



Secure Global Roaming for 802.11 WLANs

Technical Whitepaper
Copyright 2002 by VeriSign, Inc.

VeriSign, Inc.
487 East Middlefield Road
Mountain View, CA 94043
USA
<http://www.verisign.com>

Secure Global Roaming 802.11 Wireless Local Area Networks

Providing Trusted Infrastructure for Secure Global Roaming on WLANs

Introduction

After several years of standards development, the adoption of *Wireless Local Area Networks* (WLAN)s is now growing rapidly. Using laptops and other devices equipped with wireless networking cards that conform to the IEEE 802.11b (Wi-Fi™) standard [802.11], ever more corporations are connecting employees to their business LANs over wireless links, achieving the benefit of increased mobility without sacrificing functionality or bandwidth. Frost & Sullivan has forecasted that Wi-Fi manufacturer's revenue will reach \$884 million by 2002. More than 12 million Wi-Fi compatible products are anticipated to be installed by the end of 2001.

But as engineers have been working nonstop to enable wireless networking products, network administrators and corporate officers have been struggling to come to grips with the security & authentication issues implied by a world in which wireless laptops can easily gain access to sensitive corporate resources. These security threats are real. What is worse, the original implementation of the 802.11 Media Access Layer security scheme called WEP (for *Wired Equivalent Privacy*) has been found to have serious cryptographic weaknesses, regardless of its underlying cryptographic key size (see References at the end of this paper). However, appropriate security solutions for wireless LANs are already in place, and the 802.11 community is moving forward quickly with plans to both fix existing problems and make the process of securing wireless networks easier for everyone concerned.

This VeriSign Technical WhitePaper provides technical and educational background on 802.11 based wireless networking and discusses available solutions to the associated security issues in the context of secure roaming for WLAN clients.

Technical Setting

In 1997, the Institute of Electrical and Electronics Engineers (IEEE) ratified the 802.11 specification as a standard for wireless local area networks (WLAN)s. The initial version of 802.11 provided for 1 Mbps and 2 Mbps data rates and underlying radio signaling methods.

In 1999, the IEEE ratified the 802.11b standard for data transmission rates up to 11Mbps. With the introduction of 802.11b, wireless performance became comparable to typical wired networks. Explosive growth of 802.11b followed, and continues today.

Meanwhile, industry bodies such as the Wireless Ethernet Compatibility Alliance have formed to certify interoperability of Wi-Fi™ (IEEE 802.11) products and to promote Wi-Fi™ as a global wireless LAN standard (<http://www.weca.net>). Today, over 80 vendors have received Wi-Fi certifications for a variety of devices, including wireless network cards and associated wireless access points.

Network Topologies supported by 802.11

The 802.11 standard defines two modes: an *infrastructure mode* and *ad hoc mode*. In *infrastructure mode*, the wireless network consists of at least one Access Point (AP) that is simultaneously connected both to wired network infrastructure and to a set of wireless end stations (STAs) (which are most frequently laptop computers) over radio links. Such a configuration is called a Basic Service Set (BSS). An *Extended Service Set (ESS)* is a set of two or more BSSs forming a single subnetwork.

