Post-IP technologies virtualization and security

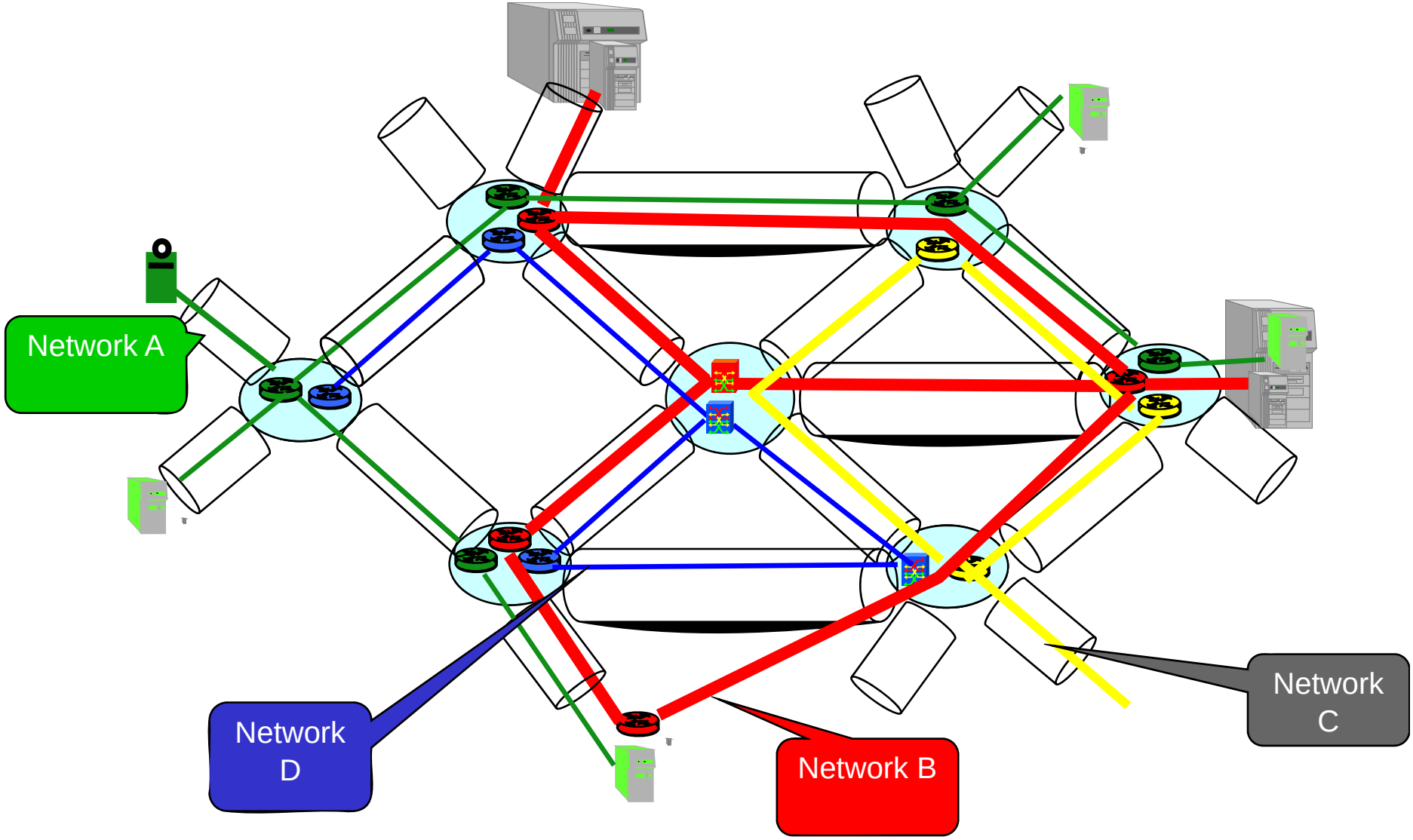
Guy Pujolle

Virtualization for a post-IP network

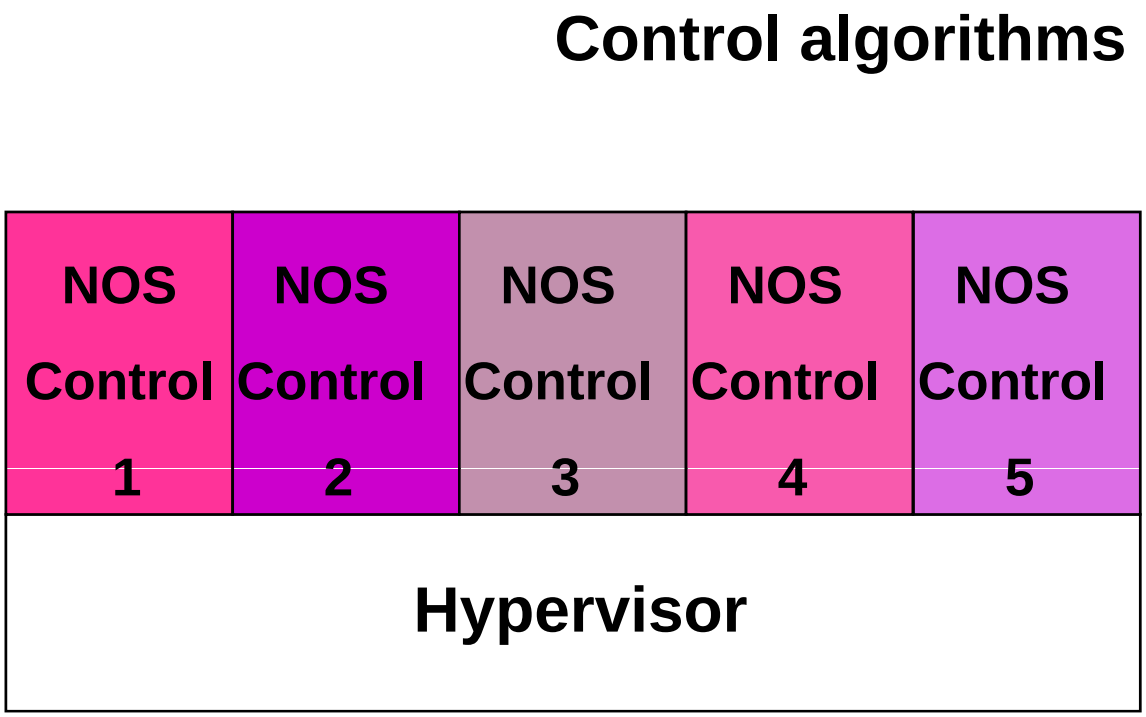
Geni

- Intel would like to propose a generic router
- Intel proposes to have a generic hardware with virtual network operating system
