LLCPS
draft-urien-tls-llcp-01.txt

Pascal Urien

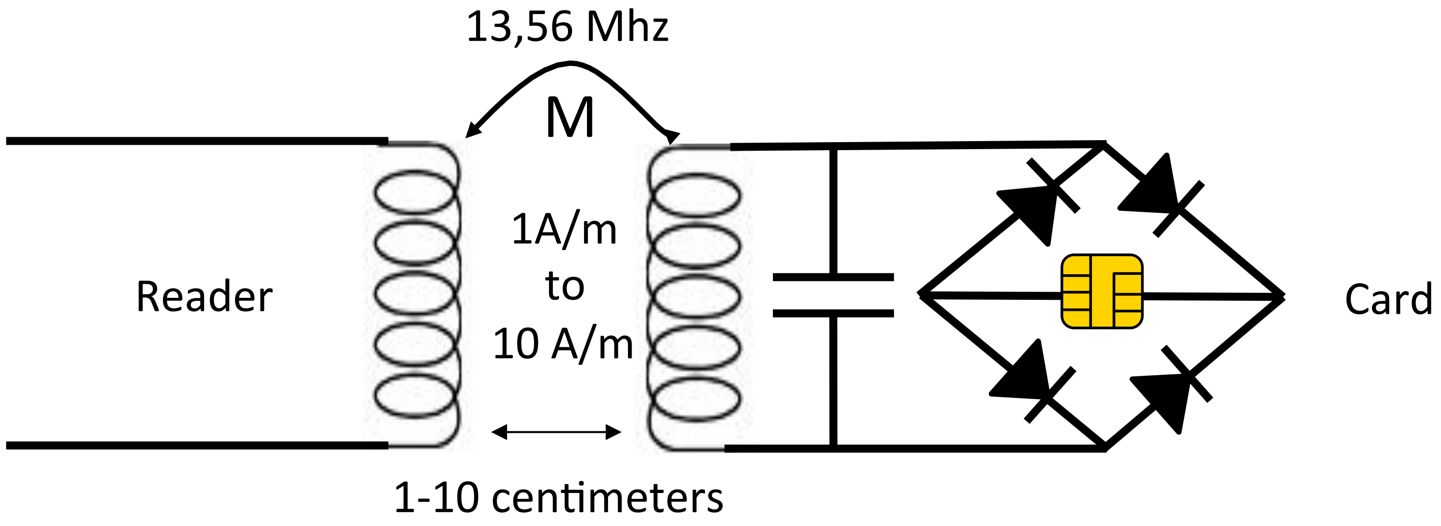
Pascal.Urien@Telecom-ParisTech.fr

IETF 86, Orlando, FL, USA
March 15th 2013

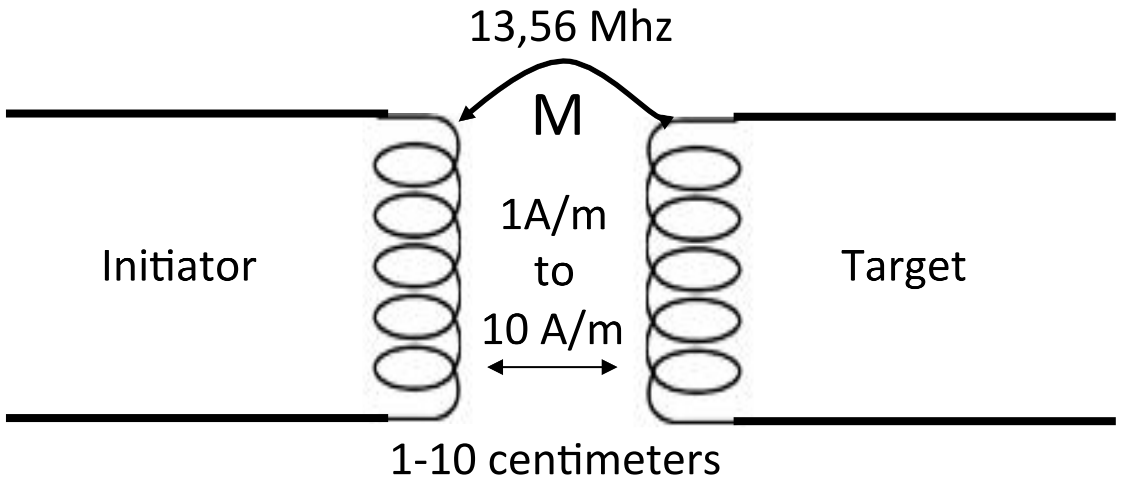
What is NFC ?

