TLS and DTLS Security Modules

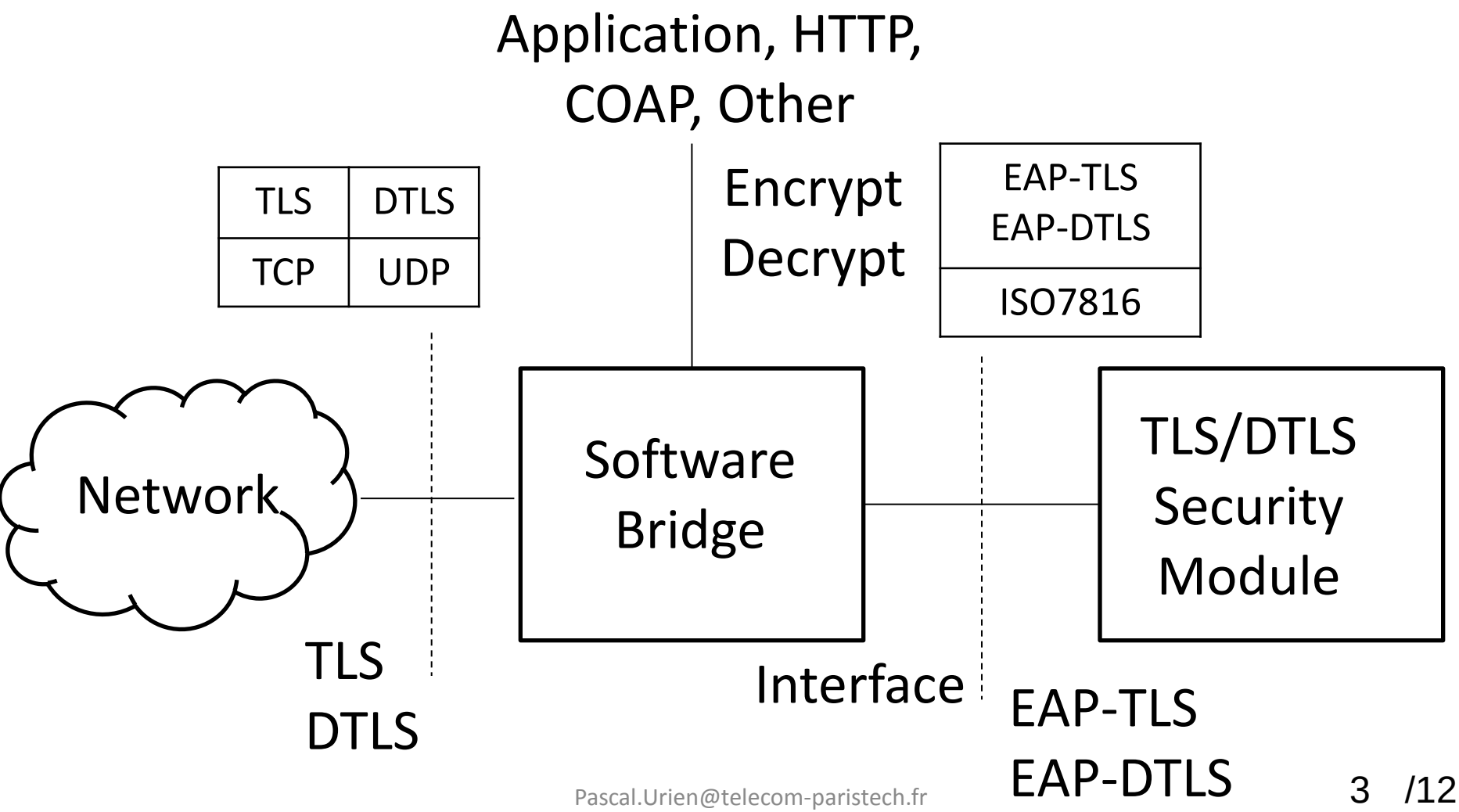
Pascal Urien@Telecom-ParisTech.fr

draft-urien-uta-tls-dtls-security-module-00

GOALs

- TLS and DTLS are widely used
  - HTTPS
  - Extensible Authentication Protocol (EAP)
  - Constrained Application Protocol (CoAP)
- TLS and DTLS Security Modules
  - Trustworthy computing of TLS/DTLS
  - No IPv4 or IPv6 flavors
  - Well defined Binary Encoding Rules (BER) for TLS/DTLS transport
  - EAP-TLS (RFC 5216) defines a framework for the transport of TLS flights.
  - EAP-TLS could also embed DTLS flights. Informally EAP-DTLS

