Ontario

Government of Ontario
Information & Technology Standards

Wireless Local Area Networks (WLANs)

Mandatory and Non-Mandatory Technical Standards and Specifications

Government of Ontario IT Standard (GO-ITS)

Document Number: 39.1
Version Number: 1.0
Status: Approved

Prepared for the Information Technology Standards Council (ITSC) under the delegated authority of the Management Board of Cabinet (MBC)

Review Date: 2005-11-08

Foreword

Government of Ontario Information & Technology Standards are the official publications on the standards, guidelines, technical reports and preferred practices adopted by the Information Technology Standards Council under delegated authority of the Management Board of Cabinet. These publications support the Ministry of Government Services' responsibilities for coordinating standardization of Information and Technology in the Government of Ontario. Publications that set new or revised standards provide policy and enterprise architecture guidance as well as administrative information for their implementation. In particular, they describe where the application of a standard is mandatory and specify any qualifications governing its implementation.

Table Of Contents

1. Introduction

1.1 Background

A Wireless Local Area Network (WLAN) is a network communication system that uses Ultra High Frequency (UHF) radio, i.e., electromagnetic, waves rather than wires to communicate between computer devices such as mobile computers (e.g. laptops, notebooks, iPAQ pocket PCs), integrated personal digital assistants (PDAs), cellular devices (e.g. cell phones, low-end smart phones, and PDAs), portable storage devices (e.g. USB flash drives, memory sticks, removable hard drives) and other computer peripherals.

WLANs are considered a valuable asset to the Government of Ontario's Information & Information Technology infrastructure for the following reasons:

- Anytime, anywhere access to real-time information in the organization
- No longer constrained by the location of the network port or existing LAN cabling
- Eliminates the need to pull cable through walls and ceilings
- Compatible with existing networks with ever-increasing performance comparable to LANs
- Standards-based products from multiple vendors are interoperable with one another
- Comprehensive security that can meet the needs of specific applications and installations

This standard was developed by the Wireless Standards Working Group, sponsored by the Information Technology Standards Council (ITSC) and the Corporate Architecture and Standards Branch (CASB) within the Office of the Corporate Chief Technology Officer (OCCTO).

1.2 Purpose

This standard defines mandatory WLAN security requirements, technical standards and specifications. The goal of this standard is to address connectivity and security requirements for the corporate WLAN reference architecture to ensure operations excellence regarding the delivery of corporate WLAN services and to ensure that the use of WLANs does not result in unacceptable risks to Government of Ontario Programs, Services and Resources.

This standard reflects the general direction of the OPS as reflected in the wireless / mobile strategy for the government. The general requirements pertaining to wireless LAN connectivity and security include:

- Assumes medium to high levels of security

- Desire for conformance to the 802.11i standard, of which WPA2 is an instantiation of the mandatory aspects of this standard;
- Authenticates end-point device based on port level 802.1x;
- Supports quality of service, generally compliant to the emerging 802.11e, initially in order to provide for service level management metrics, positioning for voice over IP;
- Isolation of wireless traffic based on Virtual Local Area Networks (VLAN) technologies.

1.3 Scope

1.3.1 In Scope

- WLAN Connectivity and Quality of Service (QoS)
- WLAN Security, Authentication & Authorization, Data Encryption and Network Management
- Technical Standards and Specifications for WLAN Connectivity and Security to provide interoperability across the OPS

1.3.2 Out of Scope

- Architecture best practices and principles
- Cellular technologies
- Directives, legislation, regulations and statues
- Evaluation criteria for RFPs
- Information classification, disclosure, disposal, retention and usage policies
- Mobile architecture, standards and strategies
- Privacy and security guidelines and policies
- Procurement policies and strategies
- Satellite technologies
- Service level agreements and metrics

1.4 Applicability Statements

Government of Ontario IT Standards and Enterprise Products apply (are mandatory) for use by all ministries/clusters and to all former Schedule I and IV provincial government agencies under their present classification (Advisory, Regulatory, Adjudicative, Operational Service, Operational Enterprise, Trust or Crown Foundation) according to the current agency classification system.