- A router can support simultaneously CISCO IOS and Juniper Junos and Alcatel OS and Nortel OS, etc.
- Cisco reaction was to virtualize the different releases of IOS.

Virtual router



Virtualization of the Control Plane

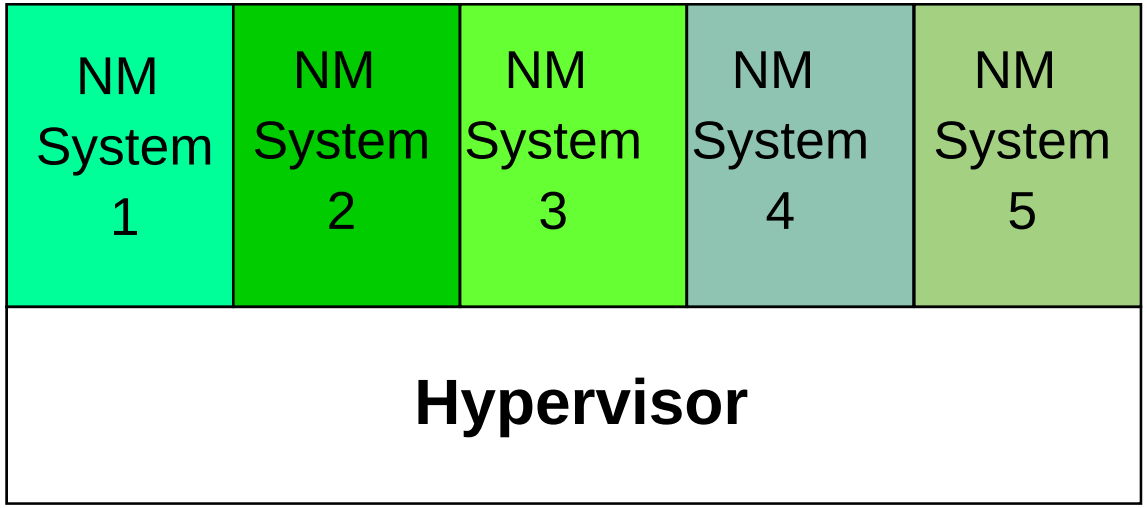


Why virtualization?

