CORE Working Group
Internet Draft
Intended status: Experimental

P. Urien
Telecom Paris
Ethertrust

22 March 2026

Expires: September 2026

Remote APDU Call Secure Lite(RACSL)
draft-urien-core-racsl-00.txt

Abstract

The Remote APDU Call Lite protocol (RACSL) is a lightweight version of the Remote APDU Call Secure protocol (RACS). RACS is designed for Grids of Secure Elements (GoSE), where servers host Secure Elements (SEs), i.e., tamper-resistant chips providing secure storage and cryptographic capabilities. It supports commands for GoSE inventory and data exchange with secure elements. RACSL targets environments hosting a limited number of secure element-typically one-within an IoT device managed by a microcontroller. It provides commands for data exchange with secure elements, in particular for managing their embedded applications. These commands are transported over TLS 1.3 pre-shared key (PSK) sessions, which MAY be secured using a TLS Identity Module (TLS-IM) application hosted within a secure element. RACSL can be used to update TLS-IM applications or to remotely access computing and storage resources hosted in secure elements.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 2026.
.

Copyright Notice

Table of Contents

1 Introduction

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

According to the [EUROSMART] association, nine billion such secure devices were shipped in 2023. They are widely deployed for electronic payment (EMV cards), telecommunications (SIM/USIM modules), identity (electronic passports), ticketing, and access control.

According to the [ISO7816] standards, secure elements process ISO7816 request messages and return ISO7816 response messages, known as APDUs (Application Protocol Data Units).

Four APDU cases are defined:

- Case 1: A request consists of four bytes (CLA, INS, P1, P2). The response comprises two bytes (SW1, SW2).

- Case 2: A request consists of CLA, INS, P1, P2, and LE. The response comprises LE bytes plus SW1 and SW2. Typically, LE length (P3 = LE) is one byte; for extended APDUs, LE length is three bytes, with the MSB (P3) set to zero.

- Case 3: A request consists of CLA, INS, P1, P2, LC, followed by LC bytes. The response comprises two bytes (SW1, SW2). Typically, LC length (P3 = LC) is one byte; for extended APDUs, LC length is three bytes with the MSB set to zero.

- Case 4: A request consists of CLA, INS, P1, P2, LC, LC bytes, and LE. The response comprises LE bytes plus SW1 and SW2. Typically, LC length is one byte; for extended APDUs, LC length is three bytes with the MSB set to zero, and LE length is two bytes.

APDUs are transported using protocols such as T=0, T=1, or T=CL (contactless).

A set of GlobalPlatform [GP] standards controls the lifecycle of embedded software within secure elements, including application downloading, activation, and deletion. These standards rely on APDU exchanges between the secure element and a loader entity.

According to [GP], applications stored in secure elements are identified by an Application Identifier (AID), up to sixteen bytes in length.

2 Secure Elements in Network Node

An Internet node MAY use one or several secure elements, typically to provide trusted cryptographic services. The goal of the RACSL (Remote APDU Call Secure Lite) protocol is to remotely manage and update these applications.

The IETF draft [TLS-IM] defines an interface for a secure element application that performs procedures associated with TLS 1.3 [RFC8446] in pre-shared key (PSK) mode, combined with Diffie-Hellman key exchange over finite fields or elliptic curves (DHE or ECDHE), hereafter referred to as TLS 1.3-PSK.

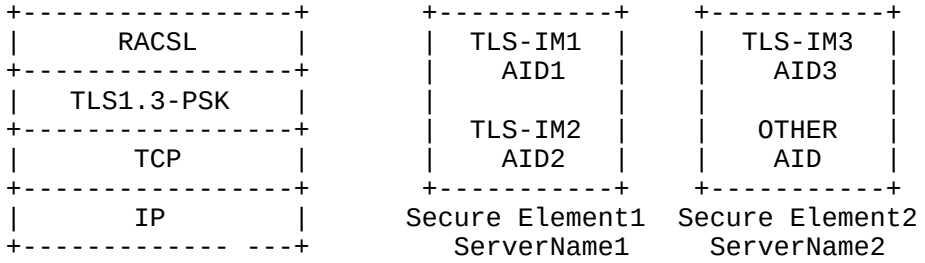
According to [GP], a TLS-IM application is identified by an AID.

An Internet node supporting TLS-PSK MAY use a TLS-IM application stored within a secure element. According to [GP], an application must be deleted before uploading a new version. Therefore, a secure element MAY store two or more TLS-IM applications with different AIDs.

3 RACSL Protocol

3.1 TLS1.3 with pre-shared-key

The RACSL protocol is based on TLS 1.3 [RFC8446] in pre-shared key (PSK) mode with Diffie-Hellman key exchange (DHE or ECDHE). Multiple PSK identities MAY be used, each associated with a PSK.



3.2 Server Name Indication

Each secure element is identified by a server name [RFC8446] conveyed in the Server Name Indication (SNI) extension and included in the ClientHello message.

3.3 PSK identity

In the RACSL context, a PSK identity is associated with an Application Identifier (AID) bound to a TLS-IM application that performs PSK-related procedures.
This AID SHALL NOT depend on the server name. When multiple secure elements are available, a dedicated mechanism SHOULD be used to select the secure element hosting the TLS-IM application used for TLS-PSK session establishment.

psk-identity1	AID1
psk-identity2	AID2
psk-identity2 [	AID3

4 APDU Serialization

Once a TLS 1.3 session has been established, a secure element is selected based on the server name. Three commands are available to send APDUs. Each command is expressed as ASCII text terminated by carriage return (CR) and line feed (LF) characters.

4.1 Poweron

This command powers on the secure element associated with the server name.

Syntax: on CR LF

4.2 Send APDU

This command sends an APDU encoded in hexadecimal format (two characters per byte). It returns a set of bytes encoded in hexadecimal format.

Syntax: A [hexadecimal encoding] CR LF

Example:
>> A 00A4040006010203040700 (select aid=010203040700)
<< 9000 (SW1=90, SW2=00)

4.3 Poweroff

This command powers off the secure element associated with the server name.

Syntax: off CR LF

5 IANA Considerations

This draft does not require any action from IANA.

6 Security Considerations

This entire document is about security.

7 References

7.1 Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119,DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, https://www.rfc-editor.org/info/rfc8446.

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

[GP-SPI-I2C] GlobalPlatform Technology, APDU Transport over SPI/I2C Version 0.0.0.39, July 2019

7.2 Informative References

[EUROSMART] Eurosmart, https://eurosmart.com

[GP] Global Platform, https://globalplatform.org/

[TLS-IM] "Identity Module for TLS Version 1.3", draft-urien-tls-im-10.txt, January 2024.

[RACS] "Remote APDU Call Secure (RACS)", draft-urien-core-racs-19.txt, February 2024

8 Authors’ Addresses

Pascal Urien
Telecom Paris - Ethertrust
19 place Marguerite Perey
91120 Palaiseau
France
Email: Pascal.Urien@telecom-paris.fr