|  |
| --- |
| Revision of chapter 7.4 |
| Date: 2016-09-14 |
| **Authors:**  |
| Name  | Affiliation  | Phone  | Email  |
| Max Riegel | Nokia Bell Labs | +49 173 293 8240 | maximilian.riegel@nokia.com |
|  |  |  |  |
|  |  |  |  |
| **Notice:**This document does not represent the agreed view of the OmniRAN TG It represents only the views of the participants listed in the ‘Authors:’ field above. It is offered as a basis for discussion. It is not binding on the contributor, who reserve the right to add, amend or withdraw material contained herein.  |
| **Copyright policy:**The contributor is familiar with the IEEE-SA Copyright Policy <<http://standards.ieee.org/IPR/copyrightpolicy.html>>.  |
| **Patent policy:** The contributor is familiar with the IEEE-SA Patent Policy and Procedures:<[http://standards.ieee.org/guides/bylaws/sect6-7.html#6](http://standards.ieee.org/guides/bylaws/sect6-7.html)> and <[http://standards.ieee.org/guides/opman/sect6.html#6.3](http://standards.ieee.org/guides/opman/sect6.html)>. |

Abstract

This document proposes revised text for the functional description of authentication and trust establishment.

7 Functional Decomposition and Design 3

7.4 Authentication and Trust Establishment 3

7.4.1 Introduction 3

7.4.2 Roles and identifiers 3

7.4.2.1 User 4

7.4.2.2 ServiceProvider 4

7.4.2.3 Subscription 4

7.4.2.4 Terminal 5

7.4.2.5 Access network 5

7.4.2.6 Subscription Service 5

7.4.3 Use Cases 5

7.4.3.1 AN with direct relation to SS 5

7.4.3.2 AN with relation to SS relayed over another SS 5

7.4.3.3 AN with relation to the SS of a roaming consortia 5

7.4.4 Functional Requirements 5

7.4.5 Authentication specific attributes 6

7.4.5.1 User 6

7.4.5.2 ServiceProvider 6

7.4.5.3 Subscription 7

7.4.5.4 Terminal 7

7.4.5.5 Access Network 7

7.4.5.6 Subscription Service 7

7.4.6 Authentication specific basic functions 7

7.4.6.1 Identification request 7

7.4.6.2 Identification notify 7

7.4.6.3 Authentication process 7

7.4.6.4 Trust establishment 7

7.4.6.5 Trust revocation 7

7.4.7 Detailed procedures 8

7.4.7.1 Direct service access 8

7.4.7.2 Service access with relay of authentication over another subscription service 8

7.4.8 Mapping to IEEE 802 Technologies 8

7.4.8.1 Overview 8

7.4.8.2 IEEE 802.3 specifics 8

7.4.8.3 IEEE 802.11 specifics 8

7.4.8.4 IEEE 802.16 specifics 8

7.4.8.5 IEEE 802.22 specifics 8

# Functional Decomposition and Design

## Authentication and Trust Establishment

### Introduction

Successful mutual authentication of user and service provider creates the base for the establishment of trust for allowing access to and providing services out of a communication infrastructure. It is the foundation of security in IEEE 802 access networks.

Security of access network consists of the two aspects of securing the provisioning of services to users, and of securing the infrastructure against malicious attacks. Securing the provisioning of services mainly requires the validation of the identity of the user and the binding of the user to the mobile device, which is allowed to establish a link through the access network to the access router and to retrieve and deliver data over the authorized datapath in the access network.

Securing the infrastructure requires security means on each and every interface

* to enable the verification of the identity of the entity and its interface,
* to protect and show the integrity of all information exchanged across an interface between the peers,
* to enable non-repudiation of messages exchanged between the peers, and
* to provide encryption facilities to cypher information for avoiding interception of confidential information on the transmission path.

Security is realized through various kinds of signatures, which are shared as keys between the peers. Signatures can be passwords consisting of a sequence of characters, but might be more complex structures like digital certificates, which embed a trust hierarchy together with the keying material.

IEEE 802 access networks use port based authentication together with the Extensible Authentication Protocol (EAP) to mutually verify the identity of the user and the node of access, to control the access to the communication resources, and to generate and install a pairwise master key as the foundation of the encryption of the user data passing over the R1 reference point.



Figure 7‑1: Port based authentication architecture

The port based authentication system consists of a Supplicant System located in the terminal, an Authenticator System located in the node of attachment and an Authentication Server System, which resides in the Subscription Service. Supplicant and Authenticator have both two ports, an uncontrolled port into the Port Authentication Entity (PAE), and a controlled port for the user data and other protocol information forwarded over the datapath.

