YourApp – EveryWhere- AnyTime

Pascal.Urien@telecom-paris.fr

https://github.com/purien/TLS-SE
The Concept

- **YourApp, On-Line**
  - Is embedded in a secure element EAL 5/6 (up to 7 levels)
- **YourApp server works over a TLS1.3 embedded server**
  - TLS-SE: TLS Secure Element
- **YourApp client works over a TLS1.3 client**
  - Client credentials are (optionally) stored and used in a secure element
  - TLS-IM: TLS Identity Module
Why TLS1.3?

- State of art for communication security
  - Several years of debates between security experts at IETF.
  - Privacy enforcement with Diffie-Hellman Exchange over Elliptic Curve (ECDHE)
  - Authenticated Encryption with Associated Data (AEAD)
  - Server and client authentication based on PKI or pre-shared-key (PSK)

- TLS-SE 1.0 works with AES-128-CCM cipher-suite, ECDHE (over SECP256k1), and 32 bytes PSK.
- Next version will support PKI.
TLS1.3 -RFC 8446- Basic Exchange

Cipher-suite(s)

Key Exch

ClientHello
+ key_share*
+ signature_algorithms*
+ psk_key_exchange_modes*
+ pre_shared_key*

Public Key for ECDHE

ECDHE

PSK-ID and PSK binding

ServerHello
+ key_share*
+ pre_shared_key*
{EncryptedExtensions}
{CertificateRequest*}
{Certificate*}
{CertificateVerify*}
{Finished}

[Application Data*]

YourApp

TLS-IM (optional)

{Certificate*}
{CertificateVerify*}
{Finished}

[Application Data]

[Application Data]
YourApp example: Blockchain Keystore

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>?00CrLf</td>
<td>Get Version</td>
</tr>
<tr>
<td>?01[data]CrLf</td>
<td>Echo</td>
</tr>
<tr>
<td>cxyCrLf</td>
<td>Clear Key</td>
</tr>
<tr>
<td>gxyCrLf</td>
<td>Generate Key Pair</td>
</tr>
<tr>
<td>Xxy[PrivKey]CrLf</td>
<td>Set Private &amp; Public key</td>
</tr>
<tr>
<td>txy[Seed]CrLf</td>
<td>Set BIP32 Seed</td>
</tr>
<tr>
<td>vxyCrLf</td>
<td>Get BIP32 Seed</td>
</tr>
<tr>
<td>bxy[n₁…nₚ]CrLf</td>
<td>Set a BIP32 (p x 32bits) path</td>
</tr>
<tr>
<td>pxyCrLf</td>
<td>Get Public Key</td>
</tr>
<tr>
<td>rxyCrLf</td>
<td>Get Private Key</td>
</tr>
<tr>
<td>sxy[data]CrLf</td>
<td>Sign</td>
</tr>
</tbody>
</table>

xy= key index (two hexadecimal digits)
Scalability Issue

- Single IP:PORT
- Single IP:PORT - multiple PORTs
- Single IP:PORT - multiple TLS-SEs

TCP/IP
LAN/WAN

YourApp
TLS-SE

PORT₁

TCP/IP
LAN/WAN

YourApp
TLS-SE

PORTₙ

TCP/IP
LAN/WAN

YourApp
TLS-SE

SN₁

TCP PORT

Single IP:PORT

Pascal Urien - YourApp
Questions ?

https://github.com/purien/TLS-SE