Securing Wireless LANs with Certificate Services

PHILIP HUYNH
University of Colorado at Colorado Springs

Abstract

Wireless Local Access Network (WLAN) is used popularly in almost everywhere from the home environment to the large organizations with hundreds of wireless clients. Although WLAN has many useful features, but the securing wireless network is always a top priority for analysts and network security firms to improve. The Institute of Electrical and Electronic Engineers (IEEE), along with other standards organizations, have been redefining and improving wireless security standard to enable WLANs to stand up to the hostile security environment. This research examines the Microsoft Securing WLANs solution which is based on IEEE 802.1X and requires a Remote Authentication Dial-In User Service (RADIUS) infrastructure and a Public Key Infrastructure (PKI). The solution uses a flexible design and is suited for the organizations of several hundreds to many thousands of wireless network users.

I. Introduction

Since the discovery of WLAN security weakness, leading network vendors, standards organizations, and analysts have focused a great deal of effort on finding remedies for these vulnerabilities. This has yielded a number of responses to the concerns over WLAN security. The principal alternatives are:

- Not to deploy WLAN technology
- Stay with 802.11 static WEP security
- Use a VPN to protect data on the WLAN
- Use IPsec to protect WLAN traffic
- Use 802.1X authentication and data encryption to protect the WLAN

These alternative strategies are listed in order of the least to the most satisfactory based on a combination of security, functionality, and usability, although this is somewhat subjective. In this paper, I would like to introduce the Microsoft favor alternative: using 802.1X authentication and WLAN encryption.

The rest of the paper is organized as follows. In session II, I discuss about the 802.1X EAP-TLS solution architecture. In session III, I discuss about the extending of the solution design. Session IV is about the re-evaluation of the design criteria. I conclude in session V.

II. The 802.1X EAP-TLS Solution Architecture

In this session, I will describe the solution architecture, and then a logical design is derived based on design criteria taken from an example company. The logical design is based on 802.1X WLAN network hardware, Remote Authentication Dial-In User Service (RADIUD) authentication, and a public key.

Understanding WLAN Security

Protecting a WLAN involves three major elements

- Authenticating the person (or device) connecting to the network.
- Authorizing the person or device to use the WLAN so that you control who has access to the network.
- Protecting the data transmitted on the network

Network Authentication and Authorization

- Static WEP security relies on a simple shared secret (password or key) for authenticating users and devices to the WLAN
- The 802.1X protocol is an IEEE standard for authenticating access to a network and, optionally, for managing keys used to protect traffic.
- The 802.1X protocol involves the network user, a network access (or gateway) device such as a wireless AP, and an authentication and authorization service in the form of a RADIUS sever. The RADIUS server performs the job of authenticating the users' credentials and authorizing the users' access to the WLAN.
- The 802.1X protocol relies on an IETF protocol called the Extensible Authentication Protocol (EAP) to carry out the authentication exchange between the client and the RADIUS server.
- EAP is a general protocol for authentication that supports multiple authentication methods, based on passwords, digital certificates, or other types of credential extensible.
- EAP-TLS is an IETF standard (RFC 2716) and is probably the most widely supported authentication method on both wireless client and RADIUS servers in use today. The EAP-TLS method uses public key certificates to authenticate both the wireless clients and the RADIUS servers by establishing an encrypted TLS session between them.

WLAN Data Protection

Authentication is one part of the solution. The other significant solution component is the protecting the data communication over the LAN.

- WEP data encryption is not secured enough for serious applications.
- The 802.1X solution allows to frequently changing the encryption keys. The EAP methods generate an encryption key that is unique to each client.
- WPA is an industry standard published by the Wi-Fi Alliance, a consortium of the leading Wi-Fi vendors. WPA includes two modes, one using 802.1X and RADIUS authentication, and another simpler scheme for SOHO environment using a pre-shared key (known as WPA PSK).

Conceptual Design

As we know, there are a number of serious security vulnerabilities inherent in wireless networking. At best, these weaknesses are only partially addressed by the use of Wired Equivalent Privacy (WEP) as specified in the IEEE 802.11 standard. The solution proposed in this guide addresses the problem of how to improve the security of wireless network communications. To do this, the ideal solution needs to have the following features:

- Robust wireless client authentication. This should include mutual authentication of the client, the wireless access point (AP) and the RADIUS server.
- An authorization process to determine who will be allowed to access the wireless network.
- Access control to only permit network access to authorized clients.
- Strong encryption of wireless network traffic
- Secure management of encryption keys.
- Resilience to denial of service (DoS) attacks.

The 802.1X protocol standard for network access control combined with a secure authentication method such as EAP-TLS fulfills some of these requirements.

