WLAN üzerinde kimlik doğrulama, 3 ayrı perspektiften türlere ayrılır / çeşitlenir:

* Open AuthN (Açık Kimlik Doğrulama) 🡪 With Client Certificate (İstemci Sertifikası İle) 🡪 Host / Machine – Based AuthN (Makine
* Shared AuthN (Paylaşımlı 🡪 With Credentials (Kimlik Bilgileri İle) Bazlı Kimlik Doğrulama)

Kimlik Doğrulama) 🡪 With MAC Address (MAC Adresi İle) 🡪 User – Based AuthN (Kullanıcı Bazlı Kimlik

* EAP (Extensible AuthN Protocol) Doğrulama)

🡪 Role – Based AuthN (Rol Bazlı Kimlik

Doğrulama)

1. Yöntem Bakımından Kimlik Doğrulama
2. Open Authentication (Açık Kimlik Doğrulama):

* En basit kimlik doğrulama şekli
* Bağlanacak cihazın, hizmet kümesini (Service-Set) oluşturan erişim noktalarından (APs) herhangi birinin Hizmet Kümesi Tanımlayıcısını (SSID), başka deyişle adını ve wifi şifresini bilmesi yeterli

1. Shared Authentication (Paylaşımlı Kimlik Doğrulama):

* Yaygın olarak bireysel ve küçük çaplı işletmelerde kullanılır.
* PSK (Pre-Shared Key) denilen, bağlantının her iki tarafına (Erişim Noktası ve Cihaz) da önceden verilmiş olan bir anahtar kullanılır. Eğer her iki tarafa da verilen paylaşımlı anahtarlar eşleşirse cihaz ağa kabul edilir.

1. EAP (Extensible Authentication Protocol):

* İşletmeler ve kuruluşlar tarafından, hele ki günümüzde en yaygın olarak, kullanılan yöntem
* Çeşitli argüman seçenekleri (kimlik bilgileri / sertifikalar / MAC Adresleri) vasıtasıyla, kendisine kimlik doğrulama sorguları yapılan bir kimlik doğrulama sunucusu (RADIUS gibi) kullanır.

1. Kullanılan Argüman Bakımından Kimlik Doğrulama
2. Sertifikasyon ile Kimlik Doğrulama:

* Ağa katılmak isteyen istemciler (client) için, [Kimlik doğrulama kaynağı (mesela bir domain controller) tarafından yetkilendirmek amaçlı verilen CA (Sertifika Yetkisi) Root sertifikası ile yetkilendirilmiş] bir istemci sertifikası oluşturulur.
* Bu sertifika sayesinde kimlik doğrulama sunucusu (RADIUS), makine / kullanıcıları ağa kabul eder.

1. Kimlik Bilgileri ile Kimlik Doğrulama:

* Kimlik Doğrulama Sunucusu, kimlik doğrulama kaynağında yer alan istemcilerin kullanıcı adı, şifre gibi kimlik bilgilerini kullanarak kimlik doğrulaması yapar.

1. MAC Adresi ile Kimlik Doğrulama:

* Sadece Makine / Cihaz bazlı kimlik doğrulamada kullanılan kimlik bilgisidir.
* Zira kendisi, her cihaz için eşsiz olan bir şeydir.

1. Kimlik Doğrulamanın Üzerinde Uygulandığı Hedef Bakımından Kimlik Doğrulama
2. Host / Machine – Based Authentication (Makine / Cihaz Bazlı Kimlik Doğrulama):

* Cihaz / Host / Makine, kimlik doğrulamanın uygulandığı şeydir.
* Daha çok kişisel cihazların / makinelerin ağa katılması istendiği zaman uygulanan kimlik doğrulama çeşididir. Ancak eğer kişisel bilgisayar kavramı yoksa (mesela bir kullanıcının şahsi makinesini duruma göre bazen bir başka kullanıcı kullanıyorsa), bu kimlik doğrulama türü patlar! Bunun olmaması için kullanıcı bazlı kimlik doğrulama kullanılabilir.

1. User – Based Authentication (Kullanıcı Bazlı Kimlik Doğrulama):

* Kimlik Doğrulama işlemi, makine yerine kullanıcı üzerinde / kullanıcı esas alınarak gerçekleştirilir. Başka deyişle, kullanıcıların ağa kendilerini tanıttığı bir kimlik doğrulama çeşididir.
* Tıpkı makine bazlı kimlik doğrulamada olduğu gibi argüman olarak kimlik bilgileri yahut istemci sertifikaları kullanılabilir. Ancak MAC adresleri cihazlara has olduğu için bu tip kimlik doğrulamada kullanılamaz!

1. Role – Based Authentication (Rol Bazlı Kimlik Doğrulama):