In the unauthenticated state, the controlled port in both the supplicant as well as in the authenticator are blocked. Only authentication messages of the EAP are exchanged between the PAE in the Authenticator and the PAE in the Supplicant to verify the identities of both peers and to create and install the pairwise master key for the encryption of the data passing through the controlled port. Once the authentication with forwarding the messages from the authenticator to the authentication server succeeds successfully, the controlled ports in both the supplicant as well as the authenticator are opened and the exchange of user data and other protocol information can start.

It is good practice not to directly use the persistent password or the keying material in certificates for the cyphering process, but to derive temporary keys for the processing of the transferred information to realize integrity, non-repudiation and encryption. Temporary keys may be modified frequently to make it more difficult for an attacker to apply brute-force methods for breaking the security.

Authentication and trust establishment deals mainly with user authentication, securing the access to the access infrastructure and provisioning of right kind of services to the user.

### Roles and identifiers

Authentication and trust establishment describes the process by which trust relationship between a user and the provider of communication services is created and mapped to configurations of infrastructure performing the access to the communication services of the service provider.

Well ahead of making use of the access network to retrieve communication services from a service provider, the user of a terminal has to agree with the service provider about the terms and conditions for making use of the access network and retrieving services.

The agreement arranged between a user and a service provider is called a subscription, which consists not only of a unique identifier and some kind of shared secret for the authentication process but also of information about the service portfolio offered to the user. The service provider expects income from providing communication services. Therefore, the subscription is usually amended with conditions and parameters for accounting and charging of the consumed services.

The contractual relationship between user and service provider is mapped by technical means into the communication infrastructure, when the user seeks to access the services.



Figure ‑2: Roles involved in authentication

The following roles and identifiers are involved in the authentication and trust establishment procedures:

#### User

Entity, who is responsible for the terminal seeking access to service, and who has set-up contractual relationship with the service provider.

Identifier: User-ID

#### Service Provider

Organization, which is responsible for provisioning of service, and which provides contractual relationships to users.

Identifier: ServiceProvider-ID

#### Subscription

Contract between user and service provider about the services to be delivered, when demanded by the user. A subscription is usually accompanied by terms and conditions further detailing the offered service of the service provider.

Identifier: Subscription-ID

#### Terminal

Device, which is bound to User, and which receives information containing the service when the user initiates connection to the access network.

Identifier: see section 6.8

#### Access network

Equipment controlling access to service and delivering service on behalf of service provider

Identifier: see section 6.8

#### Subscription Service

Service entity bound to the service provider which provides service authorization to access network and access router

Identifier: see section 6.8

### Use Cases

The following use cases describe the main scenarios for authentication and trust establishment in various arrangements of relation of subscription services to access networks and access routers.

#### AN with direct relation to SS

In this case the subscription service of the Service Provider is directly connected to the access network. The user seeks and receives service directly authenticating with the Service Provider

#### AN with relation to SS relayed over another SS

In this case the subscription service of the Service Provider is not directly reachable from the access network, but has to be relayed over the subscription service of another service provider. The user seeks and receives service by making use of an intermediate subscription service for forwarding the authentication procedure.

The Service Provider of the User is not visible at the access network, but the User knows about the relation between the Service Provider and another service provider having direct relationship with the access network.

#### AN with relation to the SS of a roaming consortia

In this case the Service Provider is partner of a roaming consortia, providing forwarding of authentication for a number of operators. The access network has a relation to the subscription service of the roaming consortia and forwards any authentication indicating membership in the roaming consortia to the subscription service of the roaming consortia.

Effectively this scenario is similar to the scenario above with the distinction that the access network signals support of the roaming consortia instead of a number of individually visible operators.

### Functional Requirements

* Authentication procedure should support various methods of authentication methods.
* Authentication procedure should support mutual authentication
* Authentication procedure should support derivation and distribution of master keys from the authentication process.
* Authentication procedure should support various kinds of digital signatures for the identity verification of user and service provider.
* Authentication procedure should support hiding of the identity information between terminal and subscription service.
* Authentication procedure should support standardized forms of Network Access Identifiers (NAI).
* Authentication procedure should support anonymous terminal identifiers for the authorization of services.
* Authentication procedure should support that the same subscription is used for multiple terminals
* Authentication procedure should support multiple concurrent terminal sessions with a single subscription.
* Authentication procedure should support that a terminal can connect with the same subscription concurrently to different access networks.
* Authentication procedure should support of access to services in the service providers network.
* Authentication procedure should support roaming scenarios with either the access network or the access router operated by third-party entities.
* Authentication procedure should support roaming scenarios with authentication information being relayed by a visited subscription service.
* Authentication procedure should avoid leaking the identity or the credentials of the user in any roaming scenario
* Authentication procedure should allow for user initiated service selection when a choice of multiple services is available through an access network
* Authentication procedure should derive all required session keys for all involved entities from a single authentication process.