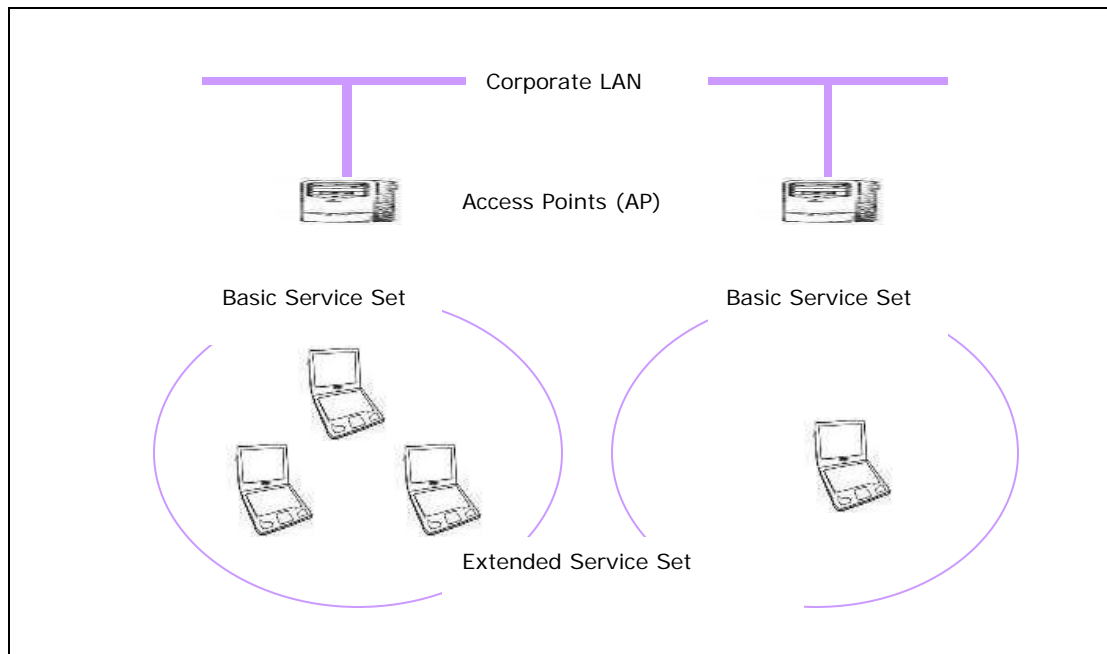


Figure 1: Infrastructure Mode for Wireless LANs

By contrast, an *ad hoc mode* 802.11 set-up is a completely wireless group of computers, each equipped with a wireless adapter, and connected directly to one another (without an AP) via radio signals as an independent wireless LAN. See Figure 2.

Since most corporate WLANs are intended to enable access to a wired LAN for services (for example, corporate databases, file servers, printers, or Internet access) they most frequently operate in infrastructure mode. We will not speak of ad hoc mode again in this paper, and will simply identify an infrastructure mode 802.11b set up as a *wireless LAN*.

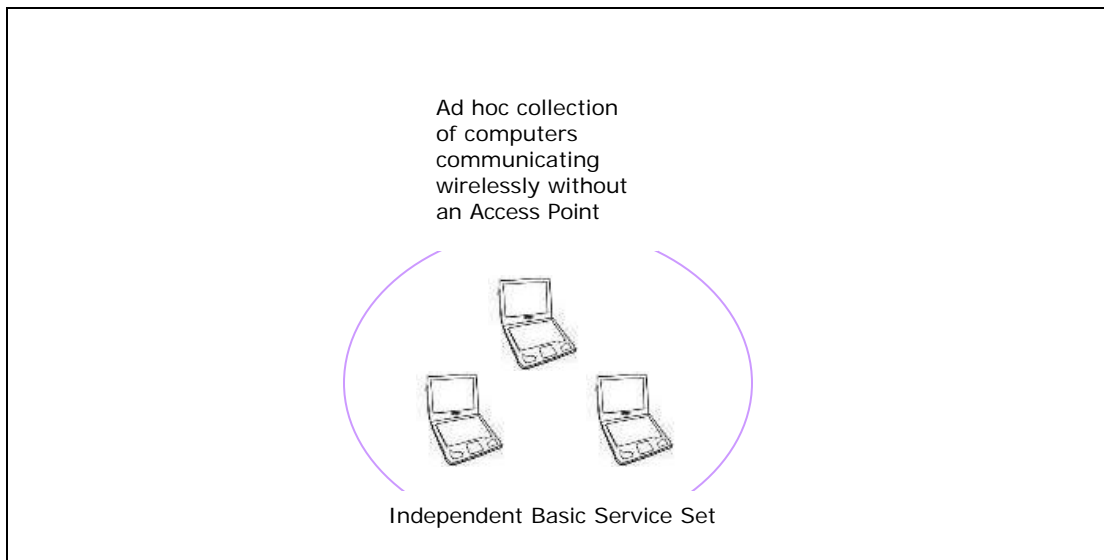


Figure 2: The ad hoc WLAN

802.11 and the 802.1X Framework

Authentication of users and/or devices within a WLAN network is crucial for the overall security of the WLAN environment. Authentication presumes identification, and both represent the foundation for controlling access to resources accessible through the WLAN connection. Furthermore, in the wireless space a connection to an Access Point (AP) itself represents a resource that is limited, as APs tend to have a maximum number of stations that it can cater to. Thus, authentication of a station to an AP is important from the perspective of resource protection and the prevention of theft-of-service.

