

1



EtherTrust Pitch



1





Introducing EtherTrust

About the company



Yvon Leroy, cofounder
Previously CEO of the
QOSMOS company

Guy Pujolle, cofounder
Worldwide expert
in Network Technologies

Michel Betirac, Partner
Previously in charge of
the SIM business units at
ST Microelectronics

Pascal Urien, cofounder
Worldwide expert in
Secure Elements
Technologies

Robert De Monts, Partner
EtherTrust coach in California
Interim CEO/COO, Board
Member,
fund raising & M&A experience

Simon Elharbi
Technical expert, 18 years
experience of trusted technologies

Core Technology



EtherTrust markets software for Secure Elements and designs innovative solutions that strengthen the security & trust of Cloud and Internet of Things applications

The EtherTrust TLS Stack (ETS) works with all the Secure Elements of the market.

EtherTrust designs Secure Elements Servers, powered by the RACS protocol.

Customers/Partners



THALES



NEOWAVE

implementa



A High Tech Small Company

Spinoff from Telecom ParisTech and the University of Paris 6

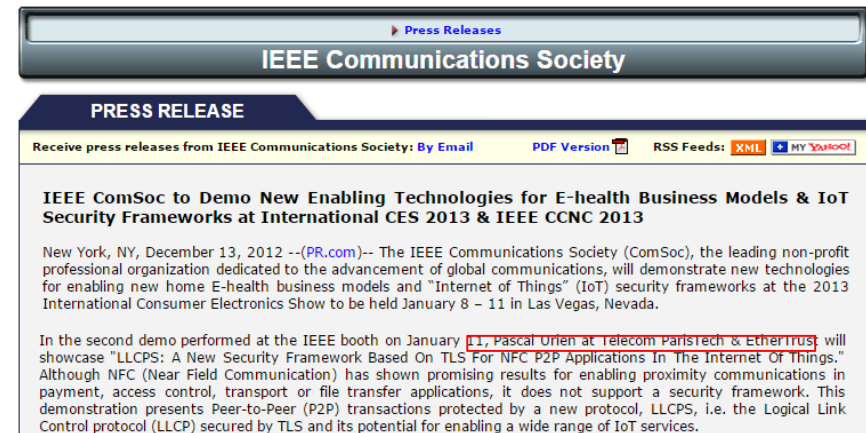
EtherTrust SAS, 2009

Awarded by the 11th national contest for the support of innovative start-ups (" 11^{ème} concours national d'aide à la création d'entreprises de technologies innovantes ") organized by the French ministry of research and universities

Finalist of the " Grand prix de l'innovation de la ville de Paris 2009"

- **Five patents in progress**
- **Normalization actions thanks to IETF drafts**
- <https://tools.ietf.org/html/draft-urien-core-identity-module-coap-00>
- <https://tools.ietf.org/html/draft-urien-core-racs-00>
- <https://datatracker.ietf.org/doc/draft-urien-uta-tls-dtls-security-module/>

- **Participation to European projects**
- **FEDER, OnDemand**
- <http://www.systematic-paris-region.org/fr/projets/ondemand>
- **FP7 , SecFuNet**
- <http://www.gta.ufrj.br/secfunet/index.php/institutions>
- **FUI20, PODIUM**
- <http://ethertrust.com/podium/>



IEEE Press release, 2013



Sesames Awards, 2008

CES 2015, Eureka Park, EtherTrust was one of 66 FrenchTech Startups



General information

Company : EtherTrust <http://www.ethertrust.com>

Contact : Simon ELRHARBI - simon.elrharbi@ethertrust.com

Targeted topics

SU-INFRA01-2018-2019-2020	Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure	IA
SU-DS01-2018	Cybersecurity preparedness	IA
SU-DS05-2018-2019	Critical sectors: Privacy Accountability	IA



Competencies

Organisation competencies

- **Security**

Organisation experience in the European project

- **EtherTrust is involved with several projects in the SC fields and also in the NFC Technologies:**

OnDemand (FEDER – France))

SECFUNET (Security fo Future Networks – FP7)

PODIUM (FUI – France)

The skills you can bring

- **SE based Infrastructure for securing on-line payment, remote access, cloud storage, IoT and Blockchain.**
- **TLS stacks that are embedded in SE to enable strong mutual authentication based on certificates and asymmetric keys**