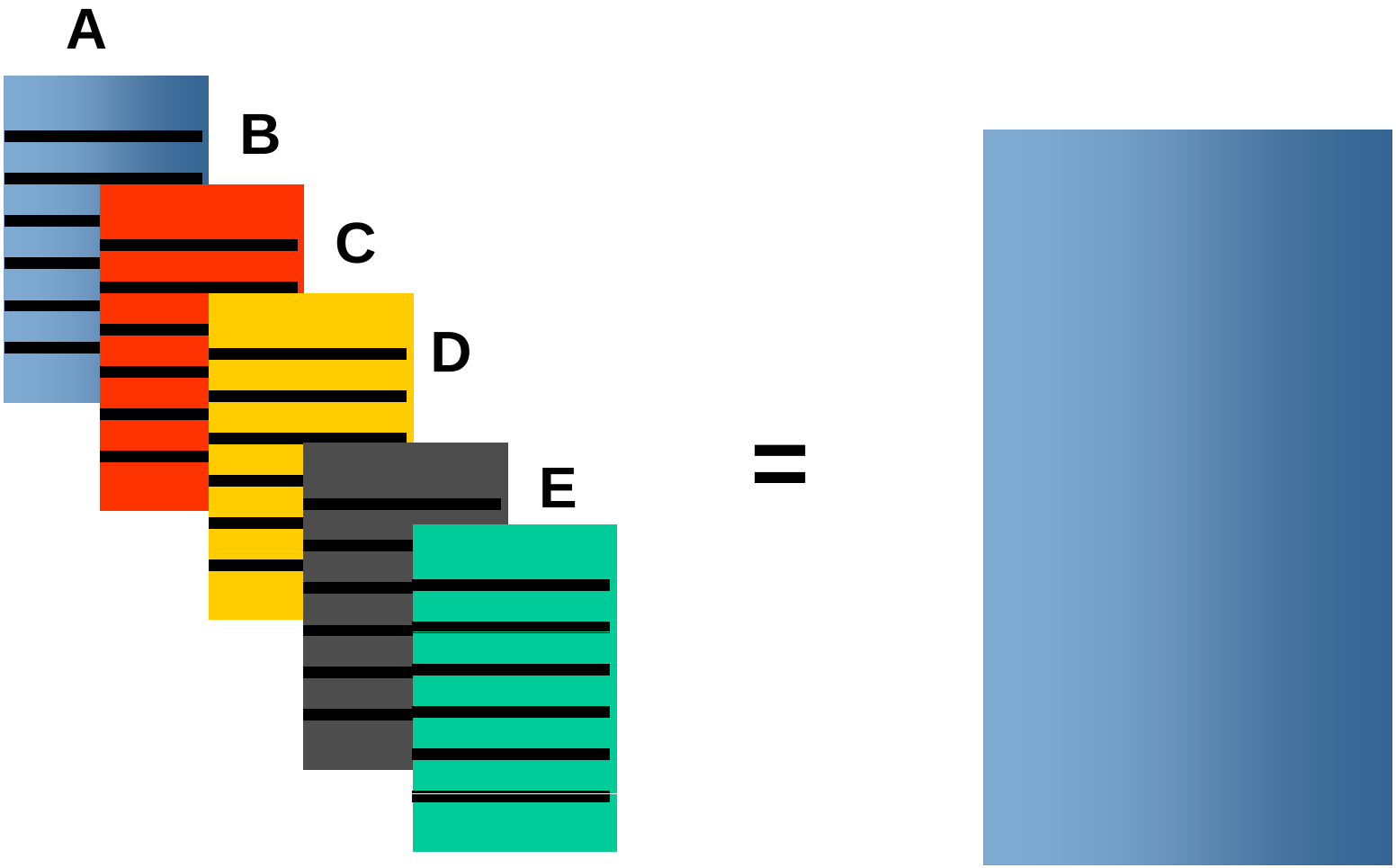
- A better use of the resources
- Sharing of the resources for the routing schemes
- Security of the machines against attacks
- Isolation of the traffic in the virtual machines

- Management and control
- Need an hypervisor
- How to move the virtual entities (router, etc.)