The 802.1X standard defines an architectural framework for WLAN security within which authentication between communicating entities takes place. The 802.1X Framework [802.1X] recognizes three main entities involved in the establishment of an authentication session that results in the agreement of a common key used between a station and the AP. These are the Supplicant, the Authenticator and the Authentication Server. The 802.1X Framework uses the *Extensible Authentication Protocol* (EAP) [RFC2284] over LANs (or in this case, WLANs), in which certain types can be introduced into EAP. One suitable extension in the context of 802.1X authentication is that of EAP-TLS [RFC2716].

In general, EAP provides a standard mechanism for support of additional authentication methods within PPP [RFC1661]. This includes support for a number of authentication schemes (e.g. smart cards, Kerberos, Public Key, One Time Passwords, etc.). Since mutual authentication is important for open WLAN environments, where any previously unknown station can

connect to an Access Point, it is desirable that authentication is conducted in both directions. That is, mutual authentication – and not just server-to-client authentication – is desirable in many environments, including WLANs. EAP-TLS [RFC2716] takes the advantages of the mature TLS of the TLS protocol [RFC2246] within a PPP context. These include protected cipher suite negotiations, mutual authentication and key management in general.

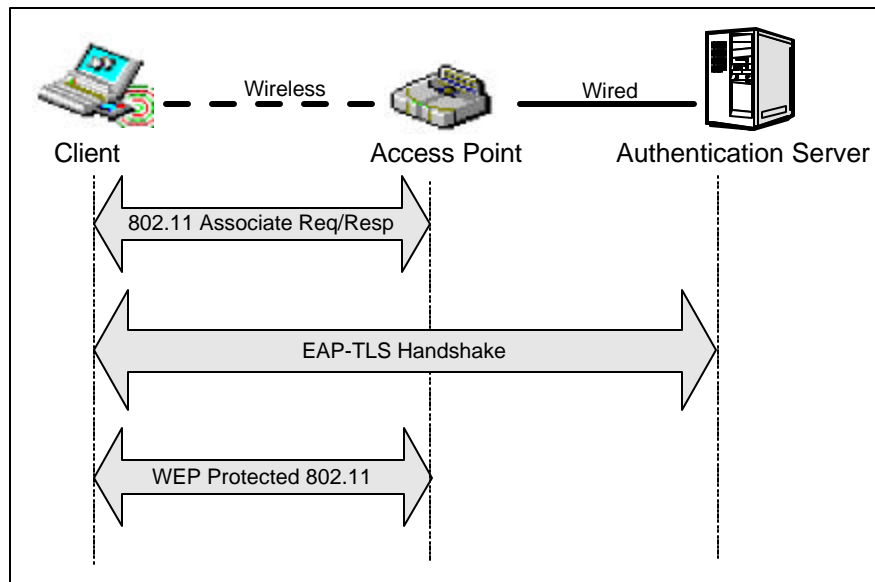


Figure 3: Basic EAP-TLS Interaction

802.1X, EAP-TLS and Certificates

The 802.1X Framework for key management allows the use of the TLS handshake in the context of EAP as a transport, with the final aim of achieving key agreement between the Station (Client or laptop) with an Authentication Server (AS), which then delivers the shared key to the Access Point (AP).

A conversation in EAP-TLS consists initially of a EAP negotiation between the authenticator (AP) and the Station. The AP sends an EAP-Request/Identity to the Station, who will respond with an EAP-Response/Identity packet containing the station's userID. At this point, the AP passes the EAP packet from the Station through to the Authentication Server residing behind the AP. At this stage, the AP behave as a pass-through device since the security conversation occurs between the Station/Client with the Authentication Server (AS).

When the Authentication Server (AS) receives the identity of the Station, it sends back a EAP-TLS/Start packet, which signifies the start of the TLS

handshake encapsulated using EAP. The station, acting as the client, replies by sending an EAP-Response packet, where the data field encapsulates one or more TLS records containing the *client_hello* handshake message.

The Authentication Server in-turn replies with a EAP-Request packet whose data field encapsulates one or more TLS records, including a *server_hello* handshake message. Additional parameters include the server's TLS certificate, *server_key_exchange* data, certificate request (from the client), cipher suites, and others.

