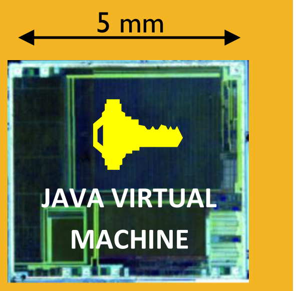
TLS/DTLS and Secure Elements provide ultimate IoT Devices Security: A Secure Smart Plug Use Case



A Secure Element (SE) is a Secure Microcontroller, equipped with interfaces such as NFC, ISO7816, SPI or I2C.

10 Billion SEs have been shipped in 2016, for SIM modules, bank cards, ePassport, PKI tokens.

Secure Smart Plug prototype includes:

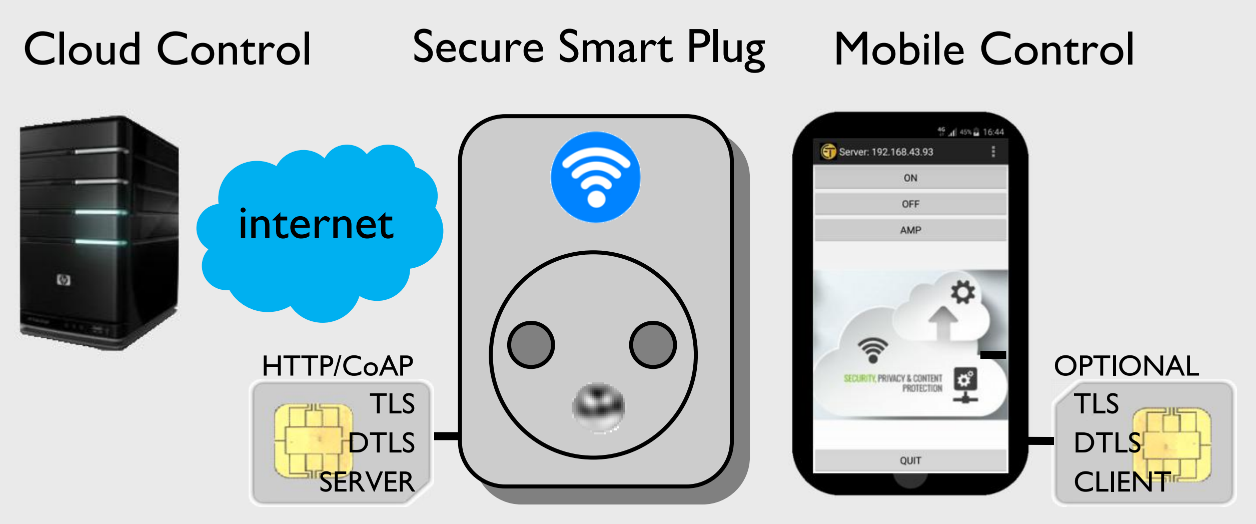
- *Raspberry PI B+*
- *Wi-Fi dongle*
- *Javacard & reader*
- *Java framework*
- *EtherTrust TLS/DTLS stack*

All communications go through the Secure Element and port 443

In October 2016, a massive Internet attack caused outages and network congestion at a large number of Web sites including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix. It was launched with the help of hacked "Internet of Things" (IoT) devices, such as CCTV video cameras and other video equipment. The devices had been turned into a large and powerful botnet.

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 and secure communications and storage.

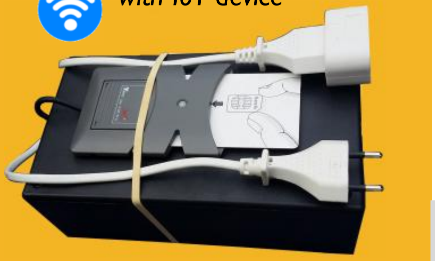


All communications with the above High Security Smart Plug go through the Secure Element and its imbedded TLS/DTLS stack. In this example the device is managed remotely by the energy operator. Selected authorized resources have direct device access through a mobile phone with an identity module (optionally imbedded in a secure element for added security, such as preventing the tampering/cloning of embedded apps). This innovative concept provides the following benefits:

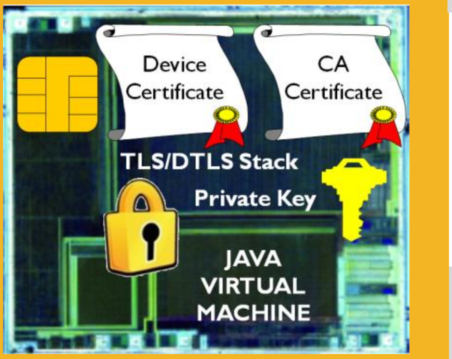
- ✓ **Strong end-to-end security**: Leverages Secure Elements and TLS/DTLS protocol. Eliminates risks associated with devices vulnerabilities, with strong and password less mutual authentication (TLS is fully processed within the crypto chip), secure key storage and computing.
- ✓ **Industry Standards Compliant:** GlobalPlatform, EMVco, HCE, IETF, DTLS/TLS.
- ✓ **Open:** Secure Element administration Middleware (cloud server or mobile device versions) is open source.

EtherTrust TLS/DTLS Security Middleware: Standard Based Technologies to secure IoT device communications

Direct TLS/DTLS communications with IoT device



Exclusively communicates through Secure Element and imbedded TLS/DTLS stack.



Administration of Secure Elements imbedded in IoT devices

EtherTrust - SAS

www.ethertrust.com

TLS/DTLS Security Modules

EtherTrust TLS/DTLS software stacks for Secure Elements provide client and server functions, with on/off card application and management APIs.

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 remote Secure Element hosted in dedicated (RACS) servers, 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 applications: 1) Security applications, such as electronic signing, authentication, encryption and decryption; 2) NFC applications such as payments with HCE (Host Card Emulation) interfaces or access control (for example corporate environments). Compatible with the NFC HCE mode available for the Android operating system

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.