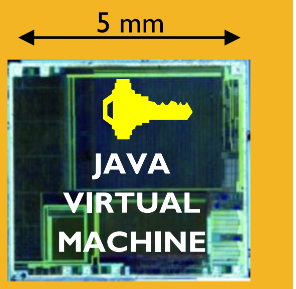
ETHER TRUST

La FRENCH TECH

CES LAS VEGAS JAN 9-12 2018

Innovative Security Architecture for Low Cost Low Power IoT Devices Based on Secure Elements



A Secure Element (SE) is a Secure Microcontroller, equipped with interfaces such as NFC, ISO7816, SPI, I2C. 10 billion of SE has been shipped in 2016, for SIM modules, bank cards, ePassport, PKI tokens.

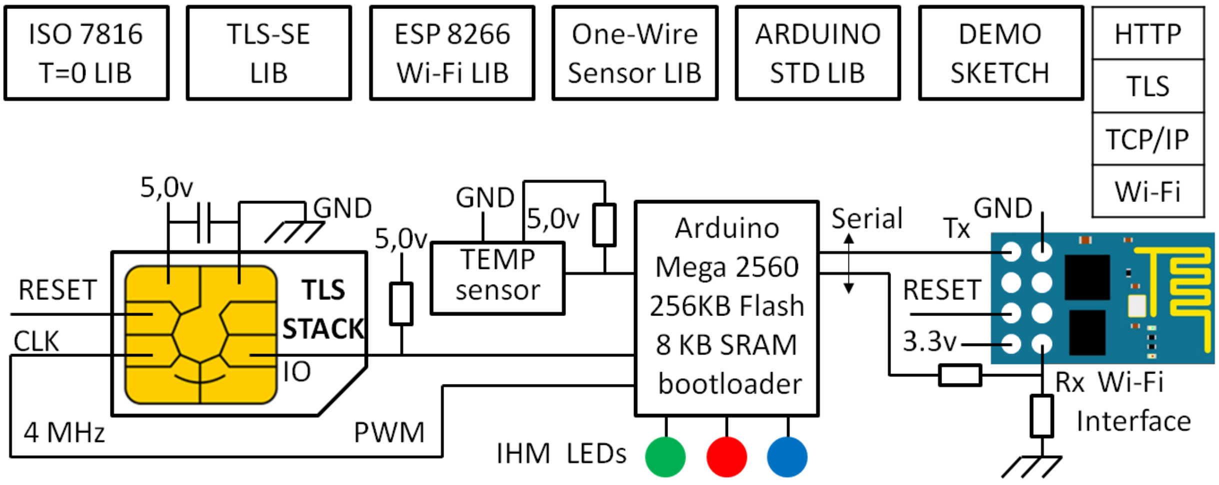
The demo board includes:
- Arduino Mega
- Wi-Fi SoC
- javacard
- C++ framework
-EtherTrust TLS/DTLS stack

All communications go through the Secure Element and port 443

We are living in a connected world. Businesses and Individuals increasingly rely on mobile and cloud applications and want protection from eavesdropping or hacking. Although many announcements claim to provide security and privacy, daily news show a different reality. In addition mobiles or IoT devices can be stolen, lost, hijacked.

It is time for the IoT industry to consider securing connected devices with Secure Elements, like Mobile Phones, Bank Cards, Identity Cards, and Hardware Authentication Tokens have been for many years.

EtherTrust TLS/DTLS Secure Identity modules imbedded in Secure Elements provide the ultimate security for IoT devices: tamper resistance, secure communications and storage.



This use case demonstrates a low cost & low power, high security, Wi-Fi connected thermometer. All object communications go through the Secure Element and its imbedded TLS/DTLS stack.

This innovative concept provides the following benefits:

- ✓ **Strong end-to-end security**: Leverages Secure Elements and TLS/DTLS protocol. Eliminates risks associated with devices vulnerabilities, with strong and password less mutual authentication (TLS is fully processed within the crypto chip), secure key storage and computing.
- ✓ **Industry Standards Compliant:** GlobalPlatform, EMVco, HCE, IETF, DTLS/TLS
- ✓ **Open:** The software framework is OpenSource.