A conceptual figure of the solution (802.1X EAP-TLS Authentication) is displayed in the following figured

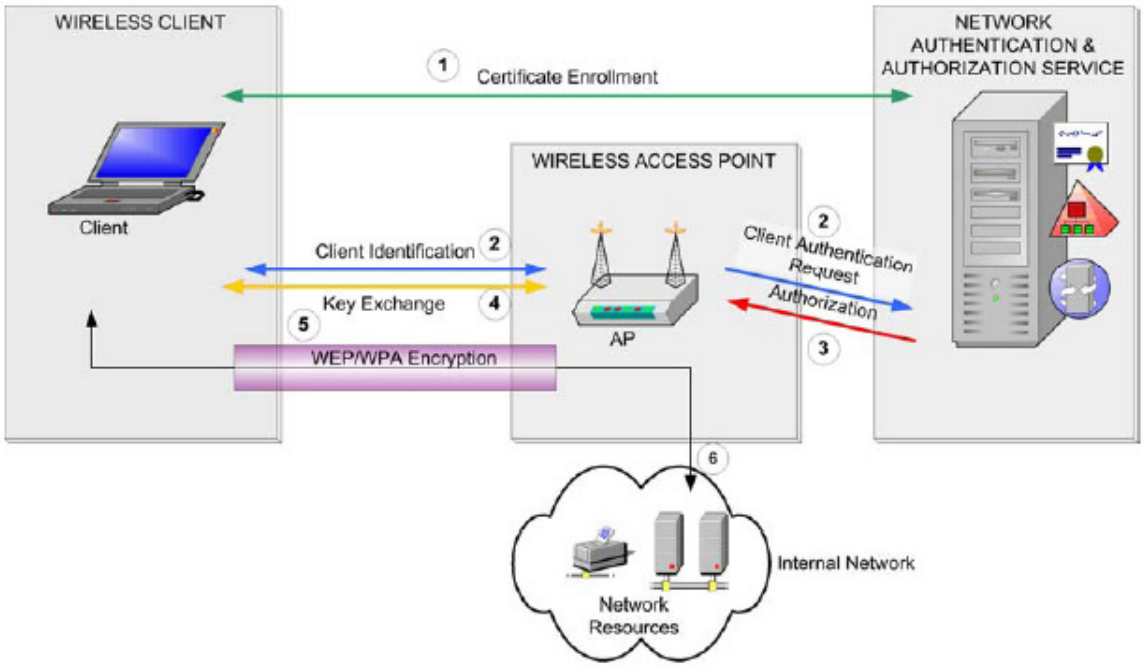

Figure 1
The solution concept based on 802.1X EAP-LTS authentication

The figure depicts four main components:

- The wireless client: a computer or device running application that requires access to network resources.
- The wireless AP: Network access point. AP implements access control functions to allow and deny access to the network and provides the capability to encrypt wireless traffic.
- The Authentication Service: This component stores and verifies the credentials of valid users and makes authorization decisions based on an access policy.
- The internal network: A secured area of networked services that the wireless client application needs to gain access.

