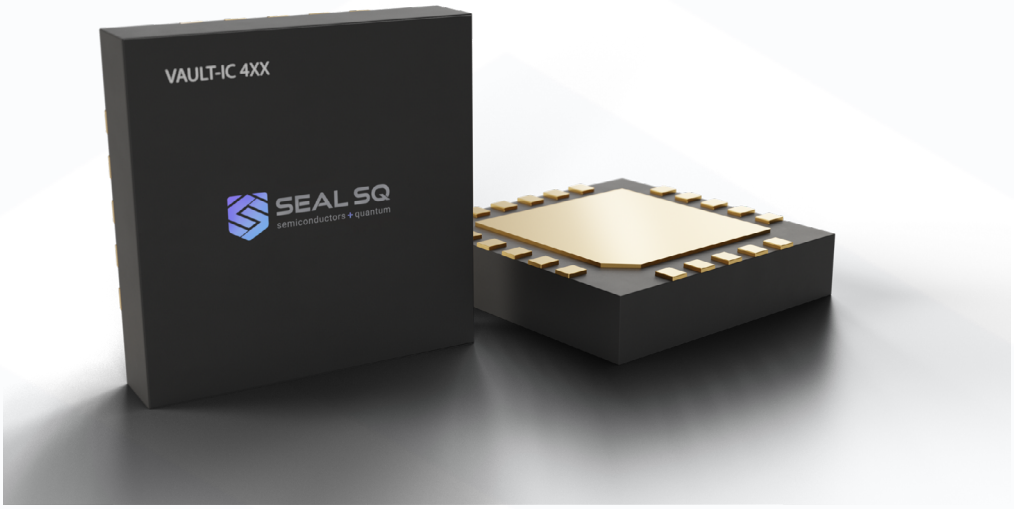
The specific messages and procedures for over the air rekeying (OTAR) are defined in the P25 standard document TIA 102. AACA-A. The wrapping method is based on the NIST publication SP800-38F, however the SP800-38F specifies two wrapping techniques. TIA standards only allow the one specified in TIA-102.AACA-A section 13.3.

The VaultIC Secure Element implements key wrapping according to the TIA standard. Since this standard specifies encrypted keys, this is the technique used for FIPS140 Level 3 key loading.

SEAL SQ P25 VaultIC Secure Elements

VaultIC405 1.2.6

The VaultIC 405 is a general-purpose Secure Element that has been designed to support P25 requirements for FIPS140 2 Levels 2&3. This Secure Element is currently being designed into radios that will be certified to the FIPS140 standard.



The proven technology used in VaultIC405 1.2.6 security modules is already widespread and used in national ID/health cards, e-passports, and many other use cases. Strong Authentication capability, secure storage and flexibility thanks to the various interfaces (SPI, I²C), low pin count and low power consumption are main features of the VaultIC405 1.2.6. Its embedded firmware provides advanced functions such as Identity-based authentication, large Cryptographic command set, various Public domain cryptographic algorithms, Cryptographic protocols, and Secure Channel Protocols.

The FIPS 140-2 Level 2 and Level 3 certification for VaultIC405 1.2.6 has completed lab testing and is in the "review pending" state. It is expected to be confirmed by the NIST Cryptographic Module Validation Program (CMVP) by Q3 2022.

Status is now on NIST website (https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/validation) validation numbers A2383 and A2384.
This part is in production now and it is available for delivery

The VaultIC408 is the next generation of Secure Elements offered by SEAL SQ. It includes all of the capabilities of the VaultIC405 along with optimized cryptographic capabilities. The P25 requirements for FIPS140 3 Levels 2&3 are supported and it is a drop in replacement for the VaultIC405.

The FIPS 140-3 Level 2 and Level 3 certification for VaultIC408 will begin H2 '22 and it is expected to be confirmed by the NIST Cryptographic Module Validation Program (CMVP) in 2023.

VaultIC408 samples are shipping now and it will be in production Q3 '22.

Conclusion

Using the commercially available off the shelf VaultIC Secure Element from SEAL SQ in a P25 radio design can shorten timelines and lower the cost compared to an in-house custom cryptographic module design. The proposed design increases the security and achieves FIPS140 certification for the P25 radio by simply integrating the certified VaultIC into the radio.

The VaultIC is specifically designed for secure operation and is optimized for speed, small size, and low power consumption. This allows the radios to be faster, smaller, and the battery life to last longer.

The P25 radio that is designed to use the VaultIC expands its available market to include opportunities that have FIPS140 Levels 2&3 requirements. These factors along with the shorter time to market due to faster development cycles will yield a higher return on investment.