Smart Card based Authentication Mechanism for FTTH Access Networks

Joaquín López Rizaldos (jolo@tid.es), Francisco Rodríguez García (frg@tid.es), Alejandro Fandiño Orgeira (orgeira@tid.es), Jose Manuel Palacios Valverde (jmpv@tid.es), Alejandro García Henderson (alejgm@tid.es) and Francisco González Vidal (vidal@dit.upm.es)

Broadband Services Platforms and Architectures, Telefónica I+D

***Abstract*—Nowadays in the fixed domain (residential lines) the authentication methods use dial-up protocols (mainly PPP) and the customer is identified by the physical line. This mechanism presents some limitations that constrain the creation of added-value services and increase the complexity of network management. In the first place, the line data has to be provisioned in the network elements what leads to long and error-prone processes. Besides, services must be based on the line data, which limits the creation of added-value portable services. We propose a new authentication method based on an ISIM card: EAP/AKA over 802.1X.**

***Index Terms* — 802.1X, Access Network, Extensible Authentication Protocol (EAP), TISPAN NGN.**

I. Introduction

Fixed line broadband access is usually identified based on the physical access. For that purpose, the access node port information is sent to the AAA Server in DHCP (Dynamic Host Configuration Protocol) Option 82 [1]. Simpler strategies based on login and password are also used by some operators but are too prone to suffering fraud. Other proposals as [2] suggest some extensions to DHCP in order to support EAP (Extensible Authentication Protocol), but require changes in the DHCP message set.

With the advent of IMS (IP Multimedia Subsystem), the Home Gateway will be equipped with an ISIM card for identification in the service domain, as specified by the HGI and ETSI TISPAN WG5 [3]. Using the ISIM (IP Multimedia Services Identity Module) card for the access authentication (network attachment) would avoid network domain and service domain authentication duality.

Moreover, the use of ISIM based authentication may bring important additional benefits. The operator would greatly simplify the slow and complex provisioning process that are required to keep track of which user is statically attached to what physical line. As far as the end user is concerned, if all the access lines are equal, any service can be provided on any line instantly, allowing nomadism, impulsive purchase of IPTV services and other scenarios.

In this paper, some of the technical challenges of the model are analyzed and an implementation is presented.

II. EAP/AKA Over 802.1X Authentication Proposal

The mechanism proposed here requires enabling 802.1X [4] in the access equipment, which will act as the 802.1X authenticator. The Home Gateway will act as the supplicant and the UAAF will take the AAA role. After successful interchange of credentials, the session will be stored in the CLF. This phase is called "port authentication". In a second stage, a standard DHCP process will take place. The NACF, acting as a DHCP server, will consult also the CLF about the authentication status of the port. An IP address is then granted. The CLF may then push the initial policies to the B-RAS (Broadband Remote Access Server) through the A-RACF. This phase is called "IP address allocation".

A. Architecture

Fig. 1 represents the architecture of the proposed solution. Following are detailed the involved elements:

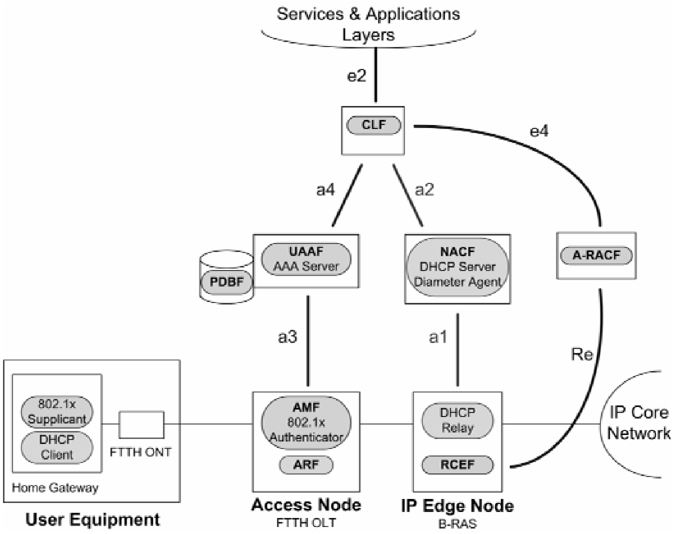

Fig. 1. EAP/AKA over 802.1X Authentication Platform proposal.

