IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Overview of 5G core network access over WLAN | | | | |
| Date: 2021-06-07 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Robert Stacey | Intel |  | +1-503-724-0893 | robert.stacey@intel.com |

Abstract

This document provides and overview of the registration and authentication process for gaining access to a 5G core network over a WLAN. It is a synthesis of 802.11 and 3GPP defined procedures. The document is provided as a tutorial, although the content may be incorporated in the AANI draft technical report on WLAN/3GPP interworking.

# Registration and authentication with a 5G core network via a WLAN

## Overview

3GPP defines two methods for gaining access to a 5G core network via a WLAN: untrusted and trusted access.

With untrusted access no assumptions are made regarding the WLAN other than that it provides an IP route to a non-3GPP interworking function (N3IWF) on the 3GPP core network. Connecting to the WLAN is a separate and independent process from connecting to the 5G core network, although WLAN connection necessarily proceeds connection to the 5G core network. The UE/TE might connect to the WLAN without connecting to the 5G core network if it does not require 5G core network services and then connect to the 5G core network when it does require 5G core network services. Alternatively, the UE/TE might initiate the 5G core network connection immediately following the WLAN connection to gain data protection and immediate access to 5G core network services.

With trusted access, the WLAN is more tightly coupled to the 5G core network. The WLAN includes a trusted gateway function (TNGF) that couples the WLAN connection process with the 5G core network connection process. With trusted access, connecting to the WLAN necessarily implies connecting to the 5G core network.

This clause is structured as follows:

* 4.2 (WLAN connection) provides an overview of the WLAN connection process.
* 4.3 (5G core network connection over an untrusted WLAN) provides an overview of the 5G core network connection process via an untrusted WLAN.
* 4.4 (5G core network connection via a trusted WLAN) provides an overview of the 5G core network connection process when the WLAN is a part of the 5G core network.

It is worth noting the trusted and untrusted are the terms used in 3GPP documents. However, the terms might be misleading since they reference different access procedures and not necessarily the degree to which the WLAN network is trusted for security purposes.

## WLAN connection

### General

A UE/TE connects to a WLAN through a process illustrated in Figure 1.



Figure 1 --- Establishing a WLAN connection

Key aspects of the process are an initial authentication exchange, an association exchange, 802.1X authentication exchange (if necessary), a 4-way handshake to establish the pairwise transient key security association (PTKSA) (if required) and DHCP exchange to obtain an IP address (if the UE/TE is using IPv4).

The exact frame exchange sequence depends on the security policy in place on the WLAN with various options described in 4.2.2 (no authentication), 4.2.3 (password authentication using SAE), 4.2.4 (Password authentication using PSK), 4.2.5 (802.1X authentication), 4.2.6 (FT authentication) and 4.2.7 (Opportunistic key caching).

A UE/TE can determine the WLAN security policy and association options prior to initiating the connection process from the beacon periodically transmitted by the AP or through a Probe Request/Response frame exchange with the AP.

A UE/TE might also use the connection process itself to discover the security policy, i.e., initiate the connection process and abort the process if the AP does not meet the UE/TE security requirements or the UE/TE cannot meet the AP’s security requirements.

### No authentication

If security policy on the WLAN does not require authentication, then either no encryption (so called open system) is used or opportunistic wireless encryption (OWE) is used. The 802.11 standard recommends that OWE be used rather than no encryption.

For both no encryption and OWE, the connection process begins with a 2-way authentication exchange: the non-AP STA sends an open system Authentication frame to the AP and the AP responds with an open system Authentication frame with the status success.

For the no encryption case, the non-AP STA then sends an Association Request frame that does not select a cypher suite or authentication method (i.e., does not include an RSN element) and the AP responds with an Association Response frame with the status code success. At this point data transfer is possible using unprotected Data frames. A PTKSA is not established and is not needed since the Data frames are unprotected.

For the OWE case, the non-AP STA sends an Association Request frame that includes an RSN element selecting use of OWE and includes a Diffie-Hellman Parameter element in the frame. The AP responds with an Association Response frames that acknowledges use of OWE and includes a Diffie-Hellman Parameter element in the frame. The Diffie-Hellman Parameter elements in the Association Request and Association Response frames contain, respectively, the non-AP STA and AP public keys.

A 4-way handshake follows to establish the PTKSA with pairwise transient keys derived from the public keys.

Data transfer using protected Data frames is now possible.

### Password authentication using SAE

Mutual authentication of the non-AP STA and AP can be achieved by demonstrating knowledge of a shared secret, where the shared secret is a password or pass phrase. The 802.11 specification defines a simultaneous authentication of equals (SAE) protocol for this purpose.

The connection process begins with a 4-way authentication exchange comprising a 2-way commit exchange followed by a 2-way confirm exchange. With the commit exchange, the non-AP STA sends an SAE Authentication frame and the AP responds with an SAE Authentication frame. With these two frames each side commits a single guess at the password. This is followed by a second 2-way exchange where the non-AP STA sends an SAE Authentication frame and AP responds with an SAE Authentication frame. These two frames confirm that the other side’s password guess was correct.

Following successful completion of the 4-way authentication exchange, the non-AP STA sends an Association Request frame to the AP and the AP responds with an Association Response frame. Cypher suites are negotiated with this exchange.

