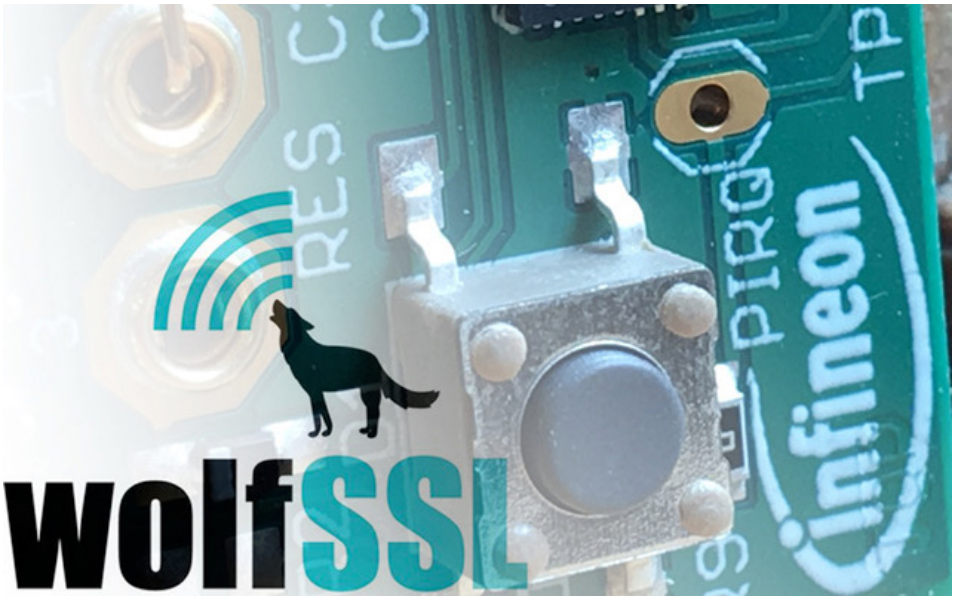
Partner Use Case

Securing the connected world with wolfSSL seamless TPM 2.0 integration

Customers can rest easy knowing their information is secured and reduce time to market with wolfSSL as a turnkey solution with the TPM 2.0 module!



Products

OPTIGA™ TPM

Use case

Application context and security requirement
In today's connected world it can be challenging for developers to combine hardware and software for countless industries and verticals.

Challenge
The Trusted Platform Module (TPM) standard is a shifting landscape that continues to evolve, sometimes very rapidly. This requires support for older solutions while striving to stay up on the latest enhancements. Many systems today consist of different architectures, and operating systems leading to additional TPM 2.0 integration efforts. The above challenges equate to a growing budget.

Implementation
wolfSSL can alleviate many aspects of these issues for customers with a turnkey solution that offers backwards compatibility and the latest enhancements. wolfSSL provides security related support for countless hardware and software combinations. wolfSSL has directly integrated the Application Programming Interface (API) of the TPM 2.0 to provide developers with a seamless well documented, ready-to-go solution.

wolfSSL targets a new release every three months and works tirelessly to stay up on the latest TPM implementation standards and device support.

Benefits for the user:
- TPM integration in a product can help manufacturers to meet some of the highest standards of trust in the security industry today.
- Fulfilling this higher trust requirement can provide in-roads to difficult-to-tap markets such as Healthcare, Transportation, Government and more.
- TPM integration can reduce time to market by taking advantage of turnkey solutions that require little or no focus during the development phase of a product.
- wolfSSL's dual license model allows commercial customers to evaluate, build, and test source code prior to purchasing.
- wolfSSL offers Basic, Standard, Premium, and 24x7 support packages in which a live cryptographic engineer can be contacted if necessary.
- End Users and Hobbyists benefit from the dual license model in that their open-source software/hardware is able to remain open source and they can freely use wolfSSL at their discretion so long as all components of their product are also open source.

