ORYX EMBEDDED

Networking and Security Solutions for RENESAS MCUs and MPUs

Oryx Embedded
165 rue Louis Barran, ZA Centr'Alp 2,
38430 Saint-Jean-de-Moirans – FRANCE
Email : info@oryx-embedded.com

Our Offer

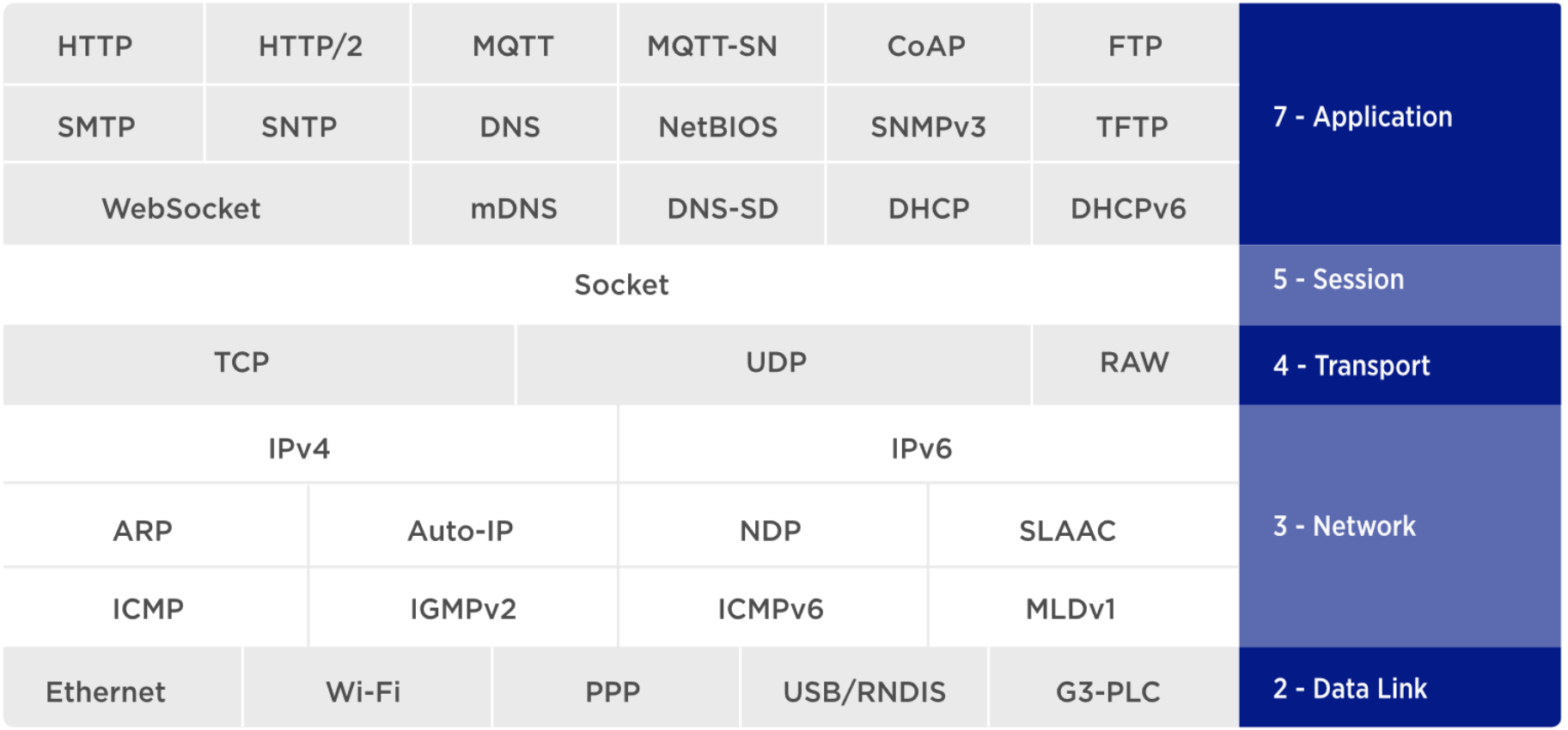
- Oryx Embedded offers a complete range of networking solutions for embedded systems, making the Internet of Things (IoT) a reality

