

Secure Connection Capability for WiLink™ Bluetooth® 4.2

ABSTRACT

The WiLink™ 8, Wi-Fi™ and *Bluetooth®*/Bluetooth low energy combination solution adds new significant Bluetooth 4.2 low energy secure connection capability to existing devices. These capabilities are compatible with the current hardware by downloading the new [TI-BT-4-2-STACK-LINUX-ADDON](#).

1 New Capabilities

Low energy (LE) secure connections – Bluetooth 4.2 security algorithm, elliptic curve Diffie-Hellman (ECDH) for key generation, and a new pairing procedure for key exchange (see [Figure 1](#)). The ECDH provides a higher security level for Bluetooth low energy authentication during the connection, to enable secure connections and protect the communication from passive eavesdropping and man-in-the-middle (MITM) attacks. Additional information can be retrieved from the Bluetooth specifications. This feature is required and requested by customers due to new regulatory requirements (for example, the new EuroPay™, MasterCard®, and Visa® EMV® standard, and the PCI DSS requirement).

TI Bluetooth Stack Linux Architecture

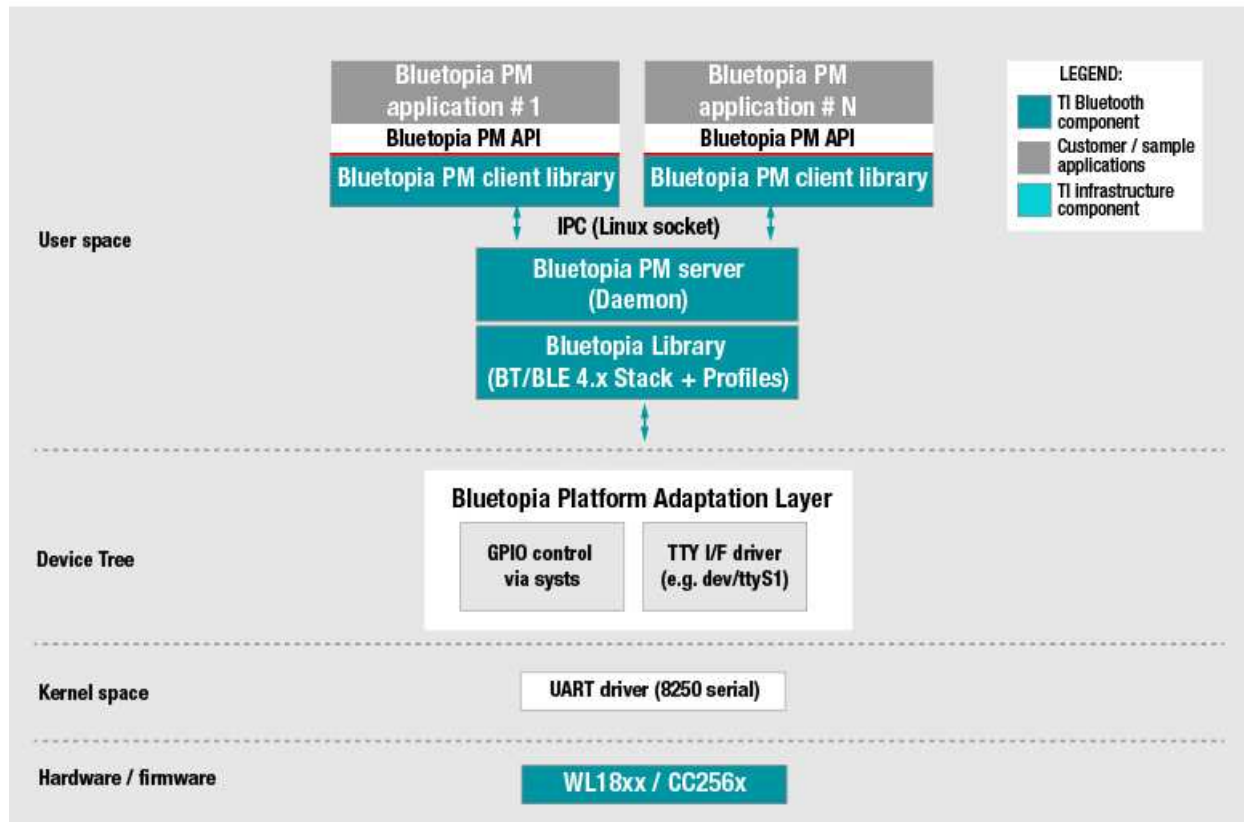


Figure 1. TI Bluetooth Stack Linux® Architecture

WiLink is a trademark of Texas Instruments.
 Bluetooth is a registered trademark of Bluetooth SIG.
 EMV is a registered trademark of EMVCo LLC.
 EuroPay is a trademark of Europay International.
 Linux is a registered trademark of Linus Torvalds.
 MasterCard is a registered trademark of MasterCard.
 Visa is a registered trademark of Visa.
 Wi-Fi is a trademark of Wi-Fi Alliance.
 All other trademarks are the property of their respective owners.

