EAP-WAI Authentication Protocol

draft-richard-emu-wai-00

Richard

2009-07-26 Stockholm, IETF 75th

Preface

WAPI is a WLAN security protocol which is brought forward by a Standard Group in China. It was invited by the ISO/IEC/JTC1/SC6 to submit it as an international proposal in June, 2009

Although WAPI is independent to the AAA,

I think WAPI should have a deployment model which would reuse the AAA architecture.

The carriers in the China agree to my idea, and we wrote this draft together.

The draft demonstrates that EAP protocol and Radius Protocol are very extensible.

Agenda

- **WAPI Overview**
- **Benefits of the EAP-WAI**
- **Design Idea**
- **EAP-WAI Process**

WAPI Overview (1/4)

WAPI is the abbreviation of

WLAN Authentication and Privacy Infrastructure

WAPI mainly includes two parts:

- **WLAN Authentication Infrastructure (WAI)**

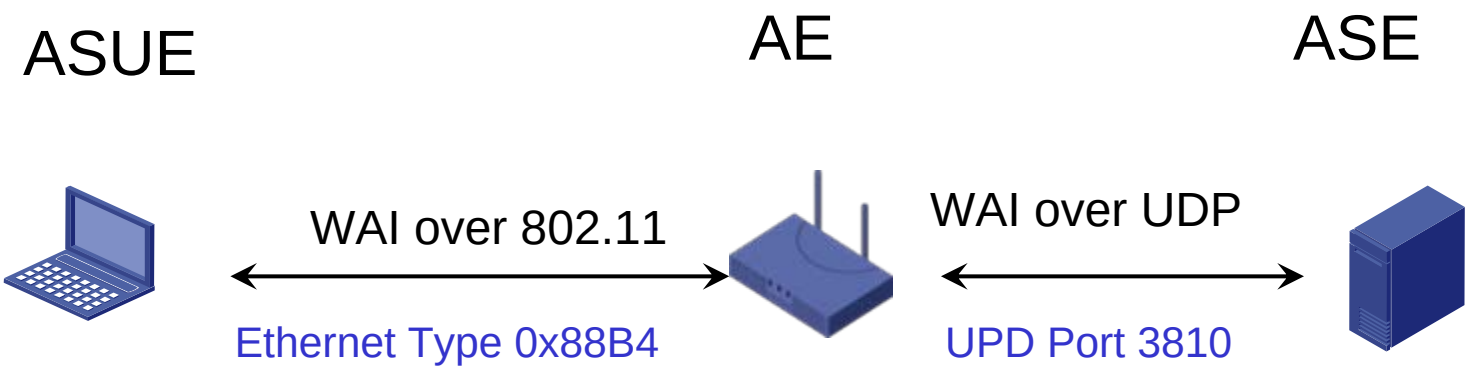
To offer the function of authentication and key management

- **WLAN Privacy Infrastructure (WPI)**

To provide the data protect (encryption) and data integration service.

WAPI Overview (2/4)

WAI Protocol



The WAI is a core part of the WAPI protocol.

ASUE Authentication Supplicant Entity

AE Authenticator Entity

ASE Authentication Service Entity

WAPI Overview (3/4)