Project idea

Describe your project idea

- **The purpose of the project is to provide the ultimate security and privacy for IoT PF and to build the mandatory elements of a TLS/DTLS Secure Identity modules embedded in Secure Element:**
Tamper resistance and secure communications and storage.
- **The design starts from the hardware and the lower layers of communications protocols and ends with diverse applications from real world use cases such as semantic Social wearable IoT data sharing and recommendation services.**

List of the complementary skills you need for your consortium

- **SE suppliers**
- **Real world use cases and Social IoT Recommendation**
- **University**



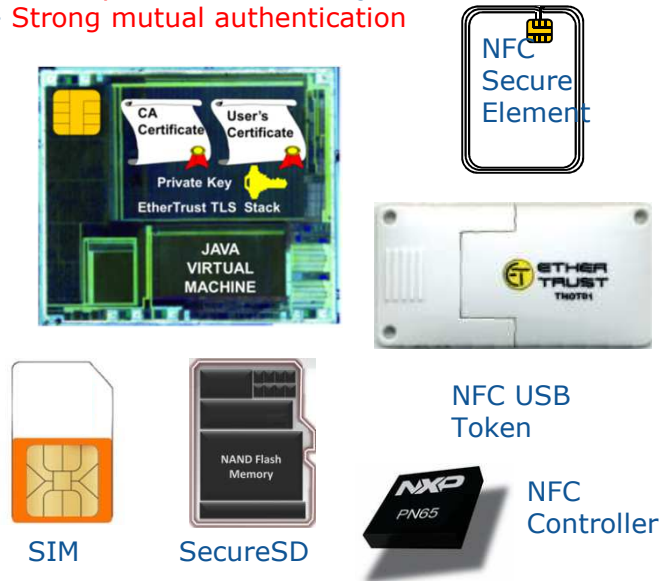
Identity & Access Control
Cloud Security (Secure Elements Server)
Mobile Security
Mobile Payments
IoT Security
Blockchain Security & Certification



Core Technology

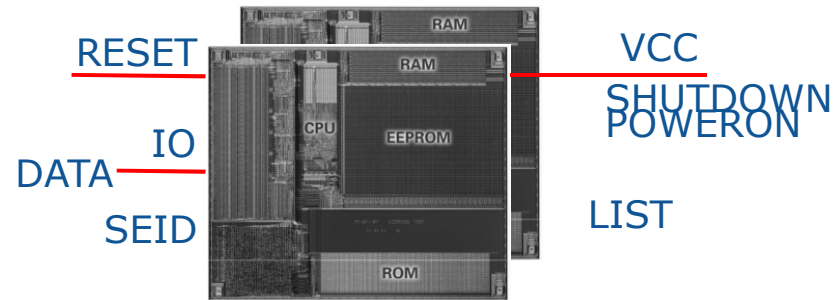
TLS/DTLS Stacks

- Basic (patented) technology, the ETS application (Client and Server) for Secure Elements.
- 20 KB memory footprint for TLS/DTLS client
 - 30 KB memory footprint for TLS/DTLS client/server
- Main benefits for customers
- Full TLS/DTLS protocol in a secure and low cost microcontroller
 - **Identity** for device and objects
 - **Strong mutual authentication**

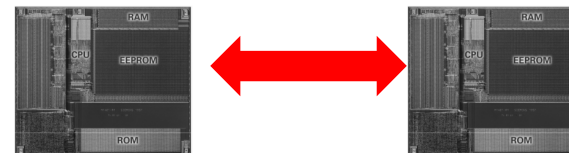


Secure Element Servers: RACS Server

<pre>BEGIN MyLabel GET-VERSION APPEND LIST APPEND POWERON MySEID APPEND RESET MySEID APDU MySEID 00A40400074A544553543030 END</pre>	<pre>BEGIN MyLabel +002 001 0.2 +004 002 MySEID OtherSEID +008 003 MySEID is powered on +005 004 MySEID resetted +006 005 9000 END</pre>
---	--



