THE USE OF DIGITAL CERTIFICATES FOR AUTHENTICATION TO A WIRELESS LAN

TECHNICAL WHITE PAPER February 2005

Digital Certificates are a vital component of network security. By establishing the identity of people and electronic assets using a wired or wireless network, Digital Certificates authenticate that their holders—people, web sites, and network resources such as routers—are who or what they claim to be. Now they are playing an increasingly vital role in providing security and validation for wireless connections and securing wireless local area networks (WLANs).

EXECUTIVE SUMMARY

Digital Certificates play an important role in securing wireless local area networks (WLANs). Currently, the most popular methods to secure WLANs using Digital Certificates are EAP-TLS, EAP-TTLS and PEAP. A brief discussion of each method is included along with a more in-depth look at some deployment scenarios for EAP-TTLS and PEAP.

BACKGROUND

Digital Certificates are electronic files that work like an online passport, providing secure communications across vulnerable and un-trusted networks. (The perfect example of an un-trusted network is the Internet.) Digital Certificates authenticate that their holders—people, web sites, and network resources such as routers—are who or what they claim to be. They also protect data exchanged online from theft or tampering.

A basic Digital Certificate contains a public key and an individual's name. Common Certificates also include an expiration date, the name of the Certificate Authority (CA) that issued the Certificate, and a serial number. Most importantly, it contains the digital signature of the Certification Authority.

TECHNOLOGY OVERVIEW

Digital Certificates are issued by a trusted third party known as a Certification Authority — or CA. The CA validates the identity of a Certificate holder and signs the Certificate to confirm that it hasn't been forged or altered in any way. When a Certificate is digitally signed by a CA, the Certificate's owner can use it as an electronic passport to prove his or her identity by presenting it to Web sites, networks or individuals that require secure access. Embedded in the Certificate is identifying information such as the owner's name and e-mail address, the name of the CA, a serial number and any activation or expiration data for the Certificate. When a user's identity is verified by the CA, the Certificate uses the holder's public encryption key to protect this data.

Digital Certificates are produced, distributed and managed using a Public Key Infrastructure—or PKI. This infrastructure enables secure transactions between customers and banking or e-commerce websites—as well as security within an enterprise network and a small or medium sized business. PKI uses pairs of encryption keys, one public and one private. The keys are known as public/private pairs, or asymmetric pairs, and are usually distributed in the form of a Certificate generated by a trusted entity within the communication framework.

Today, Digital Certificates are the basis of most communication systems that require a high level of trust between the communicating parties, including:

- **Virtual Private Network (VPN) technologies.** VPNs provide secure point-to-point or point-to-multipoint connections across the Internet.

- **Secure Socket Layer (SSL) connections.** SSL is the standard for Internet browser and server authentication as well as secure data exchange on the Internet. All the leading servers and browsers are optimized to enable SSL encryption.

- **Extensible Authentication Protocol (EAP) negotiation schemes.** EAP provides secure access to wired and wireless LANs.

While Digital Certificates have a wide range of uses, they are typically implemented in two ways:

- **Client and Server Certificates** — These Certificates require a PKI where every client has its own Certificate. This can be initially expensive because it requires special software tools, training and education. In addition, creating and securely distributing Certificates to every client in an enterprise can significantly increase administration costs. Also, if a device is lost or stolen, all Certificates need to be reissued throughout the enterprise to maintain system integrity.

- **Server Only Certificates** — This approach requires a PKI to manage and distribute Certificates to those servers within an enterprise that perform authentication. Servers are typically more secure than client devices, which make the distribution and management of Certificates much easier and more cost effective. Using Server Certificates usually requires a Certificate Chain, where the Certificate Authority can be called upon to validate a Certificate on behalf of clients.

Client and Server Certificates are usually required in IPSec VPN connections and are also required for EAP-TLS for securing wireless LANs. Server Only Certificate systems include SSL connections for securing transactions over the Internet, and EAP-TTLS and PEAP for securing wireless LANs.

An Example of Server Only Certificates

Figure 1 illustrates Certificate exchange and validation in a typical transaction between a customer and an e-commerce site over the Internet. To enable a customer to securely transmit sensitive data such as credit card details, the identity of the server must first be verified. Then a secure tunnel is established for the data transmission using a Certificate Authority (CA).

