Fundamentals of Security in Safety-critical systems

wolfSSL

Bozeman, MT : Seattle, WA : Portland, OR : Rescue, CA : Tokyo, JP : Brisbane, AU : Mobile, AL : Stockholm, SE

Smart Grid

Automotive / Smart Cars

Smart Energy

Internet of Things

Cloud Services

Appliances

Battlefield Communication

Games

VoIP

We Secure the **Internet** by **Securing Data**

M2M

Routers

Databases

Mobile Phones

Sensors

Industrial Automation

Connected Home

Applications

Printers

Origin of wolfSSL

MySQL
yaSSL
wolfSSL

2004	2004 / 2006	2014
Needs “Clean Room” SSL	2004 - **yaSSL** (C++) 2006 - **CyaSSL** (C)	wolfSSL Name Change

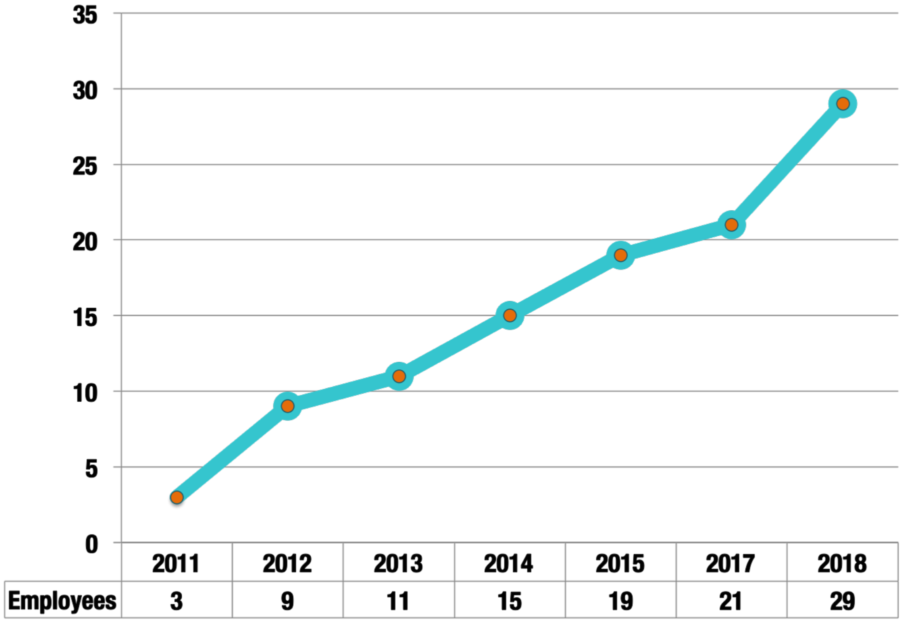
Exciting Company Growth

1,000 OEM Customers

17 Resale Partners

2 BILLION

secure connections!



	2011	2012	2013	2014	2015	2017	2018
Employees	3	9	11	15	19	21	29

Automotive

- 10+ years experience
- 10% of +1000k OEM customers are Automotive
- Major customers in Japan, Germany, USA and France
- Consumed by 3 of the Top 5 Automotive vendors
- Standardized by 2 of the world’s biggest Automotive vendors

ECUs

Telematics

Infotainment

Broad Partner Program

ARM CONNECTED
intel Software Partner
NXP
MARVELL
TEXAS INSTRUMENTS
ST life.augmented
SAMSUNG
WIND
mentor embedded
Green Hills SOFTWARE
IAR SYSTEMS
RENESAS PARTNER Gold
ANALOG DEVICES
MICROCHIP
Atmel

Three Main Areas of Focus

Data in **Transit**

1

- Secured with **SSL/TLS, SSH**
- Possible Transfer Mediums: TCP/UDP/Bluetooth/Serial/etc

