

pbTLS – the embedded library

The **pbTLS** library is based on strong, reliable and efficient crypto elements (cipher suites) coded from scratch in C99 & automotive MISRA standard.

Communication secured by TLS has the following major features:

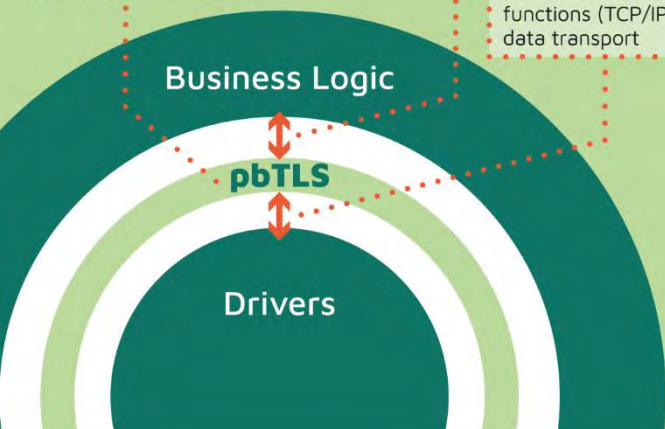
- Authenticity
- Integrity
- Privacy

IoT Device firmware with **pbTLS** inside

pbTLS transparently encrypts and decrypts application data without being noticed

New **pbTLS** API function calls

Low-Level API calls to socket send & receive functions (TCP/IP) for data transport



The **pbTLS** Library is best fit for applications with the small 32bit ARM Cortex MCUs. We deliver **pbTLS** as a static library including all required crypto components. The underlying & supported toolchains are EmBitz ARM GCC and Keil µVision v5, but the code is portable to other toolchains as well.

MEMBER OF
THE INITIATIVE

SecurITy

Trust Seal
www.teletrust.de/itsmig

made
in
Germany

POINTBLANK®



is powered by:

Steen Harbach AG
Alte Garten 60 | 51371 Leverkusen | Germany

Phone +49 214 315 212-0

info@pointblank.de

www.pointblank.de



Super Security

is no longer a matter of size.

Building Blocks of Enterprise IoT Security:

TLS & cipher middleware library for small 32-bit embedded MCU applications.

Secure IoT hardware module

Managed Services

POINTBLANK®



2017
Bundesverband IT-Sicherheit e.V.



pbTLS is the embedded TLS security solution powered by Steen Harbach AG.

Developed to secure device to device communication on the smallest network appliances for maximum security of the overall system.

The bare metal implementation **pbTLS** library is created from scratch to address the existing resource limitations in the embedded world. The Library needs 50k to 100k in MCU's flash and 500 Byte to 5k Bytes dynamically in RAM memory.

It offers the highest performance with lowest power & cost needs, and runs as a middleware on platforms with or without operating systems.

pbTLS is the innovative Transport Layer Security Library – Made in Germany.

did you know?

The Transport Layer Security Protocol (TLS) is widely used, e.g. for online banking as https, to implement strong End-to-End application layer security.

But how can TLS be used to secure device to device communication on even the smallest network attached appliances?

The answer is close-to-hardware programming with hardware engine support and implementation of needed protocols independent of an operating system = bare metal.

managed services

Enterprise IoT Security:

The integration of IoT into the enterprise business requires a complex arrangement of components from front-end (devices) to back-end (Enterprise Cloud or Data Centre).

IoT from A to Z:

- Devices with built-in TLS and PKI
- IT and cloud services for Big Data processing and secure remote automation
- PKI tools and services

Steen Harbach AG offers consistent consultancy and implementation for all essential integration steps.

- IT and project management
- Design and deployment of secure systems, infrastructure and services including PKI
- Managed services, infrastructure and application support, GxP
- Lifecycle management
- Development and implementation of secure protocols and applications for industry 4.0 based on IoT devices

pbTLS benchmarks

Performance – Platform STM:

MCU: STM32F415RG, ARM Cortex M4 @168 MHz
all cipher processing in software
complete handshake and transaction: 768 ms

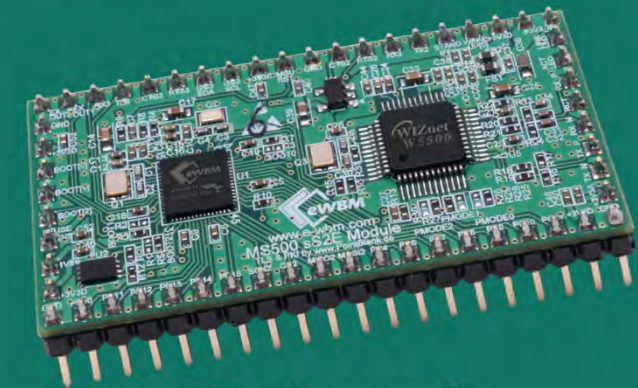
Performance – Platform eWBM:

MCU: MS500, ARM Cortex M0 @96 MHz
all cipher processing in hardware accelerator
complete handshake and transaction: 600 ms

ss2E secure IoT module

The Hardware:

the “secure Sensor-to-Ethernet” module is a plug and play solution to add secured communication to any legacy serial sensor or actuator device.



ss2E modules features



- Hardware crypto MCU by our partner **eWBM MS500**: ARM Cortex M0 incl. 4 MB Flash
- secure memory for the PKI certificates
- **W5500** Hardware TCP/IP for Ethernet I/F
- multiple UART, SPI, I2C and IO options
- act as server or client to connect to any IT backend infrastructure
- pre-programmed with FW & PKI certificates
- supports external Wi-Fi modules
- customisation services and SDK available