Solution Design Criteria

Target Organization

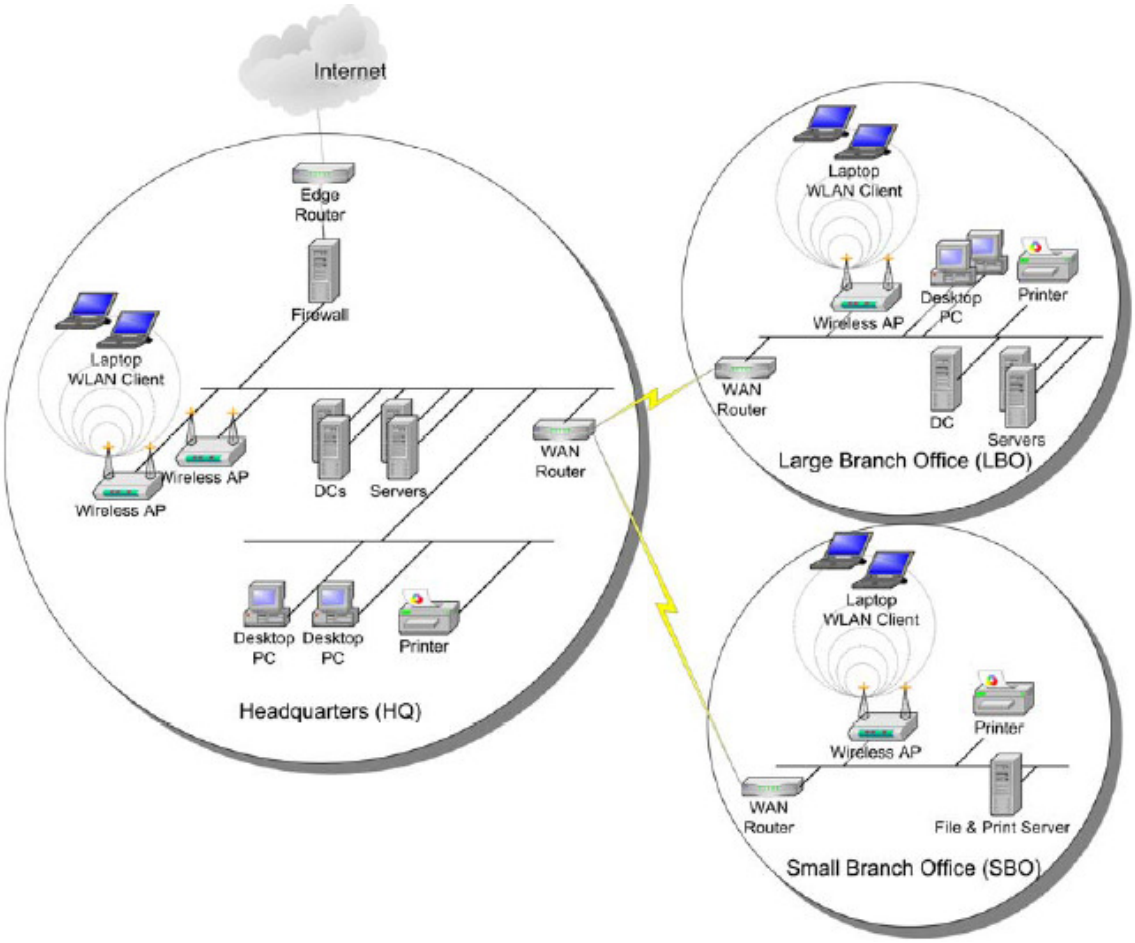

Figure 2
The schematic of the target organization's network and physical layout

Organization Requirements

There are some key requirements for the WLAN securing solution.

- Improve the security of WLAN to eliminate or substantially reduce the following threats:
  - Intruders eavesdropping on data transmissions across the WLAN
  - Intruders intercepting and modifying data transmissions on the WLAN
  - Intruders or other unauthorized users connecting to the WLAN and introducing viruses or other hostile code onto the internal network.
  - Network-level (rather than radio-level) DoS attacks.
  - Intruders making use of the corporate WLAN to gain Internet access.
- The security measures should not reduce the usability of the network and not lead to any significant increase in help desk calls.
- The design should be capable of supporting a broad variety of clients and devices.
- Availability 24/7 service
- Scalability should exist to cope with higher levels of use in the future possibly beyond 100 percent of the existing workforce.

- Reusability of components

Solution Design Criteria

From the requirements, the criteria can be derived to support the solution design.

- Security:
  - Robust authentication and authorization of wireless clients
  - Robust access control to limit access to authorized clients
  - High strength encryption of wireless network traffic
  - Secure management of encryption keys
  - Resilience to DoS attacks
- Scalability:
  - Basic design that scales up and down to include a broad range of organizations
- Min/Max users supported
  - 500 - 15,000+ WLAN users
  - 500 – 15,000+ certificate users
- Number of sites supported
  - Multiple large sites – with local authentication domain controllers and MS IAS.
  - Supported with resilience to WAN failure
  - Multiple small sites supported with no resilience to WAN failure
- Component reuse (use of existing infrastructure)
  - Use Active Directory, network services, and Microsoft Windows XP clients
- Component reuse (usability by future applications)
  - Support for other network access applications (VPN and 802.1X wired network access) by the authentication infrastructure.
  - Support wide variety of applications, for example VPN – by PKI.
- Availability
  - Resilience to single component or network link failure
- Extensibility
  - Support future capabilities and standards 802.11i, WPA, 802.11a for WLAN
  - Certificate infrastructure is extensible to support most common uses of public key certificates, i.e. secure e-mail, smart card logon, Web service Security
- Manageability
  - Integration into existing corporate management solutions
- IT organization structure
  - Favors centralized IT
- Standard conformance
  - Adherence to current relevant standards and a clear migration path to future relevant standards.