Virtualization of the Management Plane



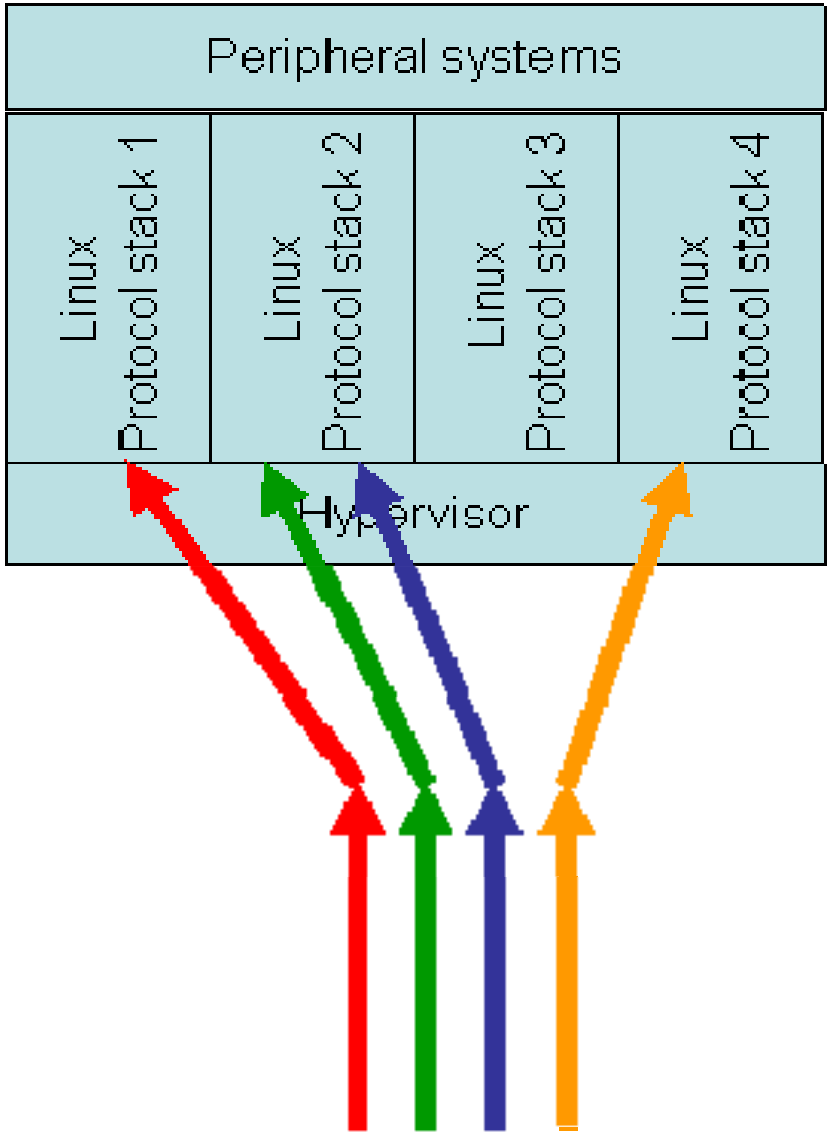
Protocol virtualization



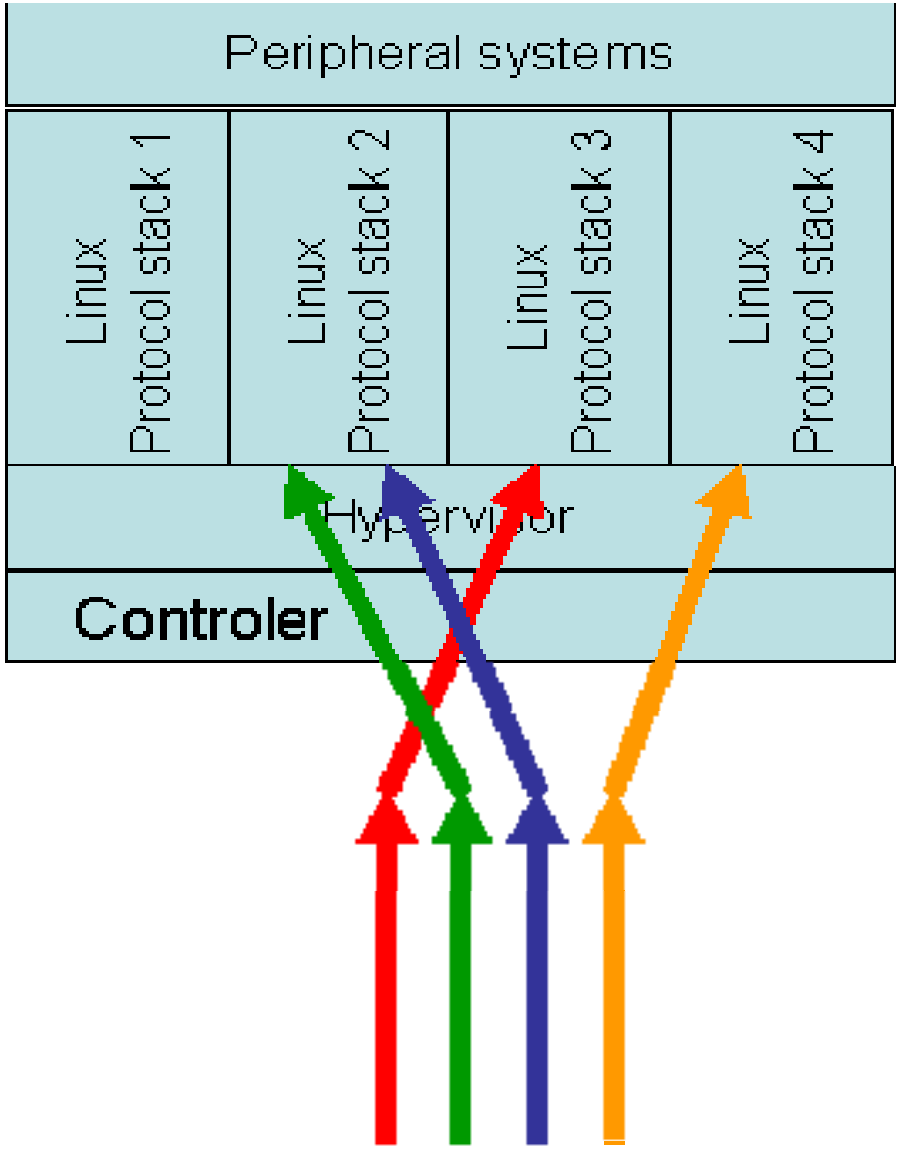
A = IP stack is mandatory in the core network

