Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**x.509 security enhancement for 802.16e**	
Date Submitted	**2004-11-02**	
Source(s)	David S. McGinniss Sprint 1532 Sequoia Rd. Naperville, IL 60540	Voice: 886-3-5914579 Fax: 886-3-5829733 mailto: jjlee@itri.org.tw mailto: TMLin@itri.org.tw mailto: yryang@itri.org.tw
Re:	IEEE P802.16e/D5-2004	
Abstract	This adds x.509 SS certificates as an 802.16e requirement.	
Purpose	The purpose of this document is to prevent cloning of 802.16e SS and BS devices.	
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>.	

X.509 certificates and extensions to prevent cloning of devices in 802.16e

David S. McGinniss
Sprint

Motivation

Operators will need authorization of 802.16e devices designed to be delivered with as few SKU°¶ s as possible for worldwide retail distribution. These devices will offer many profiles for operation in different bandwidths and frequencies. Verification that the device is unique and has certain characteristics is desired.

Background

The 802.16e products will be produced en mass with support for a variety of profiles and suitable for operation on many operator networks worldwide. In a retail environment this device will be common and open to cloning if security is not put in place to prevent it. The certificate in the SS embedded by the manufacturer should be required and be in write once memory. The CA should be a higher level body governing certification as this will prevent verification issues if a manufacturer no longer is in business.

The extended attributes of the x.509 should be used to offer assistance to the backend system in determining authorization and key attributes of the device. As stated in the 802.16d document the extended attributes are constrained and should be augmented to facilitate quick assessment of device capabilities. This can help backend systems designed to provide over the air subscription and provisioning information about the device immediately upon entry of an unconfigured device. In its simplest form a SKU manufacture date and serial number would require that specified operational characteristics along with initial configuration be supplied to the CA and distributed in some standard for to the operators. Any method to distribute the required information as part of the certificate is welcomed.

Proposed Text changes

Replace the current section text with.
Section 7.6.2 of the 802.16-2004 base document

7.6.2 SS x.509 SS certificated are required. These manufacturer issued SS certificates shall be stored in SS permanent, write-once memory. SSs that have fac-tory-installed RSA private/public key pairs shall also have factory-installed SS certificates. SSs that rely on internal algorithms to generate an RSA key pair shall support a mechanism for installing a manufacturer issued SS certificate following key generation. The CA certificate of the Manufacturer CA that signed the SS certificate shall be embedded into the SS software. If a manufacturer issues SS certificates with multiple Manufacturer CA certificates, the SS software shall include ALL of that manufacturer's CA certificates. The specific Manufacturer CA certificate installed by the SS [i.e., advertised in Authentication Information messages and returned by the management information base (MIB) object] shall be that identifying the issuer of that modem's SS certificate.°®It is recommended that a higher organizational unit maintain CA authority.

Section 7.6.1.4.1 of the 802.16-2004 base document

7.6.1.4.1 Manufacturer certificate
countryName=<Country of Manufacturer>
[stateOrProvinceName=<state/province>]
[localityName=<City>]
organizationName=<Company Name>

organizationalUnitName=WirelessMAN
[organizationalUnitName=<Manufacturing Location>]
commonName=<Company Name> <Certification Authority>

The countryName, organizationName, and commonName attributes shall be included and shall have the values shown. The organizationalUnitName having the value °ß WirelessMAN°® shall be included. The organizationalUnitName representing manufacturing location should be included. If included, it shall be preceded by the organizationalUnitName having value °ß WirelessMAN.°® The stateOrProvinceName and localityName may be included. Other extended attributes are allowed and may be included.

7.6.1.4.2 SS certificate
countryName=<Country of Manufacturer>
organizationName=<Company Name>
organizationalUnitName=<manufacturing location>
commonName=<Serial Number>
commonName=<MAC Address>
deviceSku=<SKU>
DateofManufacture=<Manufacture Date>

The MAC address shall be the SS°¶ s MAC address. It is expressed as six pairs of hexadecimal digits separated by colons (:), e.g., °ß 00:60:21:A5:0A:23.°® The Alpha HEX characters (A-F) shall be expressed as uppercase letters.
The organizationalUnitName in an SS certificate, which describes the modem°¶ s manufacturing location, should be the same as the organizationalUnitName in the issuer Name describing a manufacturing location. Each SKU shall be unique and manufacturer will provide detailed capability information pertinent to device capabilities along with the SKU to the CA.