The CA generates a Certificate for the e-commerce server to use for secure transactions with its customers. When a customer wants to make a purchase, the e-commerce server presents a Certificate to the customer that the customer then checks with the CA. This process is the basis of the Secure Socket Layer (SSL) security framework that protects almost all commerce and banking activity on the Internet today.

The greatest benefit of using a CA to validate a Certificate is that the customer's PC does not need to store a unique Certificate for every site on which it conducts business. Both EAP-TTLS and PEAP use a similar process to eliminate the need for individual client Certificates.

EAP-TLS, EAP-TTLS AND PEAP

Since strong authentication and encryption key management services were not previously provided by 802.11 standards, other techniques have been developed. A popular approach is to use one the various EAP types to run over the 802.1X port-based authentication framework, including EAP-TLS, EAP-TTLS and PEAP. Figure 2 illustrates the basic differences between the various EAP protocols.

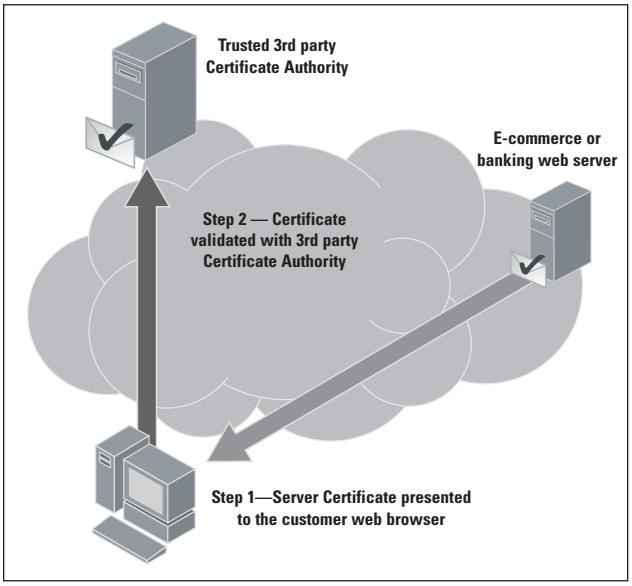

Figure 1 — Example of Digital Certificate used in SSL for securing transactions over the Internet

Figure 2: Comparison of EAP-TLS, EAP-TTLS and PEAP

	EAP-TLS	EAP-TTLS	PEAP
Server Certificate	Required	Required	Required
Client Certificate	Required	Optional	Optional
Certificate Validation	Through certificate chain or Online Certificate Status Protocol (OCSP)		
Effect of private key compromise	Re-issue all Certificates	Re-issue server Certificate only (unless using client Certificate for initial TLS negotiation)	
Protocol Structure	Establish TLS session and validate Certificate on both client and server	Two phases: (1) Establish TLS between client and TTLS server (2) Exchange attribute-value pairs between client and server	Two phases: (1) Establish TLS between client and PEAP server (2) Exchange attribute-value pairs between client and server
User Identity exchange protected	No	Yes	Yes
Fast Session Reconnect	No	Yes	Yes
Encryption Key Integration	WEP, TKIP or AES keys can be dynamically allocated using external protocol (e.g. RADIUS)		

EAP-TTLS OR PEAP DEPLOYMENT SCENARIOS

EAP-TTLS and PEAP use virtually the same mechanism for protecting the authentication between client and network. First, a Transport Layer Security (TLS) tunnel is built between the client and the TTLS/PEAP server. This tunnel protects the transmission of the client's credentials, such as username and password. Once the user's credentials are authenticated, a second TLS tunnel is built so that encryption key information can be sent to the client. After the client has the encryption key data, the TLS tunnels are torn down and all communication is secured using WEP, TKIP (WPA) or AES depending on the device capabilities.

Figure 3 shows how the initial TLS tunnel can be built when using EAP-TTLS or PEAP in an enterprise environment using an Active Directory structure within a Windows Server (2000/2003) Domain.

While the client device in this example is a PDA configured to connect to a specific domain, it can also be a laptop or a bar code scanning device. The local authentication server has a Certificate generated by the Certificate Authority (CA) from within the Windows Domain.