within the virtual protocol

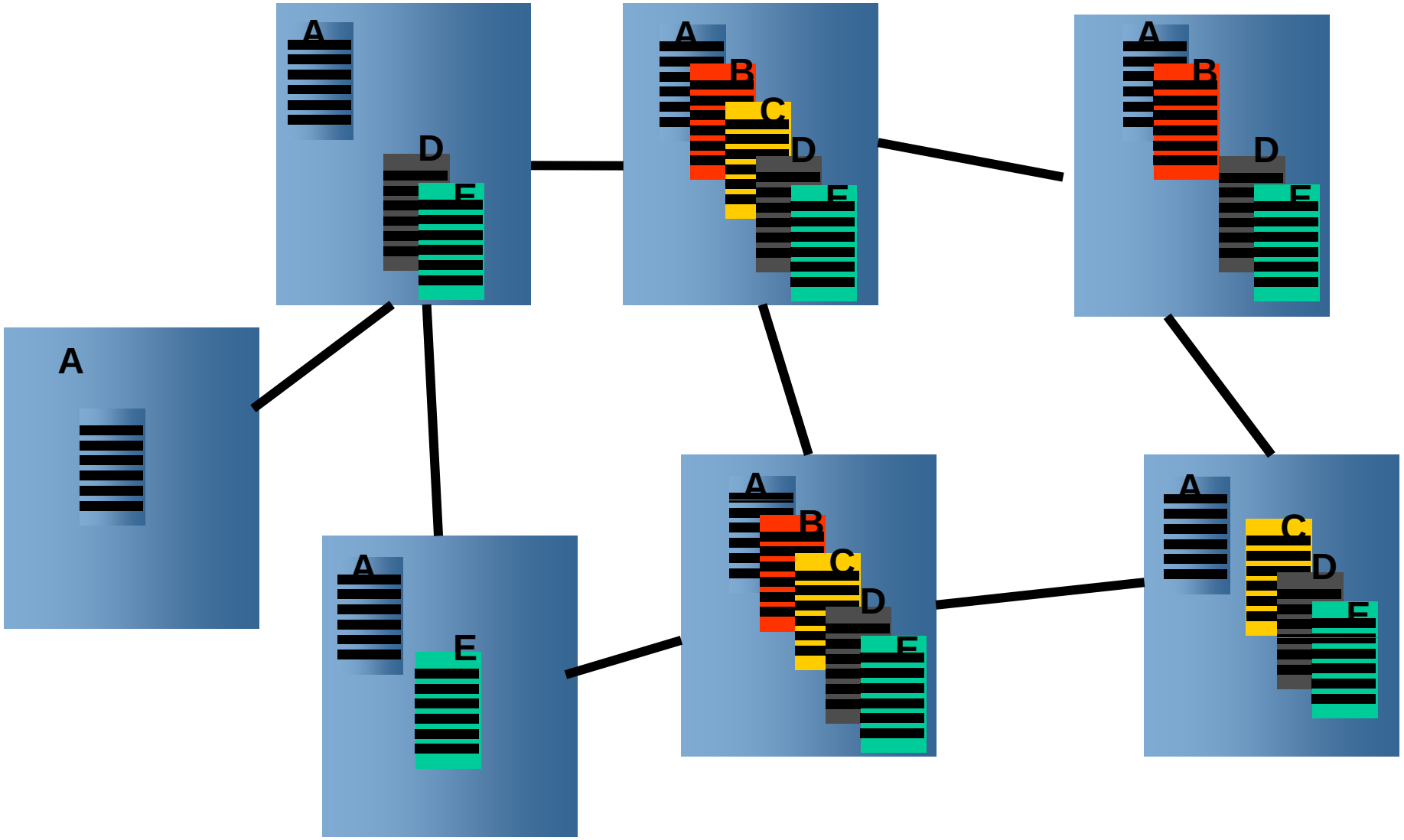
Virtualization of the Data Plane



Virtualization of the Data Plane



Virtualization of the protocols



Post-IP security through a strong authentication and closed traceability

Why two-factor authentication is needed

Password issues

- **Attackers can sniff out what's typed on keyboards, simply by recording keystroke sounds**
  - Recommendation to enhance security with **two-factor authentication** that combines passwords with one-time-password tokens or **smartcards**, or with biometric recognition, like fingerprint readers
- **A well known two-factor authentication device is the RSA SecurID token**
  - This token works with a proprietary authentication infrastructure called ACE.

Two-factor authentication

Our proposal

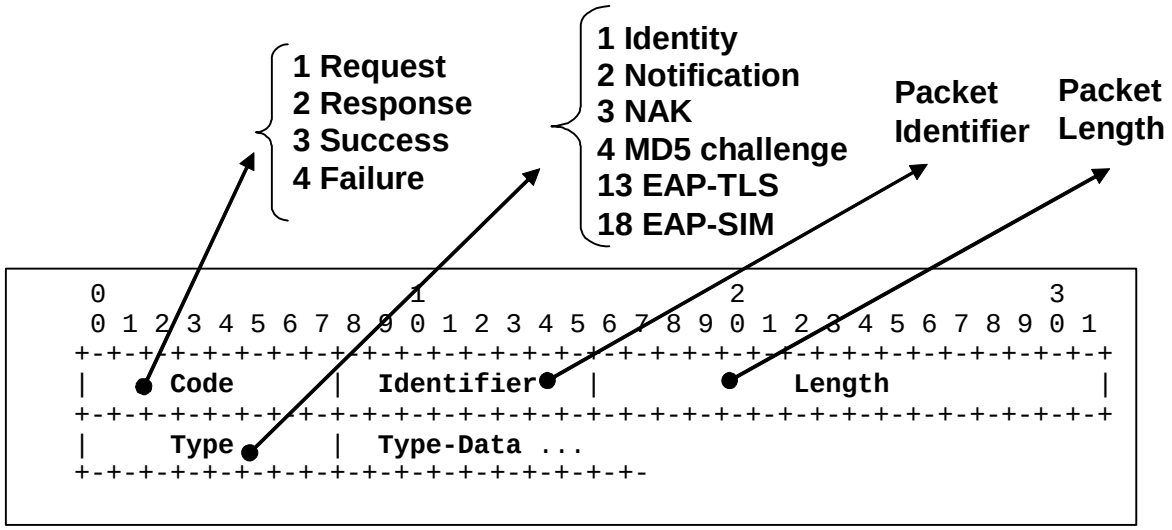
- Tokens are based on the Java Card technology
- They execute Java applications supported by the open code project *OpenEapSmartcard* .
- The authentication platform is fully based on IETF standards (mainly the *Extensible Authentication Protocol*, EAP), no proprietary features
- Our authentication scenario deals with the classical SSL/TLS protocol (more precisely EAP-TLS), which is widely deployed through the WEB, and which relies on Public Key Infrastructure (PKI)

What is EAP ?

EAP is an IETF standard

- **The Extensible Authentication Protocol (EAP) was introduced in 1999, in order to define a flexible authentication framework.**
  - ***EAP***, RFC 3748, "Extensible Authentication Protocol, (EAP)"
  - ***EAP-TLS***, RFC 2716, "PPP EAP TLS Authentication Protocol“
  - ***EAP-SIM***, RFC 4186, " Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM) “
  - ***EAP-AKA***, RFC 4187, " Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA) “

What is EAP ?



