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

IETF 120 - HotRFC
Personal Server

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

TCP/IP HOST

Secure Element Processor (SEP)

IOSEv5  Server (Internet of Secure Elements [3] [6])
Raspberry Pi, Ubuntu, Windows
- SEP= Arduino IDE+ ISO7816 LIB
- Oracle Javacard SDK

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

Grid of Secure Elements

TCP/IP HOST (Raspberry Pi)
Nano Server

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

TCP/IP HOST

NET-WORK

ISO7816 Interface, Other

TLS-SE

SHELL

TLS-SE-APP

Secure Element

TCP/IP HOST (Wi-Fi Interface)

Secure Element

- Arduino IDE
- Oracle Javacard JDK
Low Power Consumption

<table>
<thead>
<tr>
<th>Personal Server</th>
<th>HOST RASPi 3B</th>
<th>SEP</th>
<th>SE</th>
<th>Nano Server</th>
<th>HOST ESP32+Wi-Fi</th>
<th>SE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Consumption</td>
<td>1.60 W</td>
<td>0.10W</td>
<td>0.05W</td>
<td>Power Consumption</td>
<td>0.2W</td>
<td>0.05W</td>
</tr>
</tbody>
</table>

- 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

\[ V_{R3} = \frac{I_{BAT} \times R_3}{1200} \]
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: