FIPS Compliant versus FIPS Validated

ABSTRACT

Security matters, whether it's a door lock, a wireless camera, or an ultrasound scanner. To find that proven, tested security, you want to stick with FIPS Validated.

Contents

1 The Federal Information Processing Standard (FIPS) 2
2 Why does all of this matter? 2
3 What does TI offer in terms of FIPS Validation? 2

Trademarks

SimpleLink, WiLink are trademarks of Texas Instruments.
Bluetooth is a registered trademark of Bluetooth SIG Inc..
Wi-Fi is a registered trademark of Wi-Fi Alliance.
All other trademarks are the property of their respective owners.

Copyright © 2018–2019, Texas Instruments Incorporated

1 The Federal Information Processing Standard (FIPS)

The Federal Information Processing Standard, or FIPS 140-2, is a US government security standard for certifying cryptographic modules. The standard covers ports and interfaces, authentication, physical security, key management, and more. As this standard becomes a requirement in more areas, component manufacturers are using terms “FIPS Compliant” and “FIPS Validated” to denote security in their parts. One of these terms can only claim security, while the other indicates tested and proven security.

The validation process for FIPS requires looking at different aspects of the cryptographic module. At level 1, the main focus is the software and algorithms used in the crypto. Level 2 tries to show evidence of tampering, such as coatings and seal. Level 3 tries to prevent the tampering, and level 4 responds to the tampering with the deletion of information.

This validation must be done by independent, accredited third-party laboratories. Vendors may select any laboratory, and all of the labs are accredited by the National Voluntary Laboratory Accreditation Program. The vendor then works to create the test reports for the module, and submit them to the National Institute of Standards and Technology (NIST) for review. This process can cost hundreds of thousands of dollars for component manufacturers and designers. Only after all of this can a module be deemed “FIPS 140-2 Validated.”

Due to the cost and time associated with FIPS validation, component manufacturers wishing to save money might stick with claiming “FIPS Compliant.” This could mean that some parts, but not all, are FIPS validated. For example, the manufacturer may have validated their AES algorithm, but did not submit the entire module for review.

For those looking for a secure solution, “FIPS Compliant” does not provide a fully proven module.

2 Why does all of this matter?

Quite simply, security matters. Whether you are building a door lock, wireless camera, or an ultrasound scanner, security is always important in providing a successful product. To find that proven, tested security, you want to go with “FIPS Validated.”

3 What does TI offer in terms of FIPS Validation?

TI's SimpleLink™ CC3235x devices are FIPS 140-2 Level 1 validated and you can find the certificate here: https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3312.

TI’s WiLink™ WL1837 Combo Wi-Fi® / Bluetooth® module is validated and you can find the certificate here: https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3257.

Copyright © 2018–2019, Texas Instruments Incorporated

Revision History

NOTE: Page numbers for previous revisions may differ from page numbers in the current version.

Changes from Original (August 2018) to A Revision	Page
• Added paragraph to Section 3	2

Copyright © 2018–2019, Texas Instruments Incorporated

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, or other requirements. These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale (www.ti.com/legal/termsofsale.html) or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265
Copyright © 2019, Texas Instruments Incorporated