Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Certificate Profile for x.509 BS Certificates in 802.16e**
Date Submitted	**2005-03-17**

Source(s)	Jeff Mandin Streetwaves Networking Amatzia 5 Jerusalem, Israel	Voice: 972-50-5724-587 Fax: 972-50-5724-587 mailto:jeff@streetwaves-networks.com
	David McGinniss Sprint	mailto:david.s.mcginniss@mail.sprint.com

Re:	Recirc
Abstract	**Certificate Profile for x.509 BS Certificates in 802.16e**
Purpose	Acceptance into TGe Draft document
Notice	This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.
Patent Policy and Procedures	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:chair@wirelessman.org> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.

Certificate Profile for x.509 BS Certificates in 802.16e

Jeff Mandin
Streetwaves Networking

1 Problem Statement

802.16e adds BS certificates but does not include a BS Certificate profile. We must describe the format of the BS certificate and describe how it constitutes a credential of identity to the SS.

2 Overview of Solution

1. The BS Cert provides Operator credentials, which the SS should (but is not mandated) to verify against a list of one or more accepta ble operators. An SS might elect to forgo the verification of the operator credentials in the BS certificate and instead rely on credentials provided in subsequent EAP authentication.

2. Manufacturer certificates are not needed in the BS, as there is no need for the SS to verify the provenance or authenticity of the BS hardware.

3. BS certificates need not be created if the operator does not support RSA authentication

3 BS Certificate fields

3.1 CommonName field

The CommonName field provides the identity of the BS to be used in the RSA authentication. Accordingly in the BS certificate this field contains the operator-configured BS_ID (which in turn includes the 3-byte operatorId).

3.2 Organization Name field

The OrganizationName field contains the name of the Operator.

4 Specific text changes

[**Add new section 7.6.1.4.3**]

7.6.1.4.4 BS certificate

countryName=<Country of Operation>
organizationName=< Name of Infrastructure Operator>

organizationalUnitName=<WirelessMAN>
commonName=<Serial Number>
commonName=<BS Id>

The BS Id field shall contain the operator-defined BSId[1]. It is expressed as six pairs of hexadecimal digits separated by colons (:), e.g., "00:60:21:A5:0A:23." The Alpha HEX characters (A-F) shall be expressed as uppercase letters.

The attributes listed above shall be included. Other attributes are not allowed and shall not be included.

[Modify 7.6.1.6 as follows:]

7.6.1.6 tbsCertificate.issuerUniqueID and tbsCertificate.subjectUniqueID

The issuerUniqueID and subjectUniqueID fields shall be omitted for <u>all</u> ~~both~~ of the PKM's certificate types.

.

[1] the BSId is an operator-defined value, consequently the BS certificate is typically issued by the Operator, who must ensure that the BS ID is unique within the operator's network.