Data at **Rest**

2

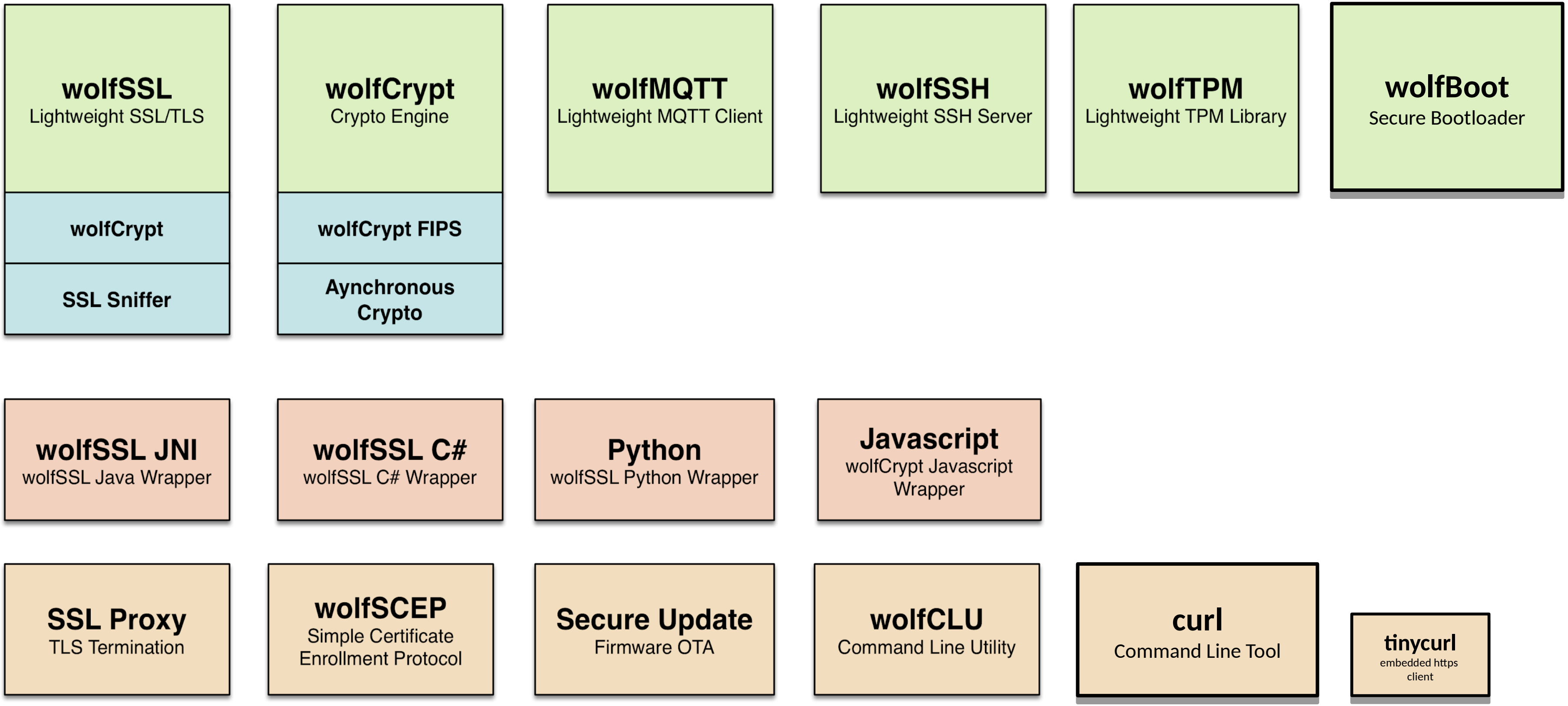
- Secured with **Cryptography**

Firmware Updates

3

- Secured with **SSL/TLS**, **crypto**, **MQTT**
- Prevent malicious firmware flashing and updates