- Home Gateway: Requires both 802.1X and DHCP client functionality. It must host an ISIM card running the EAP/AKA algorithm [5], [6].
- Access Node (FTTH OLT): The access node will act as the 802.1X authenticator. It applies initial filters, permitting only EAP over 802.1X incoming packets. During EAP authentication, it maps user EAP packets into RADIUS messages and vice versa. It should also include remote-circuit-id value into NAS-Port-Id AVP in RADIUS packets and into Option 82 in DHCP packets to allow the CLF matching authentication and IP addressing notifications related to the same user. Once network access is granted, the Access Node allows user access.

- IP Edge Node (B-RAS): Once the user is successfully authenticated, IP Edge Node receives DHCP packets from the user. The DHCP Relay function proxies DHCP packets to the DHCP server (NACF). The RCEF (Resource Control Enforcement Function) module enforces the quality of service and gating settings requested by A-RACF.
- UAAF: The main function of UAAF entity is user authentication and authorization. It performs the server side of EAP/AKA algorithm. When the user is successfully authenticated, the new session is pushed to the CLF.
- PDBF: Contains user profile data, such as subscriber id (ISIM), network profile or initial gating settings.
- NACF: It deals with IP address allocation.
- CLF: It collects authentication and IP address allocation data and requests A-RACF to apply user network profile. It also provides e2 interface to upper layers, which can obtain user session information (e.g. Subscriber ID).
- A-RACF (Access-Resource and Admission Control Function): When the authentication and addressing processes finish, the CLF requests the A-RACF to apply QoS Policies and Gating Settings to the authenticated user.

B. *Flow interaction*

Both port authentication and IP address allocation have the same life cycle: initial authentication (binding), re-authentication (renewal) and disconnect (release). Only initial authentication/binding stage is detailed in this paper.

Initial connection consists of three stages: Authentication (EAP/AKA over 802.1X), IP Address Allocation (DHCP) andd QoS and Gating Settings enforcement.

1) User Authentication and Authorization Stage: The 802.1X Authenticator blocks all traffic of unauthenticated users. As the AMF entity in the access node detects a user packet, it requests the user to start the EAP authentication process, which is shown in Fig. 2:

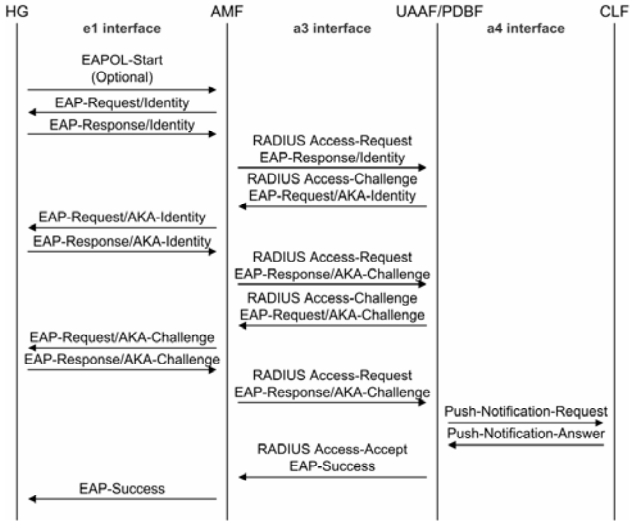
HG
AMF
UAAF/PDBF
CLF
e1 interface
a3 interface
a4 interface
EAPOL-Start (Optional)
EAP-Request/Identity
EAP-Response/Identity
RADIUS Access-Request EAP-Response/Identity
RADIUS Access-Challenge EAP-Request/AKA-Identity
EAP-Request/AKA-Identity
EAP-Response/AKA-Identity
RADIUS Access-Request EAP-Response/AKA-Challenge
RADIUS Access-Challenge EAP-Request/AKA-Challenge
EAP-Request/AKA-Challenge
EAP-Response/AKA-Challenge
RADIUS Access-Request EAP-Response/AKA-Challenge
Push-Notification-Request
Push-Notification-Answer
RADIUS Access-Accept EAP-Success
EAP-Success

