

Online TLS Secure Element for Low-Power High-Security Personal Servers

Pascal.Urien@Telecom-Paris.fr

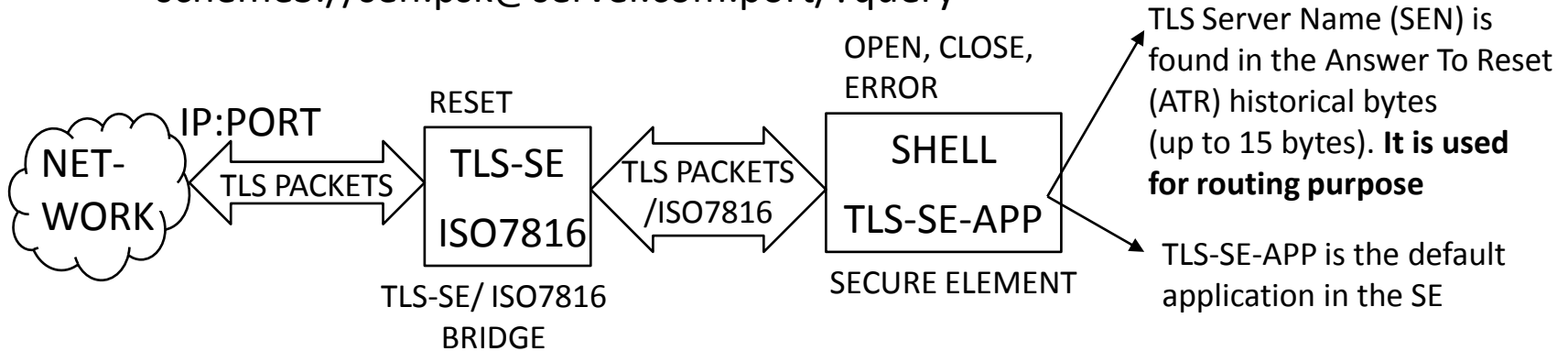
Pascal.Urien@EtherTrust.com

Motivation

- On-line vault for internet users (individuals, small & medium size businesses)
 - On-line secure elements
 - 10 billions secure elements are manufactured every year, among which 6 billions of javacards, which are programmed with a subset of the java language (i.e. javacard)
 - High security level: EAL6+ (according to Common Criteria standards)
- Open technologies
 - No Non-disclosure Agreements (NDA)
 - Open hardware, for example Arduino Integrated Development Environment (IDE)
- Services
 - Key Management System (KMS)
 - Secure Storage