wolfSSL Products



wolfSSL
Lightweight SSL/TLS

wolfCrypt

SSL Sniffer

wolfCrypt
Crypto Engine

wolfCrypt FIPS

Aynchronous Crypto

wolfMQTT
Lightweight MQTT Client

wolfSSH
Lightweight SSH Server

wolfTPM
Lightweight TPM Library

wolfBoot
Secure Bootloader

wolfSSL JNI
wolfSSL Java Wrapper

wolfSSL C#
wolfSSL C# Wrapper

Python
wolfSSL Python Wrapper

Javascript
wolfCrypt Javascript Wrapper

SSL Proxy
TLS Termination

wolfSCEP
Simple Certificate Enrollment Protocol

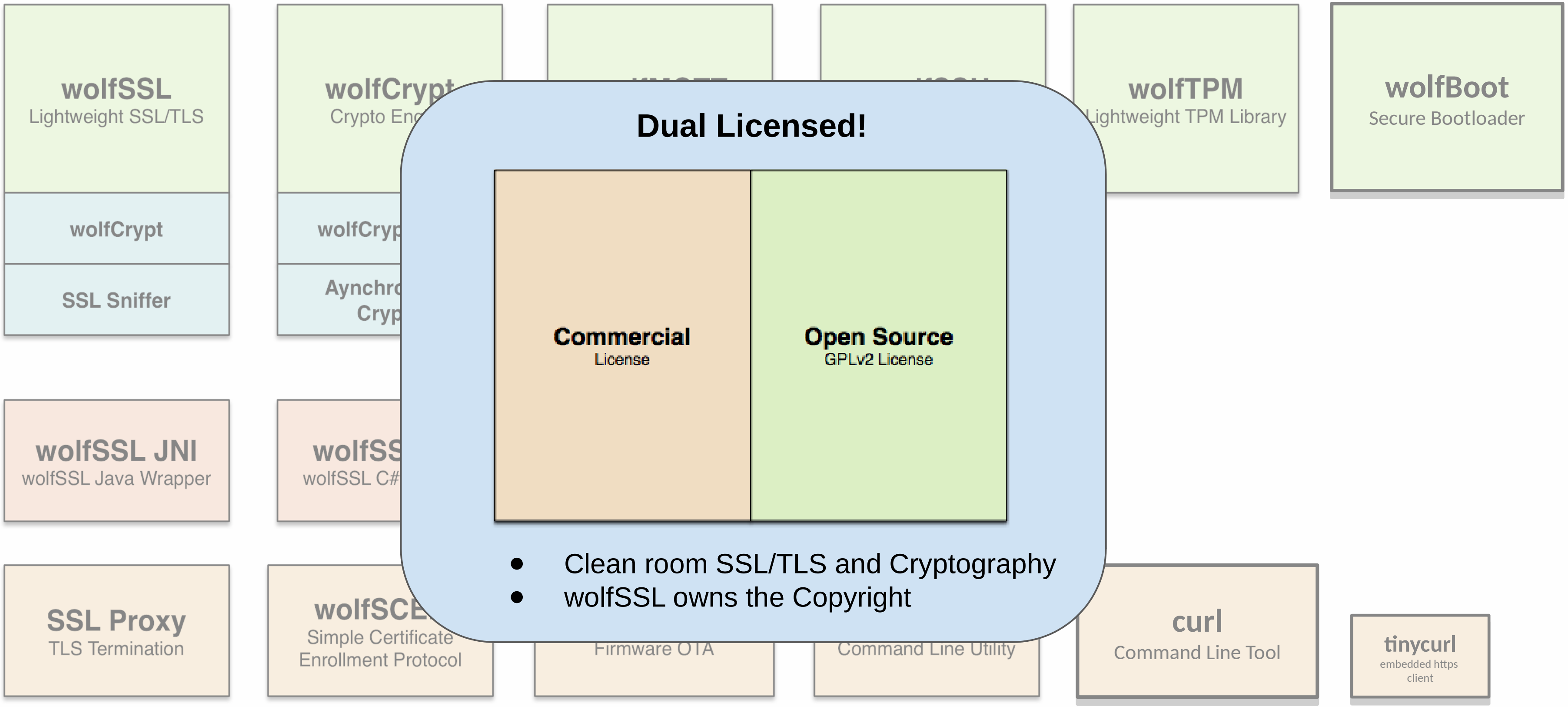
Secure Update
Firmware OTA

wolfCLU
Command Line Utility

curl
Command Line Tool

tinycurl
embedded https client

wolfSSL Product Licensing



wolfSSL
Lightweight SSL/TLS

wolfCrypt

SSL Sniffer

wolfCrypt
Crypto Enc

wolfCryp

Aynchro
Cryp

wolfTPM
Lightweight TPM Library

wolfBoot
Secure Bootloader

wolfSSL JNI
wolfSSL Java Wrapper

wolfSS
wolfSSL C#

SSL Proxy
TLS Termination

wolfSCE
Simple Certificate
Enrollment Protocol

Firmware OTA

Command Line Utility

curl
Command Line Tool

tinycurl
embedded https
client

Dual Licensed!