Kindly refer to http://intra.pmed.mbs.gov.on.ca/mbc/pdf/Agency_Establishment&Accountability-Dir.pdf for a list of provincial government agencies with their classification under the current classification system, as well as their previous Schedule under the former Schedule system.

Additionally, this applies to any other new or existing agencies designated by Management Board of Cabinet as being subject to such publications, i.e. the GO-ITS publications and mandatory Enterprise Products - and particularly applies to Advisory, Regulatory, and Adjudicative Agencies (see also procurement link, OPS paragraph). Further included is any agency which, under the terms of its Memorandum of Understanding with its responsible Minister, is required to satisfy the mandatory requirements set out in any of the Management Board of Cabinet Directives (*cf*. Operational Service, Operational Enterprise, Trust, or Crown Foundation Agencies).

As new GO-IT standards are approved, they are deemed mandatory on a go-forward basis (Go-forward basis means at the next available project development or procurement opportunity). When implementing or adopting any GO ITSC standards or GO ITSC standards updates, ministries and I&IT Cluster must follow their organization's pre-approved policies and practices for ensuring that adequate change control, change management and risk mitigation mechanisms are in place and employed.

For the purposes of this document, any reference to ministries or the Government includes applicable agencies.

1.4.1 Migration Requirements

The following connectivity and security requirements apply to WLAN migration efforts:

- IEEE 802.11b products must be migrated towards or replaced by IEEE 802.11g products for the following reasons:
    - Most IEEE 802.11b products are not upgradeable to support WPA2 and AES because of hardware requirements
    - Throughput performance of IEEE 802.11g within the 2.4GHz band is comparable to that of IEEE 802.11a within the 5 GHz band
    - Investment protection through backwards compatibility with legacy IEEE 802.11b products ensures easy migration of existing WLANs
- IEEE 802.11 products must comply with the IEEE 802.11g standard and must operate

within the 2.4GHz band for interoperability reasons unless otherwise exempted

- IEEE 802.11 products must not enable Wired Equivalent Privacy (WEP)
- IEEE 802.11 products that currently comply with Wi-Fi Protected Access (WPA) must be migrated towards or replaced by IEEE 802.11 products that comply with WPA2
- IEEE 802.11 products that can support IEEE 802.11e may be used to enhance the Quality of Service (QoS) of WLAN services

A wide variety of FIPS 140-2 certified WPA2 compliant IEEE 802.11 products are now available. Therefore, IEEE 802.11 products must comply with WPA2 and service providers must provide a clear migration path from WPA to WPA2. The main difference between the two is that WPA uses RC4 encryption whereas WPA2 uses FIPS 140-2 certified AES encryption.

1.4.2 Governance for New WLAN Installations

The Cluster Chief Information Officer (CIO) must approve installations of Wireless LAN implementations within the scope of their responsibilities. This includes ensuring that WLAN installations conform to the GO-ITS technical standards recommended by the Information Technology Standards Council (ITSC) and approved by the Corporate Architecture Review Board (ARB). And also applies to reviewing and recommending exemptions to the approved WLAN standard should business or other needs dictate such a path.

1.5 Impacts to Existing Standards

GO-ITS/GO-SPP Number	Describe Impact	Recommended Action (alternatively provide a page number where details can be found)
GO-ITS 24 Omnibus IT Standard	Technical standards and specifications in GO-ITS 24 and the Technical Standards Knowledge Management (TSKM) system must be updated to ensure integrity	GO-ITS 24 and the Technical Standards Knowledge Management (TSKM) system were reviewed to determine which technical standards and specifications needed to be added, edited and removed. Changes to both were done accordingly.

