(HotRFC) lightning talk session
IETF 114
"Internet Of Secure Elements“
Call to Research/Collaboration

Pascal.Urien@Telecom-Paris.fr

About Secure Elements

- Small 5x5 mm^2 secure microcontrollers, with high Evaluation Assurance Level (EAL) up to EAL6+ given a scale ranging from one to seven, according to Common Criteria (CC) standards
- Today 8/16 bits CPU, up to 10KB SRAM, 100KB non volatile memory + crypto processors
- Next generation 32bits core, 60MHz clock, up to 2048KB FLASH, 64KB SRAM + crypto processors
- Legacy communication: serial (ISO7816) , emerging I^{2}C, SPI
- Binary Encoding Rules: small packets (about 256 bytes), i.e. ISO7816 APDUs
- Programming environment: Javacard (a subset of Java) six billions devices deployed every year, other languages (C).
- Secure software management(list/delete/upload) environment: Global Platform Secure Channel Protocol (SCP), using ISO7816 APDUs

Why connecting Secure Elements to Internet ?

- On-line trusted cryptographic resources for internet user.
  - Identified by Uniform Resource Identifier
- Issues
  - Additional processor (server) is required with network interface and TCP/IP connectivity
  - Global Platform support for on-demand applications
  - Protocol to access to secure element resources
  - Secure element naming
  - Attestation procedure for on-demand application

IETF drafts

- Remote APDU Call Secure (RACS). Transport of GP/ISO7816 over TLS both for client and Server with X509 certificate
  - draft-urien-core-racs-16
  - Secure Element are identified by Secure Element IDentifier (SEID)
- TLS for Secure Element (TLS-SE). TLS1.3 server in secure element
  - draft-urien-tls-se-04.txt
  - Secure element are identified by TLS Server Name (Secure Element Name, SEN) find in the ISO7816 Answer To Request message retuned upon physical reset.
  - TLS-SE use TLs pre-shared-key (TLS-PSK)
- Attestation procedure as described in Internet Of Secure Element (IOSE) draft relies on two properties
  - draft-urien-coinrg-iose-05.txt
  - Secure element cannot be cloned
  - Secure Element manage only a single TLS session at a given time

Open Software

- TLS-SE for javacard (JC 3.0.4)
  - https://github.com/purien/TLS-SE
- IOSEv5 (Windows, Ubuntu, Raspberry Pi)
  - https://github.com/purien/IoSE
  - RACS + TLS
  - Multiple communication interfaces
    - PC/SC, I^2C, SIM Array