Fig. 2. Stage 1: User Authentication and Authorization

If EAP/AKA authentication succeeds the user gains access to the network. The Access Node removes blocking filters and permits traffic flows with the user MAC address and through the logical port where the user is plugged. UAAF also notifies the CLF that the user has been successfully authenticated.

2) IP Allocation Stage: Once the user is authenticated, the CPE requests an IP address. DHCP is used and the NACF allocates the IP address as specified in [7]. The NACF notifies the CLF about the IP address allocation.

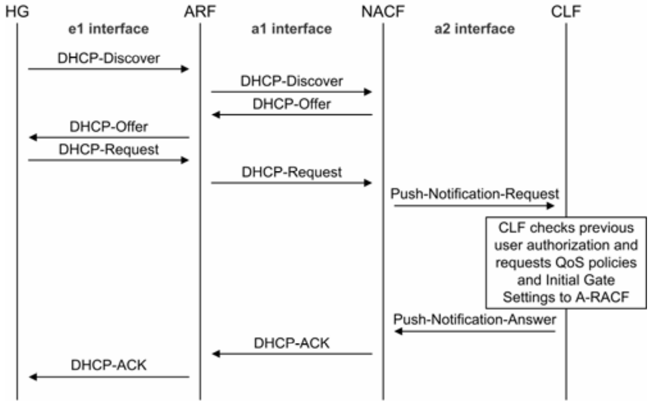

Fig. 3. Stage 2: IP Address Allocation

3) Initial QoS Profile and Gate Settings Enforcement: When the CLF receives the notifications of successful authentication and addressing phases, it requests the A-RACF to apply Initial QoS Profile and Gating Settings. These parameters have been received from UAAF (PDBF) in the authentication stage. A-RACF requests the enforcement to the RCEF entity that resides in the B-RAS.

III. Conclusion

In this paper, a novel user authentication and addressing mechanism for fixed networks is presented. User identity is based on ISIM card instead of the physical access line. This approach is beneficial both for the operator, that may avoid some of the costs and complexity of the provisioning systems that have to match the client identity with the physical line accessed, and for the end user, that can be allowed to subscribe instantly value added services, and can be easily provided with nomadism capabilities.

Although the solution proposed has been successfully validated in an FTTH environment, it could be deployed over several access networks types (xDSL, FTTx,…). The proposal is full TISPAN compliant and allows a smooth migration path, since 802.1X protocol is widely deployed in Ethernet-based access network equipment and EAP/AKA algorithm requires only to be implemented in AAA servers.

References

[1] DSL Forum TR-101, Migration to Ethernet-Based DSL Aggregation, April 2006.
[2] Internet Draft, Authentication Extensions for the Dynamic Host Configuration Protocol (draft-pruss-dhcp-auth-dsl-02), November 2007.
[3] ETSI TS 185 006 V2.0.0, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Customer Devices architecture and Reference Points.
[4] IEEE Standard for Local and metropolitan area networks, Port-based Network Access Control, IEEE Standard 802.1X, December 2004.
[5] RFC 3748, Extensible Authentication Protocol (EAP), June 2004.
[6] RFC 4187, Extensible Authentication Protocol for 3rd Generation Authentication and Key Agreement, Internet Society, January 2006.
[7] ETSI ES 282 004 V1.1.1, Telecommunication and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Subsystem (NASS).