SECURE DEVICE IDENTIFICATION

INVENTOR:

LUTHER E. SMITH

Description

This the use of Media Access Control (MAC) Address Randomization to provide privacy and protection has created an issue of how to identify individual devices. The need for being able to identify individual device allows for services such as authentication, allow/deny lists, parental controls, accounting and more.

The base of this invention is the during registration and/or association, the device indicates that the device will be using a randomized MAC Address. Once the registrar component receives the indication that the device will be using a randomized MAC Address, then will send a the registrar's Public Key Infrastructure (PKI) public key to the device. The device will then using the registrar's PKI public key encrypt the device's true MAC Address and send the encrypted string containing the true device MAC Address to the registrar. The registrar then associates the device true MAC Address with the randomized MAC Address used by the device. This allows the registrar to make use of the device's true MAC Address in services that currently use MAC Address to preform those services.

While this still allows for the device to use a randomized MAC Address over public accessible physical communication layers, such as RF, coax, twisted pair, Ethernet, optical fiber, etc, this can be used to none publicly accessible physical layers to enable MAC Address Randomization through the ecosystem.

Example of uses are wireless devices to respective base stations, modems to modem terminations systems, optical devices to optical termination devices, server to server, server to switch/router, and router to router.

In lieu of registration and/or association this same process could be performed within Dynamic Host Configuration Protocol (DHCP) function. The risk of randomized MAC Addresses is the DHCP Internet Protocol (IP) address pool could be exhausted as a discrete IP Address are assigned an unique IP Addressed. The use of true MAC Address would allow device true MAC Address, not the randomized MAC Address, to be associated with a given IP Address. Having the true device MAC Address known to the DHCP server, will allow the DHCP server to reissue that same IP Address to the device as long as the IP Address lease has not expired. The result of issuing the same IP Address will reduce the risk of IP Address pool exhaustion. The reuse of the same IP Address for a given device allows applications that depend on reoccurring IP Address assigned to a single device to operate as currently designed.

