Objectives

- **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

EAP method
Smartcard
Client
Type = X

EAP method
Smartcard
Server
Type = Y

Smartcard
Interface
Entity
Type = Y

Smartcard
Interface
Entity
Type = X

EAP
Peer Layer
EAP
Auth. Layer

EAP
Layer
EAP
Layer

Lower
Layer
Lower
Layer

Authentication
Peer
Server

---

03/29/2012

Slide 3/4
Conclusion

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