Commercial
License

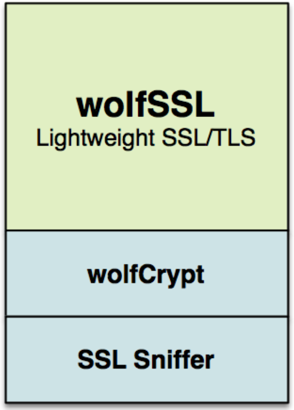
Open Source
GPLv2 License

- Clean room SSL/TLS and Cryptography
- wolfSSL owns the Copyright

wolfSSL SSL / TLS Library

LIGHTWEIGHT. PORTABLE. Written in C.

- Up to **TLS 1.3** and **DTLS 1.2**
- **20-100 kB** footprint
- **1-36 kB** RAM per session
- Up to **20X Smaller** than OpenSSL
- Long list of supported operating systems



Windows, Linux, Mac OS X, Solaris, ThreadX, VxWorks, FreeBSD, NetBSD, OpenBSD, embedded Linux, WinCE

Haiku, OpenWRT, iPhone (iOS), Android, Nintendo Wii and Gamecube through DevKitPro, QNX, MontaVista, NonStop

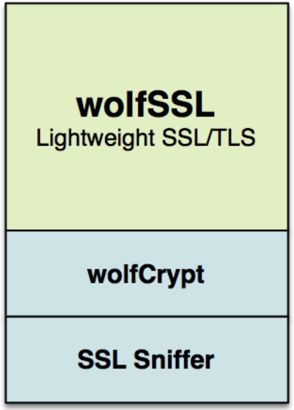
TRON/ITRON/uITRON, Micrium uC/OS, FreeRTOS, SafeRTOS, Freescale MQX, Nucleus, TinyOS, HP/UX, ARC MQX

wolfSSL SSL / TLS Library

TLS Designed from scratch. Modular, configurable, optimized

Provides top-quality security technologies
for all types of embedded systems

- Built-in hardware acceleration and assembly optimization
- Wide range of configuration options, to the single algorithm/feature
- Portable and easy to integrate
- Callback-based API for bare metal and OS integration
- Mature codebase
- Professional support
- Open Source
- Fast Release cycle



wolfCrypt Cryptographic Library

- Used by wolfSSL for cryptographic operations
- Supported Algorithms Include:

Hash Functions
MD2, MD4, MD5, SHA-1, SHA-2, SHA-3, RIPEMD, BLAKE2b

Block Ciphers
AES, DES, 3DES, Camellia, IDEA

Stream Ciphers
ARC4, RABBIT, HC-128, ChaCha20

Authenticated Ciphers
AES-GCM, AES-CCM, Poly1305

Public Key Options
RSA, ECC, DSS, DH, EDH, (Curve25519, Ed25519)

Password-based Key Derivation
HMAC, PBKDF, PBKDF2

Federal Information Processing Standards (FIPS) 140-2

Mandatory standard for the protection of sensitive or valuable data within Federal systems.

wolfCrypt FIPS 140-2 Level 1 *Certificate #2425*

wolfCrypt v4 FIPS 140-2 Level 1 *Certificate #3389*

wolfCrypt FIPS 140-3 *Validation coming soon*

FIPS-READY

wolfCrypt MISRA-C compliant

wolfCrypt MISRA C 2012

Checked with PC-Lint
Follows all mandatory rules

Rules exception documentation available

Advisory rules compliance in progress

More module added following market interests or requests

- Current MISRA-2012 validated modules:

Hash Functions
SHA-2 (sha256)

Block Ciphers
AES-GCM, AES-CBC (128, 192, 256)

Authenticated Ciphers
AES-GCM

Public Key Options
RSA

Math implementation
Single precision, 64-bit

Random library

DO-178

DO-178

guidelines dealing with the safety of safety-critical software used in airborne systems

The FAA certifies airplanes, engines and propellers
Components are certified only as part of an airplane or engine
Software is part of the system components and every line of code must be clean and traceable to requirement and test