The *server_key_exchange* parameters represents the server's contribution to the establishment of a master key between the authentication server and the station/client. Thus, if in fact the establishment of a master key is intended (as it is within 802.1X), the client must respond with a EAP-Request message that contains, among others, its contribution (*client_key_exchange*).

The certificate request from the AS signals the requirement from the AS that the client/station authenticate itself using a public key certificate.

Global WLAN Roaming

The primary reason WLANs were developed was to allow wire-free connections between a client and an Access Point, as a basis for further access to resources and services on the Internet.

The next step in this process is *wireless roaming*, in which a client can move across multiple Access Points in one domain, and across multiple Access Points in differing domains. Currently, the most prevalent model for *wired roaming* consists of a dial-up connection from a client (laptop) through a (dial-up) ISP, to a Home Domain (e.g. corporate network). This model presumes the prior existence of a business relationship between the client (or its corporation) and one Internet Service Provider (ISP).

The business case for WLAN wireless roaming is self-evident: consumers with the laptops (Stations/Clients) are willing to pay for connections to any Access Point anywhere on the globe provided by Wireless ISPs (WISP), and be able to access their Home Domains and access other services on the open Internet. This is true even today in the case of dial-up services. The provision of an *automatic detection* capability for clients seeking connectivity and providing *simple connectivity* and login to the corporate network, provides the Wireless ISP with various benefits, including revenue from increased sales, increased enterprise customer base, and reduction in operating costs through improved account management, billing and effective use of the WISP's infrastructure.

Given the increasing mobility of the workforce, providing *secure* wireless roaming is an important challenge today. Furthermore, the necessity of

maintaining a business relationship with only *one* WISP holds true, despite the fact that the connection from the roaming client to the corporate network may traverse multiple domains and ISPs.

Digital Certificates: Cornerstone of Global Roaming

From the perspective of Wireless ISPs (WISP), providing access to roaming users to the Internet through the WISP's network is equivalent to providing access to the WISP's resources. To that extent, it is in the interest of a WISP to provide services to legitimate users only, as bogus users represents loss of revenue to the WISP and perhaps a degradation of service level to other legitimate users.

Digital certificates represents the strongest method for a user to prove his or her credentials to a Wireless ISP. Furthermore, the same certificate can be used for subsequent authentications and authorizations, such as when a user wishes to connect to a home corporate network. Thus, digital certificates in a WLAN environment becomes a single unified means to satisfy multiple requirements:

- *802.1X/802.11 authentication:*
certificates provides the strongest method for a WISP to authenticate a user and to verify the relationship between the WISP and the certificate's issuing organization (e.g. corporation), without the WISP necessarily having prior arrangements with the organization.
- *Pay-Per-Use:*
Having a digital certificate, therefore, allows the WISP to provide a pay-per-use service model, whereby the user (or the user's organization) can be charged for connecting through the WISP either to the open Internet or to the user's home corporation. The user's digital certificate is thus additionally used to provide irrefutable proof of transaction pertaining to the user's use of the WISP's services.
- *Logging, accounting & billing:*
Wireless ISPs can use certificates as the basis for logging connections around the globe, accounting of resource usages by a given customer or pay-per-use user, and finally for billing. The digital certificate can contain additional information regarding certificate's issuing organization (e.g. corporation) for billing purposes.
- *Inter-ISP connections:*
Global roaming presumes inter-ISP relationships pre-existing before a user can connect through, from a remote WISP or ISP in a foreign

country. A user's certificate can be forwarded by intermediary (transit) ISPs to request services from other ISPs, thereby at each hop allowing an ISP to verify the certificate and to arrange for billing according to that certificate.

- *Virtual Private Networks:* An increasing number of corporations are using software based VPNs for their mobile workforce based on certificates. A traveling employee can connect to the corporate's VPN gateway by establishing a secure IPsec tunnel whose encryption key is negotiated using the Internet Key Exchange (IKE) protocol using certificates.