GO-ITS 25.5 (WLAN Security Requirements) and GO-ITS 25.5.1 (WLAN Security Best Practices)	Best practices and requirements in GO-ITS 25.5 must align with recommendations included in this standard	GO-ITS 25.5x standards were reviewed to ensure integrity

1.6 Impacts to Existing Environment

Impacted Infrastructure (includes Common Components and other applications)	**Describe Impact**	**Recommended Action (alternatively provide a page number where details can be found)**
WLAN Connectivity	IEEE 802.11b products must be migrated towards or replaced by IEEE 802.11g products	Requires input from the ITSM and Change Management Branch to recommend an action plan regarding WLAN connectivity migrations
WLAN Security	IEEE 802.11 products must not use WEP. Any WPA installations must be migrated to WPA2 (see note below regarding migration path)	This approach was recommended by the Corporate Security Branch
WLAN Security	Service providers must provide a clear migration path from WPA to WPA2	Requires input from the ITSM and Change Management Branch to recommend an action plan regarding WLAN security migrations

1.7 Requirements Levels

GO-ITS and GO-SPP documents may combine mandatory and non-mandatory information as required to effectively describe the requirements of a standard or standards procurement profile. Therefore, it is important to indicate clearly when a requirement is mandatory.

Where indicated throughout this document, the words “MUST”, “MUST NOT”, “SHOULD”, “SHOULD NOT”, and “MAY” are to be interpreted as described below:

MUST

This word, or the terms "REQUIRED" or "SHALL", means that the definition is an absolute requirement of the specification.

Please Note: New standards or standards procurement profiles are NOT retroactive although they MUST be complied with at the next procurement or project opportunity.

MUST NOT

This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.

SHOULD

This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

Please Note: The word “SHOULD” is considered a preferred practice that may have already been vetted, may be advantageous to use and may expedite the approval process.

SHOULD NOT

This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

MAY

This word, or the adjective "OPTIONAL", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation that does not include a particular option MUST be prepared to interoperate with another implementation that does include the option, though perhaps with reduced functionality. In the same vein an implementation that does include a particular option MUST be prepared to interoperate with another implementation t*hat does not include the option* (except, of course, for the feature the option provides.)

1.8 Recommended Versioning and/or Change Management

This document will be reviewed on an ongoing basis to take into account the evolution of connectivity, security and other related requirements for wireless technologies. Changes or additions to this document shall be established in writing and communicated to all appropriate personnel. The Corporate Architecture and Standards Branch within OCCTO will provide advice on the interpretation and application of these requirements and manage any updates to the document when the need arises.

1.9 Publication Details

Check One	Publish on the Internal or External web site?
☐	Intranet Web Site (Internal)
☒	Internet Web Site (External)

This standard is available at the following GO-ITS Internet Web Site:

http://www.itstandards.gov.on.ca

1.10 Contact Information

	Administrative Contact	Technical Contact
Full Name	Paul Daly	Brian Bisaillon
Position	Standards Coordinator	Standards Technical Coordinator
Organization	Ministry of Government Services	Ministry of Government Services
Division	Office of the Corporate Chief Technology Officer (OCCTO)	Office of the Corporate Chief Technology Officer (OCCTO)
Branch	Corporate Architecture and Standards Branch (CASB)	Corporate Architecture and Standards Branch (CASB)
Section	Technical Standards	Technical Standards
Office Phone	1-416-326-9035	1-416-212-0940
E-mail Address	paul.daly@mgs.gov.on.ca	brian.bisaillon@mgs.gov.on.ca

1.11 Acknowledgements

The following list of individuals and stakeholder groups contributed to the development of this

standard, including those who helped write the standard and provided subject expertise as well as those groups or individuals contacted for input/comments.

1.12 Development Team

Full Name	Cluster/Area
Edwin Lang	HSC – Specification Editor
Andrew Marks	OCCSD – Network Office
Brian Bisaillon	OCCTO – CASB
Carl Burton	CAC
Colin Easton	OCCTO – CASB
Earl Kuntz	OCCIO – Corporate Security
Gilbert Chan	EBC
Jeff Trafford	TC
Jim O'Neil	LRC
Mike Hrycko	CSC
Paul Daly	OCCTO – CASB
Raj Chauhan	OCCS – SPPM
Tim Dafoe	OCCIO – Corporate Security
Victor Khait	JC

2. Mandatory Technical Standards and Specifications

2.1 WLAN Connectivity

2.1.1 Technical Standard: Wireless (IEEE 802.11)

2.1.1.1 Technical Specification: IEEE Std 802.11-1999

This standard is part of a family of standards for local and metropolitan area networks. This family of standards deals with the Physical and Data Link layers as defined by the International Organization for Standardization (ISO) Open Systems Interconnection (OSI) Basic Reference Model (ISO/IEC 7498-1: 1994). The access standards define seven types of medium access technologies and associated physical media, each appropriate for particular applications or system objectives. Other types are under investigation.