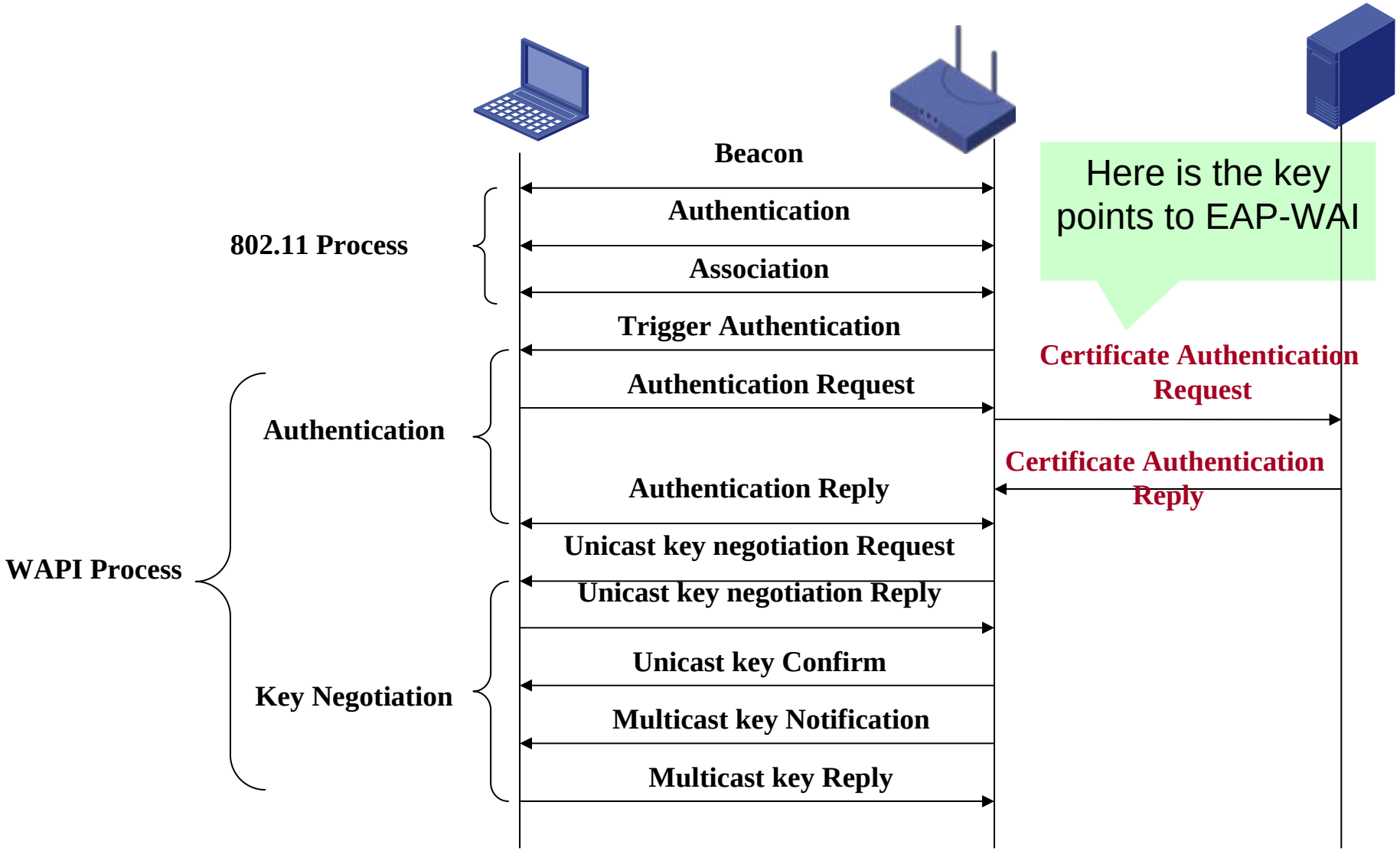
The Highlight of WAPI

- Although it depends on the three entities, it is independent to AAA architecture;
- Supports the mutual authentication between station (ASUE) and the WLAN devices (AE);
- The public-key certificate is an important part of the construction of WAPI system. The identity of ASUE and AE can be uniquely identified by the certificate;
- During the authentication phase, both WLAN device (AE) and station (ASUE) would send their certificates to the ASE. The ASE verify the legality of both certificates and would send the result of verification to the station and WLAN devices.

The Behavior of AE is NOT pass-through

WAPI Overview (4/4)

The main process



Agenda

- **WAPI Overview**
- **Benefits of the EAP-WAI**
- **Design Idea**
- **EAP-WAI Process**

Benefits of the EAP-WAI

If WAPI supports the deployment model of reusing AAA architecture, then:

- **Independent software vendor (ISV) could easily make the current AAA server support the ASE function;**
- **As the deployment of the additional ASE server could be not required, it would reduce the costs of the WAPI infrastructure's deployment and maintenance**
- **The WAPI offers the link-level security to the ASUE, e.g., the authentication and confidentiality. Besides them, ASUE needs the authorization and accounting service. The AAA already supports such functions well, and the WAPI could easily reuse such services if it could reuse AAA architecture.**

Agenda

- **WAPI Overview**
- **Benefits of the EAP-WAI**
- **Design Idea**
- **EAP-WAI Process**

Design Idea (1/2)

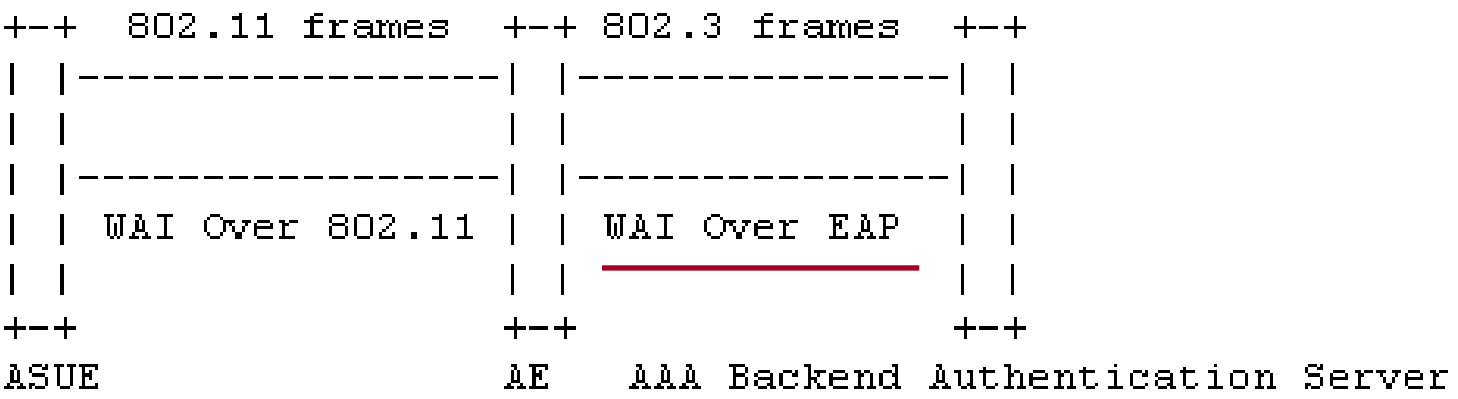
In order to reuse the AAA architecture and avoid the influence to the station (ASUE), the EAP packet SHOULD be exchanged between the AE and the AAA server.

