PKIX Working Group
Internet-Draft
March 2004
Expires: September 2004

R. Housley
Vigil Security
T. Moore
Microsoft

Certificate Extensions and Attributes Supporting Authentication in PPP and Wireless LAN

<draft-ietf-pkix-wlan-extns-05.txt>

Status of this Memo

Abstract

This document defines two EAP extended key usage values and a public key certificate extension to carry Wireless LAN (WLAN) System Service identifiers (SSIDs).

1. Introduction

Several Extensible Authentication Protocol (EAP) [EAP] authentication methods employ X.509 public key certificates. For example, EAP-TLS [EAP-TLS] can be used with PPP [PPP] as well as IEEE 802.1X [802.1X]. PPP is used for dial-up and VPN environments. IEEE 802.1X defines port-based, network access control, and it is used to provide authenticated network access for Ethernet, Token Ring, and Wireless LANs (WLANs) [802.11].

Automated selection of certificates for PPP and IEEE 802.1X clients is highly desirable. By using certificate extensions to identify the intended environment for a particular certificate, the need for user input is minimized. Further, the certificate extensions facilitate the separation of administrative functions associated with certificates used for different environments.

IEEE 802.1X can be used for authentication with multiple networks. For example, the same wireless station might use IEEE 802.1X to authenticate to a corporate IEEE 802.11 WLAN and a public IEEE 802.11 "hotspot." Each of these IEEE 802.11 WLANs has a different network name, called Service Set Identifier (SSID). If the network operators have a roaming agreement, then cross realm authentication allows the same certificate to be used on both networks. However, if the networks do not have a roaming agreement, then the IEEE 802.1X client needs select a certificate for the current network environment. Including a list of SSIDs in a certificate extension facilitates automated selection of an appropriate X.509 public key certificate without human user input. Alternatively, a companion attribute certificate could contain the list of SSIDs.

1.1. Conventions Used In This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [STDWORDS].

1.2. Abstract Syntax Notation

All X.509 certificate [X.509] extensions are defined using ASN.1 [X.208, X.209].

2. EAP Extended Key Usage Values

RFC 3280 [PROFILE] specifies the extended key usage X.509 certificate extension. The extension indicates one or more purposes for which the certified public key may be used. The extended key usage extension can be used in conjunction with key usage extension, which

indicates the intended purpose of the certified public key. For example, the key usage extension might indicate that the certified public key ought to be used only for validating digital signatures.

The extended key usage extension definition is repeated here for convenience:

```
id-ce-extKeyUsage OBJECT IDENTIFIER ::= {id-ce 37}

ExtKeyUsageSyntax ::= SEQUENCE SIZE (1..MAX) OF KeyPurposeId

KeyPurposeId ::= OBJECT IDENTIFIER
```

This specification defines two KeyPurposeId values: one for EAP over PPP, and one for EAP over LAN (EAPOL). Inclusion of the EAP over PPP value indicates that the certified public key is appropriate for use with EAP in the PPP environment, and the inclusion of the EAPOL value indicates that the certified public key is appropriate for use with the EAP in the LAN environment. Inclusion of both values indicates that the certified public key is appropriate for use in either of the environments.

```
id-kp  OBJECT IDENTIFIER  ::=  { iso(1) identified-organization(3)
         dod(6) internet(1) security(5) mechanisms(5) pkix(7) 3 }

id-kp-eapOverPPP  OBJECT IDENTIFIER  ::=  { id-kp 13 }

id-kp-eapOverLAN  OBJECT IDENTIFIER  ::=  { id-kp 14 }
```

The extended key usage extension may, at the option of the certificate issuer, be either critical or non-critical. If the extension is marked as critical, then the certified public key MUST be used only for the purposes indicated. However, if the extension is marked as non-critical, then extended key usage extension MAY be used to support the location of an appropriate certified public key.

If a certificate contains both a critical key usage extension and a critical extended key usage extension, then both extensions MUST be processed independently, and the certificate MUST only be used for a purpose consistent with both extensions. If there is no purpose consistent with both critical extensions, then the certificate MUST NOT be used for any purpose.