Secure Element to Secure Element Communications





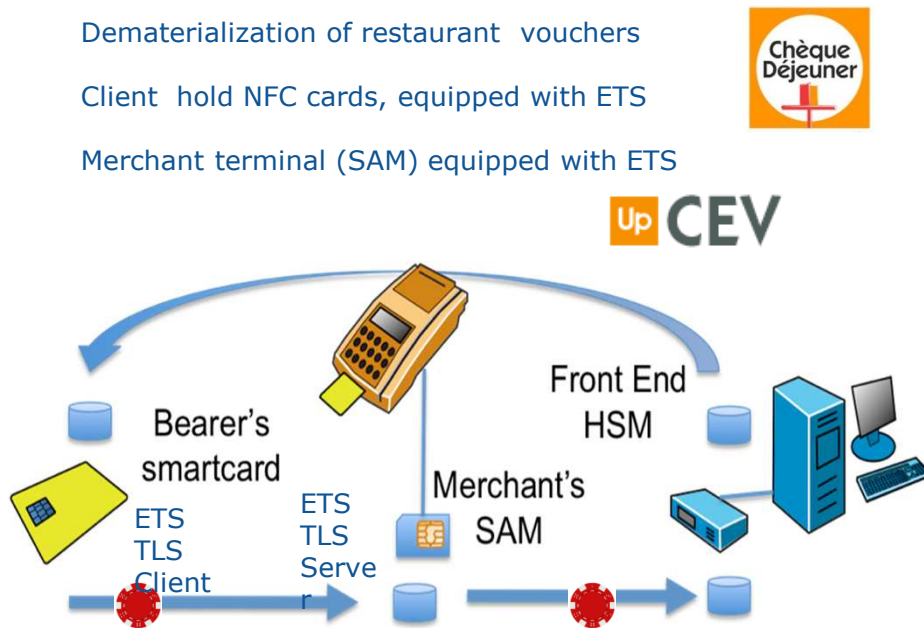
Past Projects

Prepaid Platform for Chèque Déjeuner

Dematerialization of restaurant vouchers

Client hold NFC cards, equipped with ETS

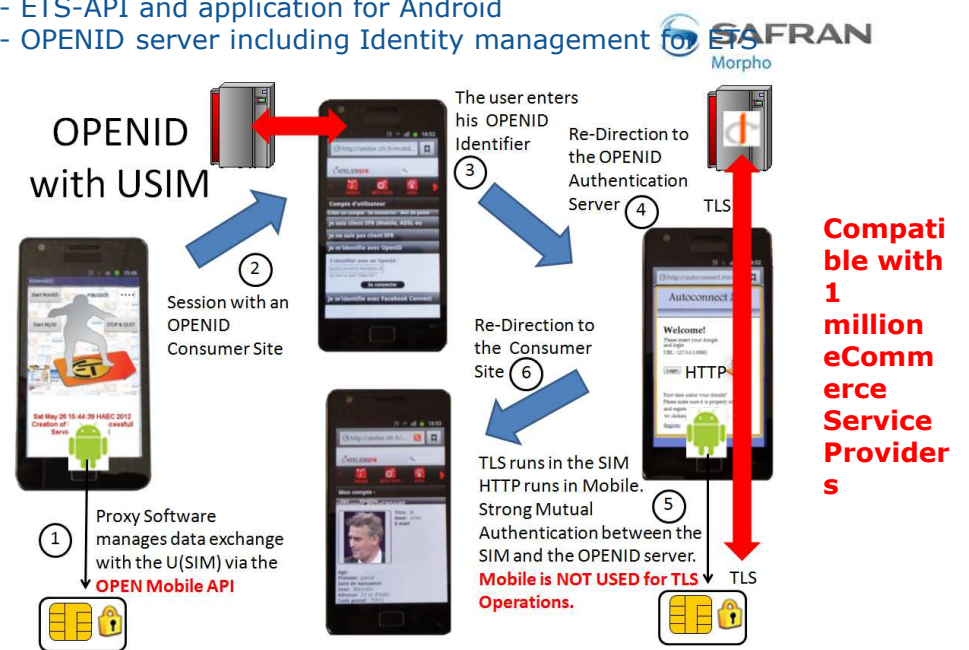
Merchant terminal (SAM) equipped with ETS



OPENID Platform for Mobile Operators

OPENID (patented) Platform designed for Safran Morpho, EtherTrust released the following components

