Identity Modules for CoAP
draft-urien-core-identity-module-coap-05.txt

Abstract

   This document defines identity modules based on Secure Elements
   processing DTLS/TLS stacks for CoAP devices. The expected benefits
   of these secure microcontrollers are the following :
   - Secure storage of pre-share keys or private keys
   - Trusted simple or mutual authentication between CoAP devices and
   CoAP clients.
   - The device identity is enforced by a non cloneable chip.
   - Trusted cryptographic support.
   - Low power consumption for DTLS/TLS processing.

Requirements Language

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
   document are to be interpreted as described in RFC 2119.

Copyright Notice

   Table of Contents

1 Overview

The CoAP [CoAP] protocol MAY be secured by the DTLS protocol [DTLS] over an UDP/IP stack; the TLS support [TLS] is also under definition [CoAP-TLS] over a TCP/IP stack.

According to [CoAP] four security modes are available, NoSec, PreSharedKey, RawPublicKey, and Certificate. When DTLS is used with the PreShareKey or Certificate modes there is a need to store secrets such as symmetric or asymmetric keys, which authenticate the CoAP device.

In that case a Secure Element (SE) MAY be used in order to fully run the DTLS or TLS protocol. According to the data throughput or other security considerations the DTLS/TLS session MAY be exported from the secure element after the exchange of the finished messages.

This class of Secure Element is referred by this draft as an identity module (IdMod).

The expected benefits of identity modules are the following :

- Secure storage of pre-share keys or private keys
- Trusted simple or mutual authentication between the CoAP device and the CoAP client.
- The device identity is enforced by a non cloneable identity module.
- Trusted cryptographic support.
- Low power consumption for DTLS/TLS processing.

2 What is a Secure Element

A Secure Element (SE) is a tamper resistant microcontroller (see figure 1) equipped with host interfaces such as [ISO7816], SPI (Serial Peripheral Interface) or I2C (Inter Integrated Circuit).

The typical area size of these electronic chips is about 5x5 mm2. They comprise CPU (8, 16, 32 bits), ROM (a few hundred KB), non volatile memory (EEPROM, FLASH, a few hundred KB) and RAM (a few ten KB). Security is enforced by multiple hardware and logical countermeasures.

According to the [EUROSMART] association height billion of such secure devices were shipped in 2013. Secure elements are widely deployed for electronic payment (EMV cards), telecommunication (SIM modules), identity (electronic passports), ticketing, and access control (PKCS15 cards).

Most of secure elements include a Java Virtual Machine (JVM) and therefore are able to execute embedded program written in the

JAVACARD language. Because these devices are dedicated to security

purposes they support numerous cryptographic resources such as
digest functions (MD5, SHA1, SHA2...), symmetric cipher (3xDES, AES)
or asymmetric procedures (RSA, ECC).

A set of Global Platform [GP] standards control the lifecycle of
embedded software, i.e. application downloading, activation and
deletion.

As an illustration a typical low cost Secure Element has the
following characteristics:

- JAVACARD operating system;
- Compliant with the GP (Global Platform) standards;
- 160 KB of ROM;
- 72 KB of EEPROM;
- 4KB of RAM;
- Embedded crypto-processor;
- 3xDES, AES, RSA, ECC;
- Certification according to Common Criteria (CC) EAL5+ level;
- Security Certificates from payment operators.

According to the state of art, TLS/DTLS stacks may run in secure
elements, for example written as a javacard applications.

```
          +-----+   +-----+   +-----+   +--------------------+
 ISO  <=>|  IO |   | CPU |   | ROM |   | Non Volatile Memory |
 7816    +--+--+   +--+--+   +--+--+   +----------+----------+
            |         |         |                 |
      ======+===+=====+=========+================+=+==========
                |                 |                 |
         +------+------+   +-----+-----+   +-------+-------+
         |  Security   |   |  Crypto   |   | Random Number |
         |  Register   |   | Processor |   |   Generator   |
         +-------------+   +-----------+   +---------------+
```