- IEEE Std 802.11-1999: LAN/MAN Standards Committee. "IEEE Standards for Information Technology -- Telecommunications and Information Exchange between Systems -- Local and Metropolitan Area Network -- Specific Requirements -- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications." IEEE-SA Standards Board. 1999-03-18.
    - Remote link: http://standards.ieee.org/getieee802/download/802.11-1999.pdf

2.1.1.2 Technical Specification: IEEE Std 802.11g-2003

This amendment specifies the extensions to IEEE 802.11 for wireless local area networks (WLANs) providing mechanisms for dynamic frequency selection (DFS) and transmit power control (TPC) that may be used to satisfy regulatory requirements for operation in the 5 GHz band in Europe.

- IEEE Std 802.11g-2003: LAN/MAN Standards Committee. "IEEE Standard for Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications--Amendment 4: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band." IEEE-SA Standards Board. 2003-06-12.
    - Remote links: http://standards.ieee.org/getieee802/download/802.11g-2003.pdf

2.1.1.3 Technical Specification: IEEE Std 802.11i-2004

This amendment allows for security improvements in existing wireless LAN products (through firmware upgrades). Most current products can be upgraded to use certain IEEE 802.11i features, such as Temporal Key Integrity Protocol and IEEE 802.1x authentication. This provides a considerable security improvement over the Wired Equivalent Privacy feature in the original standard. The amendment also contains options for backward compatibility with the original standard. Even greater security can be gained in new products having new hardware architecture. Products coming on the market are using features of IEEE 802.11i, such as AES methods, key caching and pre-authentication for persistent authentication, which allows mobile stations to switch from one access point to another without incurring the time overhead of a key exchange each time.

- IEEE Std 802.11i-2004: LAN/MAN Standards Committee. "Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003). IEEE Standard for Information technology--Telecommunications and information exchange between system--Local and metropolitan area networks--Specific requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications--Amendment 6: Medium Access Control (MAC) Security Enhancements." IEEE-SA Standards Board. 2004-06-23.
    - Remote link: http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

2.1.1.4 Quality of Service (QoS)

Please Note: This section is a placeholder for the IEEE 802.11e standard that has not yet been published by the IEEE. Therefore, IEEE 802.11e is not a mandatory requirement.

2.2 WLAN Security

The IEEE 802.11i standard is also known as WPA2. It supersedes the previous security specification, Wired Equivalent Privacy (WEP) that has severe security weaknesses. WPA was introduced as an intermediate solution to WEP insecurities until IEEE 802.11i was approved as the IEEE's interoperable Wireless security implementation. WPA2 uses AES encryption whereas WEP and WPA use only the RC4 stream cipher.

2.3 Port Based Access Control

2.3.1 Technical Standard: IEEE 802.1X-2001

Port-based network access control makes use of the physical access characteristics of IEEE 802 Local Area Networks (LAN) infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails.

- IEEE Std 802.1X-2001: LAN/MAN Standards Committee. "IEEE Standards for Local and Metropolitan Area Networks: Port-Based Network Access Control." IEEE-SA Standards Board. 2001-06-14.
    - Remote link: http://standards.ieee.org/getieee802/download/802.1X-2001.pdf

2.3.2 Technical Standard: Remote Authentication Dial In User Service (RADIUS)

This document describes a protocol for carrying authentication, authorization, and configuration information between a Network Access Server that desires to authenticate its links and a shared Authentication Server.

- RFC2865: C. Rigney. S. Willens. A. Rubens, et al. "Remote Authentication Dial In User Service (RADIUS)." Internet Engineering Task Force (IETF). 2000-06-01.