- Near Field Communication (NFC)
- A proximity communication protocol (a few centimeters) using the 13,56Mhz frequency
  - Works with electromagnetic field coupling ranging from 1 to 10 A/M
  - Data throughput from 106 To 848 kbps
  - According to Google one million of NFC enable smartphones are sold every week. 100 millions of NFC chips were manufactured by NXP last year
  - Main markets: payment, access control, transport.
- Two working modes
  - Reader/Writer and Card Emulation. A device named "Reader" feeds another device called "Card", thanks to a 13,56 MHz electromagnetic field coupling. This mode is typically used with contactless smartcards or with NFC RFIDs.
  - Peer To Peer (P2P). Two devices, the "Initiator" and the "Target" establish a NFC communication link. In the "Active" mode these two nodes are managing their own energy resources. In the "Passive" mode the Initiator powers the Target via a 13,56 MHz electromagnetic field coupling.
- **This draft focuses on the P2P mode security**
  - **No security features today**
  - **The basic idea is to reuse TLS**

NFC Modes



Reader/Writer - Card



Peer To Peer

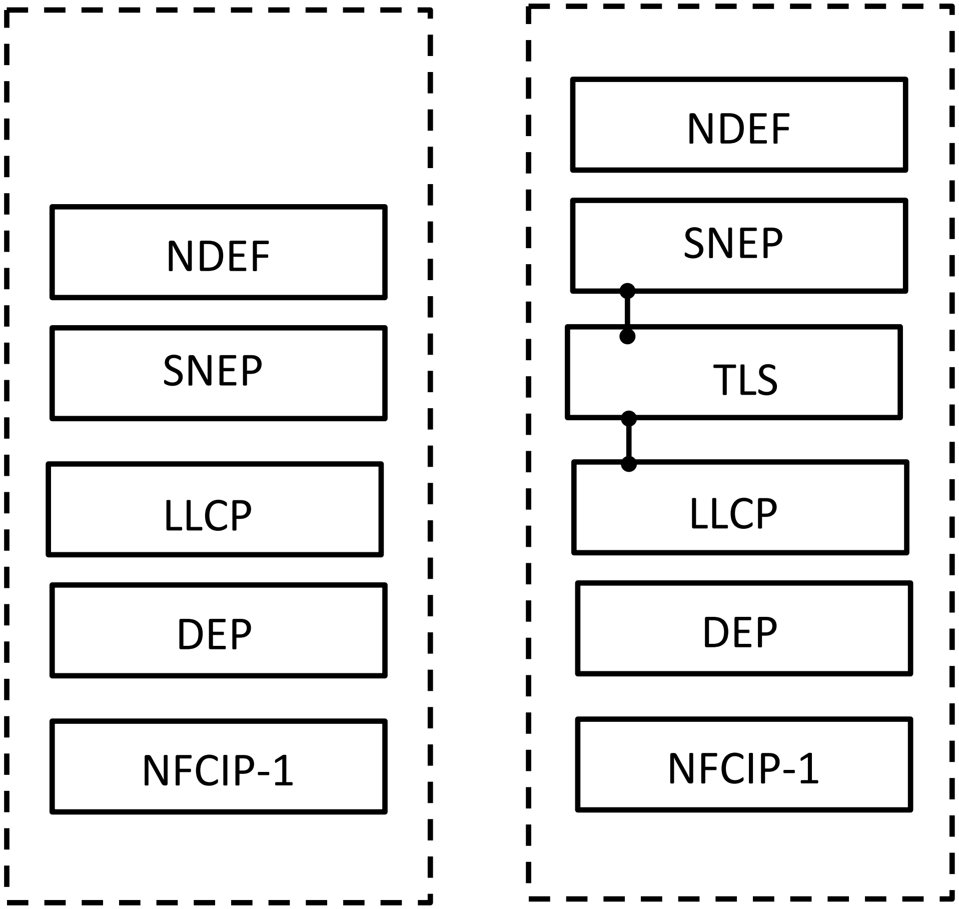
NFCIP-1

- The NFCIP-1 layer is usually running in a microcontroller chip that drives the NFC radio. An NFC session occurs in four logical steps.
  - 1) **Initialization and Anti-collision**, the Initiator periodically probes the presence of a Target.
  - 2) **Activation and Parameters Selection**, once a Target has been detected a set of parameters are notified or negotiated; in particular LLCP services are selected.
  - 3) **Data Exchange**, frames are exchanged via the Data Exchange Protocol (DEP); the Initiator sends (DEP) requests acknowledged by Target responses; the packets size ranges from 64 to 256 bytes; **DEP provides error recovery mechanisms, so upper layers such as LLCP, exchange error free packets**.
  - 4) **De-Activation**, the initiator can release the NFC session at any time, via Release-Request/Response messages.

LLCP - Logical Link Control Protocol

- The LLCP Protocol looks like a light version of the IEEE 802.2 LLC standard.
  - But LLCP works over DEP, which is error free
