
83rd IETF
Paris, France, March 25-30, 2012

“EAP support in smartcards”

draft-urien-eap-smartcard-22.txt

Pascal.Urien@Telecom-ParisTech.fr

■ EAP Methods for Secure Elements

- Client and Server

■ What are Secure Elements

- Tamper resistant microcontrollers.
- Small computing resources (typically RAM 10KB, E²PROM 72KB).
- Most of them run a Java Virtual Machine, .NET is also supported.
- SIM/USIM, Smart card, Secure Controller, NFC Controller.

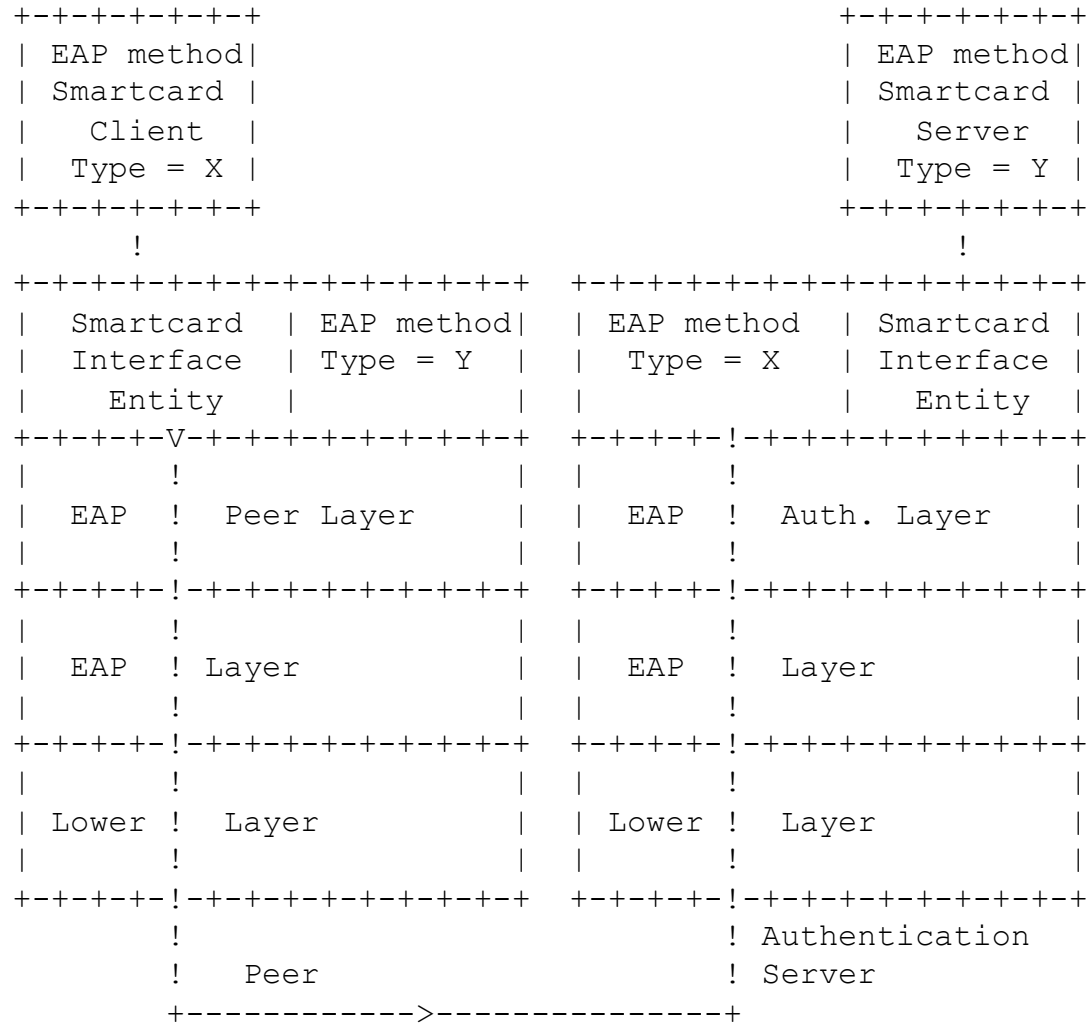
■ Resource constraints

- Small memory footprint (typically < 32KB).

■ ISO7816 interface

- Generic EAP Method interface
- Three use cases, with detailed test vectors.
 - EAP-SIM, EAP-AKA, EAP-TLS

General Architecture



- **Open Implementation**
- **Tested with multiple Secure Elements.**
- **Proposed as experimental RFC**