

PKIX Working Group  
Internet-Draft  
Obsoletes: [RFC 3770](#)  
April 2005  
Expires: October 2005

R. Housley  
Vigil Security  
T. Moore  
Microsoft

Certificate Extensions and Attributes Supporting  
Authentication in Point-to-Point Protocol (PPP)  
and Wireless Local Area Networks (WLAN)  
<[draft-ietf-pkix-rfc3770bis-03.txt](#)>

#### Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at  
<http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at  
<http://www.ietf.org/shadow.html>.

#### 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). This document obsoletes [RFC 3770](#).

Internet-Draft

April 2005

## 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, Wireless LANs (WLANs) [[802.11](#)], and other IEEE 802 networks.

Automated selection of client certificates for use with PPP and IEEE 802.1X 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 supplicant needs to 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.

This document defines extended key usage values and a WLAN-specific certificate extension for use in certificates issued to clients of PPP and WLANs.

### 1.1. Changes since [RFC 3770](#)

This document is primarily same as [RFC 3770](#). Three changes are included:

- \* This document now uses the same normative reference for ASN.1 as [RFC 3280](#) [[PROFILE](#)]. The intent is to have the same dependencies.

- \* The discussion of the critical bit in the certificate extension in [section 2](#) is aligned with [RFC 3280](#). Also, the discussion of the key usage certificate extension was expanded.

- \* [RFC 3770](#) contained a typographical error in the object identifier for the Wireless LAN SSID Attribute Certificate Attribute. [Section 4](#) corrects the typographical error.
- \* Clarified that the SSID extension may appear in certificates that do not include the extended key usage extension.
- \* Uses the terms "peer", "EAP Server", and "supplicant" as they are defined in [\[EAP\]](#) and [\[802.1X\]](#). [RFC 3770](#) used "client" and "server".

## [1.2](#). 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](#)].

## [1.3](#). Abstract Syntax Notation

All X.509 certificate [[X.509](#)] extensions are defined using ASN.1 [[X.680](#),[X.690](#)].

## [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.

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

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 by a peer with EAP in the PPP environment. The inclusion of the EAPOL value indicates that the certified public key is appropriate for use by a peer with the EAP in the LAN environment. Inclusion of both values indicates that the certified public key is appropriate for use by a peer 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.

Certificate-using applications MAY require the extended key usage extension to be present in a certificate, and they MAY require a particular KeyPurposeId value to be present (such as id-kp-eapOverPPP or id-kp-eapOverLAN) within the extended key usage extension. If multiple KeyPurposeId values are included, the certificate-using application need not recognize all of them, as long as the required KeyPurposeId value is present.

If a certificate contains a key usage extension, the KeyUsage bits that are needed depends on the EAP method that is employed.

If a certificate contains both a key usage extension and an 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 extensions, then the certificate-using application MUST NOT use the certificate 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. The list of SSIDs MAY be used to select the correct certificate for authentication in a particular WLAN.

If the extended key usage extension appears in the same certificate as the SSID extension, then the extended key usage extension MUST indicate that the certified public key is appropriate for use with the EAP in the LAN environment by including the id-kp-eapOverLAN KeyPurposeId value.

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

Housley & Moore

[Page 4]

---

Internet-Draft

April 2005

succeeds. However, by maintaining a cache of Access Point (AP) MAC addresses or EAP 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 7 }
```

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 peer determine the correct certificate to present when trying to gain access to a WLAN. In most situations, including EAP-TLS, the peer will have the opportunity to validate the certificate provided by the EAP server before transmitting one of its own certificates to the EAP server. While the peer may not be sure that the EAP server has access to the corresponding private key until later in the protocol exchange, the identity information in the EAP server certificate can be used to determine whether or not the peer certificate ought to be provided. When the same peer certificate is used to authenticate to multiple WLANs, the list of SSIDs is available from 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 peer certificates ought to be used for the each WLAN.

SSID values are unmanaged; therefore SSIDs may not be unique. Hence, it is possible for peer 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). The OIDs used in this document 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.
- [EAP] Aboba, B., Blunk, L., Vollbrechtand, J., Carlson, J., and H. Levkowetz, Ed. "Extensible Authentication Protocol (EAP)", [RFC 3748](#), June 2004.
- [STDWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [X.509] ITU-T. Recommendation X.509: The Directory - Authentication Framework. 2000.
- [X.680] ITU-T Recommendation X.680: Information Technology - Abstract Syntax Notation One, 1997.
- [X.690] ITU-T Recommendation X.660 Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), 1997.

### [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.
- [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-extns2005(37) }
```

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 7 }

END

Internet-Draft

April 2005

## 9. IPR Considerations

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, or will be disclosed, and any of which I become aware will be disclosed, in accordance with [RFC 3668](#).

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](mailto:ietf-ipr@ietf.org).

## 10. Author's Address

Russell Housley  
Vigil Security, LLC  
918 Spring Knoll Drive  
Herndon, VA 20170  
USA  
[housley@vigilsec.com](mailto:housley@vigilsec.com)

Tim Moore

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

Housley & Moore

[Page 10]

---

Internet-Draft

April 2005

## 11. Full Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

