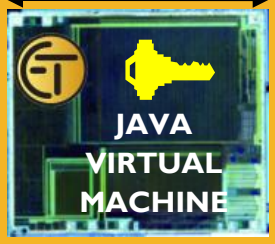
EtherTrust "Liberate your Security" Platform: Leveraging expertise in Mobile Payment to provide ultimate Security for Mobile to IoT Communications

5 mm



A Secure Element (SE) is a Secure Microcontroller, equipped with interfaces such as NFC, ISO7816, SPI or I2C. 9 billion of SE has been shipped in 2015, for SIM modules, bank cards, ePassport, PKI tokens.

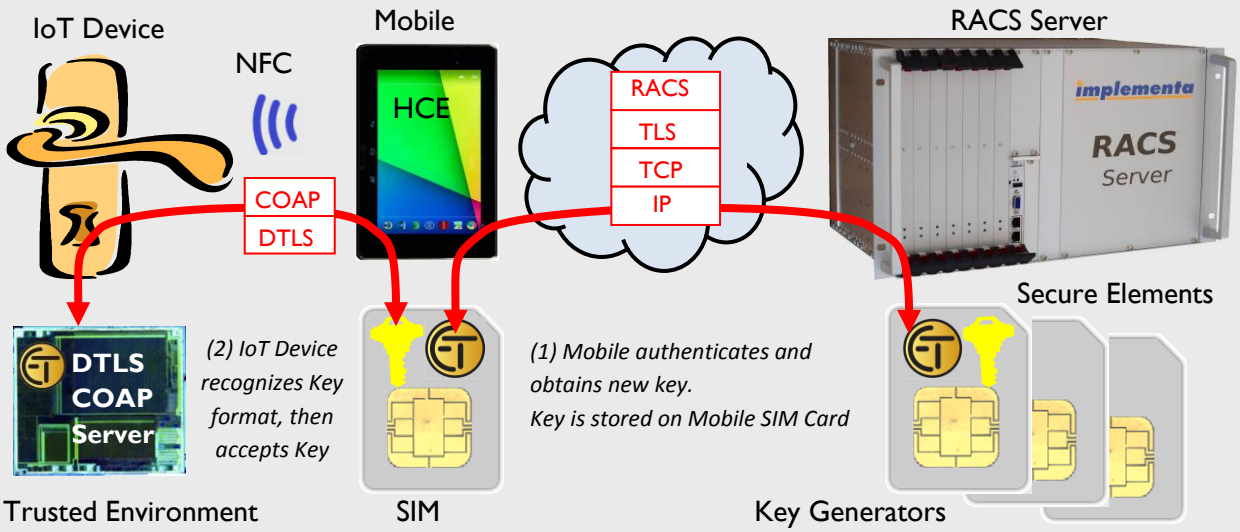
To improve the IoT security EtherTrust "Liberate Your Security!" platform emphasizes two main concepts: **isolation** and **granularity**.

Isolation means that sensitive procedures (such as TLS/DTLS stacks) are executed in tamper resistant Secure Elements stored either locally or in the cloud.

Granularity means that security, in the cloud for example, is enforced at the atomic level (the secure chip).

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 IoT devices or mobiles can be stolen, lost, hijacked, or spoofed.

To address such issues, billion of Secure Elements (SE) have been deployed as SIM modules in mobile phones, secure chips in Payment and Identity Cards, and in hardware authentication tokens. EtherTrust "Liberate Your Security!" software platform **facilitates the deployment and use of a Secure Element based infrastructure** for such uses as securing **IoT infrastructure, online payment, remote access, and cloud storage.**



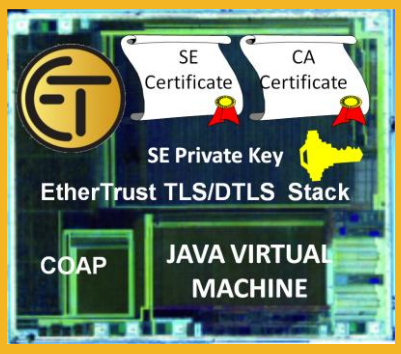
Providing ultimate end-to-end communication security between IoT devices, Mobile and Cloud applications. Communications are encrypted using TLS/DTLS. Certificates are stored in Secure Elements.

To Providers of **Payment Cards**, **Smart Card Authentication**, and **Cloud based HSM**, EtherTrust patented "Liberate Your Security!" platform offers:

- ✓ **End to End Development Platform**, with APIs for Secure Elements, POS Terminals, IoT Devices, Server administration and life cycle management.
- ✓ **Comprehensive support:** EtherTrust supports most types of secure elements, devices (Android, Windows, Raspberry Pi, POS terminals), and Windows and Linux Servers.
- ✓ **Strong end-to-end security**: Leverages Secure Elements and TLS/DTLS protocol, eliminates risks associated with devices vulnerabilities.
- ✓ **Industry Standards Compliant:** (IETF, COAP, TLS/DTLS, GP, EMVco, HCE,..)
- ✓ **Open:** Server Management Middleware is OpenSource.

Cloud of Secure Elements and DTLS/TLS Security Modules: Open Technologies dedicated to the IoT Security

RacsServer:443/SEID



implementa gmbh
www.implementa.com
info@implementa.com

EtherTrust - SAS
www.ethertrust.com
info@ethertrust.com

EtherTrust "Liberate Your Security" platform comprises the following components:

RACS Servers

Remote APDU Call Protocol Secure Server Software (RACS) for more effective and secure cloud based storage of cryptographic keys (SE based "HSM like" servers).

The RACS protocol is an emerging open IETF draft: http://tools.ietf.org/html/draft-urien-core-racs-00.
implementa RACS Servers are highly reliable and scalable devices to host any number of SEs in the cloud with secure RACS compliant remote access.

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 devices 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 KitKat operating system, these APIs enable remote use of secure elements identified by their network locator.

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 in https://tools.ietf.org/html/draft-urien-uta-tls-dtls-security-module-00

Server Administration APIs (C)

Management Software for RACS servers to 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 implementa

implementa provides industrial-strength communication products and solutions. For more than 15 years implementa has been specializing in wireless and smartcard technologies. Implementa is the market leader for cloud-based SIM and SE solutions.

About EtherTrust

EtherTrust markets software for secure elements and designs innovative solutions that strengthen the security of IoT and Cloud applications. In 2009 it was awarded by the 11th national contest for the support of innovative start-ups organized by the French ministry of research and universities.