In order to prove the validity of the Certificate, the client checks with the CA. After the Certificate is validated, the device constructs a TLS tunnel and transmits the user's credentials. If the Certificate can't be validated, the TLS tunnel is not built and the authentication fails.

The local authentication server can then check the user's credentials and construct a second TLS tunnel to pass on the encryption key information to be used for data transmission. To provide enhanced security, this second TLS tunnel is built using specific information about the client and user. As a result, the first TLS tunnel is specific to the authenticating server, while the second TLS tunnel is specific to the particular session being initiated.

The example shown in Figure 4 is a smaller scale deployment where the local authenticating server is also its own CA. In this instance the authentication process is identical to the Windows Domain example except that all traffic is kept locally. This configuration may make sense in a small/medium-size business environment where there is no over-arching Windows Domain or where WAN links are intermittent dial-up connections.

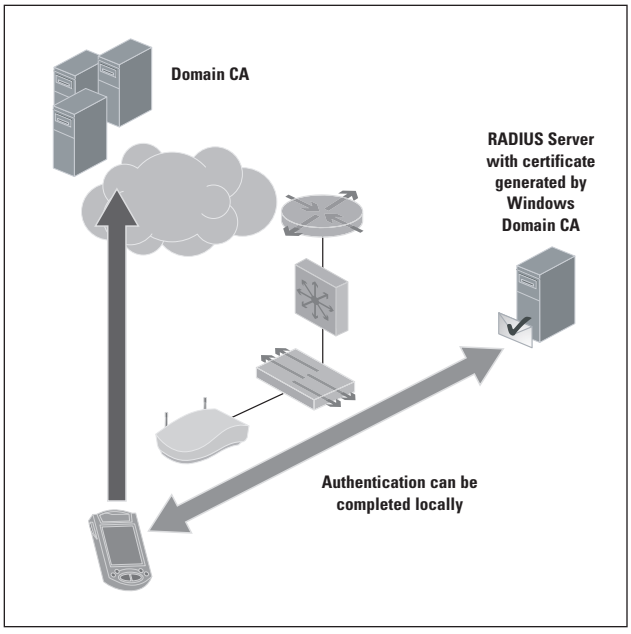

Figure 3 — Local Authentication Server Certificate is validated against the Windows Domain Certificate Authority