- Our portfolio includes professional-grade TCP/IP components as well as TLS/DTLS, Secure Shell (SSH) and Cryptography solutions

Agenda

- CycloneTCP – Professional-grade dual stack (IPv4 and/or IPv6)
  - Main Features
  - Transport Layer & Multiples Interfaces
  - Focus on IoT Protocols such as MQTT
- CycloneSSL - Secure network protocols (TLS/DTLS)
  - Main Features
  - TLS Protocol Status
  - Focus on TLS 1.3
- ORYX – Demos on RENESAS evaluation boards
- ORYX – Download full ANSI C source code

CycloneTCP - Stack Model



CycloneTCP - Main Features

- Professional-grade dual stack (IPv4 and/or IPv6) dedicated to embedded applications
- Supports most popular architectures (MCUs and MPUs)
  - ARM Cortex-M3/M4/M7, Cortex-A5/A8/A9, RX600, RISC-V…
- Large database of network drivers
  - Renesas Microcontrollers with built-in MAC: RA6M2, RA6M3, RA6M4, RX62N, RX63N, RX64M, RX65N, RZ/A1L, RZ/A1M, RZ/A1H, RZ/A2M, Synergy S5D9, Synergy S7G2
  - Renesas Ethernet PHYs: uPD60610; uPD60611
- Professional-grade source code
  - Strict conformance to RFC standards, rigorously tested
  - Proprietary, fully supported and highly maintainable

CycloneTCP - Flexibility

- Flexible memory footprint
- Industry standard compilers supported
- Supports industry standard RTOS
  - FreeRTOS / RTX / CMSIS-RTOS / µC/OS / embOS / ThreadX / …
- Dual licensed software
  - Open source (GPLv2)
    - Freely available to open source developers
    - No time limit for evaluation
  - Commercial license
    - Closed source code (no need to release source code)
    - Royalty-free licenses
    - Professional technical support & services

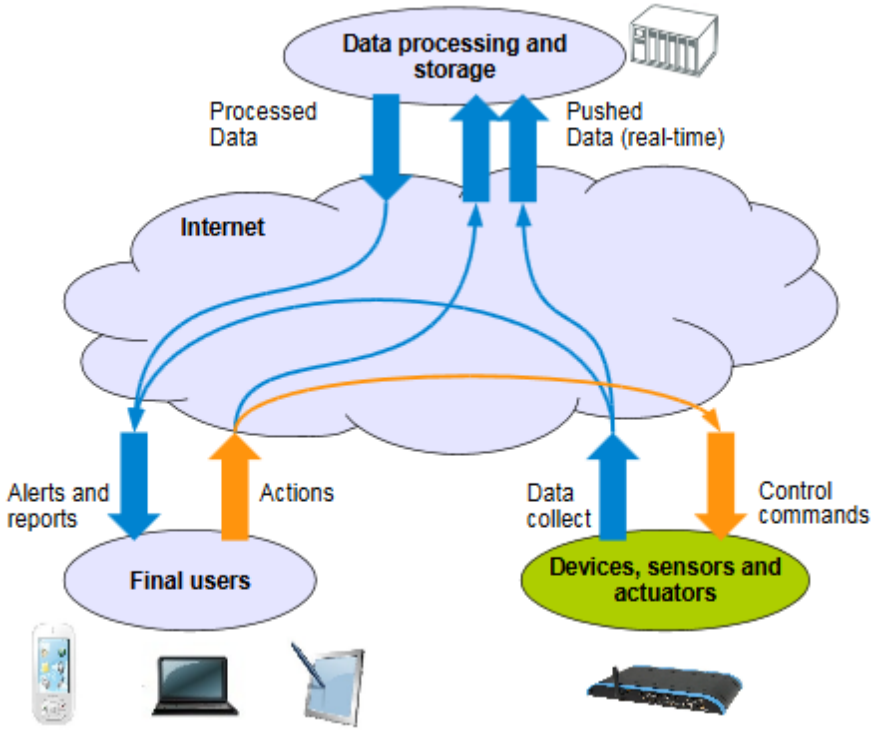
CycloneTCP - Transport Layer

- Built-in support for multiple interfaces
  - LAN, Wi-Fi, Cellular Modem, PLC, Ethernet over USB, Ethernet over SPI