Solution Logical Design

Conceptual Design Review

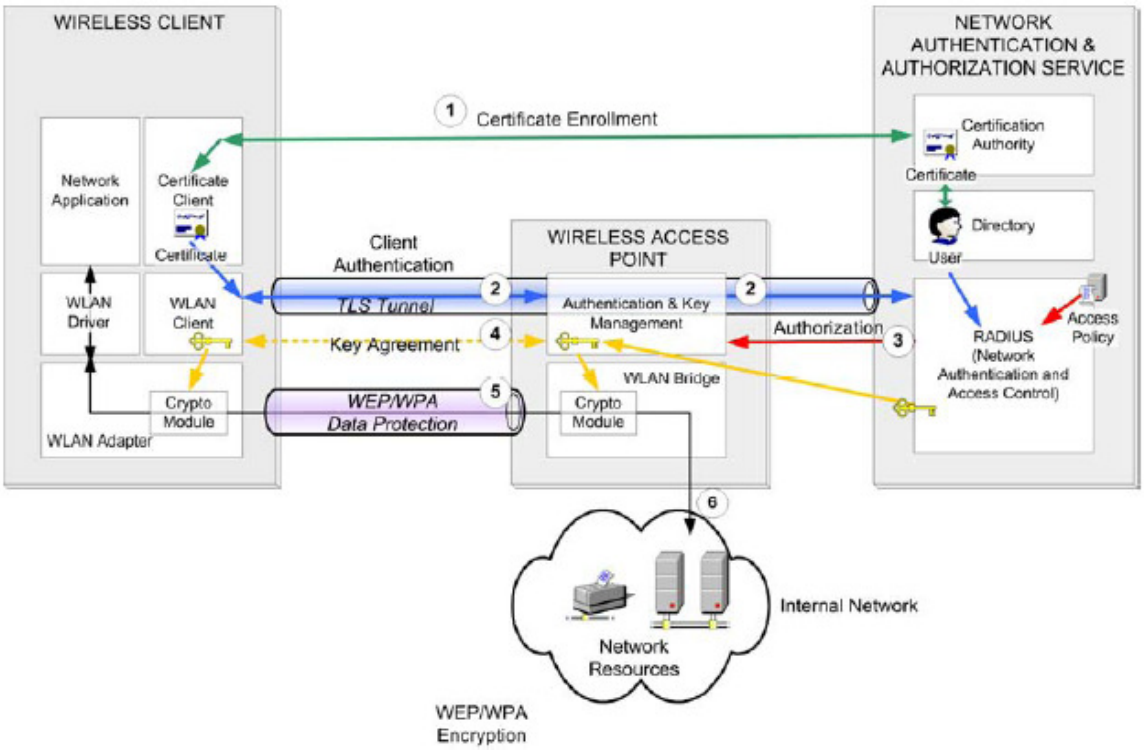

Figure 3
The conceptual view of the network access process

Logical Design

The IT services in the design are grouped into the following categories:

- WLAN components – Wireless clients and Access Points (AP)
- RADIUS components
- PKI component – Certificates Authorities (CA)
- Infrastructure services component