EAP Message Format.

What is EAP ?

An *Esperanto* for Access Control in IP infrastructures.

- ***Wireless LAN***
  - Wi-Fi, IEEE 802.1x
  - WiMAX mobile, IEEE 802.16e , PKM-EAP
- ***Wired LANs***
  - ETHERNET, IEEE 802.3
  - PPP, RFC 1661, “The Point-to-Point Protocol (PPP)”
- ***VPN (Virtual Private Network) technologies***
  - PPTP, RFC 2637 , " Point-to-Point Tunnelling Protocol "
  - L2TP, RFC 2661 , " Layer Two Tunnelling Protocol "
  - IKEv2, RFC 4306, "Internet Key Exchange Protocol“
- ***Authentication Server***
  - RADIUS, RFC 3559, “RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)”
  - DIAMETER, RFC 4072, "Diameter Extensible Authentication Protocol Application“
- ***Voice Over IP***
  - UMA, Unlicensed Mobile Access, http://www.umatechnology.org

What is EAP ?

EAP components

- **According to RFC 3748, EAP implementations conceptually consist of the four following components:**
  - 1- The lower layer is responsible for transmitting and receiving EAP frames between the peer and authenticator.
  - 2- The EAP layer receives and transmits EAP packets via the lower layer, implements duplicate detection and retransmission, and delivers and receives EAP messages to and from EAP methods.
  - 3- EAP peer and authenticator layers. Based on the Code field, the EAP layer de-multiplexes incoming EAP packets to the EAP peer and authenticator layers.
  - 4- EAP methods implement the authentication algorithms, and receive and transmit EAP messages. **EAP methods can be implemented in Java Card systems.**

What is EAP ?

