Ubiquitous AI Corporation

RA Ecosystem Partner Solution

Ubiquitous TLS

Light Weight TLS/SSL Protocol for IoT devices

1. Overview

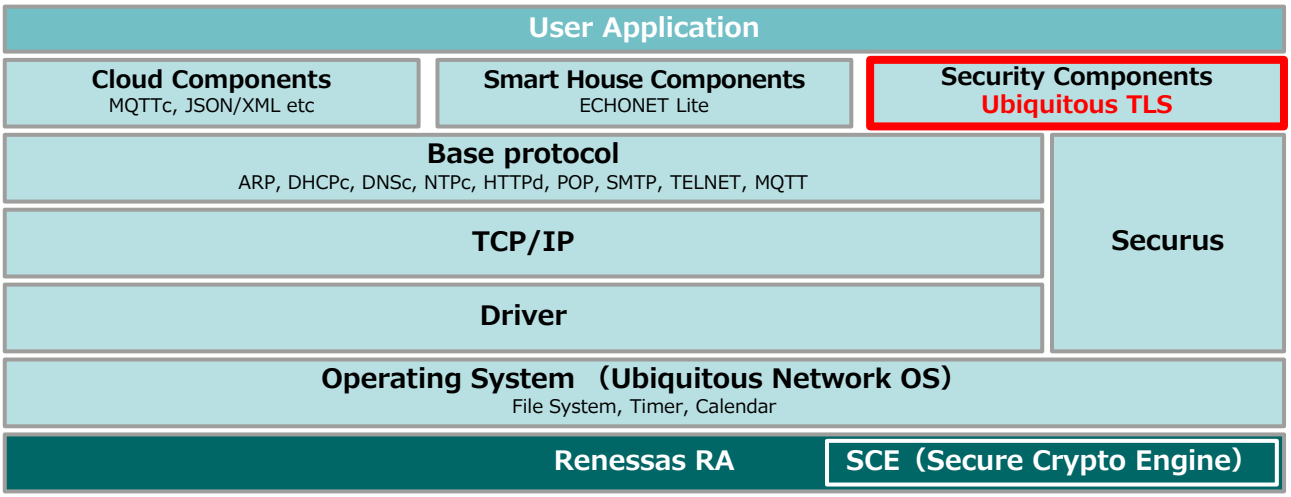
Ubiquitous TLS is designed for hardware resource limited IoT devices. The protocol stack running on RA MCUs will enable safety internet connection of various IoT devices such as sensor device, smart appliance, wearables, network camera and payment terminal.

2. Features

- TLS 1.2／1.3
- Supported NIST standardized SHA-2 Certificate
- OCSP（Online Certificate Status Protocol），SNI（Server Name Indication）
- Ubiquitous AI Corporation originally designed software product for extensive development environment and platform.

3. Block Diagram

Easily integrated into our own platform「Ubiquitous Network Framework」or other party's security middleware.



4. Target market & Applications

- Consumer
- Industrial
- Healthcare
- Home Appliance
- Automotive
- OA
- Smart Home
- IoT Devices

https://www.ubiquitous-ai.com/products/tls/

2020.07

Ubiquitous AI Corporation

Cipher Suite

TLS1.3
TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_CCM_SHA256

TLS1.2 (AEAD)	TLS1.0/1.1/1.2
TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_CCM TLS_RSA_WITH_AES_256_CCM TLS_DHE_RSA_WITH_AES_128_CCM TLS_DHE_RSA_WITH_AES_256_CCM TLS_ECDHE_ECDSA_WITH_AES_128_CCM TLS_ECDHE_ECDSA_WITH_AES_256_CCM TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_DES_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_RC4_128_SHA TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_RC4_128_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

【Related products】

- **Ubiquitous Network Framework :** Originally designed TCP/IP stack based middleware for enabling communication features on your embedded applications.
- **Ubiquitous TPM Security :** Security software solution utilizing TPM with high tamper resistance
- **Ubiquitous Securus :** Secure hardware to prevent data leakage and tampering

Web Inquiry form : https://www.ubiquitous-ai.com/en/contact/product/

Email : sales@ubiquitous-ai.com