This is in turn followed by a 4-way handshake to establish the PTKSA with pairwise transient keys derived from the shared secret.

Data transfer using protected Data frames is now possible.

### Password authentication using PSK

Pre-shared key (PSK) is an older form of password authentication that is still widely deployed. The connection process using PSK authentication begins with a 2-way authentication exchange using open system Authentication frames.

The non-AP STA then sends an Association Request frame and the AP responds with an Association Response frame. With this exchange, the non-AP STA and AP negotiate cypher suites and the use of the PSK authentication method.

This is followed by a 4-way handshake, that both demonstrates that each side has knowledge of the shared secret and establishes a PTKSA with pairwise transient keys derived from the shared secret.

Data transfer using protected Data frames is now possible.

### 802.1X authentication

For 802.1X authentication, the connection process begins with the non-AP STA sending an open system Authentication frame to the AP. The AP responds with an open system Authentication frame with status code success.

The non-AP STA then sends an Association Request frame and the AP responds with an Association Response frame. With this exchange, the non-AP STA and AP negotiate cypher suites and the use of the 802.1X authentication method.

802.1X authentication follows and is performed using EAPOL messages encapsulated in Data frames. The Data frames are unprotected, however, the EAP exchange carried in the EOPOL messages will protect sensitive content. The data exchange is with the AP but the EAPOL message content is relayed to an authentication server (AS) over a secure connection.

Successful 802.1X authentication results in master key distribution from the AS to the non-AP STA and AP. The non-AP STA and AP then use the 4-way handshake to establish a PTKSA with pairwise transient keys derived from the master keys.

Data transfer using protected Data frames is now possible.

### FT authentication

The 802.11 standard defines a streamlined protocol called fast BSS transition for fast association following an initial association and for fast transition between APs in an ESS. The initial connection process is similar to that in 4.2.3 (Password authentication using SAE), 4.2.4 (Password authentication using PSK) and 4.2.5 (802.1X authentication) with some modifications to the details of the exchange to support key caching. Subsequent transitions by the non-AP STA to other APs in the ESS (reassociation) and/or subsequent associations by the non-AP STA with an AP in the ESS then incur minimal overhead due to key caching.

Describe the streamlined exchange here:

-> FT Authentication

<- FT Authentication

-> Association Request

<- Association Response

--PTKSA established--

### Opportunistic key caching

An alternative to FT authentication is opportunistic key caching. A non-AP STA that has previously connected to the WLAN using one of the procedures described in 4.2.3 (Password authentication using SAE), 4.2.4 (Password authentication using PSK) or 4.2.5 (802.1X authentication) can opportunistically determine if a cached PMKSA is in place with the AP.

The non-AP STA performs an initial 2-way authentication exchange using open system Authentication frames.

The non-AP STA then identifies the PMKSA (by its PMKID) from a previous authentication in the Association Request frame. If the AP supports key caching and the PMKSA identified by the PMKID is available, then this is indicated in the Association Response frame. If the PMKSA is in place, authentication is not needed (possession of the PMKID confirms identity).

The non-AP STA and AP then use the 4-way handshake to establish a PTKSA based on the cached PMK.

Data transfer using protected Data frames is now possible.

## 5G core network connection over an untrusted WLAN

If the UE/TE requires services from a 5G core network and the WLAN over which it is transiting is untrusted, then the UE/TE establishes an IPsec tunnel to the N3IWF that provides access to that network. The entire procedure occurs after the WLAN connection has been established.

The specific N3IWF to which the EU/TE connects is preconfigured, although the IP address might be resolved through a DNS lookup (a service provided by the access network). The procedure used to establish the IPsec tunnel is illustrated in Figure 2.



Figure 2 – IPsec tunnel establishment

The connection to the N3IWF, is established with an initial IKEv2 message exchange. This initial IKEv2 exchange establishes contact and secures the signaling between the UE/TE and N3IWF. 5G NAS messages encapsulated over a 3GPP defined EAP method called EAP-5G can then be securely exchanged.

Using these 5G NAS messages, the UE/TE identifies itself and receives a 5G-Start packet that provides further information on the 5G core network. The UE/TE then sends a 5G NAS message that includes access network (AN) parameters and a registration request.

The N3IWF selects an AMF based on local policy and the received AN parameters and forwards the registration request to the selected AMF in an N2 message.

The AMF may request further identification from the UE, select an AUSF and invoke authentication with the UE/TE. If so, the UE/TE and AUSF mutually authenticate using messages relayed through the AMF. If successfully authenticated, the AUSF sends an anchor key to the AMF from which the AMF derives NAS security keys and the N3IWF security key.

The N3IWF security key is used to establish the IPsec tunnel through a subsequent IKE AUTH exchange. The resulting IPsec tunnel provides both encryption and integrity protection.

## 5G core network connection over a trusted WLAN

If the UE/TE is gaining access to a 5G core network over a WLAN that is trusted, then the WLAN is effectively part of the 5G core network and the authentication process for the WLAN connection is the authentication process for access to the 5G core network with an additional step after the WLAN connection established to create the NAS messaging channel. This process is illustrated in Figure 3.



Figure 3 – Trusted WLAN connection with 5G core network registration

Figures