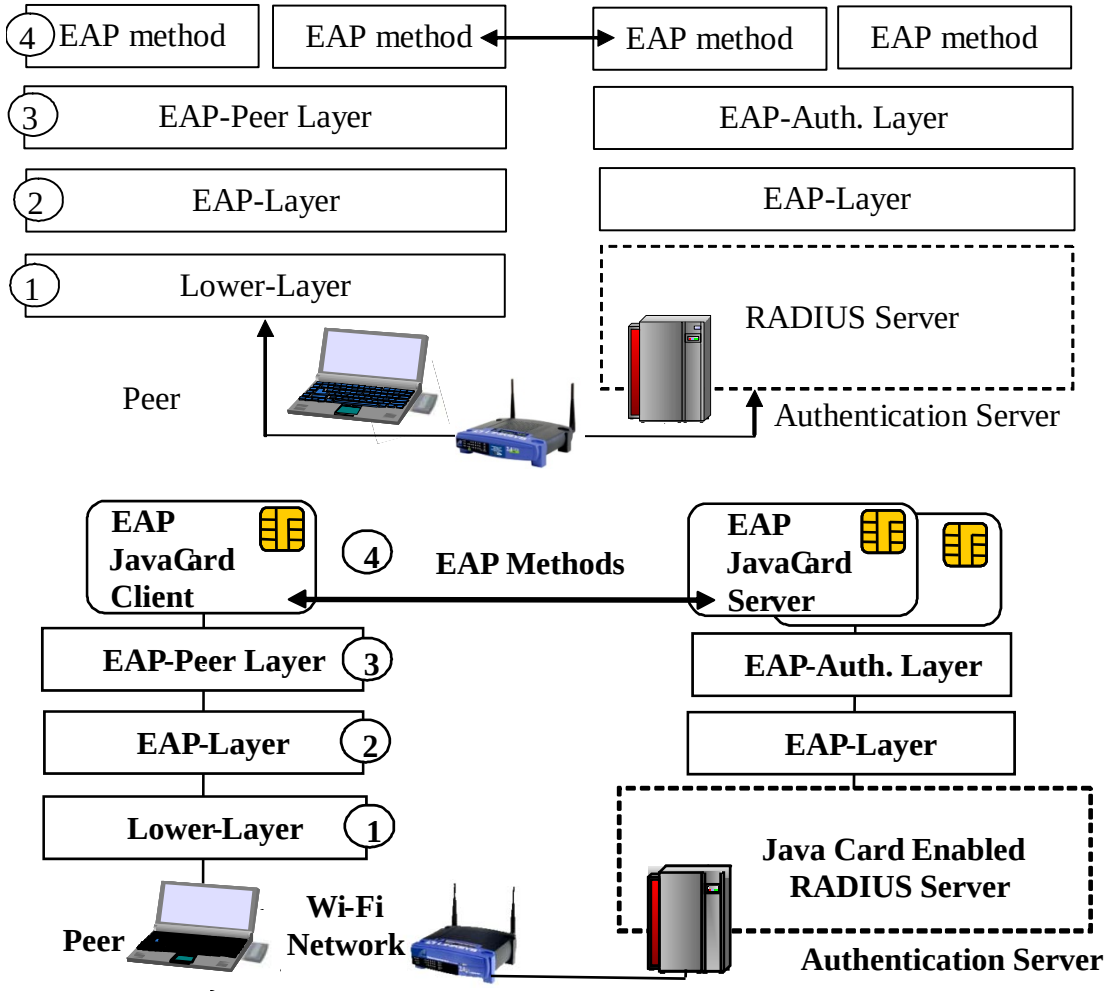
EAP Java Card Technology

Full Software Implementations

Partial Software Implementations

+

EAP JavaCard Technology

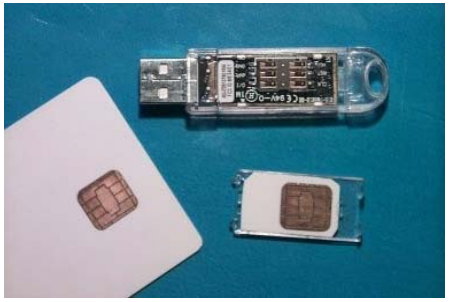


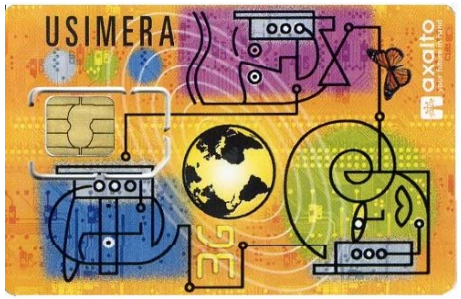
The open platform,

OpenEAP Smartcard

Why open Java Card technology code ?

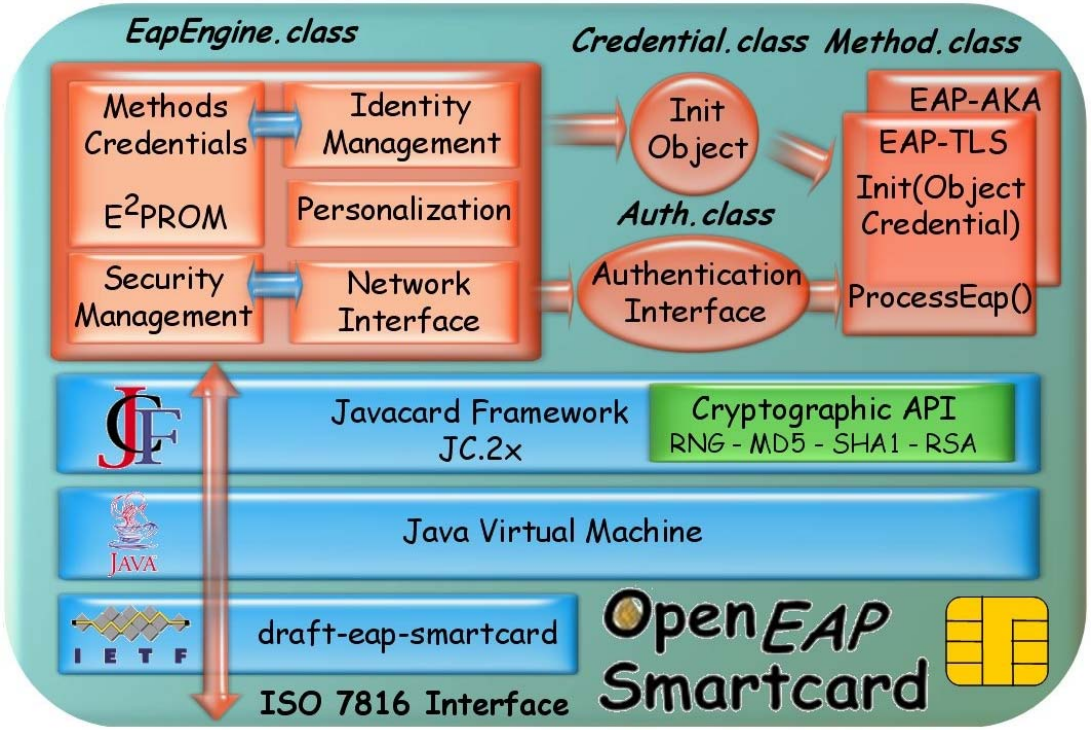
- Internet and WEB technologies are based on *open code*.
- No proprietary features.
- Good security principle that enables code reviewing.
- Fair choice among multiple Java Card systems