- Remote link: ftp://ftp.isi.edu/in-notes/rfc2865.txt

2.3.2.1 Technical Specification: RADIUS Accounting

This document describes a protocol for carrying accounting information between a Network Access Server and a shared Accounting Server.

- RFC2866: C. Rigney. "RADIUS Accounting." Internet Engineering Task Force (IETF). 2000-06-01.
  - Remote link: ftp://ftp.isi.edu/in-notes/rfc2866.txt

2.3.2.2 Technical Specification: RADIUS Accounting Modifications for Tunnel Protocol Support

This document defines new RADIUS (Remote Authentication Dial In User Service) accounting Attributes and new values for the existing Acct- Status-Type Attribute designed to support the provision of compulsory tunneling in dial-up networks.

- RFC2867: G. Zorn, B. Aboba, D. Mitton. "RADIUS Accounting Modifications for Tunnel Protocol Support." Internet Engineering Task Force (IETF). 2000-06-01.
  - Remote link: ftp://ftp.isi.edu/in-notes/rfc2867.txt

2.3.2.3 Technical Specification: RADIUS Attributes for Tunnel Protocol Support

This document defines a set of RADIUS (Remote Authentication Dial In User Service) attributes designed to support the provision of compulsory tunneling in dial-up networks.

- RFC2868: G. Zorn, D. Leifer, A. Rubens, et al. "RADIUS Attributes for Tunnel Protocol Support." Internet Engineering Task Force (IETF). 2000-06-01.
  - Remote link: ftp://ftp.isi.edu/in-notes/rfc2868.txt

2.3.2.4 Technical Specification: RADIUS Extensions

This document describes additional attributes for carrying authentication, authorization and accounting information between a Network Access Server (NAS) and a shared Accounting Server using the Remote Authentication Dial In User Service (RADIUS) protocol described in RFC 2865 and RFC 2866.

- RFC2869: C. Rigney, W. Willats, P. Calhoun. "RADIUS Extensions." Internet Engineering Task Force (IETF). 2000-06-01.
  - Remote link: ftp://ftp.isi.edu/in-notes/rfc2869.txt

2.3.2.5 Technical Specification: IANA Considerations for RADIUS (Remote Authentication Dial In User Service)

This document describes the Internet Assigned Numbers Authority (IANA) considerations for the Remote Authentication Dial In User Service (RADIUS).

- RFC3575: B. Aboba. "IANA Considerations for RADIUS (Remote Authentication Dial In User

Service)." Internet Engineering Task Force (IETF). 2003-07-01.

- Remote link: ftp://ftp.isi.edu/in-notes/rfc3575.txt

2.3.2.6 Technical Specification: RADIUS and IPv6

This document specifies the operation of RADIUS (Remote Authentication Dial In User Service) when run over IPv6 as well as the RADIUS attributes used to support IPv6 network access.

- RFC3162: B. Aboba. G. Zorn. D. Mitton, et al. "RADIUS and IPv6." Internet Engineering Task Force (IETF). 2001-08-01.
  - Remote link: ftp://ftp.isi.edu/in-notes/rfc3162.txt

2.3.2.7 Technical Specification: Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)

This document describes a currently deployed extension to the Remote Authentication Dial In User Service (RADIUS) protocol, allowing dynamic changes to a user session, as implemented by network access server products. This includes support for disconnecting users and changing authorizations applicable to a user session.

- RFC3576: M. Chiba, G. Dommety, M. Eklund, et al. "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)." Internet Engineering Task Force (IETF). 2003-07-01.
  - Remote link: ftp://ftp.isi.edu/in-notes/rfc3576.txt

2.3.2.8 Technical Specification: RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)

This document defines Remote Authentication Dial In User Service (RADIUS) support for the Extensible Authentication Protocol (EAP), an authentication framework that supports multiple authentication mechanisms. In the proposed scheme, the Network Access Server (NAS) forwards EAP packets to and from the RADIUS server, encapsulated within EAP-Message attributes. This has the advantage of allowing the NAS to support any EAP authentication method, without the need for method- specific code, which resides on the RADIUS server. While EAP was originally developed for use with PPP, it is now also in use with IEEE 802.