Architecture



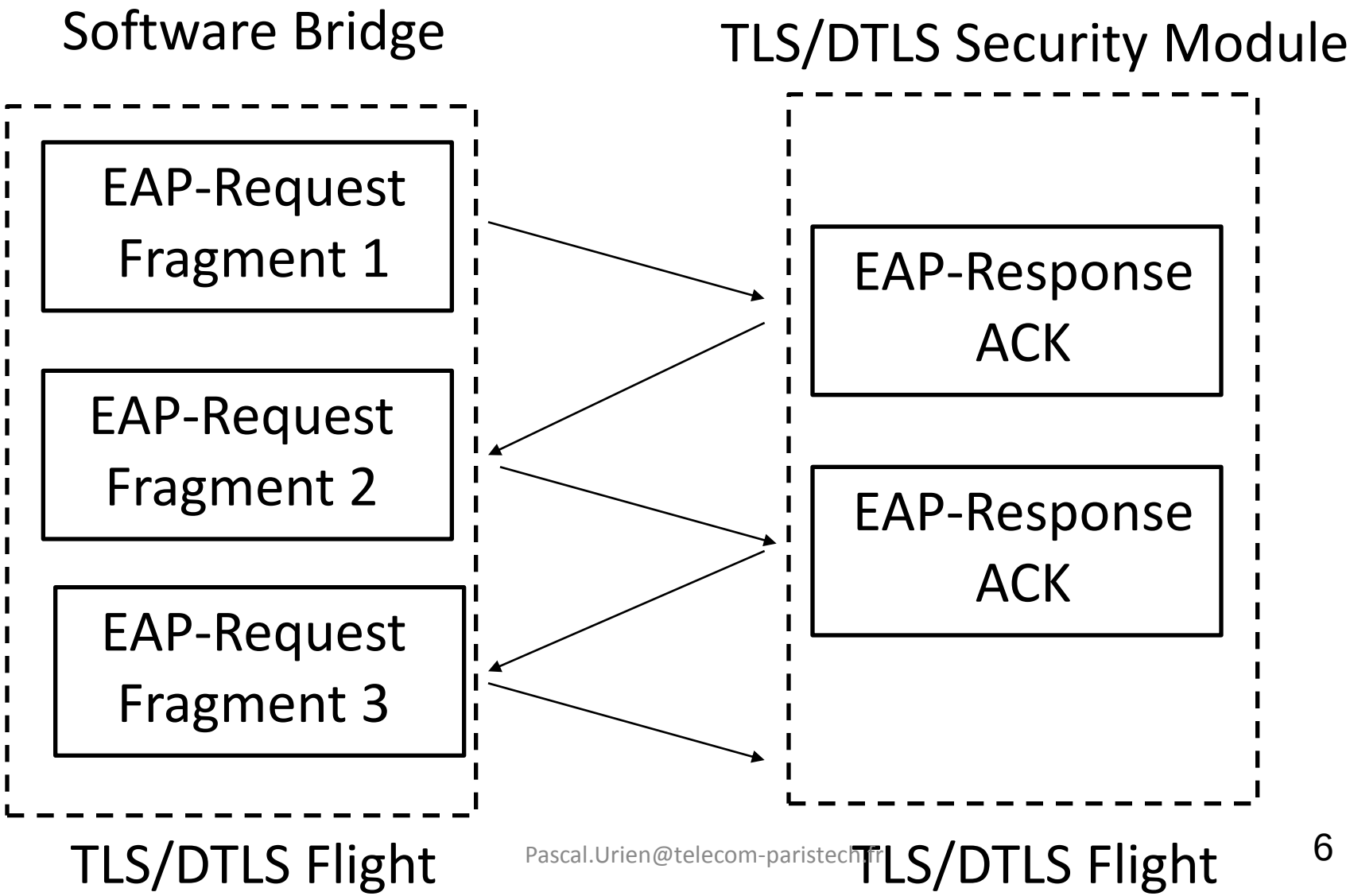
EAP-TLS over ISO7816

- ISO7816 secure micro-controllers
  - Usually referred as smartcards
  - More precisely Secure Elements
- About 10 billions of chips manufactured every year
- EAP Support in Smartcard
  - draft-urien-eap-smartcard-29.txt
  - ISO7816 interface for EAP-TLS
  - Two main commands
    - Reset
    - Process-EAP
  - Memory footprint about 25KB (code+data)

