TLS Working Group
Internet Draft
Intended status: Experimental

P. Urien
Telecom Paris
Ethertrust

16 March 2025

Expires: September 2025

TLS For Secure Element Rendez Vous
draft-urien-tls-se-rdv-00.txt

Abstract

TLS for Secure Element (TLS-SE) is a TLS 1.3 profile for secure element. The pre-shared-key (psk) mode requires two security attributes, psk-identity and psk value, somewhat similar to login and password parameters used for classical users accounts. A rendez vous mechanism works with two accounts with different privileges. A root account generates contents and creates guest account with dedicated access rights for these contents. It is a kind of trusted publish-subscribe mechanism based on a TLS1.3 server running in a secure element.

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 2025.

.

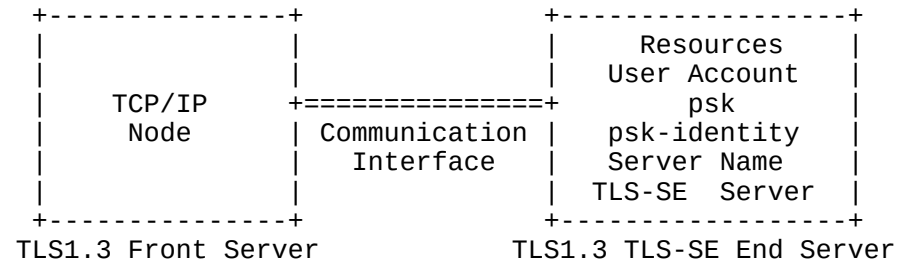
Copyright Notice

Table of Contents

1 Overview

TLS for Secure Element (TLS-SE) [TLS-SE] is an ISO7816 [ISO7816] interface for a TLS 1.3 [RFC8446] server running in a secure element. This server is identified by a TLS server name (SN), and is connected to an electronic board providing internet connectivity. When TLS pre-shared-key (PSK) is used, a couple of attributes (PSK-Identity, PSK) is associated to a user account. Each account, accesses to secure element resources according to a specific security policy. A root account manages all embedded resources, while other accounts have limited rights fixed by root user. Thanks to these mechanisms TLS-SE devices can be used to securely shared information over internet in a way similar to publish-subscribe architecture.

2 Uniform Resources Identifier for TLS-SE resources



One or several TLS-SE [TLS-SE] secure elements are connected to a TCP/IP node thanks to a communication interface, such as ISO7816, I2C, or SPI [GP-SPI-I2C]. The TCP/IP node is a front TLS1.3 server. A TLS-SE device is a TLS end server identified by the Server-Name (SN) attribute.

A resource is identified by the following Uniform Resource Identifier (URI)

schemeS://SEN:PSK(ID)@IP:PORT/?query

where
- scheme is the syntax used over TLS
- S means secured by TLS
- SEN is the TLS Server-Name used by the TLS-SE application
- PSK is the pre-shared-key
- ID is the psk-identity
- IP is the front TLS server IP address
- PORT is the front TLS server port
- query is a request encoded according to the scheme syntax

2 User accounts in secure element

2.1 Root account

A TLS-SE device MUST comprise at least a couple of attributes (psk-identity, psk) which identifies a root account. The root account manages all secure element resources such as secure storage or cryptographic procedures. It MAY also create or delete other accounts, referred as guest, associated with different (psk-identity, psk) tuples, and define a specific access policy for each of them.

2.2 Guest account

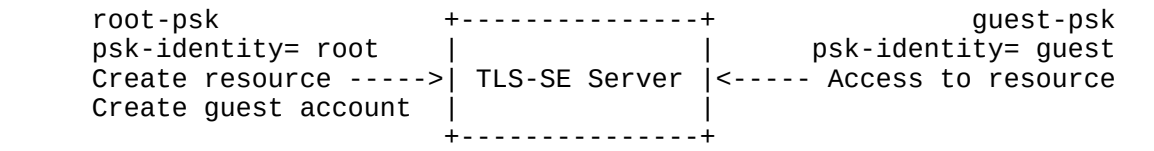
Guest accounts are created and deleted by root. They access to embedded resources according to specific access policies.

3 Rendez-Vous

The "Rendez-Vous" mechanism is managed by the root account. A resource is created, and is made available for a guest, according to a specific access policy.

For example the root creates a data record, and gives a read right for a particular guest. Out of band mechanisms are used to notify the associated URI.

In a similar way the root creates a cryptographic key, and gives an encrypt/decrypt right for a particular guess. Out of band mechanisms are used to notify the associated URI.