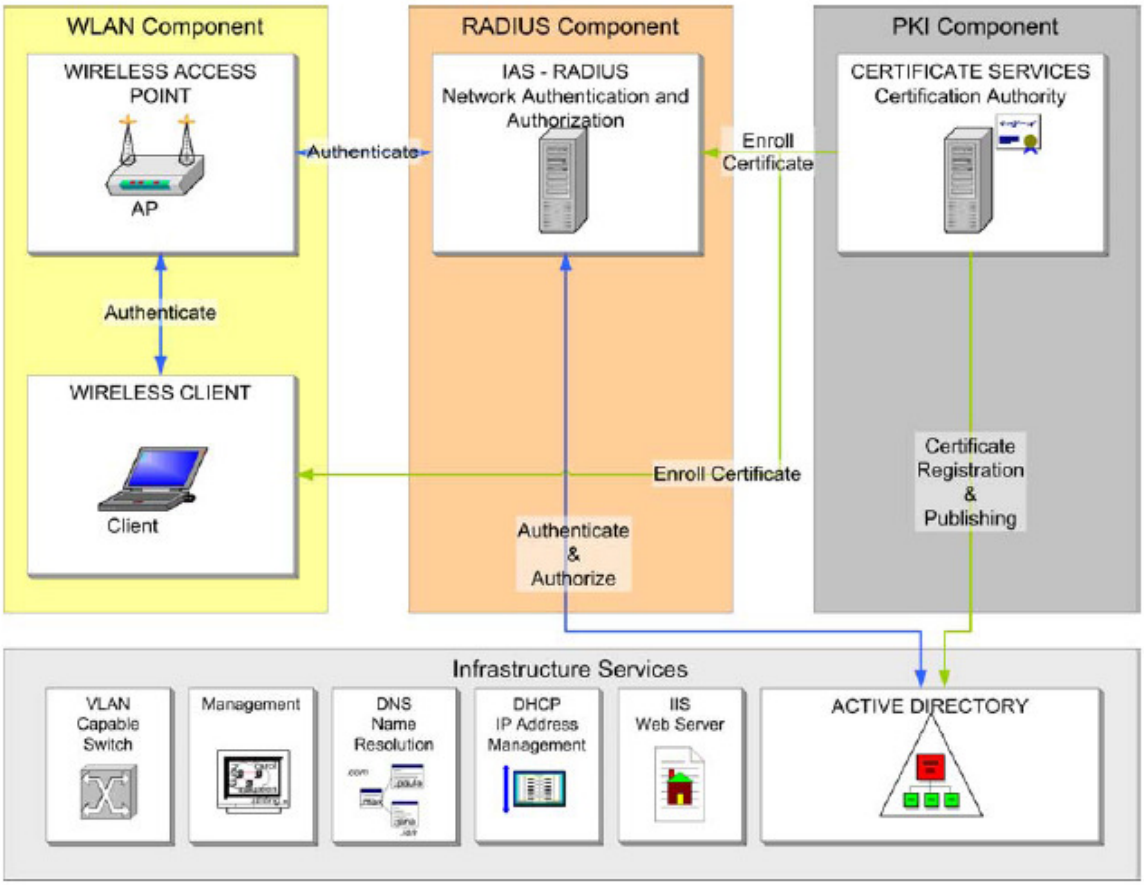

Figure 4
The logical design of the secure WLAN solution

Logical Physical Level

Headquarters

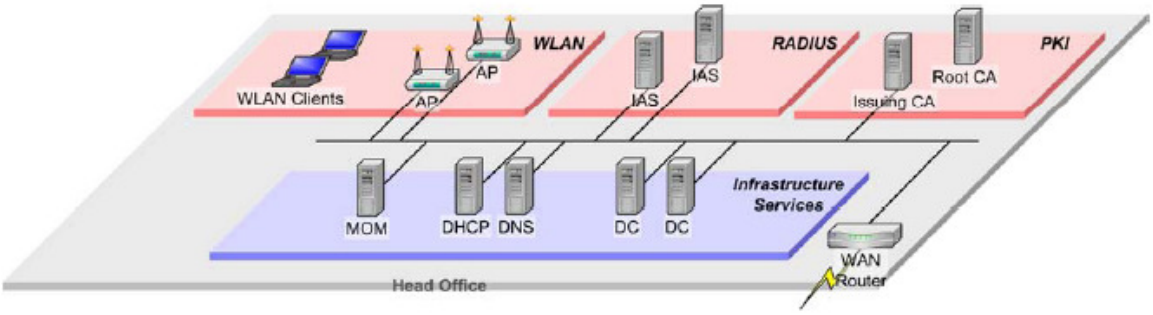

Figure 5
The head office server implementation

Large Branch/Regional Office

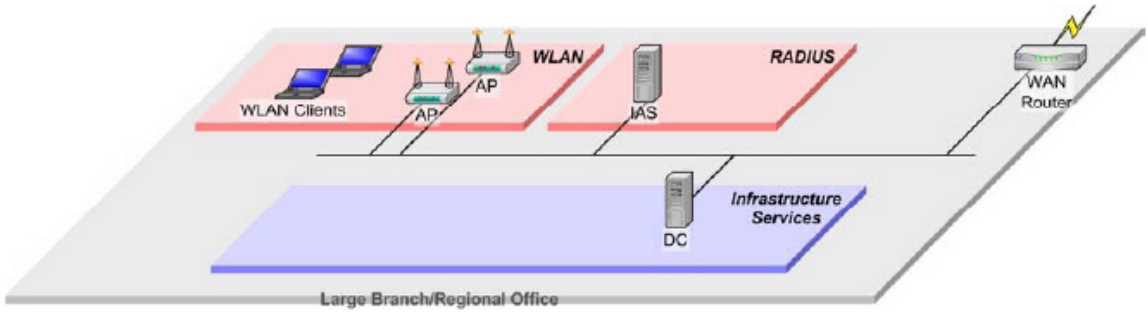

Figure 6
The physical layout for a large branch office

Small Branch Office

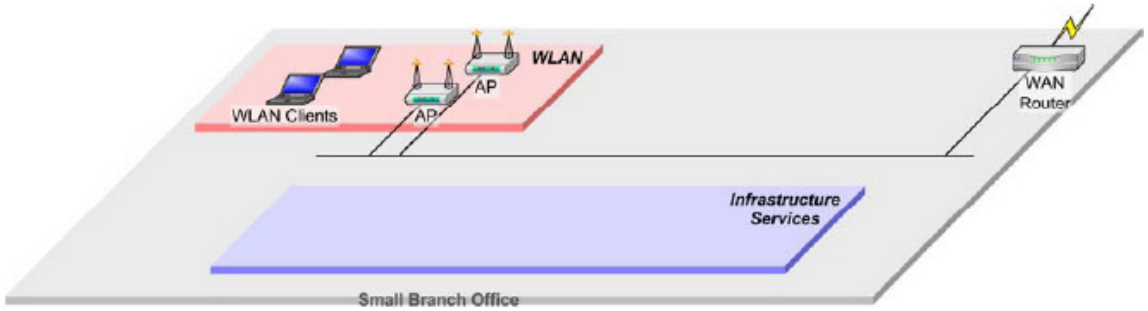

Figure 7
The physical layout for a small branch office

Scaling Strategy

One of the key design criteria is to ensure that the design can scale.

