Fact sheet

Motorola APX radios: leading the way in P25 two-way communications security

APX radios awarded FIPS 140-3 Level 3 validation

The APX™ series of P25 two-way radios is one of the first to achieve Federal Information Processing Standards (FIPS) 140-3 Level 2 & 3 validation, offering government agencies the next level of information assurance.

Why FIPS 140-3 Level 3?

Threats are evolving and so are the standards to assure your agency's sensitive information. With FIPS 140-3 the standard has been strengthened to detect and prevent physical tampering, protect device firmware and software from unauthorized changes as well as authenticate the user and their permissions to provide enhanced data security.

Motorola Solutions has answered this call by designing the APX series of P25 portable and mobile radios to be FIPS 140-3 Level 3 validated. This ensures that keys and cryptographic operations are protected from misuse and exploitation, safeguarding both the integrity of data and the operational capabilities of users.

Using FIPS 140-3 means that voice and data in transit are encrypted using crypto- graphically strong keys, stored in the hardware security module, to ensure that an intruder cannot easily break it.

FIPS is recognized by the U.S. federal government

FIPS 140-3 is recognized by the U.S. federal government standard and internationally. The standard is publicly available and independently validated and certified by a third-party organization.

FIPS 140-3 level 3 enhances FIPS 140-3 Level 1 & 2

FIPS 140-3 Level 1 defines basic security requirements for cryptographic modules including the use of an approved algorithm, software and/or firmware (SW/FW) integrity techniques and the use of production grade components for physical security.

FIPS 140-3 Level 2 builds on the Level 1 requirements by adding features such as:

- Tamper Evidence: attempts to physically tamper with the encryption module will result in visible damage to the module.
- Software and/or Firmware Security: requires approved digital signature or keyed message authentication.
- User Authentication: verifies the role of a user and what functions that role is allowed to perform with the module.

FIPS 140-3 Level 3 encompasses Levels 1 and 2 while increasing security measures with:

- Tamper Detection and Response Mechanisms: detects an attack and provides an active response by preventing access to sensitive data.
- Environmental Testing: environmental failure protection (EFP) or environmental failure testing (EFT) for temperature and voltage.
- Secured Keyfill: improves protection of keys through encrypted keyfill.
- High-Level Design Assurance: ensures high-level design, deployment, low-level testing, and radio operation measures are met to deliver proper security implementation.
- FIPS Level-3 Motorola Advanced Crypto Engine (MACE) module used in APX radios does not allow exporting of traffic keys. This means the attackers can never get access to the keys as they are stored securely in the hardware security module. The keys are loaded through a secure keyfill.

MOTOROLA SOLUTIONS

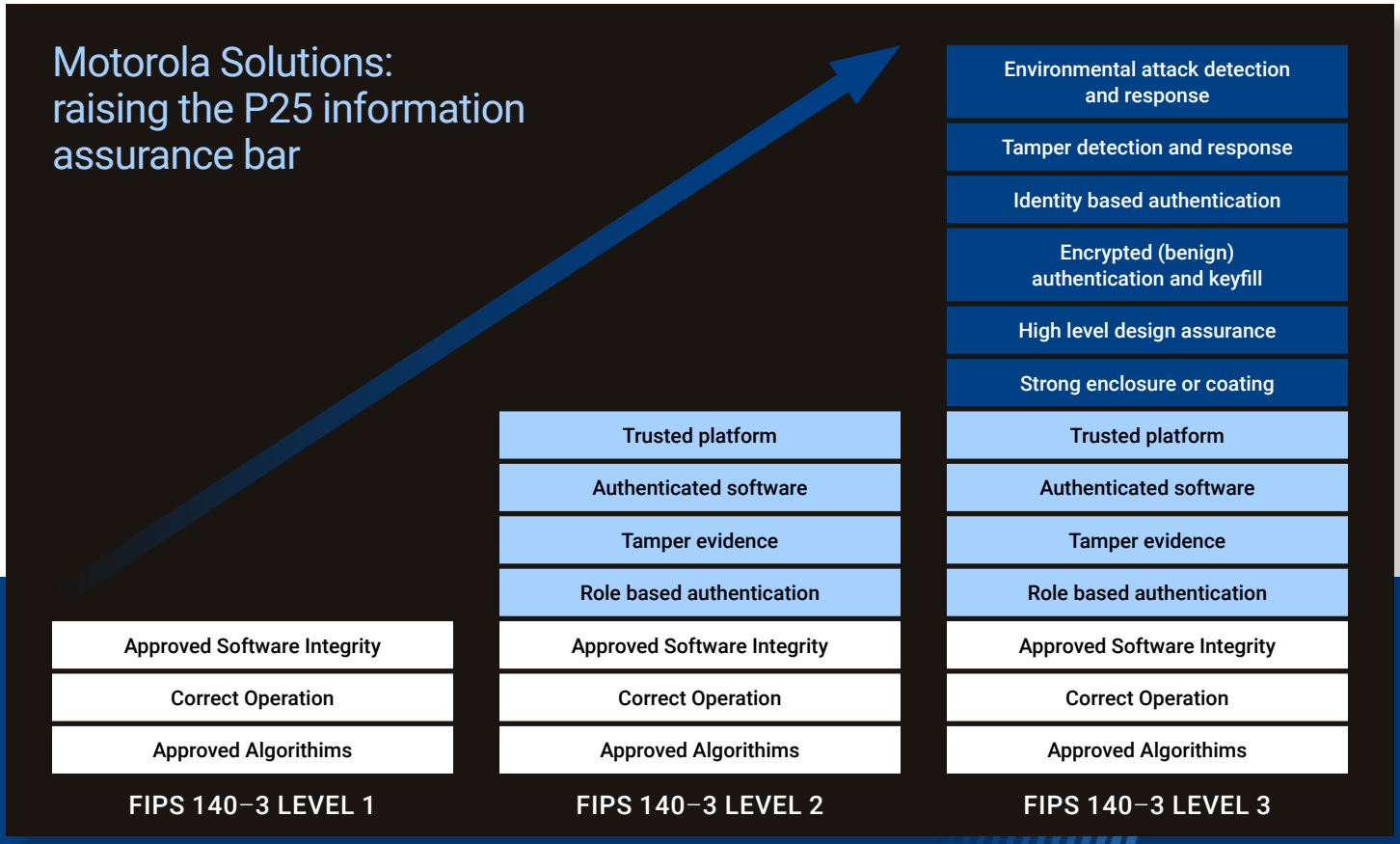
How does FIPS 140-3 Level 3 validation benefit users of APX radios?

Motorola Solutions APX radios have achieved the highest level of security available today.

Motorola Solutions has designed the APX series radios to meet FIPS 140-3 standards without sacrificing usability. We're committed to providing enhanced security for APX applications that are exposed to sophisticated adversaries every day. FIPS 140-3 Level 3 goes beyond simply detecting unauthorized access attempts; it actively blocks them, safeguarding your critical data.

With FIPS 140-3 Level 3, you can be confident that your critical security data remains protected and accessible only by authorized personnel. This advanced level of security also establishes a root of trust by validating the firmware on the chip, using a split key for code signing.

The APX P25 radios' FIPS 140-3 Level 3 validation demonstrates our dedication to developing products that offer exceptional quality, reliability, and security for mission-critical use.



We remain industry leaders in two-way radio security, holding numerous FIPS 140 security certificates for cryptographic modules

(See **http://csrc.nist.gov/groups/STM/cmvp/**)

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. **motorolasolutions.com**

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. ©2025 Motorola Solutions, Inc. All rights reserved. 04-2025 [BG05]