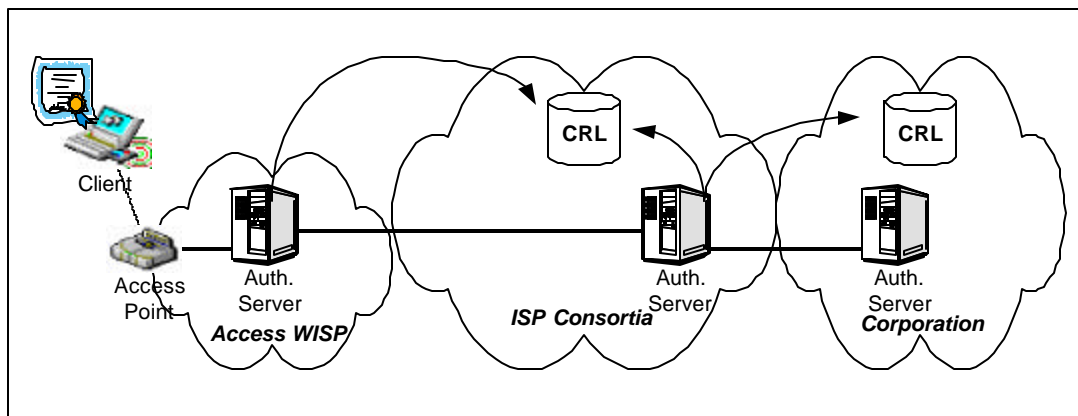


Figure 4: Certificate-Based Global WLAN Roaming

Certificate-based Roaming

There are three (3) general models of roaming that are applicable to WLAN global roaming. In the first model, a relationship among Wireless ISPs (WISP) is assumed to exist, where WISPs enter into contractual agreements with other ISPs to allow customers to access one another's access points. In this model, each WISP would need to maintain a list of originating domains, allowable users and even some kind of routing table. In general, this model does not scale as a WISP/ISP would need to enter into too many bilateral agreements with another WISP/ISP.

In the second model, a collection of WISPs and ISPs gets together in a consortia that acts as a final clearinghouse that also stores the routing table, list of member domains and possibly a list of customers. Once set up, such a body can easily add new member ISPs or WISPs that are willing to participate in the pricing and billing structure imposed by the organization.

These two models represent the traditional model for (wired) ISPs, extended for WISPs. As such, it carries-over much of the inherent operation difficulties left behind by legacy authentication/authorization systems. Furthermore, it

presumes that business relationships exist between the concerned ISPs, in order to manage and pass billing information to each other.

In the third model, certificates are used as the centerpiece for access to the Internet. Here, each WISP can act as a proxy to authenticate a user that presents a certificate, wishing to obtain connectivity. The WISP can deploy the 802.1X framework with EAP-TLS, and use Authentication Servers (ASs) belonging to its own organization or ASs belonging to an external organization. The WISP can then verify the *Certificate Revocation List* (CRL) issued by the Certificate Authority (CA) issuing that certificate (e.g. corporate's CRL via the *Online Certificate Status Protocol* (OCSP) [RFC2560]).

In this third model, a WISP or an ISP may even issue its own certificates, or rely on the ISP consortium to be the root CA that issues certificates for the WLAN roaming certificates. Any transit ISP or WISP can verify the certificate and check its status. Figure 4 illustrates this concept in the context of a consortium of WISPs/ISPs, where the consortium becomes a CA and where a common CRL is shared with the member-corporations. Other CA hierarchies and CRL distribution models are also possible.

VeriSign Certificate-based Global Roaming: a Roadmap

VeriSign leadership in Authentication Services, Naming Services and Transactions Services offers all parties within the WLAN market a consistent and all-encompassing set of functionalities that satisfy the need for a truly global, secure and trusted infrastructure for WLAN roaming (see Figure 5):

- **Name Services:** The DNS and naming infrastructure is crucial for IP mobility, as roaming clients will need to be assigned temporary foreign addresses to which traffic destined for its home address is re-routed. This is true in the WLAN environment, both in the current IPv4 internetworks and in the evolving IPv6 internetworks, as WLAN clients are in essence Mobile IP clients.
- **Authentication Services:** Certificate-based roaming represents the most effective and efficient method for truly global WLAN roaming. VeriSign worldwide presence in thirteen (13) physical locations around the globe provides a secure, timely and reliable infrastructure for authentication services in any WLAN environment. In Figure 5, the WLAN Authentication Servers (AS) in all domains, from the Access WISP, the transit ISPs to the Corporate network have the ability to utilize VeriSign's global Authentication Services to perform a variety of security-related functions, including certificate enrollment, certificate validation, certificate revocation and renewal in real-time, thereby providing roaming clients and WISPs/ISPs a 24x7 level of service that is necessary for today's mobile workforce. Clients having a single certificate may utilize the

certificate to also establish VPNs (e.g. via IPsec tunnels) all the way to their home corporate network.