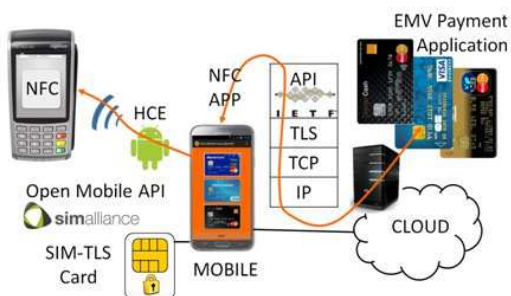
- ETS for SIM www.safran-group.com/fr/atom
- ETS-API and application for Android
- OPENID server including Identity management for ETS



Payments in the Cloud: SIMulation

SIMulation

NFC Application Security



Experiment



Security

- ✓ No payment application in the SIM.
- ✓ The SIM secures the access to the payment application server.
- ✓ The payment application running in the mobile is bound the SIM thanks to security features provided by the Open Mobile API.

Technological Components

Four open components widely supported by the mobile industry

Host Card Emulation

NFC device emulation, available since Android 4.4

The SIM Module

The SIM secures the access to the payment application server and runs the well known TLS protocol

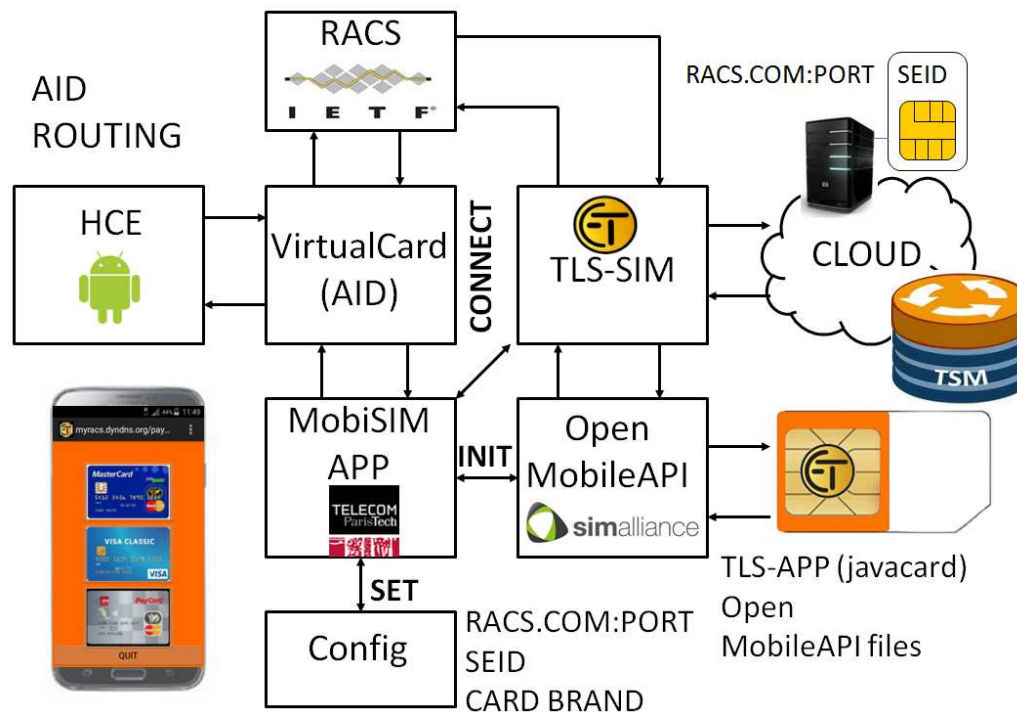
Payment Application Server

The server hosts payment applications. In this project they are stored in legacy bank cards. Future version could deal with virtualized or tokenized devices

Open Mobile API

The industry standard for SIM access in Android mobile. Widely available in the market