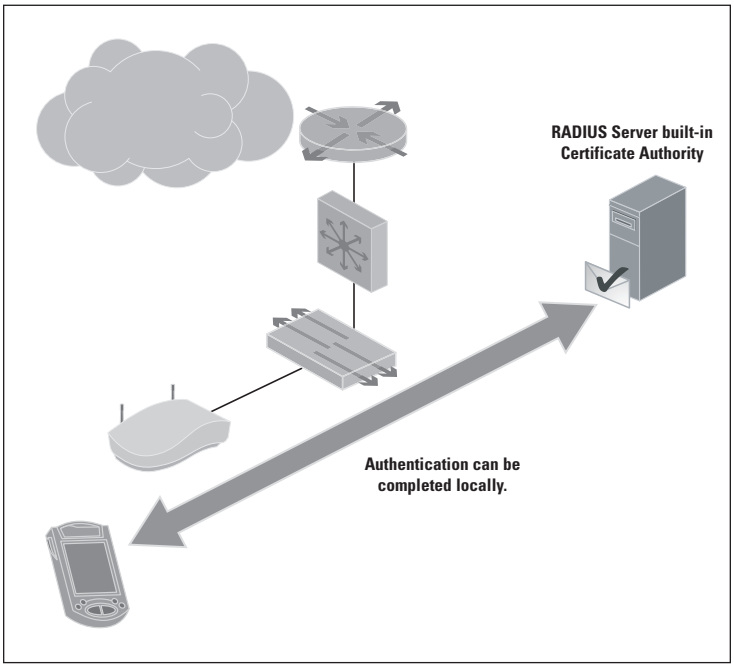

Figure 4 — Local Authentication is also the Certificate Authority

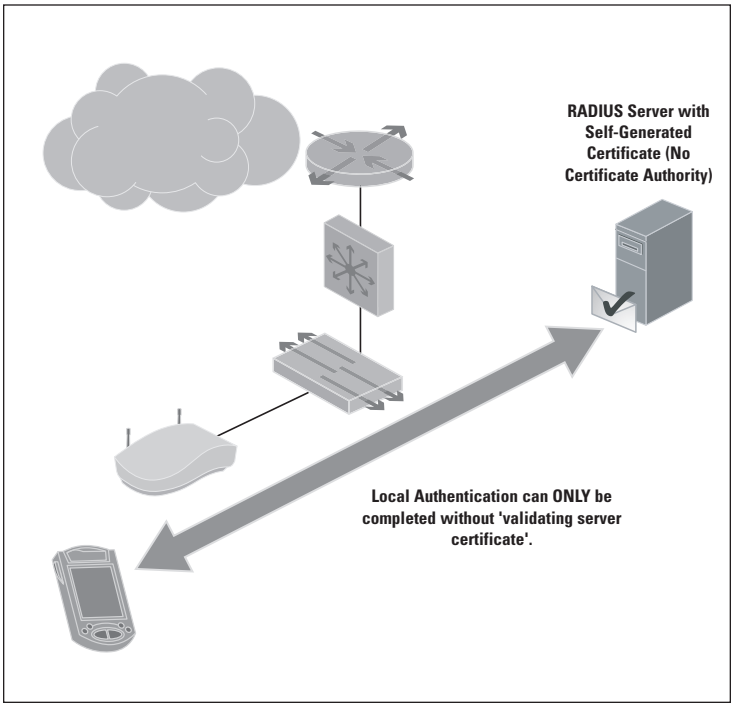

Figure 5 — Client uses OCSP to check that the server certificate hasn't expired

In this last scenario, shown in Figure 5, there is no CA. This may be because of cost or the setup is a proof-of-concept pilot. The authentication process can only be completed if the client does not try to prove that the server Certificate is valid, which would require reference to a CA. Using an Online Certificate Status Protocol (OCSP), the client looks at the Certificate to ensure that it's not out of date and then simply accepts that it is valid.

Using EAP-TTLS or PEAP in this configuration only provides "one-way" authentication, since only the server checks the validity of the client. In the previous configurations, the client can prove the validity of the server to which it is authenticating, which results in a superior level of system security.

BENEFITS

Securing network traffic over a WLAN using Digital Certificates can help enterprises protect valuable information, while allowing users the freedom and mobility of wireless communications. Users can logon securely to network services and authenticate, encrypt, sign and decrypt electronic transactions with confidence.

Protecting sensitive information with a Digital Certificate is not limited to online transactions or web site forms. Certificates can also secure email communication and ensure the safety of all outbound e-mail communication, verifying that mail coming from an e-mail address is really from that address.

CHALLENGES

Today, enterprises are rapidly adopting WLAN technology as they realize the huge productivity gains that are achieved through mobility and instant access to information. Physical network wires are one of the primary obstacles to attackers seeking to hack their way onto a LAN. On a WLAN this obstacle disappears — user credentials and data are broadcast from both the client and the wireless access point in a radius which may reach 300 feet or more. The challenge is to prevent the hijacking of user credentials during authentication negotiation. And once authentication is complete, it is vital to protect the privacy of the data being transmitted between client and access point.

Digital Certificates can also be difficult to install. Some users don't want to bother to download a Certificate just to surf a Web site, which can limit their usability in certain situations such as B2B communications and secure intranets.

In addition, Digital Certificates are device specific. Users with Certificates installed on their work computers and wireless devices must also install Certificates on their home computers to access enterprise applications and data from the home devices.

THOUGHT LEADERSHIP/ADVICE

Using any of the approaches previously outlined, enterprises that have delayed migrating to WLANs because of security concerns can now safely adopt this valuable technology with Symbol Technologies' WLAN solutions. According to Synergy Research Group, in 2003 Symbol achieved the number one market share leadership position for wireless local area network (WLAN) switches and the number two position overall for enterprise WLAN equipment. Advanced security is a key reason for this success. Symbol's enterprise class security features include:

- A stateful-inspection firewall
- Comprehensive Network Access Translation (NAT) server with multiple application level gateways capable of supporting up to 40 applications
- Support for Kerberos, 802.1X/EAP, WPA, and planned support for IEEE 802.11i (when ratified)
- A built-in secure Web authentication database

THE FUTURE

Ultimately, no matter how good an authentication and encryption scheme may be, hackers may find ways around it. As a result, it may be impossible to design an impenetrable security technology. Nonetheless, the goal of any security policy is to make it extremely difficult for unauthorized people to gain access to network resources and information.