Solution

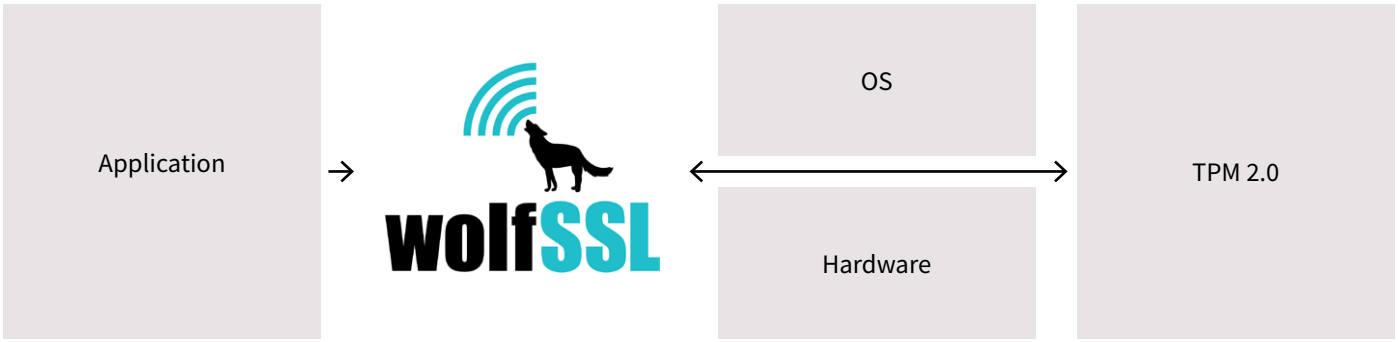
TPM 2.0 establishes trust by providing a mechanism for integrity. Integrity checks include code source authenticity and device tampering detection per device ID. TPM modules provided by Infineon allow storage of sensitive data including the aforementioned IDs, private keys, hardware measurements used to detect device tampering, and other sensitive data. Furthermore, cryptographic operations can be run from the dedicated chip and when available certain algorithms can take advantage of on-board hardware crypto to reduce execution time. This can result in faster, trusted, secured communication!

wolfSSL source code is designed to be easy to understand and work with. Developers working with the wolfSSL source code often express how impressively logical the API design is and how it translates to reduced development time and effort. Working with a given TPM module is as easy as defining a pre-processor macro for the TPM version and APIs remain consistent across standards allowing for easy migration between platforms. wolfSSL is flexibly designed for embedded systems and offers tradeoffs of speed, size, and functionality. This modular design makes it possible to support even the most constrained environments.

wolfSSL offers FIPS 140-2 level 1 validated cryptography for use in the TPM 2.0 module. This further enhances trust and opens up more marketing opportunities. wolfSSL will take care of all underlying API calls to the TPM 2.0 module so users only need to learn the wolfSSL high level APIs and everything else is taken care of under-the-hood.

Main benefits of the Infineon product

The Infineon OPTIGA™ TPM 2.0 acts as a secured environment for storing keys inside the chip. The advantage is the high level of security with the Trusted Computing Group (TCG) certification and the functional compliance to the TCG specification. This enables seamless integration and application of the OPTIGA™ TPM into the scenario.



Partner

Partners from the Infineon Security Partner Network help you secure your devices and applications: understand which threats can undermine your business, propose solutions that will protect your business, build and implement such security solutions and, when relevant manage their operation. They have been selected by Infineon on the basis of their system security competence and ability to design and deliver strong and trustworthy security solutions. Their activities are diverse and include security consulting, security solution provision, electronic design, systems integration and trust services management. For some, offers are off-the-shelf; while for others, offers are custom-built.

wolfSSL

wolfSSL focuses on providing lightweight and embedded security solutions with an emphasis on speed, size, portability, features, and standards compliance. Dual licensed to cater to a diversity of users ranging from the hobbyist to the user with commercial needs, we are happy to help our customers and community in any way.
Our products, wolfSSL embedded SSL/TLS library, wolfCrypt, and wolfCrypt FIPS, are open source; giving customers the freedom to look under the hood. They are also designed to offer optimal performance, rapid integration, the ability to leverage hardware crypto, and support for the most current standards. All products are backed by a dedicated and responsive support and development team.

wolfSSL's contribution to the Infineon Security Partner Network

The Trusted Platform Module standard is a shifting landscape that continues to evolve, sometimes very rapidly. This requires support for older solutions while striving to stay up on the latest enhancements. Many systems today consist of different architectures, and operating systems leading to additional TPM 2.0 integration efforts. wolfSSL can alleviate many aspects of these issues for customers with a turnkey solution that offers backwards compatibility and the latest enhancements.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 11 / 2017

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices please contact your nearest Infineon Technologies office (www.infineon.com).