- RFC3579: B. Aboba, P. Calhoun. "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)." Internet Engineering Task Force (IETF). 2003-09-01.
  - Remote link: ftp://ftp.isi.edu/in-notes/rfc3579.txt

2.3.3 Technical Standard: Point-to-Point Protocol (PPP)

2.3.3.1 Technical Specification: Extensible Authentication Protocol (EAP)

This document defines the Extensible Authentication Protocol (EAP), an authentication framework

that supports multiple authentication methods. EAP typically runs directly over data link layers such as Point-to-Point Protocol (PPP) or IEEE 802, without requiring IP. EAP provides its own support for duplicate elimination and retransmission, but is reliant on lower layer ordering guarantees. Fragmentation is not supported within EAP itself; however, individual EAP methods may support this. This document obsoletes RFC 2284. A summary of the changes between this document and RFC 2284 is available in appendix A [of RFC3748, subtitled 'Changes from RFC2284'].

- RFC3748: B. Aboba. L. Blunk. J. Vollbrecht, et al. "Extensible Authentication Protocol (EAP)." Internet Engineering Task Force (IETF). 2004-06-01.
    - Remote link: ftp://ftp.isi.edu/in-notes/rfc3748.txt

2.3.3.2 Technical Specification: PPP EAP TLS Authentication Protocol

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. PPP also defines an extensible Link Control Protocol (LCP), which can be used to negotiate authentication methods, as well as an Encryption Control Protocol (ECP), used to negotiate data encryption over PPP links, and a Compression Control Protocol (CCP), used to negotiate compression methods. The Extensible Authentication Protocol (EAP) is a PPP extension that provides support for additional authentication methods within PPP. Transport Level Security (TLS) provides for mutual authentication, integrity-protected ciphersuite negotiation and key exchange between two endpoints. This document describes how EAP-TLS, which includes support for fragmentation and reassembly, provides for these TLS mechanisms within EAP.

- RFC2716: B. Aboba, D. Simon. " PPP EAP TLS Authentication Protocol." Internet Engineering Task Force (IETF). 1999-10-01.
    - Remote link: ftp://ftp.isi.edu/in-notes/rfc2716.txt

2.4 WLAN Data Encryption

2.4.1 Technical Standard: Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext.

- FIPS Publication 197: "Advanced Encryption Standard (AES)." National Institute of Standards and Technology (NIST). 2001-11-26.
    - Remote link: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

2.4.1.1 Technical Specification: Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)

This document proposes several new ciphersuites. At present, the symmetric ciphers supported by Transport Layer Security (TLS) are RC2, RC4, International Data Encryption Algorithm (IDEA), Data Encryption Standard (DES), and triple DES. The protocol would be enhanced by the addition of

Advanced Encryption Standard (AES) ciphersuites.

- RFC3268: P. Chown. "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)." Internet Engineering Task Force (IETF). 2002-06-01.
    - Remote link: ftp://ftp.isi.edu/in-notes/rfc3268.txt

2.4.1.2 Technical Specification: Advanced Encryption Standard (AES) Key Wrap Algorithm

The purpose of this document is to make the Advanced Encryption Standard (AES) Key Wrap algorithm conveniently available to the Internet community. The United States of America has adopted AES as the new encryption standard. The AES Key Wrap algorithm will probably be adopted by the USA for encryption of AES keys. The authors took most of the text in this document from the draft AES Key Wrap posted by NIST.

- RFC3394: J. Shaad, R. Housley. "Advanced Encryption Standard (AES) Key Wrap Algorithm." Internet Engineering Task Force (IETF). 2002-09-01.
    - Remote link: ftp://ftp.isi.edu/in-notes/rfc3394.txt

2.4.2 Technical Standard: Counter with CBC-MAC (CCM)

2.4.2.1 Technical Specification: CCM

Counter with CBC-MAC (CCM) is a generic authenticated encryption block cipher mode. CCM is defined for use with 128-bit block ciphers, such as the Advanced Encryption Standard (AES).