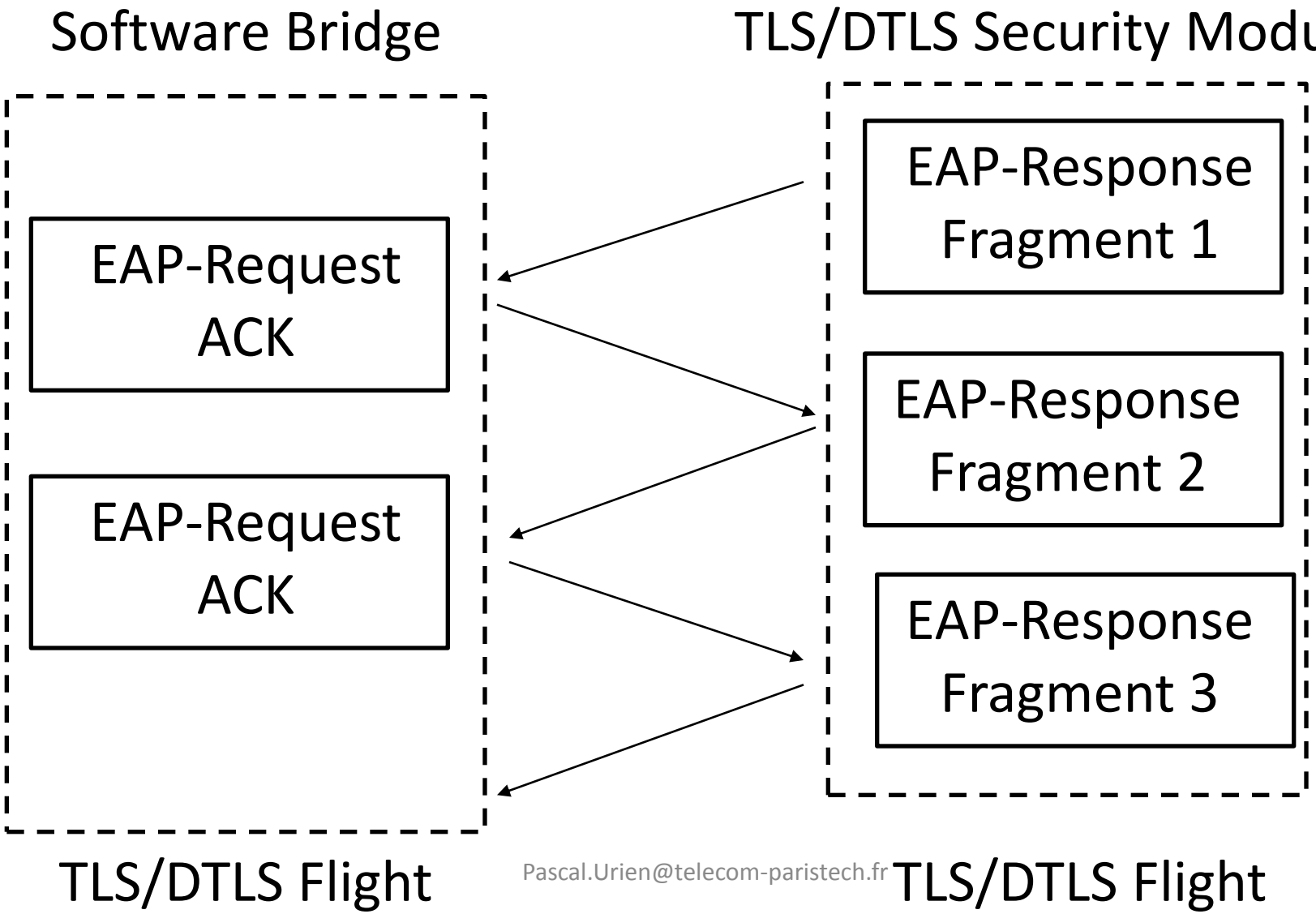
ISO7816 Interface

Command	Class	INS	P1	P2	Lc	Le
Process-EAP	-	80-88	00	00	xx	yy
Reset-State	-	19	10	00	00	01

EAP-TLS TLS/DTLS Flights Segmentation-Reassembly



EAP-TLS TLS/DTLS Flights Segmentation-Reassembly



Pascal.Urien@telecom-paristech.fr

Fragments Size

50 - 100 - 200 hundred bytes

"EAP-DTLS" DTLS over EAP

```
 Security Module          Software Bridge
-------------------      -------------
                         <- EAP-Request/
                         EAP-Type=EAP-TLS
                         Flags
                         (TLS Start)
EAP-Response/
EAP-Type=EAP-TLS
Flags
(DTLS client-hello) ->                              Flight 1
                         <- EAP-Request/
                         DTLS Hello-Verify-Request  Flight 2
                         (contains cookie)
EAP-Response/
EAP-Type=EAP-TLS
Flags
(DTLS client-hello
 with cookie)       ->                              Flight 3
                         <- EAP-Request/
                         EAP-Type=EAP-TLS
                         Flags
                         (DTLS server-hello,
                           DTLS certificate,         Flight 4
                  [DTLS server-key-exchange,]
                   DTLS certificate-request,
                      DTLS server-hello-done)
EAP-Response/
EAP-Type=EAP-TLS
Flags
(DTLS certificate,
 DTLS client-key-exchange,
 DTLS certificate-verify,                           Flight 5
 DTLS change-cipher-spec,
 DTLS finished) ->