- LLCP packets include a mandatory two bytes header comprising the DSAP (Destination Service Access Point, 6 bits), the SSAP (Source Service Access Point, 6 bits) and the PTYPE (4 bits) indicating the class of the PDU (Protocol Data Unit).
- LLCP services are identified by a fix SAP or a service name
- LLCP supports two transport modes
  - Connected mode
    - INFORMATION PDUs are acknowledged by RR (Receiver Ready) PDUs
  - Non connected mode
    - Unumbered Information (UI) PDUs are not formerly acknowledged

Example of SNEP service secure by TLS



Legacy NFC P2P stack

This draft
SN= com.ietf.tls.x (x=snep)

SNEP: Simple NDEF Exchange Protocol
SNEP Put Packet

10 SNEP Version
02 Put
00 00 00 0E Payload Length

NDEF Record :
(NFC Text Record Type Definition)

D1: 1 1 0 1 0 001
01: Type Length
0A: Payload Length
54: Type= ‘T’, Text
02: ID= UTF8
65 6E: “EN”
53 61 6D 70 6C 65 20: "Sample "

LLCPS: TLS over LLCP

- Two transport modes
  - Connected
    - Works with a service name such as "com.ietl.tls.x". A service name (like "com.ietf.tls.snep") easily identifies the P2P application transported by TLS
    - INFORMATION PDU are formerly acknowledged by RR PDU
  - Non Connected
    - Works with a well known SAP value (to be defined)
    - One SAP per P2P application transported by TLS
    - UI (Unnumbered Information) PDU are implicitly acknowledged by SYMM PDU
- TLS packets are segmented in a set of INFORMATION or UI PDUs

LLCPS configuration

- Two classes of NFC nodes
  - Initiator / Target
- Two roles
  - Server / Client
- For some classes of applications Initiator/Server and Target/Client could be a natural choice
- But other configurations (Initiator/Client, Target/ Server) are possible for usual P2P applications

LLCPS PDUs

- LLCPS deals with eight PTYPEs:
  - **CONNECT** (connection to the "com.ietf.tls.x" service),
  - **CC** (Connection Confirm),
  - **DISC** (Disconnect),
  - **DM** (Disconnected Mode),
  - **INFORMATION** (TLS messages, connected mode),
  - **UI** (Unnumbered Information),
  - **RR** (Receiver Reader), i.e. the acknowledgment of an INFORMATION PDU)
  - **SYMM** (Symmetry) that indicates an inactivity over LLCP and avoids timeout at the DEP level.