- RFC3610: D. Whiting, R. Housley, N. Ferguson. "Counter with CBC-MAC (CCM)." Internet Engineering Task Force (IETF). 2003-09-01.
    - Remote link: ftp://ftp.isi.edu/in-notes/rfc3610.txt

2.4.3 Technical Standard: Temporal Key Integrity Protocol (TKIP)

Both WPA and WPA2 use the Temporal Key Integrity Protocol (TKIP). TKIP is defined within the IEEE documentation for 802.11i-2004:

- Remote link: http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

2.4.4 Technical Standard: Secure Hash Standard (SHS)

To specify a Secure Hash Algorithm to be used by both the transmitter and intended receiver of a message in computing and verifying a digital signature.

- FIPS Publication 180-2: "Secure Hash Standard (SHS)" National Institute of Standards and Technology (NIST). 2002-08-01.
    - Remote link: http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf

2.4.5 Technical Standard: Transport Layer Security (TLS)

This document specifies Version 1.0 of the Transport Layer Security (TLS) protocol. The TLS protocol provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

- RFC2246: T. Dierks. C. Allen. "The TLS Protocol Version 1.0." Internet Engineering Task Force (IETF). 1999-01-01.
    - Remote link: ftp://ftp.isi.edu/in-notes/rfc2246.txt

2.4.5.1 Technical Specification: Transport Layer Security (TLS) Extensions

This document describes extensions that may be used to add functionality to Transport Layer Security (TLS). It provides both generic extension mechanisms for the TLS handshake client and server hellos, and specific extensions using these generic mechanisms. The extensions may be used by TLS clients and servers. The extensions are backwards compatible - communication is possible between TLS 1.0 clients that support the extensions and TLS 1.0 servers that do not support the extensions, and vice versa.

- RFC3546: S. Blake-Wilson. M. Nystrom. D. Hopwood, et al. "Transport Layer Security (TLS) Extensions." Internet Engineering Task Force (IETF). 2003-06-01.
    - Remote link: ftp://ftp.isi.edu/in-notes/rfc3546.txt

2.5 WLAN Network Management

2.5.1 Technical Standard: IEEE Std 802.1F-1993

Management information and procedures applicable across the entire family of IEEE 802 LAN/MAN standards within the architectural framework for LAN/MAN Management specified in IEEE Std 802-1990 are identified. Common management information, such as attributes to represent MAC address and managed objects to represent configurable gauges, are specified. The need of developers of LAN/MAN management specifications for common procedures to develop, describe, and register management information is addressed.

- IEEE Std 802.1F-1993: Technical Committee on Computer Communications. "IEEE Standards for Local and Metropolitan Area Networks: Common Definitions and Procedures for IEEE 802 Management Information." IEEE-SA Standards Board. 1993-11-09.
    - Remote link: http://standards.ieee.org/getieee802/download/802.1F-1993.pdf

2.5.2 Technical Standard: Management Information Base (MIB)

2.5.2.1 Technical Specification: RADIUS Authentication Client MIB

This memo defines a set of extensions that instrument RADIUS authentication client functions.

- RFC2618: B. Aboba. G. Zorn. "RADIUS Authentication Client MIB." Internet Engineering Task

Force (IETF). 1999-06-07.

- Remote link: ftp://ftp.isi.edu/in-notes/rfc2618.txt

2.5.2.2 Technical Specification: RADIUS Authentication Server MIB

This memo defines a set of extensions that instrument RADIUS authentication server functions.

- RFC2619: G. Zorn. B. Aboba. "RADIUS Authentication Server MIB." Internet Engineering Task Force (IETF). 1999-06-07.
  - Remote link: ftp://ftp.isi.edu/in-notes/rfc2619.txt

2.5.2.3 Technical Specification: RADIUS Accounting Client MIB

This memo defines a set of extensions that instrument RADIUS accounting client functions. These extensions represent a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. Using these extensions IP-based management stations can manage RADIUS accounting clients.

- RFC2620: B. Aboba, G. Zorn. " RADIUS Accounting Client MIB." Internet Engineering Task Force (IETF). 1999-06-01.
  - Remote link: ftp://ftp.isi.edu/in-notes/rfc2620.txt

2.5.2.4 Technical Specification: RADIUS Accounting Server MIB

This memo defines a set of extensions that instrument RADIUS accounting server functions. These extensions represent a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. Using these extensions IP-based management stations can manage RADIUS accounting servers.