Figure 1. A typical hardware architecture of a Secure Element

3 **Identity Module for CoAP**

```
                                 Open
              Open               | Decrypt(CoAP)
              | Send-Flight      | | Encrypt(CoAP)
              | | Recv-Flight    | | | Close           Reset
              | | | Close        | | | |               | Process
              | | | |            | | | |               |    |
           +-V-V-V-V-+        +--V-V-V-V--+  EAP over +- V----V--+
    TCP/   | Socket   | DTLS/TLS |  DTLS/TLS |  ISO7816 | Identity |
    UDP <=>|  Agent   | flights  |  ISO7816  |  Messages |  Module   |
    IP     |          | <======> |   Agent   | <=======> |          |
           +---------+         +----------+           +----------+
```
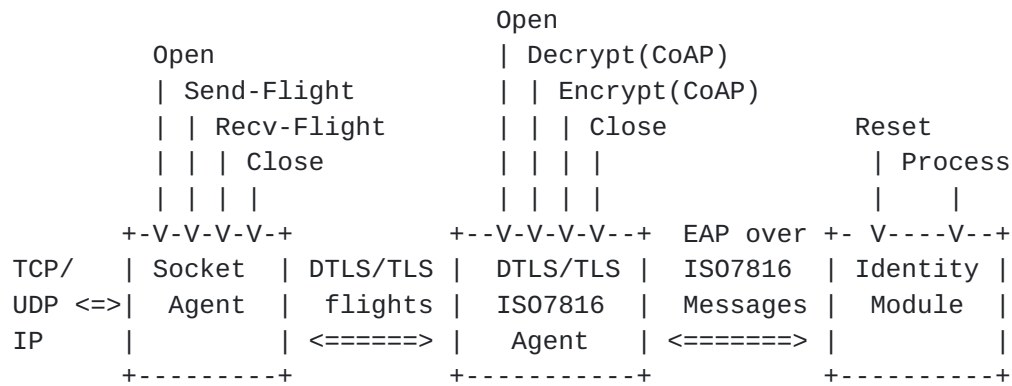
Figure 2. CoAP Identity module framework

ISO7816 interface for Secure Elements providing TLS/DTLS stacks are
detailed in [DTLS/TLS-SM]. The Identity module MUST support two
commands Reset and Process.

TLS/DTLS packets are transported by the EAP protocol over ISO7816
messages. This mechanism previously detailed by [EAPSC] provides a
double segmentation procedure thanks to EAP and ISO7816 facilities.

A DTLS/TLS-ISO7816 software agent sends and receives DTLS/TLS
flights to/from sockets over EAP/ISO7816 messages to/from the
identity module. Conceptually this component interface SHOULD have
four procedures Open, Close, Encrypt and Decrypt.

A socket software agent extracts and send DTLS/TLS flights from/to
UDP/TCP packets. Conceptually this component interface SHOULD have
four procedures Open, Close, Recv-Flight, Send-Flight.

4 **DTLS/TLS profile for CoAP security modules**

To be done.

5 **IANA Considerations**

This draft does not require any action from IANA.

[6](#) References

[6.1](#) Normative References

[TLS] Dierks, T., Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 5746, August 2008

[DTLS] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, January 2012.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, June 2014.

[CoAP-TLS] A TCP and TLS Transport for the Constrained Application Protocol (CoAP), draft-ietf-core-coap-tcp-tls-02, April 2016.

[ISO7816] ISO 7816, "Cards Identification - Integrated Circuit Cards with Contacts", The International Organization for Standardization (ISO).

[6.2](#) Informative References

[GP] Global Platform Standards, http://www.globalplatform.org

[EUROSMART] The EUROSMART association, http://www.eurosmart.com

[DTLS/TLS-SM] Urien, P., "TLS and DTLS Security Modules", draft-urien-uta-tls-dtls-security-module-05.txt, December 2017

[EAPSC] Urien, P., "EAP Support in Smartcard", draft-urien-eap-smartcard-34.txt, December 2017

[7](#) Authors' Addresses

Pascal Urien
Telecom ParisTech
23 avenue d'Italie
75013 Paris   Phone: NA
France   Email: Pascal.Urien@telecom-paristech.fr