                         <- EAP-Request/
                         Flags
                         EAP-Type=EAP-TLS
                         (DTLS change-cipher-spec,  Flight 6
                          DTLS finished)
EAP-Response/
EAP-Type=EAP-TLS
Flags          ->
```

Software Bridge

- Send and Receive TLS/DTLS flights to/from the network.
- Perform segmentation/reassembly operations with the security module.
- For DTLS, security modules don't perform handshake segmentation/reassembly operations
  - This works because DTLS cryptographic calculations deal with non-fragmented handshake messages
- Provide an interface for applications
  - Sending of encrypted and HMACed record packets.
  - Decryption and checking of received encrypted and HMACed record packets.

Encryption/Decryption Operations

Encryption

```
Process-EAP-Encrypt(Type)
                              <- EAP-Request/
                              EAP-Type=EAP-TLS
                              Flags
                             (Payload= Clear Text)
   EAP-Response/
   EAP-Type=EAP-TLS
   Flags
   (Payload= TLS Encrypted
    Record Layer Message)->
```

Decryption

```
Process-EAP-Decrypt
                              <- EAP-Request/
                              EAP-Type=EAP-TLS
                              Flags
                              (Payload= TLS Encrypted
                               Record Layer Message)
   EAP-Response/
   EAP-Type=EAP-TLS
   Flags
   (Payload= TLS Clear
    Record Layer payload)->
```

Questions ?