Ubiquitous AI Corporation

RA Ecosystem Partner Solution

Ubiquitous TLS

株式会社ユビキタスAIコーポレーション

概要

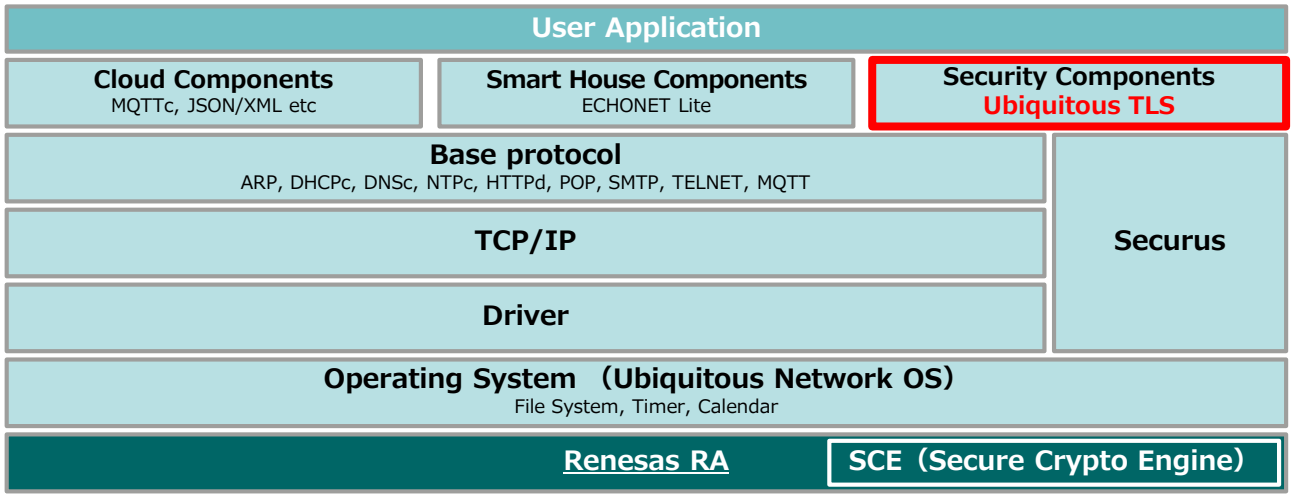
Ubiquitous TLS は、ユビキタスAIコーポレーションが独自開発した TLSプロトコルスタックです。ハードウェアリソースが制限された IoT 機器に最適な省リソースかつ処理速度を備え、センサーデバイスやスマート家電、ウェアラブル、ネットワークカメラ、決済端末など、多様な IoT 機器の安全なインターネット接続を実現します。

主な機能

- TLS 1.2／1.3 対応
- NIST の標準に採用されているSHA-2 証明書に対応
- OCSP（Online Certificate Status Protocol）、SNI（Server Name Indication）対応
- フルスクラッチでの自社開発製品のため、幅広い開発環境への対応と迅速な技術サポートが可能
- TLS バージョンの異なるサーバー側への API 互換性により可用性を維持
- RAファミリに対応

ブロック図

IoT デバイス向け軽量通信プロトコル「Ubiquitous Network Framework」他プロトコル製品群や暗号処理／秘匿情報管理向け製品などユビキタス社の幅広い商品群と組合せ可能



ターゲット市場および用途

- コンシューマ機器
- 産業機器
- ヘルスケア機器
- ホームアプライアンス
- 車載機器
- OA機器
- スマートホーム
- IoT機器

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

2021.04

Ubiquitous AI Corporation

Cipher Suite（暗号スイート）

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

【関連製品】

- Ubiquitous TLS と合わせてご利用可能な TCP/IP プロトコルスタック

  IoT デバイス向け軽量通信プロトコル「**Ubiquitous Network Framework**」

- 証明書や鍵情報の耐タンパ領域への保存や処理の分離によって、強固なセキュリティを実現するソリューション

  TPM セキュリティソリューション「**Ubiquitous TPM Security**」

- IoT デバイス向け耐タンパセキュリティソリューション「**Ubiquitous Securus - セキュラス**」