For more than 15 years, Symbol has provided wireless innovations and technologies to customers around the world in a wide range of industries. Symbol believes that wireless LANs should be no less secure than their wired counterparts. Using appropriate techniques described in this paper, enterprises can implement an effective, flexible and transparent wireless security solution. Looking ahead, Symbol will continue to develop and implement standards-based security technologies that will provide continually higher levels of protection.

SUMMARY

Digital Certificates are invaluable for providing secure and trusted communication over insecure and un-trusted networks. They are essential for securing WLAN systems and a wide variety of transactions conducted over the Internet. Of the EAP types that use Certificates to secure WLANs only EAP-TLS is a fully endorsed standard. However the management overhead for producing and distributing client Certificates has limited its use to environments that have a mature and well understood PKI in place.

EAP-TTLS and PEAP were developed to overcome the burden of issuing client Certificates. Using these methods, the client can check the validity of the Certificate on the server to which it authenticates by referring to a trusted Certificate Authority, such as the CA within a Windows Domain. It is possible to use EAP-TTLS and PEAP without a trusted CA. However this only provides one-way authentication between server and client and is not recommended other than for proof-of-concept trials.

ABOUT THE SYMBOL PRODUCT FAMILY

Symbol Technologies, Inc., The Enterprise Mobility Company™, is a global leader in mobile data management systems and services with innovative customer solutions based on wireless local area networking for voice and data, application-specific mobile computing and bar code data capture. Symbol's wireless LAN solutions are installed at more than 45,000 customer locations, and more than seven million Symbol scanners and application-specific scanner-integrated mobile computer systems are in use worldwide. Symbol and its global network of business partners provide solutions for retailing, transportation and distribution logistics, parcel and postal delivery, healthcare, education, manufacturing and other industries. Symbol enterprise mobility products and solutions are proven to increase workforce productivity, reduce operating costs, drive operational efficiencies and realize competitive advantages for the world's leading companies.

For more information on using Digital Certificates for authentication to a wireless LAN, please visit www.symbol.com. For global sales contact information, phone numbers and web site addresses around the world, you can also visit the Symbol "How to Buy" pages at www.symbol.com/howtobuy.

About Symbol Technologies

Symbol Technologies, Inc., The Enterprise Mobility Company,™ manufactures and services enterprise mobility systems, delivering products and solutions that capture, move and manage information in real time to and from the point of business activity. Symbol enterprise mobility solutions integrate advanced data capture products, radio frequency identification technology, mobile computing platforms, wireless infrastructure, mobility software and services programs under the Symbol Enterprise Mobility Services brand. Symbol enterprise mobility products and solutions are designed to increase workforce productivity, reduce operating costs, drive operational efficiencies and realize competitive advantages for the world's leading companies.

symbol®
The Enterprise Mobility Company ™

Corporate Headquarters
Symbol Technologies, Inc.
One Symbol Plaza
Holtsville, NY 11742-1300
TEL: +1.800.722.6234/+1.631.738.2400
FAX: +1.631.738.5990

For Asia Pacific Area
Symbol Technologies Asia, Inc.
(Singapore Branch)
Asia Pacific Division
230 Victoria Street #05-07/09
Bugis Junction Office Tower
Singapore 188024
TEL: +65.6796.9600
FAX: +65.6337.6488

For Europe, Middle East and Africa
Symbol Technologies
EMEA Division
Symbol Place, Winnersh Triangle
Berkshire, England RG41 5TP
TEL: +44.118.9457000
FAX: +44.118.9457500

For North America, Latin America and Canada
Symbol Technologies
The Americas
One Symbol Plaza
Holtsville, NY 11742-1300
TEL: +1.800.722.6234/+1.631.738.2400
FAX: +1.631.738.5990

Symbol Website
For a complete list of Symbol subsidiaries and business partners worldwide contact us at:
www.symbol.com
Or contact our pre-sales team at:
www.symbol.com/sales

DIGCERTWP 03/05