As AAA server's peer is station (ASUE), the WLAN Device (AE) SHOULD mimic itself as a peer (ASUE).

By this way, from the AAA server perspective, EAP-WAI is similar to the other authentication methods

Design Idea (2/2)

NO Change



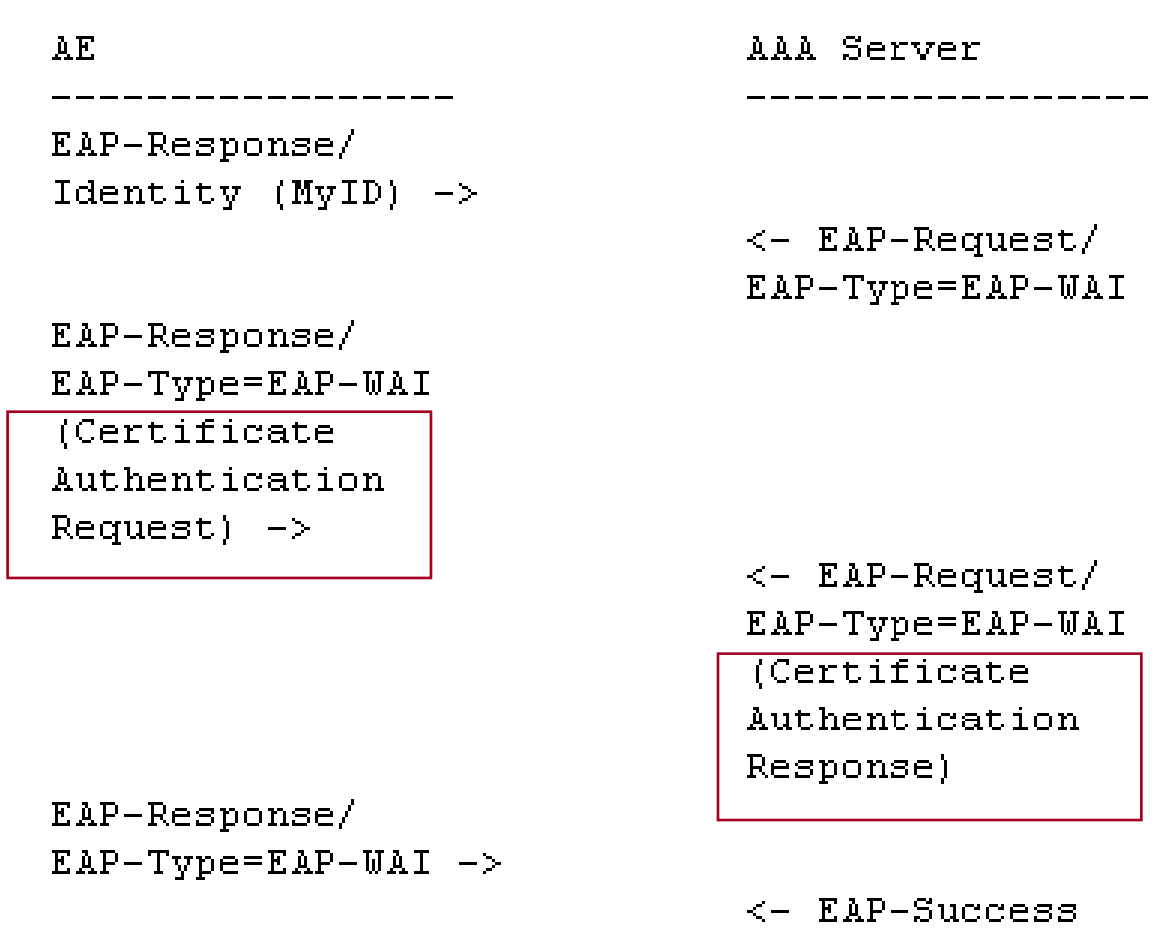
AE would mimic itself as a peer (ASUE) to AAA

For AAA, EAP-WAI is similar to the other authentication methods

Agenda

- **WAPI Overview**
- **Benefits of the EAP-WAI**
- **Design Idea**
- **EAP-WAI Process**

EAP-WAI Process



As AE SHOULD mimic a peer (ASUE), there is no need to let AE send the EAP-Request/Identity to ASUE any more

The EAP identity MAY be the subject [RFC3280] of ASUE's certificate.

Thank You

Any Question?