Large Organization

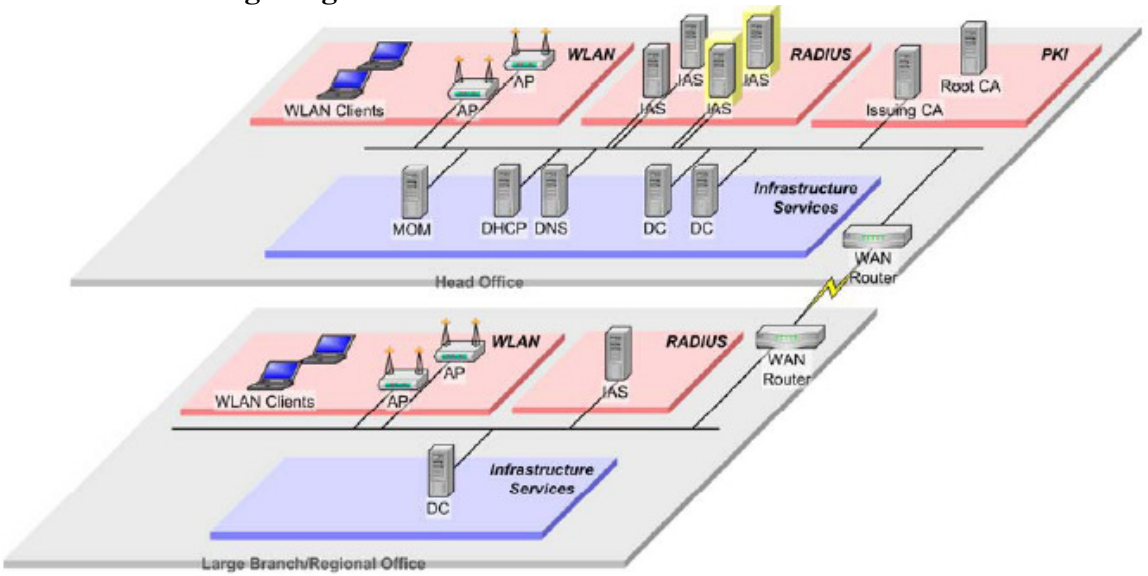

Figure 8
The solution scaled for a large organization

Small Organization

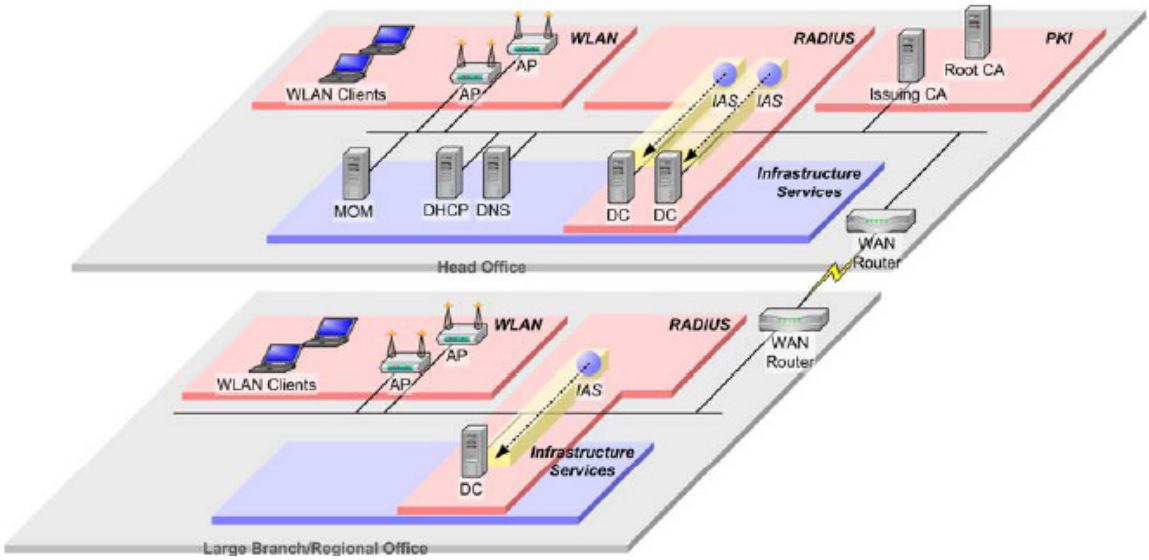

Figure 9
The solution scaled for a small organization

III. Extending the Design

Another key design criterion of the solution is the reusability of the components in future applications. The RADIUS component and the PKI component can be reused to provide authentication and other security services for a variety of applications.

Other Network Access Services

This solution's RADIUS design can provide authentication, authorization, and accounting services for other network access servers, such as 802.1X wired network authentication, and VPN and remote access authentication.