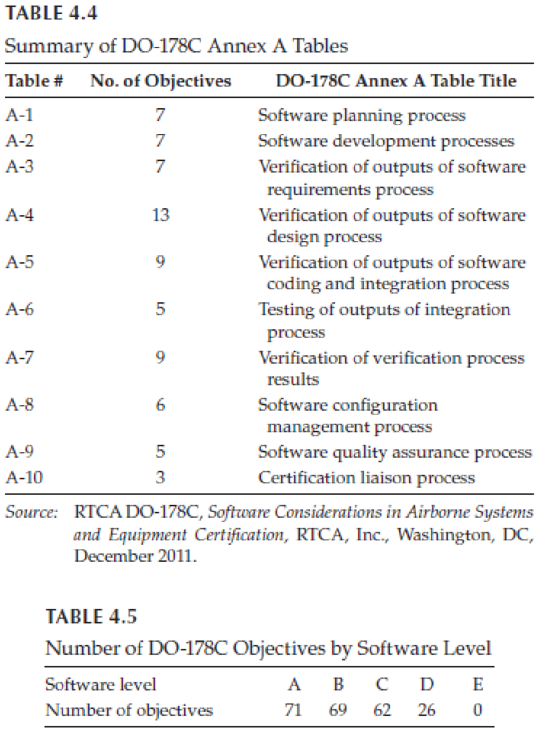


TABLE 4.4

Summary of DO-178C Annex A Tables

Table #	No. of Objectives	DO-178C Annex A Table Title
A-1	7	Software planning process
A-2	7	Software development processes
A-3	7	Verification of outputs of software requirements process
A-4	13	Verification of outputs of software design process
A-5	9	Verification of outputs of software coding and integration process
A-6	5	Testing of outputs of integration process
A-7	9	Verification of verification process results
A-8	6	Software configuration management process
A-9	5	Software quality assurance process
A-10	3	Certification liaison process

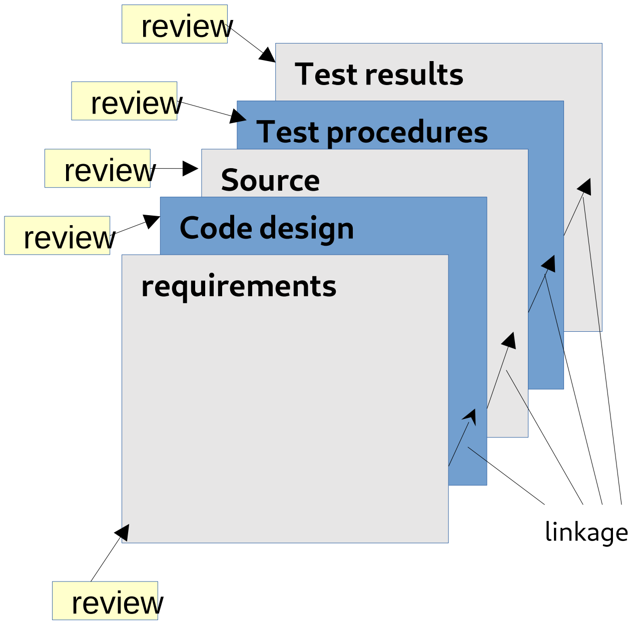
Source: RTCA DO-178C, *Software Considerations in Airborne Systems and Equipment Certification*, RTCA, Inc., Washington, DC, December 2011.

TABLE 4.5

Number of DO-178C Objectives by Software Level

Software level	A	B	C	D	E
Number of objectives	71	69	62	26	0

wolfCrypt development model:



wolfCrypt DO-178 support

DO-178 wolfCrypt

Dynamic memory allocation is forbidden

Secure boot with RSA signature verification (wolfBoot)

- Current DO-178 validated modules:

Hash Functions
SHA-1, SHA-2, SHA-3

Block Ciphers
AES-GCM, AES-CBC (128, 192, 256)

Stream Ciphers
ChaCha20

Authenticated Ciphers
AES-GCM, AES-CCM, Poly1305

Public Key Options
RSA (Sign + Verify)

cURL

SECURE ACCESS TO WEBSERVICES (and much more...)