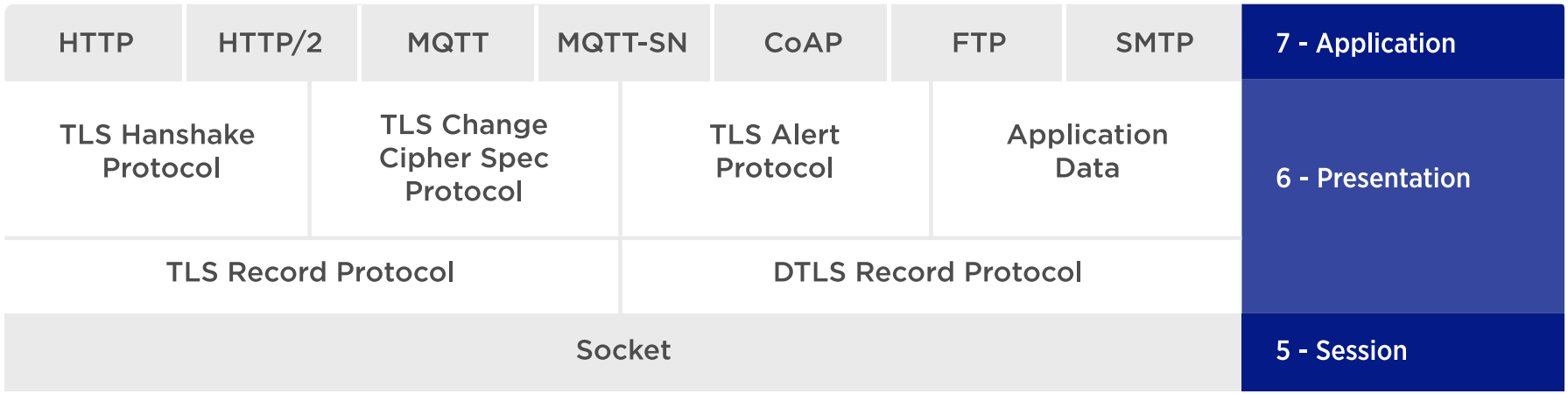
- Ethernet is the most common medium…but CycloneTCP can also be deployed over some other technologies:
  - PPP (GPRS/UMTS modem, Iridium modems)
    - Most of cellular modems supporting PPP can be used with CycloneTCP
  - Wi-Fi
    - Support for Wi-Fi chips without built-in TCP/IP stack
    - Concurrent use of Soft-AP and Infra modes is made possible (when supported by the hardware)
  - Ethernet Switches
    - 100Base-TX and Gigabit Ethernet switches

CycloneTCP – Focus on MQTT

- Publish/subscribe messaging
- Simple... but efficient protocol!
- Lightweight implementation
- Low bandwidth requirements
- Open standard, Cloud connection
- Many transport protocols supported
  - TCP (optionally over SSL/TLS)
  - WebSockets (WS)
  - Secure WebSockets (WSS)
- Communication made easy (no firewall issues)
- Home automation and industrial monitoring applications (scalable architecture)



CycloneSSL - Stack Model



CycloneSSL - Main Features

- Lightweight SSL/TLS & DTLS implementation
- Secure communications over the Internet
  - IoT Protocols (CoAP, MQTT)
  - Electronic mail (SMTPs)
  - Web server (HTTPs)
  - File transfer (FTPs)
  - VoIP
- Client and/or server operation
- Rich set of cipher suites
- Elliptic Curve Cryptography (ECC) support
- Crypto library available separately (CycloneCrypto)

CycloneSSL - Secure Protocols

- Industrial customers require more and more connectivity…
  …but security is now a MUST HAVE!
- Some applications:
  - Automatic firmware updates for end devices
  - Monitoring / status reporting
  - Remote control of a process
- Standard protocols require an extra security layer:
  - Secure FTP (FTP over SSL/TLS)
  - Secure HTTP (HTTP over SSL/TLS)
  - SNMPv3 agent with data authentication (MD5/SHA-1/SHA-2) & data privacy (DES / AES)
  - Secure WebSockets (wss://)