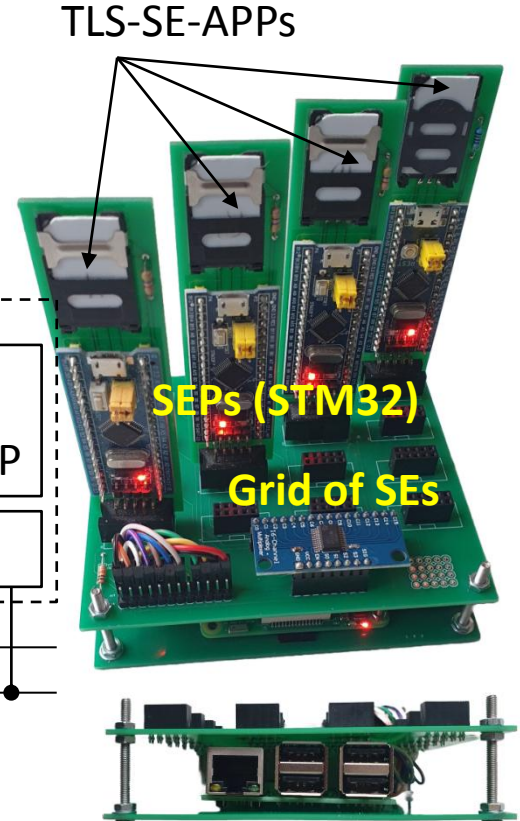
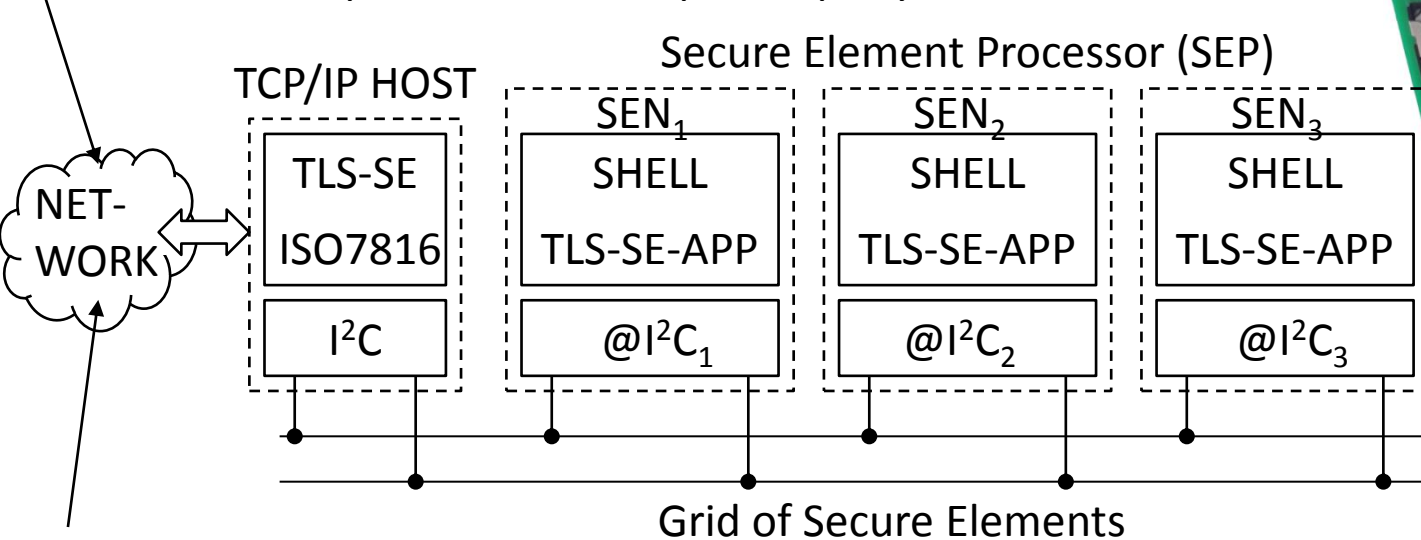
TLS-SE

- TLS for Secure Element (TLS-SE [1])
 - a TLS1.3 pre-shared-key (PSK) profile for secure elements (SE)
- 2 kinds of servers
 - Nano servers, are working with a single element
 - Personal servers are using grids of secure elements
- Uniform Resource Identifiers (URI) for Secure Element resources
 - schemeS://sen:psk@server.com:port/?query



Personal Server

schemeS://sen:psk@server.com:port/?query



On-Demand TLS-SE-APP use the RACS (Remote APDU Call Secure [4]) protocol (ISO7816/TLS-PKI)

IoSev5 Server (Internet of Secure Elements [3] [6])
 Raspberry Pi, Ubuntu, Windows

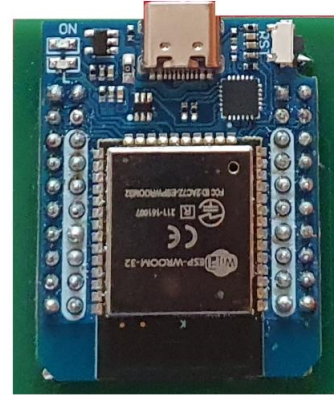
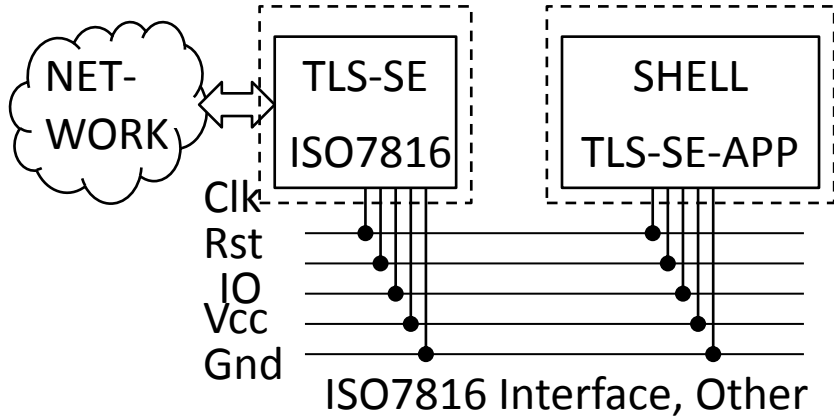
- SEP= Arduino IDE+ ISO7816 LIB
- Oracle Javacard SDK