4 Example

4.1 Writing operation with root account

psk-identity is root

Server Name is key1.com

RxNET
16030300F8010000F403035BD19B1B1C65E63B0AF76336564D8E126FDD38FCDC
31CC6CC0D57BE9BEED595B000002130401000C9002D0003020001002B000302
0304000D001E001C060305030403020308060805080A0804080906010501
040102010033004700450017004104E744613691E94E64959DB785E2EF8589DE
0FE843B94E04B62E75D78C7B6C34644C3D2031D31745DB2A5F71CFA943542257

```
9ADF9ADA8BCE5DBB01632A40F5052A000A000600040018001700000000D000B00
0008 6B6579312E636F6D 0029002F000A0004 726F6F74 000000000021202E
8241F586AD78A9D767CA761624517935BCD99D1C3265E386FBAD67225498E8

Tx: 00D80001F016030300F8010000F40303
    5BD19B1B1C65E63B0AF76336564D8E12
    6FDD38FCDC31CC6CC0D57BE9BEED595B
    000002130401000C9002D0003020001
    002B0003020304000D001E001C060305
    030403020308060B0805080A080408
    090601050104010201003300470045 00
    17004104E744613691E94E64959DB785
    E2EF8589DE0FE843B94E04B62E75D78C
    7B6C34644C3D2031D31745DB2A5F71CF
    A9435422579ADF9ADA8BCE5DBB01632A
    40F5052A000A000600040018001700000
    000D000B0000086B6579312E636F6D00
    29002F000A0004726F6F740000000000
    21202E8241F586AD78A9D767CA761624
    517935BCD9
Rx[101ms]:
9000
Tx: 00D800020D9D1C3265E386FBAD672254
    98E8
Rx[396ms]:
    160303008102000 07D03038968138C01
    02FEE1A71A65BD7C1FF12B1A6C7D1ADF
    4EABFEF4CA1F2CE89498590013040000
    55002900020000003300450017004104
    54AE904C21CBF67106A551B2191EF3C3
    260817A2B81DC7DFF5C4246CE729D617
    66F29B6B34EFD1E8805565ED8636701E
    2C745075774E8C998661B8780D20638A
    002B00020304
    9F1C
Tx: 00C000001C
Rx[40ms]:
    170303001750FC6821BA8D491FD75F10
    CF193E16C3701FEBBC1283B8
    9F3A
Tx: 00C000003A
Rx[101ms]:
    1703030035ED588DC0A217F525449ADF
    88C31C2E75C8B83557DFA0D0AC27331F
    542818CECC3CDFE57A879A9D96F6369F
    4B0A697E022E05D86379
    9000
TxNET
160303008102000 07D03038968138C0102FEE1A71A65BD7C1FF12B1A6C7D1ADF
4EABFEF4CA1F2CE894985900130400005500290002000000330045001700410 4
54AE904C21CBF67106A551B2191EF3C3260817A2B81DC7DFF5C4246CE729D617
```

```
66F29B6B34EFD1E8805565ED8636701E2C745075774E8C998661B8780D20638A
002B000203041703030017 50FC6821BA8D491FD75F10CF193E16C3701FEBBC12
83B81703030035ED588DC0A217F525449ADF88C31C2E75C8B83557DFA0D0AC27
331F542818CECC3CDFE57A879A9D96F6369F4B0A697E022E05D86379

RxNET
1703030035675062F7FB7D6C1D4D61A753755A273F3582D691AF9A47AB725B66
4750ACE4B84E001F30F89D98A138C0145F7E71A5B3F23E416BCB
Tx: 00D800033A1703030035675062F7FB7D
    6C1D4D61A753755A273F3582D691AF9A
    47AB725B664750ACE4B84E001F30F89D
    98A138C0145F7E71A5B3F23E416BCB
Rx[218ms]:
9001

TLS-PSK OPEN

Writing 32 bytes at record 00, encoded in hexadecimal
Z001234567890ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF
Return: OK

RxNET
1703030056 80A9EFBA1AAD90DBB8B454C60B02FCFD32F8FFBB8B6C356654F482
B88C916D4F2F3E23D80E8884A2E2F98C449E61565A0501B416961E90405F4C82
12A0EAB8BCB7A91BD6FB2DF86C79C6ECCF58EED1C633057B6461DB

Tx: 00D800035B1703030056 80A9EFBA1AAD
    90DBB8B454C60B02FCFD32F8FFBB8B6C
    356654F482B88C916D4F2F3E23D80E88
    84A2E2F98C449E61565A0501B416961E
    90405F4C8212A0EAB8BCB7A91BD6FB2D
    F86C79C6ECCF58EED1C633057B6461DB
Rx[126ms]:
    1703030015 4B56A506A564B0E77B9C37
    903B66D1A3EBF75C6D49
    9000

TxNET
1703030015 4B56A506A564B0E77B9C37903B66D1A3EBF75C6D49
```