3. WLAN SSID Public Key Certificate Extension

The Wireless LAN (WLAN) System Service identifiers (SSIDs) public key certificate extension is always non-critical. It contains a list of SSIDs. When more than one certificate includes an extended key usage

extension indicating that the certified public key is appropriate for use with the EAP in the LAN environment, then the list of SSIDs MAY be used to select the correct certificate for authentication in a particular WLAN.

Since SSID values are unmanaged, the same SSID can appear in different certificates that are intended to be used with different WLANs. When this occurs, automatic selection of the certificate will fail, and the implementation SHOULD obtain help from the user to choose the correct certificate. In cases where a human user is unavailable, each potential certificate MAY be tried until one succeeds. However, by maintaining a cache of Access Point (AP) MAC addresses or authentication server identity with which the certificate has successfully authenticated, user involvement can be minimized. RADIUS [RADIUS1, RADIUS2] is usually used as the authentication service in WLAN deployments. The cache can be used to avoid future human user interaction or certificate selection by trial-and-error.

The WLAN SSID extension is identified by id-pe-wlanSSID.

```
id-pe  OBJECT IDENTIFIER  ::=  { iso(1) identified-organization(3)
         dod(6) internet(1) security(5) mechanisms(5) pkix(7) 1 }

id-pe-wlanSSID  OBJECT IDENTIFIER  ::=  { id-pe 13 }
```

The syntax for the WLAN SSID extension is:

```
SSIDList  ::=  SEQUENCE SIZE (1..MAX) OF SSID

SSID  ::=  OCTET STRING (SIZE (1..32))
```

4. WLAN SSID Attribute Certificate Attribute

When the public key certificate does not include the WLAN SSID certificate extension, then an attribute certificate [ACPROFILE] can be used to associate a list of SSIDs with the public key certificate. The WLAN SSIDs attribute certificate attribute contains a list of SSIDs, and the list of SSIDs MAY be used to select the correct certificate for authentication in a particular WLAN environment.

The WLAN SSID attribute certificate attribute is identified by id-aca-wlanSSID.

```
id-aca  OBJECT IDENTIFIER  ::=  { iso(1) identified-organization(3)
  dod(6) internet(1) security(5) mechanisms(5) pkix(7) 10 }

id-aca-wlanSSID  OBJECT IDENTIFIER ::= { id-aca 6 }
```

The syntax for the WLAN SSID attribute certificate attribute is exactly the same as the WLAN SSID extension:

```
SSIDList  ::=  SEQUENCE SIZE (1..MAX) OF SSID

SSID  ::=  OCTET STRING (SIZE (1..32))
```

5. Security Considerations

The procedures and practices employed by the certification authority (CA) MUST ensure that the correct values for the extended key usage extension and SSID extension are inserted in each certificate that is issued. Relying parties may accept or reject a particular certificate for an intended use based on the information provided in these extensions. Incorrect representation of the information in either extension could cause the relying party to reject an otherwise appropriate certificate or accept a certificate that ought to be rejected.

If multiple SSIDs are included in a certificate, then information can be obtained from a certificate about the SSIDs associated with several WLANs, not the WLAN that is currently being accessed. The intended use of the SSID extensions is to help a client determine the correct certificate to present when trying to gain access to a WLAN. In most situations, including EAP-TLS, the client will have the opportunity to validate the certificate provided by the server before transmitting one of its own certificates to the server. While the client may not be sure that the server has access to the corresponding private key until later in the protocol exchange, the identity information in the server certificate can be used to determine whether or not the client certificate ought to be provided. When the same client certificate is used to authenticate to multiple WLANs, the list of SSIDs is available servers associated with each WLAN. Of course, the list of SSIDs is also made available to any eavesdroppers on the WLAN. Whenever this SSID disclosure is a concern, different client certificates ought to be used for the each WLAN.