IETF 120 - HotRFC

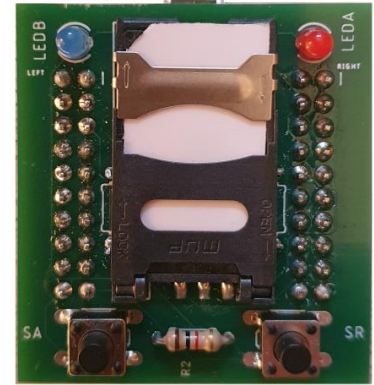
Nano Server

schemeS://sen:psk@server.com:port/?query

TCP/IP HOST Secure Element



TCP/IP HOST
(Wi-Fi Interface)



Secure Element

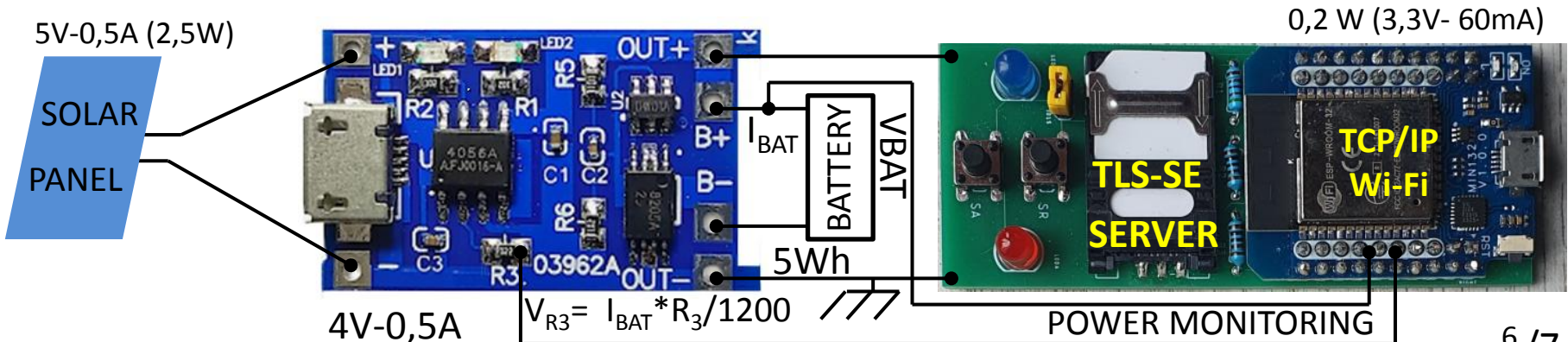
- Arduino IDE
- Oracle Javacard JDK

Low Power Consumption

Personal Server	HOST RASPi 3B	SEP	SE
Power Consumption	1,60 W	0,10W	0,05W

Nano Server	HOST ESP32+Wi-Fi	SE
Power Consumption	0,2W	0,05W

- Nano Servers [5] may be powered by solar panel
- TLS-SE-IO ([2] a kind of Remote Call Procedure, RCP) can be used to monitor battery charging



Looking for:

- We are looking for partners to develop applications for internet users enabling use of open trusted services.
- Concise Binary Object Representation (CBOR) for shell commands over TLS
- More details:
 - [\[1\] https://datatracker.ietf.org/doc/draft-urien-tls-se/](https://datatracker.ietf.org/doc/draft-urien-tls-se/)
 - [\[2\] https://datatracker.ietf.org/doc/draft-urien-core-tls-se-io/](https://datatracker.ietf.org/doc/draft-urien-core-tls-se-io/)
 - [\[3\] https://datatracker.ietf.org/doc/draft-urien-coinrg-iose/](https://datatracker.ietf.org/doc/draft-urien-coinrg-iose/)
 - [\[4\] https://datatracker.ietf.org/doc/html/draft-urien-core-racs](https://datatracker.ietf.org/doc/html/draft-urien-core-racs)
 - [\[5\] https://github.com/purien/TLS-SE](https://github.com/purien/TLS-SE)
 - [\[6\] https://github.com/purien/loSE](https://github.com/purien/loSE)