- **Transaction Services:** VeriSign's transaction services allow WISPs, ISPs and other Service Providers to perform payment transactions pertaining to a service provided to a roaming client. Features, such as Digital Receipts, together with certificates aid Service Providers in accounting and billing to their customers, be they long-term customers or *pay-per-use* access customers.

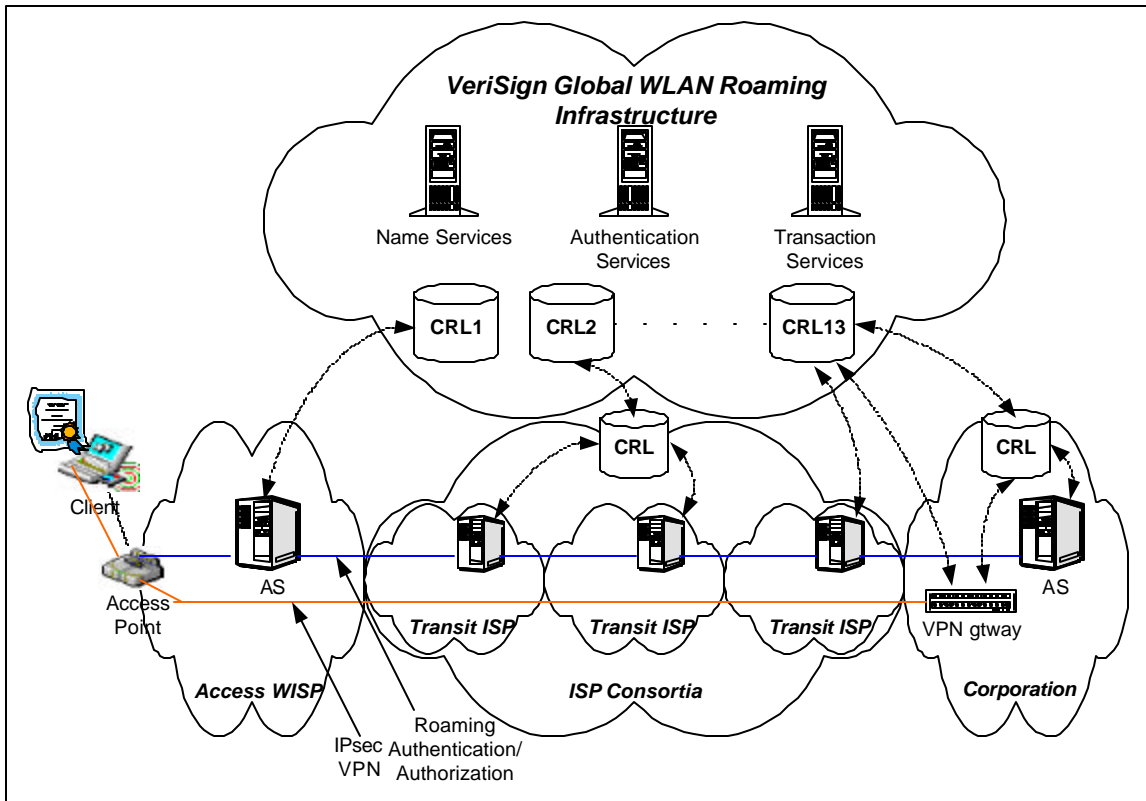


Figure 5: VeriSign Secure Global WLAN Roaming Infrastructure

References

[802.11] ANSI/IEEE, Std. 802.11 *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE, 1999.

[802.1X] ANSI/IEEE, Std. 802.1X *Standard for Port Based Access Control*, IEEE, 2001 (draft D11).

[RFC1661] W. Simpson, Editor, *The Point-to-Point Protocol (PPP)*, RFC 1661, IETF, July 1994.

[RFC2284] L. Blunk and J. Vollbrecht, *PPP Extensible Authentication Protocol (EAP)*, RFC 2284, IETF, March 1998.

[RFC2246] T. Dierks and C. Allen, *The TLS Protocol Version 1.0*, RFC 2246, IETF, November 1998.

[RFC2560] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*, RFC 2560, IETF, June 1999.

[RFC2716] B. Aboba, D. Simon, *PPP EAP TLS Authentication Protocol*, RFC 2716, IETF, October 1999.