4.2 Reading operation with guest account

```
psk-identity is guest

Server Name is key1.com

RxNET
16030300F9010000F5030344E287926C1581927C0D6AB7FAECD454D85BE7CE88
ADAA91FD4F0AD1F93819FC0000021304010000CA002D0003020001002B000302
0304000D001E001C0603050304030203080608 0B0805080A0804080906010501
040102010033004700450017 00410431A71EFFF0B95E9FF0CEADF9708EA0D71B
```

```
E70465820324B755EE8627549BDE463DE646F88654D629653E9425BDFED09EDB
FBABA235CC493303EB577C695AC1F7000A000600040018001700000000D000B00
0008 6B6579312E636F6D 00290030000B0005 6775657374 00000000002120
FAF96847AB730FAE992C475E18F9212384DD7EC66DF08CEC62564CC60D3C87DF

Tx: 00D80001F016030300F9010000F50303
    44E287926C1581927C0D6AB7FAECD454
    D85BE7CE88ADAA91FD4F0AD1F93819FC
    0000021304010000CA002D0003020001
    002B0003020304000D001E001C060305
    0304030203080608 0B0805080A080408
    0906010501040102010033004700 4500
    1700410431A71EFFF0B95E9FF0CEADF9
    708EA0D71BE70465820324B755EE8627
    549BDE463DE646F88654D629653E9425
    BDFED09EDBFBABA235CC493303EB577C
    695AC1F7000A000600040018001700 00
    000D000B0000086B6579312E636F6D00
    290030000B00056775657374000000 00
    002120FAF96847AB730FAE992C475E18
    F9212384DD
Rx[101ms]:
9000
Tx: 00D800020E7EC66DF08CEC62564CC60D
    3C87DF
Rx[397ms]:
    160303008102000 07D03031ABA22C6DC
    69DF27170FFC086E7B3CD6A2120656C0
    E57868E70043DCC9D519430013040000
    55002900020000003300450017004104
    194A75BF7C9CB96E09CFEB75CE2D4B09
    FA4EAEFFFCB8EBEA8115D637FB77D441
    F292ABBEC8833C5B452E08D2E35C3410
    9A6F8AD223E99F8EE984CEC767A98237
    002B00020304
    9F1C
Tx: 00C000001C
Rx[42ms]:
    1703030017D82DE3B01BD709F1E325E8
    671C95AA15E1286C65245AA0
    9F3A
Tx: 00C000003A
Rx[98ms]:
    17030300350DFEEC2D27131499695A19
    BD743D32D6C70382772AC7549F77CCED
    024940409070A6231CF6C4611330AC0B
    CF4B217B841AC32F4682
    9000

TxNET
160303008102000 07D03031ABA22C6DC69DF27170FFC086E7B3CD6A2120656C0
```

```
E57868E70043DCC9D5194300130400005500290002000000330045001700410 4
194A75BF7C9CB96E09CFEB75CE2D4B09FA4EAEFFFCB8EBEA8115D637FB77D441
F292ABBEC8833C5B452E08D2E35C34109A6F8AD223E99F8EE984CEC767A98237
002B0002030417030300 17D82DE3B01BD709F1E325E8671C95AA15E1286C6524
5AA017030300350DFEEC2D27131499695A19BD743D32D6C70382772AC7549F77
CCED024940409070A6231CF6C4611330AC0BCF4B217B841AC32F4682

RxNET
17030300356935F41A5C9C3EE7CCE3543957912880B4CE3395E14509A718CE89
D1C731B3AAB47B78E2BE8E87379358478A041A6DDDABD93A34B3

Tx: 00D800033A17030300356935F41A5C9C
    3EE7CCE3543957912880B4CE3395E145
    09A718CE89D1C731B3AAB47B78E2BE8E
    87379358478A041A6DDDABD93A34B3
Rx[218ms]:
9001

TLS-PSK OPEN

Reading 32 bytes at record 00: I00

RxNET
1703030016CAC2F4BBF97ABCB82F628E8674C19EBB73CE03F90AD4

Tx: 00D800031B1703030016CAC2F4BBF97A
    BCB82F628E8674C19EBB73CE03F90AD4
Rx[117ms]:
    1703030053E72D6092F22C59106D033B
    7DA402C18ED7BBB107D0C0C52B769019
    1CD5F8D99698F111B86856EC984CDA58
    5652C176C78456E41CEF089B74A4CE67
    44BCBCEB695298ED8DECF765D2FF29AA
    D7D2B75CC9E67EE7
    9000

TxNET
1703030053E72D6092F22C59106D033B7DA402C18ED7BBB107D0C0C52B769019
1CD5F8D99698F111B86856EC984CDA585652C176C78456E41CEF089B74A4CE67
44BCBCEB695298ED8DECF765D2FF29AAD7D2B75CC9E67EE7
```

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

[TLS-SE] Secure Element for TLS Version 1.3, draft-urien-tls-se-08, December 2024

8 Authors’ Addresses

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