Securely transfer critical business information between users, locations and partners in compliance with data security regulations

- cURL is an open source project that makes a command line tool and a library for transferring data using Internet protocols
- Very popular and well-established open source project, present in almost all Linux distributions
- Libcurl: more than 1 Billion users
- 200+ companies are using it in embedded Linux based products
- Typical scenario (embedded): access existing web and network services on the cloud
- tinycurl library: HTTPS 1.0 within 100k on 32bit microcontrollers

curl
Command Line Tool

tinycurl
embedded https client

Supported protocols:

DICT, FILE, FTP, FTPS, GOPHER, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMB, SMBS, SMTP, SMTPS, TELNET, TFTP

wolfMQTT

LIGHTWEIGHT, STANDARD, SECURE MESSAGE-BASED PROTOCOL

wolfMQTT

Lightweight MQTT Client

- Scenario of use: in constrained environments (low resources, small bandwidth)
- MQTT is one of the most popular and widely supported standard
- OASIS standard (ISO/IEC PRF 20922)
- Publish/subscribe mechanism based on TCP
- MQTT-over-TLS option on port 8883, using **wolfSSL**
- Easily integrated in RTOS/Bare-metal applications
- Code examples working with major commercial cloud services
- Supports latest standard (MQTT 5.0, October 2018)
- Optional support for MQTT-SN (sensor network transport layers)

wolfSSH

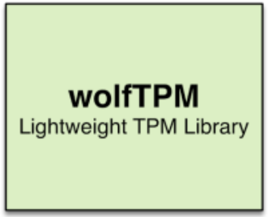
- **Portable library for server-side SSH (v2.0) with key-based and password-based authentication**
  - Supports SCP
  - Supports SSH File transfer protocol (SFTP) with a complete set of customizable primitives for remote filesystem management
  - **Full protocol interoperability with all popular SSH clients**

wolfSSH
Lightweight SSH Server

Win32/64, Linux, Mac OS X, Solaris, ThreadX, VxWorks, FreeBSD, NetBSD, OpenBSD, embedded Linux, WinCE, Haiku, OpenWRT, iPhone (iOS), Android, Nintendo Wii and Gamecube through DevKitPro, QNX, MontaVista, OpenCL, NonStop, TRON/ITRON/µITRON, Micrium's µC/OS, FreeRTOS, SafeRTOS, Freescale MQX, Nucleus, TinyOS, HP/UX, ARC MQX, TI-RTOS

wolfTPM

- **LIBRARY SOLUTION TO SIMPLIFY ACCESS TO TPM DEVICES**
  - Key Generation
  - RSA Encrypt/decrypt
  - ECDSA sign/verify
  - ECDH shared secret
  - Secure NV memory (key and sensible data storage)
  - Support for I2C and SPI Transport Interface Specification (TIS)
  - Compact, portable, no external dependencies, written in C



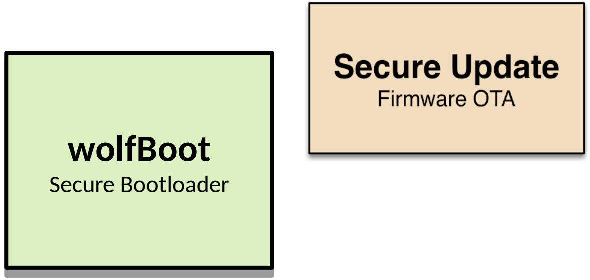
wolfTPM

Lightweight TPM Library

wolfBoot

THE SECURE BOOTLOADER FOR 32-BIT MICROCONTROLLERS

- Essential component for safe and secure remote updates
- Multi-slot partitioning of the flash device
- Integrity verification of the firmware image
- Inspired by IETF SUIT draft
- Authenticity verification of the firmware image
  using wolfCrypt's Digital Signature Algorithms (ECDSA / RSA / ED25519)



Secure Update
Firmware OTA

wolfBoot
Secure Bootloader

wolfBoot supports ARM Cortex-M and RISCV-32bit platforms.

- OS-Agnostic
- External SPI flash support
- Support for wolfTPM
- Hardware accelerators via **wolfCrypt** drivers
- Optional **DO-178 compliant** RSA verification

Thanks!

Questions?

facts@wolfssl.com

www.wolfssl.com

www.github.com/wolfssl

Bozeman, MT : Seattle, WA : Portland, OR : Rescue, CA : Tokyo, JP : Brisbane, AU : Mobile, AL : Stockholm, SE