CycloneSSL - TLS Protocol Status

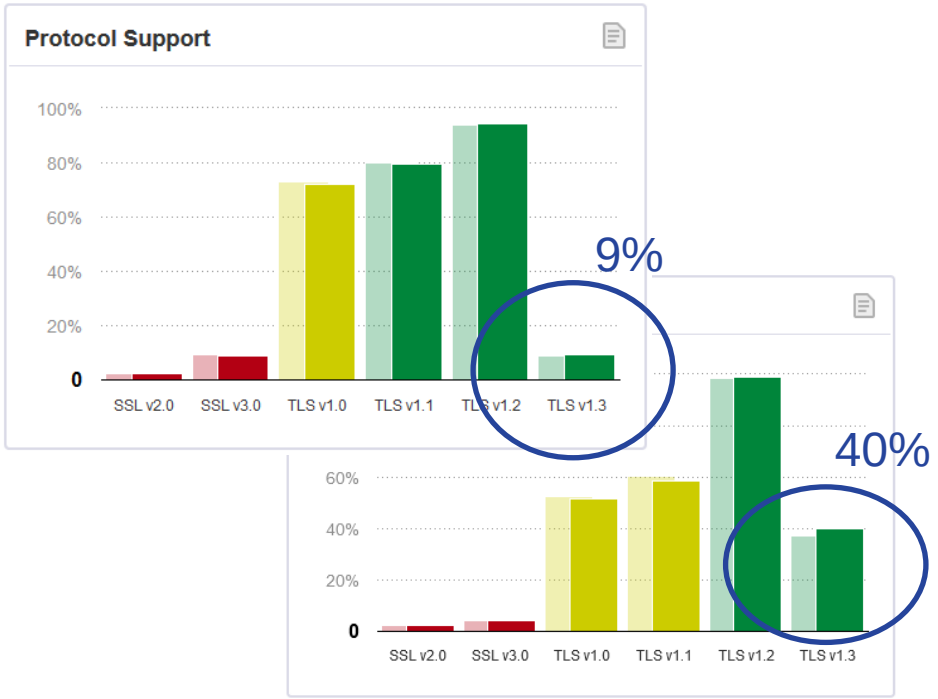
Version	Publish Date	Status
SSL 3.0	November 1996	Prohibited in 2015 (RFC 7568)
TLS 1.0	January 1999	Deprecation planned in March 2020 (RFC draft)
TLS 1.1	April 2006	Deprecation planned in March 2020 (RFC draft)
TLS 1.2	August 2008	Active
TLS 1.3	August 2018	Active

CycloneSSL - TLS 1.3 Motivations

- Prune insecure and weak cryptographic primitives
- All public-key based key exchange mechanisms now provide forward secrecy
- TLS handshake has been reworked to be more secure and faster
- Elliptic Curve Cryptography (ECC) is now in the base specification
- A zero round-trip time (0-RTT) mode was added, saving a round trip at connection for sending application data
- Make transition to TLS 1.3 possible without any fallback mechanism!

CycloneSSL - TLS 1.3 Deployment

- RFC 8446 has been released on mid August 2018.
- Chrome version 70 (October 17th, 2018) added official support for RFC 8446
- Firefox version 63 (October 23th, 2018) added official support for RFC 8446
- Today, most of secure connections on Gmail and Facebook servers make use of TLS 1.3!
- 9% of Web sites support TLS 1.3 (November 2018)
- 40% of Web sites support TLS 1.3 (November 2020)



Source: Qualys SSL Labs

ORYX Demos for RENESAS

Many demos available on standard Renesas eval boards

- RDK-RX62N
- RDK-RX63N
- RSK-RX63n
- RSK-RZ63n-256K
- RSK-RZA1H
- YSTREAM-IT-RZ-V2
- M13-RZ/A2M-EK
- M13-RA6M3-EK
- PK-S5D9
- SK-S7G2

External Links

- Download / View source code

  https://www.oryx-embedded.com/download/

- CycloneTCP

  https://www.oryx-embedded.com/products/CycloneTCP

- CycloneSSL

  https://www.oryx-embedded.com/products/CycloneSSL

- CycloneSSH

  https://www.oryx-embedded.com/products/CycloneSSH

- CycloneCRYPTO

  https://www.oryx-embedded.com/products/CycloneCRYPTO