The low energy, secure connections feature introduces a new security model. To ensure communication is secure, Bluetooth 4.2 includes major enhancements to the features involved in the communication process. These enhancements follow:

- Pairing Bluetooth 4.2 adds the numeric comparison method to the three methods already existing in Bluetooth 4.0 and Bluetooth 4.1 (Just Works, Passkey Entry, and OOB), and adds the use of an ECDH algorithm for the key exchange procedure.
- Key generation is performed by the host. In the past, key generation was performed on the controller side. This allows upgrading of the key generation algorithms without the need to change the controller. The public/private key is generated in the host and the secure connection key is generated by combining inputs from each device in the pairing process.
- The encryption algorithm uses an AES-CCM, 128-bit key and 128-bit, plain-text data, compliant with FIPS-1971. These feature enhancements set the standard and help solve MITM issues and other passive eavesdropping mechanisms. This feature was introduced to enhance the security level of Bluetooth low energy, and it is a mandatory feature for POS applications and applications that require a higher level of security.

To start evaluating WiLink 8, click [here](#).

IMPORTANT NOTICE FOR TI DESIGN INFORMATION AND RESOURCES

Texas Instruments Incorporated ("TI") technical, application or other design advice, services or information, including, but not limited to, reference designs and materials relating to evaluation modules, (collectively, "TI Resources") are intended to assist designers who are developing applications that incorporate TI products; by downloading, accessing or using any particular TI Resource in any way, you (individually or, if you are acting on behalf of a company, your company) agree to use it solely for this purpose and subject to the terms of this Notice.

TI's provision of TI Resources does not expand or otherwise alter TI's applicable published warranties or warranty disclaimers for TI products, and no additional obligations or liabilities arise from TI providing such TI Resources. TI reserves the right to make corrections, enhancements, improvements and other changes to its TI Resources.

You understand and agree that you remain responsible for using your independent analysis, evaluation and judgment in designing your applications and that you have full and exclusive responsibility to assure the safety of your applications and compliance of your applications (and of all TI products used in or for your applications) with all applicable regulations, laws and other applicable requirements. You represent that, with respect to your applications, you have all the necessary expertise to create and implement safeguards that (1) anticipate dangerous consequences of failures, (2) monitor failures and their consequences, and (3) lessen the likelihood of failures that might cause harm and take appropriate actions. You agree that prior to using or distributing any applications that include TI products, you will thoroughly test such applications and the functionality of such TI products as used in such applications. TI has not conducted any testing other than that specifically described in the published documentation for a particular TI Resource.

You are authorized to use, copy and modify any individual TI Resource only in connection with the development of applications that include the TI product(s) identified in such TI Resource. NO OTHER LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE TO ANY OTHER TI INTELLECTUAL PROPERTY RIGHT, AND NO LICENSE TO ANY TECHNOLOGY OR INTELLECTUAL PROPERTY RIGHT OF TI OR ANY THIRD PARTY IS GRANTED HEREIN, including but not limited to any patent right, copyright, mask work right, or other intellectual property right relating to any combination, machine, or process in which TI products or services are used. Information regarding or referencing third-party products or services does not constitute a license to use such products or services, or a warranty or endorsement thereof. Use of TI Resources may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

TI RESOURCES ARE PROVIDED "AS IS" AND WITH ALL FAULTS. TI DISCLAIMS ALL OTHER WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED, REGARDING TI RESOURCES OR USE THEREOF, INCLUDING BUT NOT LIMITED TO ACCURACY OR COMPLETENESS, TITLE, ANY EPIDEMIC FAILURE WARRANTY AND ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF ANY THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

TI SHALL NOT BE LIABLE FOR AND SHALL NOT DEFEND OR INDEMNIFY YOU AGAINST ANY CLAIM, INCLUDING BUT NOT LIMITED TO ANY INFRINGEMENT CLAIM THAT RELATES TO OR IS BASED ON ANY COMBINATION OF PRODUCTS EVEN IF DESCRIBED IN TI RESOURCES OR OTHERWISE. IN NO EVENT SHALL TI BE LIABLE FOR ANY ACTUAL, DIRECT, SPECIAL, COLLATERAL, INDIRECT, PUNITIVE, INCIDENTAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES IN CONNECTION WITH OR ARISING OUT OF TI RESOURCES OR USE THEREOF, AND REGARDLESS OF WHETHER TI HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

You agree to fully indemnify TI and its representatives against any damages, costs, losses, and/or liabilities arising out of your non-compliance with the terms and provisions of this Notice.

This Notice applies to TI Resources. Additional terms apply to the use and purchase of certain types of materials, TI products and services. These include; without limitation, TI's standard terms for semiconductor products (<http://www.ti.com/sc/docs/stdterms.htm>), [evaluation modules](#), and [samples](http://www.ti.com/sc/docs/sampterm.htm) (<http://www.ti.com/sc/docs/sampterm.htm>).

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265
Copyright © 2017, Texas Instruments Incorporated