ETHER TRUST

La FRENCH TECH

CES LAS VEGAS JAN 9-12 2018

EtherTrust TLS/DTLS Security Modules: Open Technologies dedicated to the IoT Security

TLS/DTLS Security Modules

Ethertrust designs TLS/DTLS stacks for secure elements, providing server and client features.

Our stacks are compatible with most commercially available secure elements. They are uniquely optimized, requiring between 20 and 30KB of memory, and a minimum of one KB of RAM.

Secure Element-side API

A small footprint TLS/DTLS stack that enables secure connections between SEs, terminal, IoT devices and servers.

EtherTrust TLS/DTLS Stack (ETS) supports most types of SE (NFC, SIM/USIM, SecureSD, SmartMX, etc.), and is compatible with emerging protocols such as CoAP (IETF) and token-requestor (EMVco). TLS/DTLS security modules are specified by an IETF draft.

Terminal/Server-side APIs

Enable applications to communicate with SE, leveraging NFC and HCE (Host Card Emulation). Supported environments include: Android (Java), Windows (DLL), and C for IoT device or POS type embedded systems.

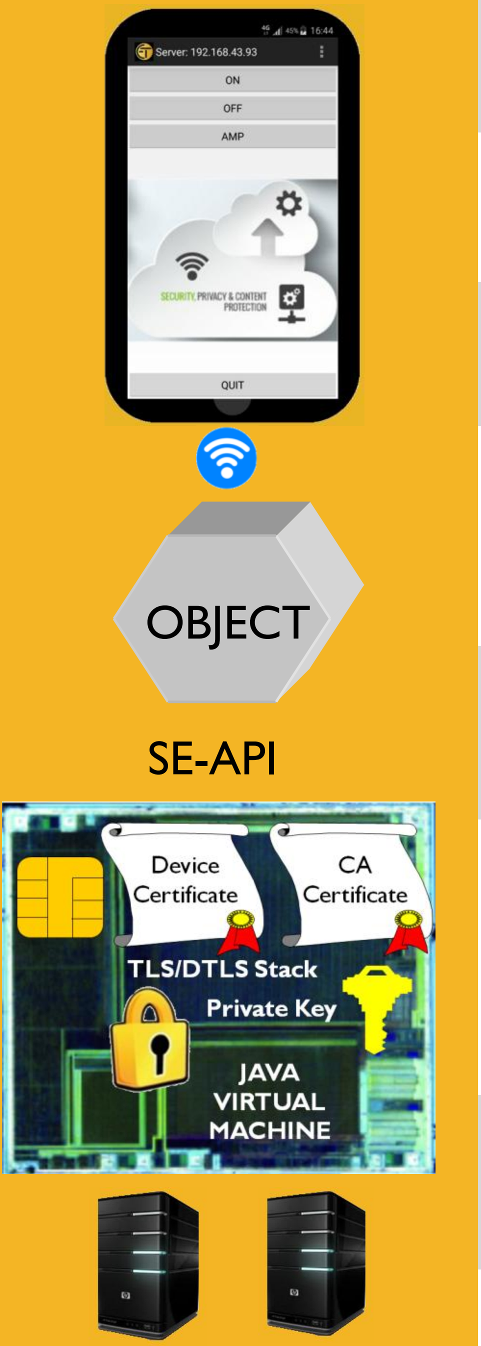
These APIs support two classes of mobile applications; 1) Security applications, such as electronic signing, authentication, encryption and decryption; 2) NFC applications such as payments with HCE interfaces or access control in corporate environments. Compatible with the NFC HCE (Host Card Emulation) mode available for the Android operating system, these APIs enable remote use of secure elements identified by their network

Server Administration APIs (C)

Management Software facilitate the remote life cycle management of SE based applications and data (i.e. application downloading, activation and deletion). Open Source based and Global Platform compliant.

About EtherTrust

EtherTrust markets software for secure elements, and designs innovative solutions that strengthen the security of IoT, Mobile, and Cloud applications. The company has received multiple national and industry specific innovation awards. EtherTrust is a key contributor to the IETF.



Administration of Secure Elements imbedded in IoT devices

EtherTrust - SAS
www.ethertrust.com