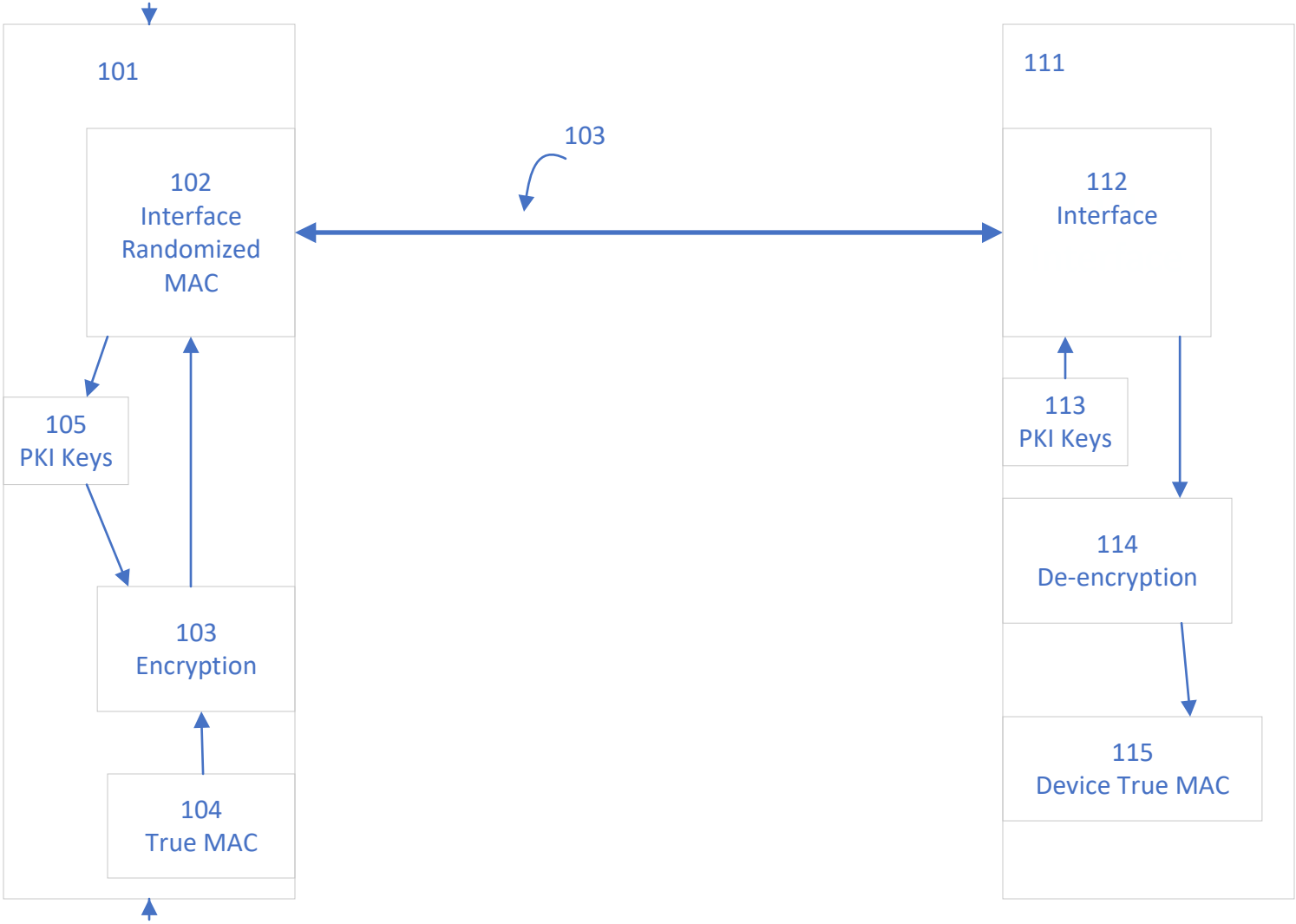
Background

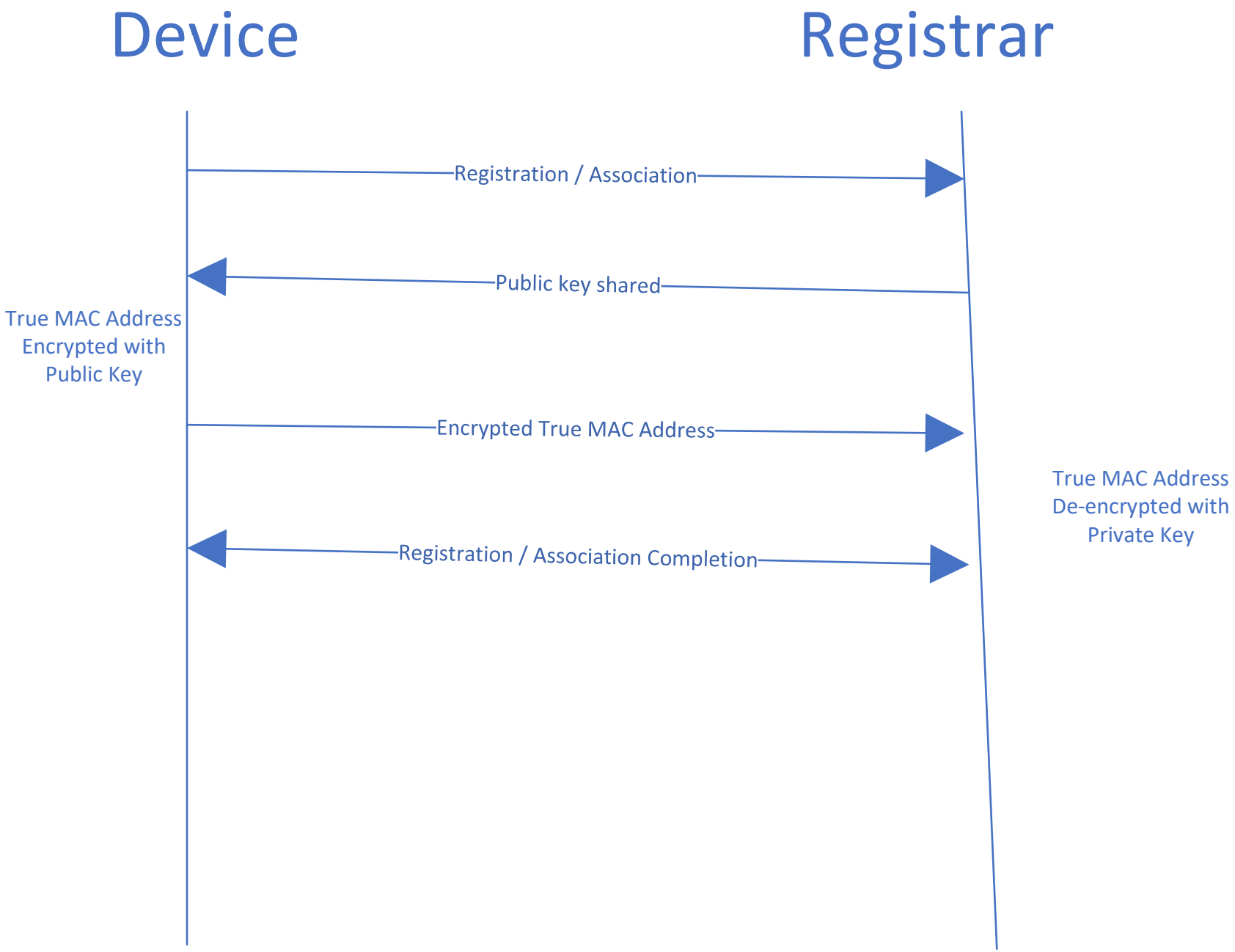
This invention is the outcome of the use of randomized MAC Address starting to be used within Wi-Fi. This move to use MAC Address randomization has trigger a lot of concern of how current systems that relay on the device's MAC Address for various functions/features.

In thinking about the issue and the solution this solution it occurred that it could be used for the DOCSIS CMs, thus the expansion from just association that is used in the Wi-Fi realm to include registration as well. Then the topic of the DHCP issue came to mind and this continued to how is could be applied to DHCP to prevent IP pool exhaustion

Abstract

A method of transferring and/or sharing a device's true Media Access Control (MAC) Address in a secure manner allowing the use of MAC Address randomization without impacting current services. The method can be used with the Dynamic Host Configuration Protocol (DHCP) function to allow the device's true MAC Address to be associated with a given Internet Protocol (IP) Address reducing the risk of IP Address pool exhaustion.


101
102
Interface
Randomized
MAC
105
PKI Keys
103
Encryption
104
True MAC
103
111
112
Interface
113
PKI Keys
114
De-encryption
115
Device True MAC


Device
Registrar
Registration / Association
Public key shared
True MAC Address Encrypted with Public Key
Encrypted True MAC Address
True MAC Address De-encrypted with Private Key
Registration / Association Completion