802.1X Wired Network Authentication

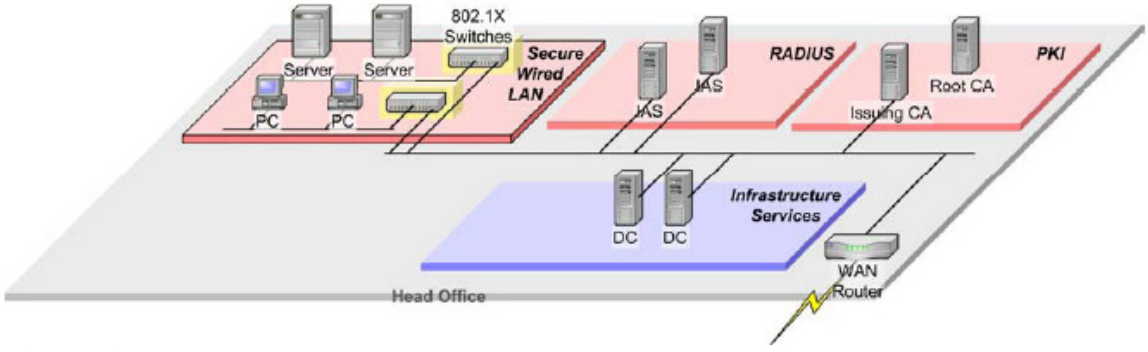

Figure 10
Using 802.1X wired authentication

VPN and Remote Dial-Up Authentication

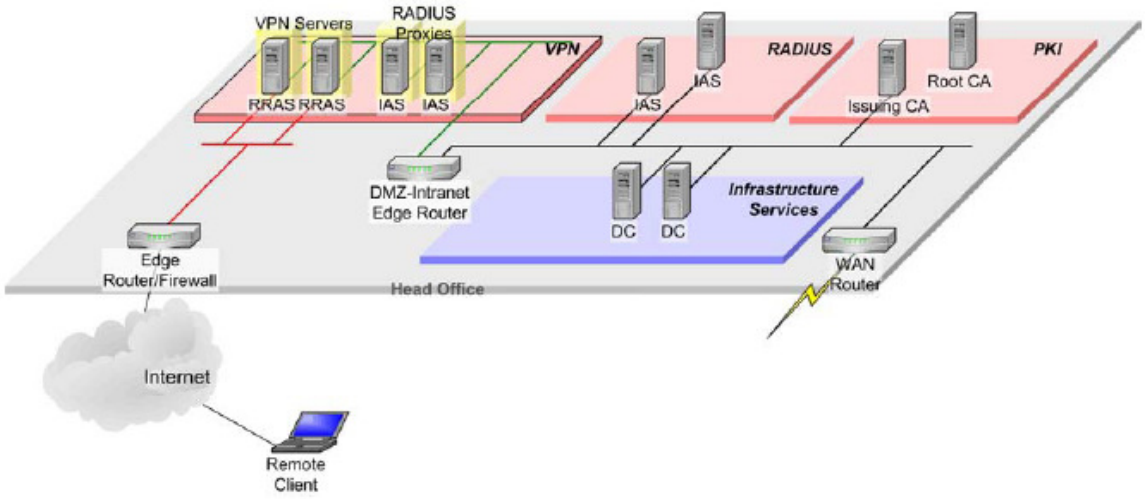

Figure 11
Extending the RADIUS component to support a VPN

PKI Applications

Because the solution criteria for reusability and extensibility are important, the PKI component was designed in the knowledge that it may be used in the future for a variety of different security applications.

The following figure illustrates a few of the applications that the PKI component could support in addition to the secure wireless application.