AID ROUTING

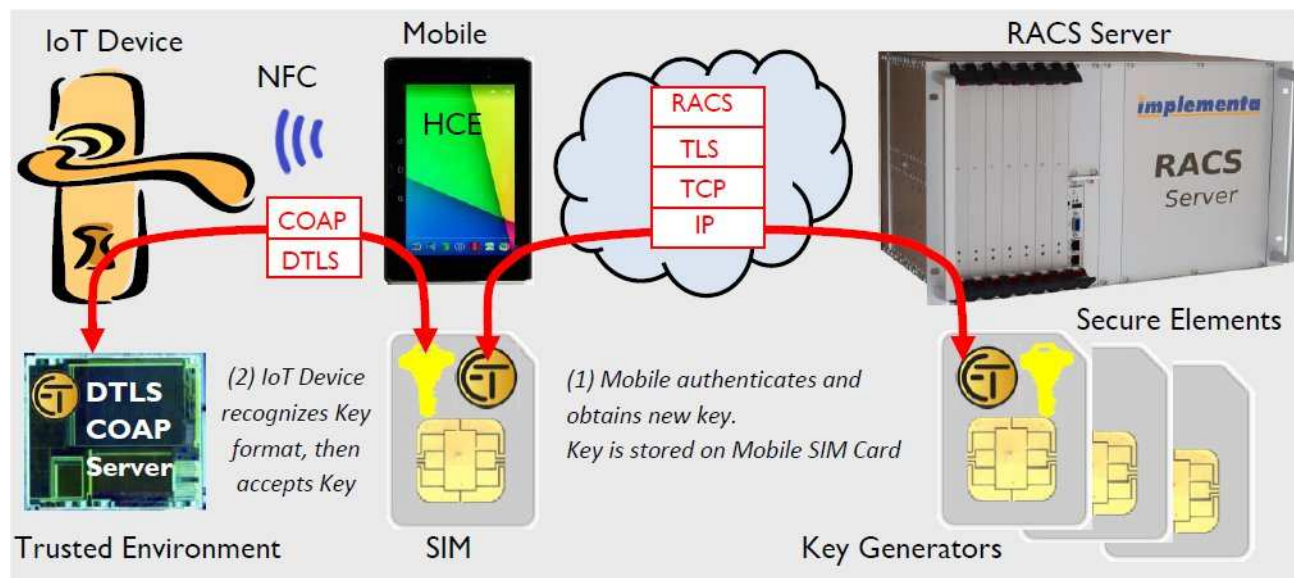


2016- IoT CoAP platform : the double TLS security model

The *Liberate your Security!* Platform with Implementa

CES 2016

<https://www.youtube.com/watch?v=39Ej-8sM0g4>

EtherTrust "Liberate Your Security!" software platform facilitates the deployment and use of a Secure Element based infrastructure for such uses as securing online payment, remote access, cloud storage, and IoT.

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, Devices, Server administration and life cycle management.

- Comprehensive support: EtherTrust supports most types of secure elements, devices (Android, Windows, POS terminals), and Windows and Linux Servers.

- Strong end-to-end security: Leverages Secure Elements and SSL/TLS protocol, eliminates risks associated with terminal vulnerabilities.

- Industry Standards Compliant: (GlobalPlatform, EMVco, HCE, SSL/TLS)

- Open: Server Management Middleware is OpenSource.


