Atmel Hardware-TLS (HW-TLS)

Hardening Transport Layer Security for IoT

In both consumer and embedded systems for industrial applications, devices are being connected on wireless networks to form complex smart device and cloud service ecosystems. There is a rapidly growing trend to secure these networks to prevent intrusions as well as to allow the ecosystem owners to control access to their network of resources. Previously, authentication on the transport (network) layer using SSL/TLS when connecting to servers was historically not done or only done one-way due to the difficulty in verifying the identity of remote devices. It was considered an acceptable level of security because remote users could authenticate themselves on the web application layer and the identity of the device being used was less important. In the new world of the Internet of Things (IoT) where autonomous devices authenticate themselves, this level of security is no longer acceptable.

The Atmel® Hardware-TLS (HW-TLS) software libraries for wolfSSL and OpenSSL enable hardware-based elliptic curve mutual authentication for TLS using the Atmel CryptoAuthentication™ ATECC508A Crypto co-processor. Currently, designers of embedded systems and IoT devices relying solely on TLS for network/ecosystem security have few options for strongly authenticating the identity or origin of the remote device. In addition, certificates and private keys are currently stored in software, which leaves them more vulnerable to attack. With Atmel HW-TLS support libraries, system designers using wolfSSL or OpenSSL can take advantage of Atmel Crypto hardware to enable strong mutual authentication between communicating devices as well as for storing keys, certificates and other sensitive data in a protected hardware device.

The wolfSSL and OpenSSL libraries allow customers using those software packages to harden their networks on the transport layer with the ATECC508A device. Unlike other hardware solutions that only offer encryption and hash acceleration, the ATECC508A embeds a root of trust within the chip that provides a unique, verifiable identity within each device that uses it. Encryption is necessary, but it only prevents eavesdropping and cannot verify the identity of the other party. Using the ATECC508A, you can now verify the identity of the entity with whom you are communicating. Additionally, with the Atmel HW-TLS libraries from wolfSSL and OpenSSL, users can significantly enhance TLS communication security by implementing hardware-based authentication and secure key storage.

Atmel HW-TLS also makes it easy to implement strong elliptic curve authentication on the transport layer as well as the application layer.

Key Features

- Elliptic Curve Authentication enables robust identification of autonomous IoT nodes
- Secure Hardware Key Storage for TLS implementations to protect security keys from intrusion as well as physical attacks
- Cryptographic Co-Processor for rapid authentication and key agreement processing; low power sleep mode, and code space reduction for host processors
- Flexible software and APIs to allow custom Application Layer security needs beyond TLS
- Atmel Certified-ID platform for secure provisioning of any IoT or cloud ecosystem
- Readily available solution with downloadable software packages for wolfSSL, OpenSSL and Atmel Studio supporting the ATECC508A device

Atmel Hardware-TLS (HW-TLS)
Hardening Transport Layer Security for IoT

ECC-256 Availability

Device	Description
ATECC508A-wolfSSL	ATECC508A crypto element hardened wolfSSL with private key protected storage and secure execution environments. Download from wolfSSL: https://wolfssl.com/wolfSSL/Home.html
ATECC508A-OpenSSL	ATECC508A crypto element hardened OpenSSL with private key protected storage and secure execution environments. Download from OpenSSL: https://wiki.openssl.org/index.php/Binaries Download from GitHub: https://github.com/AtmelCSO/cryptoauth-openssl-engine

Atmel Corporation 1600 Technology Drive, San Jose, CA 95110 USA **T :** (+1)(408) 441. 0311 **F :** (+1)(408) 436. 4200 | **www.atmel.com**