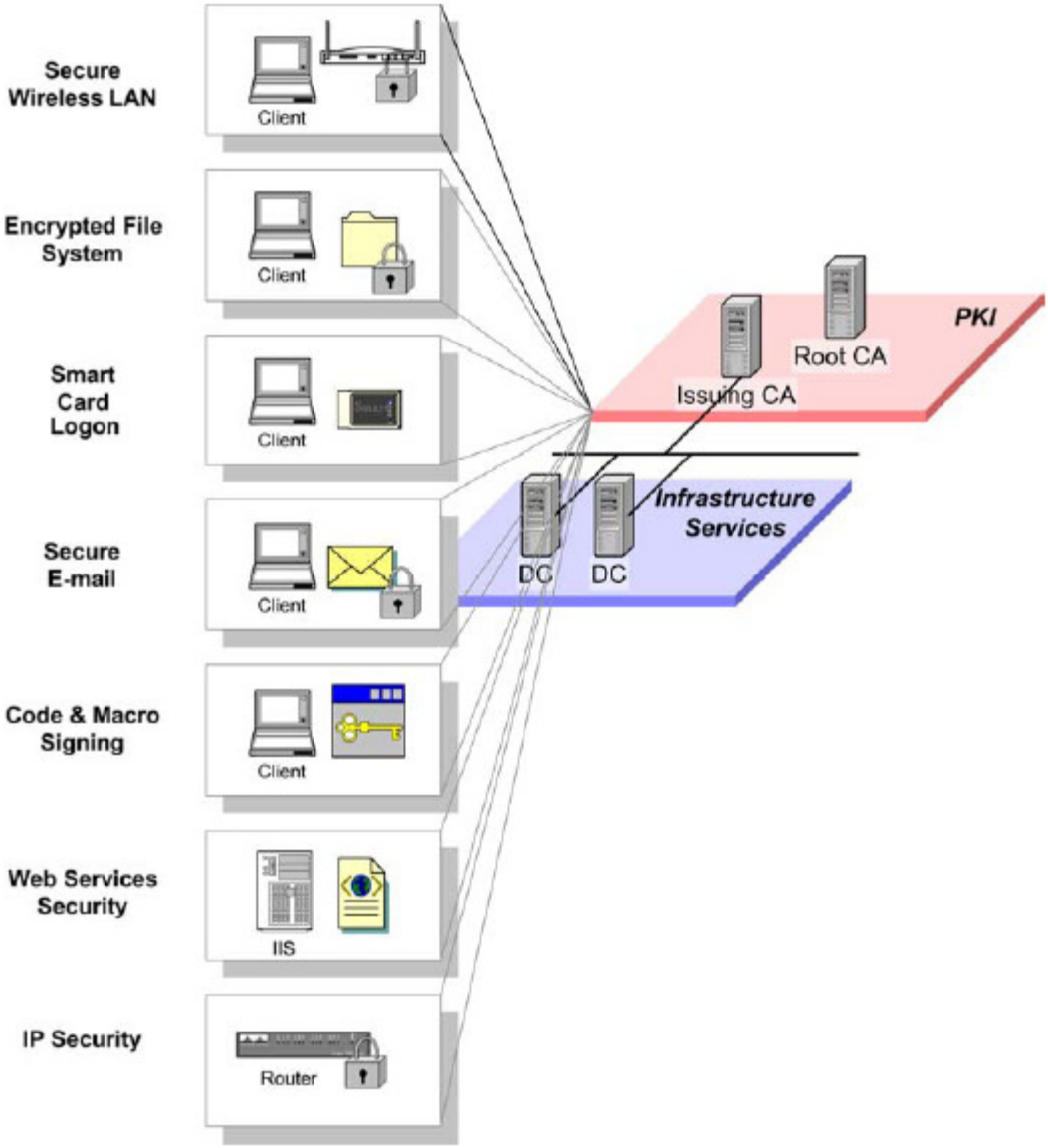

Figure 12
PKI application

IV. Design criteria Re-Evaluated

It is worth re-examining the list of design criteria for the solution to examine how well the proposed design now meets the goals set earlier.

- Security - The solution design includes robust authentication, authorization, and access control. Strong (128 bit) encryption is a function of the network hardware and is supported on most currently available devices.
- Scalability – The basic design accommodates a wide range of organizations in a cost-effective manner from a few hundred to many thousands of users.
- Component reuses (use of existing infrastructure) – The design uses Active Directory and many existing network service, such as DHCP and DNS.

- Component reuses by future applications – The RADIUS design, implemented using IAS, can be used by or easily extended to support other network access applications (such as VPN, 802.1X wired network access). The PKI is also capable of supporting simple public key applications.
- Availability – The solution design is resilient to a single component or network link failure at the head office and for all outlying offices where a RADIUS server can be deployed. Small offices without a local RADIUS server are vulnerable to a WAN failure.
- Standards compliance – The solution adhere to current official and industry standard. This is most relevant in the area of WLAN security where the solution is based on the 802.1X protocol, EAP-TLS, 128-bit dynamic or WPA.

V. Conclusion

In this paper I have introduced the design of 820.1X EAP-TLS solution from Microsoft. The design is for a sample target organization network. The criteria have been given to support the design. Then the proposed design was re-evaluated to the criteria to make sure it met the desired goals. The IEEE 802.1X EAP-TLS solution has many key benefits, such as, high security, stronger encryption, transparent, user and computer authentication, low cost, and high performance. The design can be scaled to meet the needs of organizations if different size. The design can be extended or used as the basic to build other network access solutions that include VPN and wired network access control, and the PKI can be used in different applications such as Web Services Security, Secure E-mail, and IP Security.

References

[1] IEEE Std 802.1X – 2001 (2001) IEEE Standard for Local an Metropolitan Area Network – Port based Network Access Control, The Institute of Electrical and Electronics Engineers, Inc.

[2] The Microsoft Solution for Security (MSS) Group (2004) Securing Wireless LANs with Certificate Service Release 1.6, Microsoft Corporation.

[3] Nirmala Lubusu (2003) Implementation and Performance Analysis of the Protected Extensible Authentication Protocol, Department of Computer Science, UCCS.