CES LAS VEGAS, NV
 JANUARY 5-8, 2017

HTTP

TLS

TCP/IP

Wi-Fi

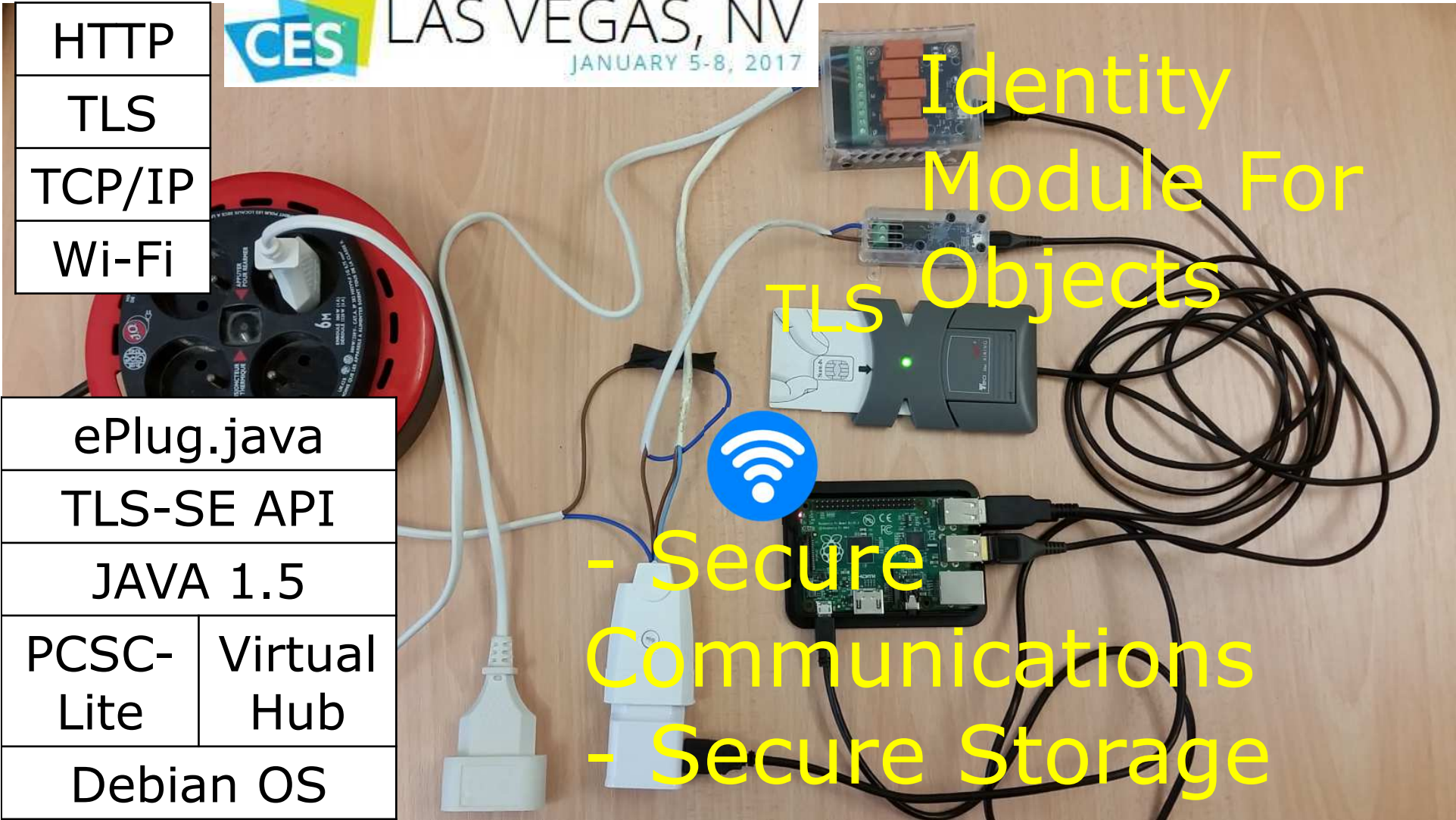
ePlug.java

TLS-SE API

JAVA 1.5

PCSC-
LiteVirtual
Hub

Debian OS



Identity
Module For
TLS Objects



- Secure
Communications
- Secure Storage



Certification in the BlockChain

<https://etherscan.io/tx/0x445c64bc7eb8b0af61a68637cda6a098811f054d53ec8f424d88d8d72d54e050>

Overview
Comments

Transaction Information
Tools & Utilities

TxHash:	0x445c64bc7eb8b0af61a68637cda6a098811f054d53ec8f424d88d8d72d54e050	<p>Transactions are generated from secure elements</p> <ul style="list-style-type: none"> -Physical -Virtual in the cloud
Block Height:	4235298 (16908 block confirmations)	
TimeStamp:	4 days 18 hrs ago (Sep-03-2017 09:39:40 PM +UTC)	
From:	0x6bac1b75185d9051af740ab909f81c71bbb221a6	
To:	0x6bac1b75185d9051af740ab909f81c71bbb221a6	
Value:	0.01 Ether (\$3.12)	
Gas Limit:	40000	
Gas Used By Txn:	26032	<p>The file name includes the hash of the file</p>
Gas Price:	0.000000021 Ether (21 Gwei)	
Actual Tx Cost/Fee:	0.000546672 Ether (\$0.17)	
Cumulative Gas Used:	1329054	
Nonce:	0	
Input Data:	<p>http://www.ethertrust.com/9QorLRTLjxH8a1gqgTS6dT7s3AujLHBGRreXJtv2WSXs9.jpg</p>	

Switch Back



Contacts



<http://www.ethertrust.com>

simon.elrharbi@ethertrust.com