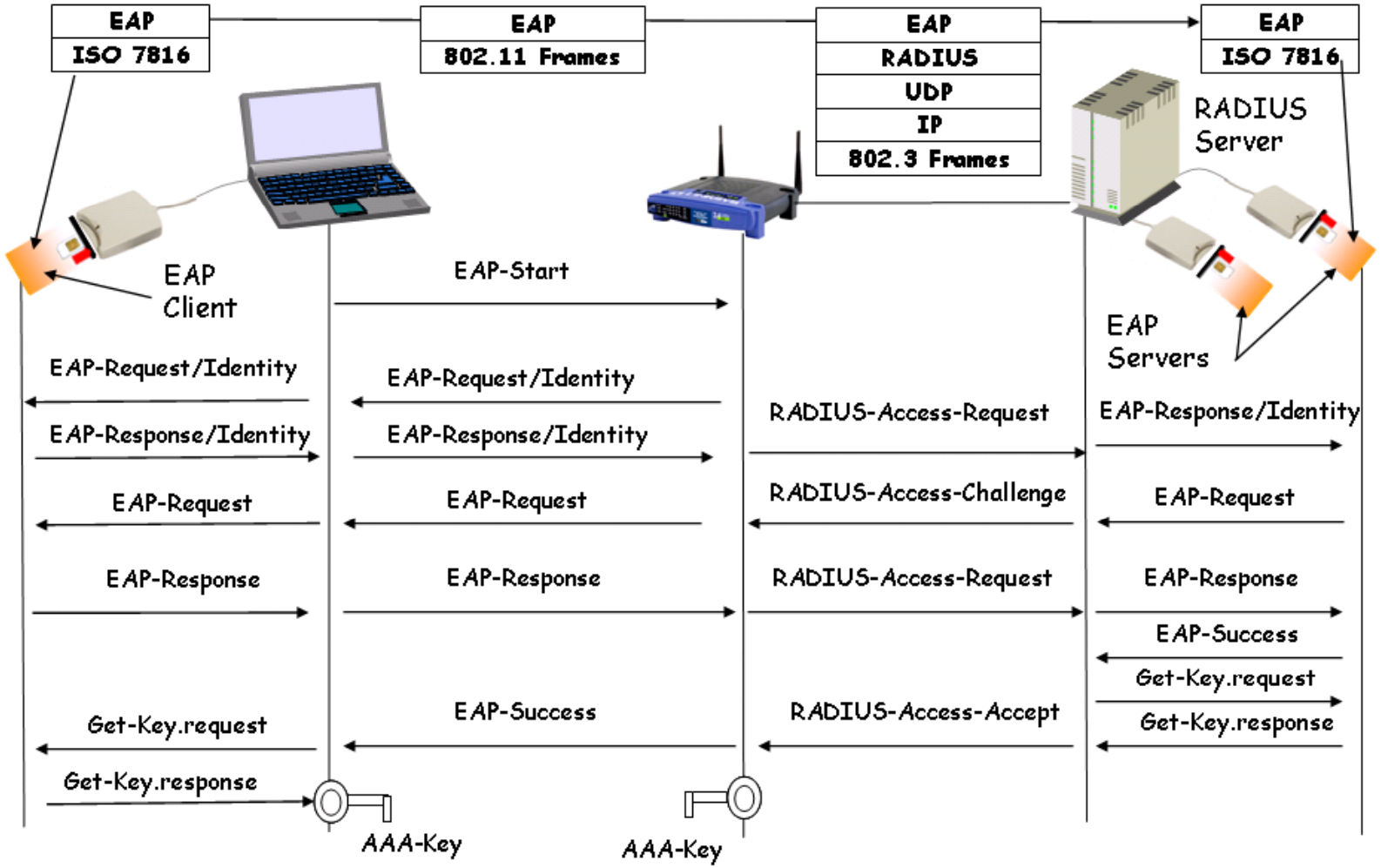
OpenEapSmartcard.

Architecture Overview

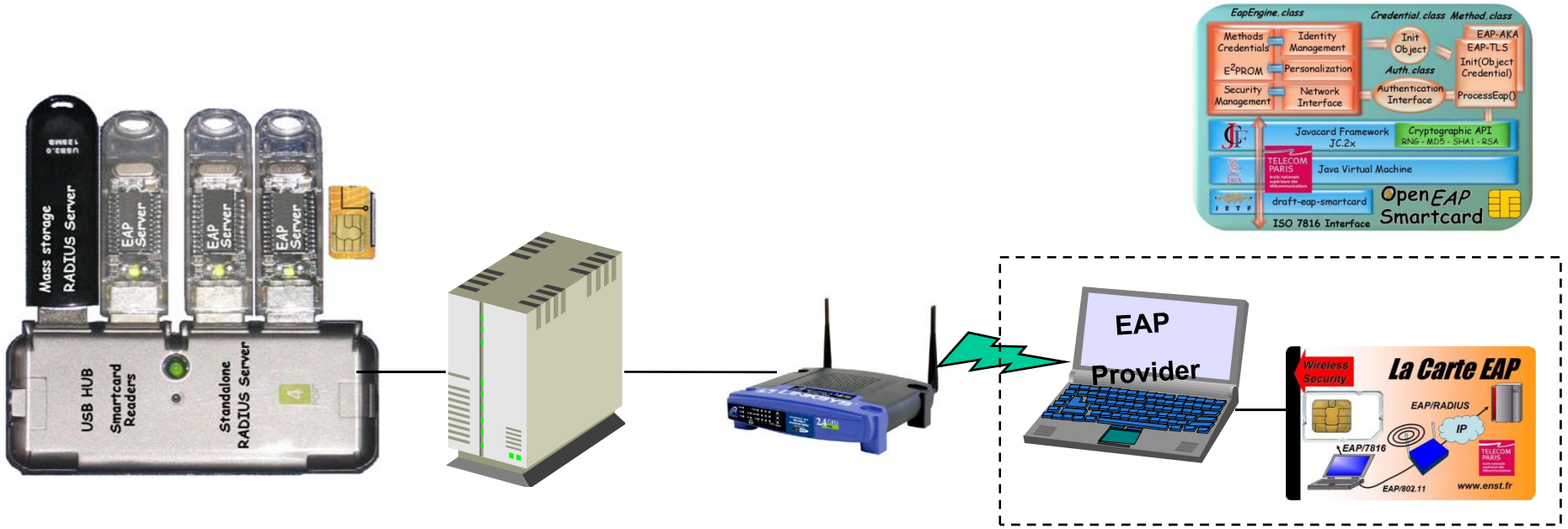


Authentication platform

Overview



The platform



Summary

- We have presented two-factor authentication tokens, based on the Java Card technology
- We have introduced the open code project *OpenEapSmartcard*, which is used by these token
- We have built an authentication architecture fully based on IETF standards.
- We have shown a real Wi-Fi platform that deals with these technologies.