Five processes

- Each LLCPS entity manages **five exclusive processes**.
- Each process manages a set of LLCP PDUs.
  - The Connection Process (CP)
    - accept() / connect()
  - The Disconnection Process (DP)
    - close(), optional
  - The Sending Process (SP)
    - send(), manages the segmentation of TLS messages in LLCP packets.
  - The Receiving Process (RP)
    - recv(), manages a reception buffer and the reassembly of LLCP packet in TLS messages.
  - The Inactivity Process (IP)
    - SYMM PDU are generated/echoed in order to avoid a LLCP timeout.

```
                Initiator                           Target
                    |                                  |
           Connection Process                Connection Process
                    |                                  |
               Send SYMM      --------------->   Receive SYMM
            Receive CONNECT  <----------------   Send CONNECT
               Send CC       ---------------->   Receive CC
             Receive SYMM    <----------------    Send SYMM
                    |                                  |
=========================TLS Session=============================
                    |                                  |
            Receiving Process                 Sending Process
                    |                                  |
               Send SYMM        ------------->  Receive SYMM
           Receive INFORMATION  <------------ Send INFORMATION
                Send RR         ------------->   Receive RR
              Receive SYMM      <-------------    Send SYMM
                    |                                  |
            Inactivity Process                Receiving Process
                    |                                  |
                Send SYMM  ------------------>  Receive SYMM
              Receive SYMM <-----------------    Send SYMM
                    |                                  |
             Sending Process                           |
                    |                                  |
            Send INFORMATION ---------------> Receive INFORMATION
               Receive RR    <--------------       Send RR
                    |                                  |
            Receiving Process                 Inactivity Process
                    |                                  |
               Send SYMM  ------------------->   Receive SYMM
             Receive SYMM <------------------     Send SYMM
                    |                                  |
                    |                          Receiving Process
                    |                                  |
               Send SYMM        ------------>   Receiving SYMM
           Receive INFORMATION  <-----------   Send INFORMATION
                Send RR         ------------>     Receive RR
              Receive SYMM      <-----------      Send SYMM
                    |                                  |
===========================End Of TLS Session======================
                    |                                  |
          Inactivity Process                  Inactivity Process
                    |                                  |
         Disconnection Process                         |
                    |                                  |
              Send DISC  ------------------->   Receive DISC
             Receive DM  <-------------------      Send DM
                    |                                  |
```

Example of Initiator/Server Target/Client LLCPS exchanges

Connected Mode

```
      Initiator                           Target
         |                                  |
 Connection Process                Connection Process
         |                                  |
         |                           Sending Process
         |                                  |
     Send SYMM      --------------->   Receive SYMM
     Receive UI    <----------------     Send UI
         |                                  |
 Receiving Process                          |
         |                                  |
     Send SYMM    ----------------->  Receive SYMM
    Receive UI    <----------------      Send UI
         |                                  |
         |                          Inactivity Process
         |                                  |
     Send SYMM    ---------------->   Receive SYMM
    Receive SYMM  <----------------    Send SYMM
         |                                  |
  Inactivity Process                Receiving Process
         |                                  |
      Send SYMM   ----------------->  Receive SYMM
    Receive SYMM  <----------------    Send SYMM
         |                                  |
   Sending Process                          |
      Send UI     ------------------>   Receive UI
    Receive SYMM  <-----------------    Send SYMM
         |                                  |
  Receiving Process                 Inactivity Process
         |                                  |
     Send SYMM    ----------------->   Receive SYMM
   Receive SYMM   <----------------     Send SYMM
         |                                  |
         |                           Sending Process
     Send SYMM      ------------>     Receiving SYMM
     Receive UI    <-------------        Send UI
         |                                  |
         |                          Inactivity Process
      Send SYMM   ----------------->  Receive SYMM
    Receive SYMM  <----------------    Send SYMM
         |                                  |
         |                                  |
Disconnection Process                       |
         |                                  |
      Send DM         -------------->   Receive DM
 Receive SYMM or DM  <------------   Send SYMM or DM
         |                                  |
```

Example of Initiator/ Server Target/Client LLCPS exchanges

Non-connected Mode

Conclusion

LLCPS is it a possible working item
for the TLS WG ?