Fact Sheet

Cogito Group

Wi-Fi Security

What is Wi-Fi Security?

Wi-Fi is a key component of enterprise networking. It enables the use technologies that can reduce costs for business and provide great flexibility to a workforce as well as make them more productive. Bring Your Own Device (BYOD), hotdesking, mobile devices, and Internet of Things (IoT) initiatives have increased the need for secure access to wireless networks. While Wi-Fi enables better business outcomes, it can present a threat vector to malicious parties. It can be used to access internal networks without needing to be on the premises.

Wireless networks have traditionally been secured using password-based credentials, which carry risks of being lost or leaked, and are difficult to change when required. Certificate-based Wi-Fi authentication using 802.1X with EAP-TLS addresses these concerns by providing credentials on a per-device basis which are used to connect to Wi-Fi networks.

These credentials can be individually revoked when lost or stolen easily, and new credentials can be automatically provisioned to devices which require access using Mobile Device Management technologies, or standard Active Directory mechanisms. This allows an end user to be connected to a Wireless network seamlessly.

802.1x with Certificate Authentication

802.1X is an IEEE standard for secure access to local area networks which is widely supported by many network equipment vendors. The standard allows a variety of authentication mechanisms to be utilised including username and password, but the most robust mechanism that requires no user interaction is certificate-based authentication[1]. Certificates – which provide a strong assertion of identity – are issued to devices from a Public Key Infrastructure (PKI). A device can then use the certificate issued by the PKI to automatically authenticate to the Wi-Fi network without any user input. This certificate can be used for other purposes as well.

In addition to the device certificate – which proves identity of the device – a certificate is issued to the Wi-Fi authentication server, which proves the identity of the network itself. This reduces the risk of rogue Wi-Fi access points, referred to as "Evil Twins", often used to surreptitiously steal data by masquerading as a trusted Wi-Fi access point[2].

802.1X TLS Stages

At a high level, 802.1X using EAP-TLS has four main stages:

1. The device connects to the network, and is prompted to authenticate
2. The device presents a credential to the authentication server
3. The server presents a credential to the device

Both parties authenticate each other's credentials.

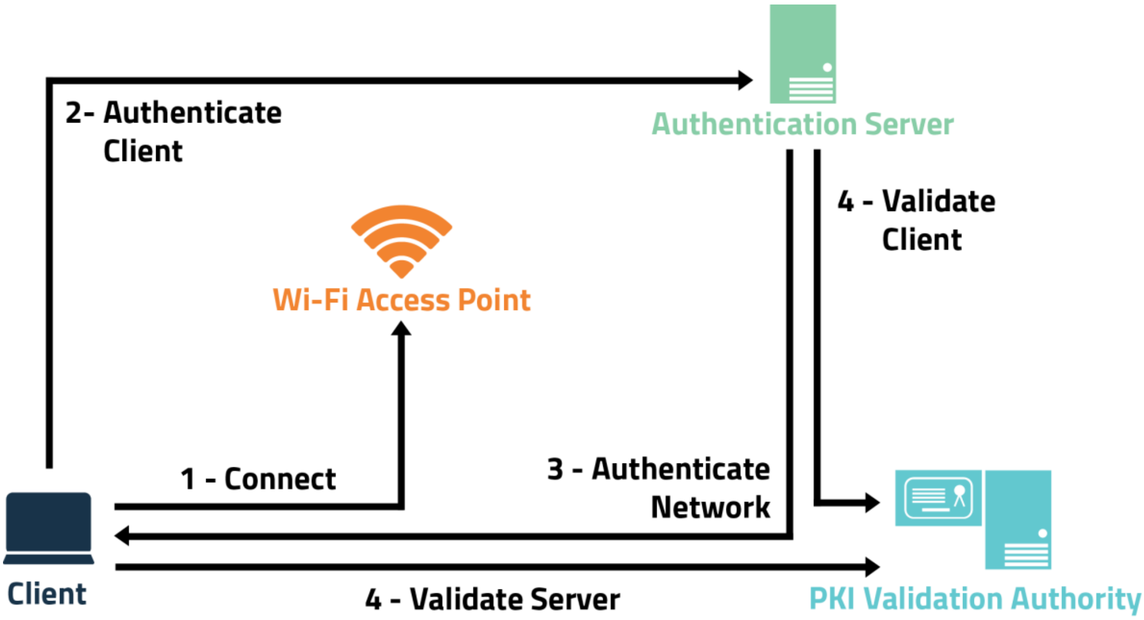

Figure 1 – 802.1X TLS Stages

Most modern devices will natively support the EAP-TLS workflow so long as a valid credential is available on the device. The authentication server present in Figure 1 can be an Active Directory domain controller or a managed service. 802.1X is a mature standard which is widely support and makes use of common, accessible protocols.

PKI with Cogito Group

Most modern equipment will support 802.1X using EAP-TLS, however the complexity in deployment often lies in the deployment and management of the PKI and distribution of certificates to devices. Cogito Group are PKI specialists, operating some of the most complex and secure Public Key Infrastructure environments in the world, including in countries such as New Zealand and Australia.

Running an effective Public Key Infrastructure requires specialist staff, equipment, and processes. Cogito Group can aid customers wishing to build their own PKI on-premises or in the cloud. Cogito Group additionally offers a managed PKI Service to ensure best practices are maintained while reducing an organisations capital and operational costs. In many cases this capability is provided as an onshore hosted cloud service in the Cogito Group Security Services infrastructure, or in a dedicated on-premise environment with on-site support.

Cogito Group can add value to PKI, with expertise in providing and supporting solutions ranging from secure Wi-Fi, remote access solutions, Physical Access Control Systems, and Data Loss Prevention – all utilising the same Public Key Infrastructure capability.

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated ICT company, specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.

[1] https://www.intel.com/content/www/us/en/support/articles/000006999/network-and-i-o/wireless-networking.html

[2] http://www.eweek.com/security/eap-tls-detailed-as-wifi-security-best-practice-at-sector