### Authentication specific attributes

#### User

* Description
* Credential (password, certificate)
* Terminal-ID

#### Service Provider

* Description
* Credential (password, certificate)

#### Subscription

* Description
* User-ID
* ServiceProvider-ID
* Supported Service
* Roaming Partner
* Service: usage credit

#### Terminal

* Supported authentication method
* Supported encryption modes/key requirements
* Credential

#### Access Network

* Supported authentication method
* Supported encryption modes/key requirements
* Credential

#### Subscription Service

* Supported authentication methods
* Associated access network
* Associated access router
* Associated subscription service (roaming partner)

###  Authentication specific basic functions

#### Identification request

Access network provides credential of subscription service, supported authentication methods and queries identity of user and terminal

#### Identification notify

Terminal provides its selection of subscription service, temporary user identity, and requested authentication method. The selected subscription service provides its certificate to the terminal for authentication.

#### Authentication process

Terminal and subscription service initiates and executes the selected authentication method. The authentication method terminates the association with the access network when authentication fails, otherwise it proceeds with trust establishment by installing the encryption keys.

#### Trust establishment

Subscription service generates the encryption keys and forwards them to the involved entities over secured channels.

#### Trust revocation

Subscription service forces the termination of a user session for a particular terminal.

### Detailed procedures

#### Direct service access

Access to service delivered by access network and access router with direct relation to service provider.



Figure 7‑3: Authentication with direct access to service provider

Once the association succeeds, the NA sends an identity\_Request to the TE. The TE responds with an Identity\_Response containing the NAI to the NA, which forwards the information to the ANC. The ANC evaluates the NAI carried over in the Identity\_Response and generates an Access\_Request message containing the NAI of the TE and the related service request. The Access\_Request is send from the ANC over R4 to the related SS.

After receipt of an Access\_Request the SS starts the EAP message exchange with the TE and verifies the identity of the subscription in the TE. When the identity of the TE is known and the requested service can be granted, the SS informs the ANC with an Access\_Accept message of the allowed service.

The ANC forwards related information over the NA to the TE embedded in a success message. The pairwise master key delivered in the Access\_Accept message from the SS to the ANC is handed over to the NA. The TE derives its copy of the pairwise master key locally out of the EAP exchanges.

#### Service access with relay of authentication over another subscription service

Access network does not have direct access to the subscription service of the Service Provider but relays authentication and key establishment over the subscription service of an intermediate subscription service.



Figure 7‑4: Authentication with relayed access to service provider

Once the association succeeds, the NA sends an identity\_Request to the TE. The TE responds with an Identity\_Response containing the NAI to the NA, which forwards the information to the ANC. The ANC evaluates the NAI carried over in the Identity\_Response and generates an Access\_Request message containing the NAI of the TE and the related service request.

The ANC discovers that the SS of service provider of the user can’t directly accessed but has a roaming relationship with an SS connected to the AN. The ANC sends the Access\_Request over R4 to the SS with the roaming relationship to the SS of the service provider. After receipt of the Access\_Request the SS of the service provider starts the EAP message exchange with the TE and verifies the identity of the subscription in the TE. The EAP messages are relayed over the SS of the roaming partner having connectivity with the AN.

When the identity of the TE is known and the requested service can be granted, the SS of the service provider informs the SS of the roaming partner with an Access\_Accept message of the allowed service. The SS of the roaming partner forwards the Access\_Accept to the ANC, which forwards related information over the NA to the TE embedded in a success message. The pairwise master key delivered in the Access\_Accept message from the SS to the ANC is handed over to the NA. The TE derives its copy of the pairwise master key locally out of the EAP exchanges.

### Mapping to IEEE 802 Technologies

#### Overview

The following table provides an overview about the authentication and trust establishment technologies supported by the various IEEE 802 technologies.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 802.3 | 802.11 | 802.16 | 802.22 |
| EAP support | 802.1X | Yes (802.11i) | Yes | Yes |
| User plane encryption | 802.1AE | Yes (802.11i) | Yes | Yes |
| Mutual authentication | EAP method | EAP method | Yes | Yes |

#### IEEE 802.3 specifics

#### IEEE 802.11 specifics

#### IEEE 802.16 specifics

#### IEEE 802.22 specifics