SSID values are unmanaged; therefore SSIDs may not be unique. Hence, it is possible for client certificates that are intended to be used with different WLANs to contain the same SSID. In this case, automatic selection of the certificate will fail, and the implementation SHOULD obtain help from the user to choose the correct certificate. In cases where a human user is unavailable, each potential certificate MAY be tried until one succeeds, disclosing the list of SSIDs associated with each certificate, which might otherwise not be disclosed. Therefore, it is RECOMMENDED that sequentially trying each certificate only be employed when user selection is

unavailable or impractical.

In practice, disclosure of the SSID is of little concern. Some WLAN security experts recommend that the SSID be masked in the beacon sent out by Access Points (APs). The intent is to make it harder for an attacker to find the correct AP to target. However, other WLAN management messages include the SSID, so this practice only forces the attacker to eavesdrop on the WLAN management messages instead of the beacon. Therefore, placing the SSID in the certificate does not make matters worse.

6. IANA Considerations

Certificate extensions and extended key usage values are identified by object identifiers (OIDs). Some of the OIDs used in this document are copied from X.509 [X.509]. Other OIDs were assigned from an arc delegated by the IANA. No further action by the IANA is necessary for this document or any anticipated updates.

7. References

Normative and informative references are provided.

7.1. Normative References

[ACPROFILE] Farrell, S., and R. Housley, "An Internet Attribute Certificate Profile for Authorization", RFC 3281, April 2002.

[PROFILE] Housley, R., Polk, W., Ford, W. and D. Solo, "Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[STDWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[X.208] CCITT. Recommendation X.208: Specification of Abstract Syntax Notation One (ASN.1). 1988.

[X.209] CCITT. Recommendation X.209: Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1). 1988.

[X.509] ITU-T. Recommendation X.509: The Directory - Authentication Framework. 2000.

7.2. Informative References

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

[802.1X] IEEE Std 802.1X, "Port-based Network Access Control", 2001.

[EAP] Blunk, L. and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", RFC2284, March 1998.

[EAPTLS] Aboba, B. and D. Simon, "PPP EAP TLS Authentication Protocol", RFC2716, October 1999.

[PPP] Simpson, W., Editor, "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[RADIUS1] Rigney, C., S. Willens, A. Rubens, and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RADIUS2] Congdon, P., B. Aboba, A. Smith, G. Zorn, and J. Roese, "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines", RFC 3580, September 2003.

8. ASN.1 Module

```
WLANCertExtn
  { iso(1) identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) pkix(7) id-mod(0)
    id-mod-wlan-extns(24) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN


-- OID Arcs

id-pe  OBJECT IDENTIFIER  ::=
   { iso(1) identified-organization(3) dod(6) internet(1)
     security(5) mechanisms(5) pkix(7) 1 }

id-kp  OBJECT IDENTIFIER  ::=
   { iso(1) identified-organization(3) dod(6) internet(1)
     security(5) mechanisms(5) pkix(7) 3 }
```

```
   id-aca  OBJECT IDENTIFIER  ::=
      { iso(1) identified-organization(3) dod(6) internet(1)
        security(5) mechanisms(5) pkix(7) 10 }


   -- Extended Key Usage Values

   id-kp-eapOverPPP  OBJECT IDENTIFIER  ::=  { id-kp 13 }

   id-kp-eapOverLAN  OBJECT IDENTIFIER  ::=  { id-kp 14 }


   -- Wireless LAN SSID Extension

   id-pe-wlanSSID  OBJECT IDENTIFIER  ::=  { id-pe 13 }

   SSIDList  ::=  SEQUENCE SIZE (1..MAX) OF SSID

   SSID  ::=  OCTET STRING (SIZE (1..32))


   -- Wireless LAN SSID Attribute Certificate Attribute
   -- Uses same syntax as the certificate extension: SSIDList

   id-aca-wlanSSID  OBJECT IDENTIFIER ::= { id-aca 6 }

   END
```

9. Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary

rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

10. Author's Address

Russell Housley
Vigil Security, LLC
918 Spring Knoll Drive
Herndon, VA 20170
USA
housley@vigilsec.com

Tim Moore
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
USA
timmoore@microsoft.com

11. Full Copyright Statement