- RFC2621: G. Zorn. B. Aboba. "RADIUS Accounting Server MIB." Internet Engineering Task Force (IETF). 1999-06-07.
  - Remote link: ftp://ftp.isi.edu/in-notes/rfc2621.txt

2.5.2.5 Technical Specification: IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines

This document provides suggestions on Remote Authentication Dial In User Service (RADIUS) usage by IEEE 802.1X Authenticators. The material in this document is also included within a non-normative Appendix within the IEEE 802.1X specification, and is being presented as an IETF RFC for informational purposes.

- RFC3580: P. Congdon, B. Aboba, A. Smith, et al. "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines." Internet Engineering Task Force (IETF). 2003-09-01.
  - Remote link: ftp://ftp.isi.edu/in-notes/rfc3580.txt

3. Errata

Created: 2005-02-10

- Working draft of the Wireless LAN GO-ITS formulated according to discussions and decisions made during the ITSC Wireless LAN Standards Working Group meeting

Approved: 2005-10-19

- Final draft version 0.62f approved by the IT Standards Council on October 19, 2005

Approved: 2005-11-08

- Approved by the Architecture Review Board on November 8, 2005
- Approved version number reset to 1.0

4. Copyright

Appendix A: Additional Information

A.1 Transitional Standards

A.1.1 Technical Standard: Wireless (IEEE 802.11)

A.1.1.1 WLAN Technical Specification: IEEE Standard 802.11b-1999

Technical Specification: IEEE Standard for Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements--Part 11: Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band

Changes and additions are provided for IEEE Std 802.11b-1999 to support the higher rate Physical Layer for operation in the 2.4 GHz band.

- IEEE Std 802.11b-1999: LAN/MAN Standards Committee. "IEEE Standard for Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements--Part 11: Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band." IEEE-SA Standards Board. 1999-09-16.
    - Remote links: http://standards.ieee.org/getieee802/download/802.11b-1999.pdf

A.1.1.2 Technical Specification (including Corrigendum): IEEE Std 802.11b-1999/Cor1-2001

This amendment specifies the extensions to IEEE Std 802.11 for Wireless Local Area Networks providing specifications for conformant operation beyond the original six regulatory domains of that standard. These extensions provide a mechanism for an IEEE Std 802.11 access point to deliver the required radio transmitter parameters to an IEEE Std 802.11 mobile station, which allows that station to configure its radio to operate within the applicable regulations of a geographic or political subdivision. This mechanism is applicable to all IEEE Std 802.11 PHY types. A secondary benefit of the mechanism described in this amendment is the ability for an IEEE Std 802.11 mobile station to roam between regulatory domains.

- IEEE Std 802.11b-1999/Cor1-2001: LAN/MAN Standards Committee. "IEEE Standard for Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications--Amendment 2: Higher-speed Physical Layer (PHY) extension in the 2.4 GHz band--Corrigendum1." IEEE-SA Standards Board. 2001-10-10.
    - Remote links: http://standards.ieee.org/getieee802/download/802.11b-1999_Cor1-2001.pdf

A.2 Emerging Standards

A.2.1 Technical Standard: Diameter Base Protocol (DBP)

A.2.1.1 Technical Specification: Diameter Base Protocol

The Diameter base protocol is intended to provide an Authentication, Authorization and Accounting (AAA) framework for applications such as network access or IP mobility. Diameter is also intended to work in both local Authentication, Authorization & Accounting and roaming situations. This document specifies the message format, transport, error reporting, accounting and security services to be used by all Diameter applications. The Diameter base application needs to be supported by all Diameter implementations.

- RFC3588: P. Calhoun, J. Loughney, E. Guttman, et al. "Diameter Base Protocol." Internet Engineering Task Force (IETF). 2003-09-01.
    - Remote link: ftp://ftp.isi.edu/in-notes/rfc3588.txt

A.3 Other References

A.3.1 OCCTO Technology Future Series

A.3.1.1 Wireless and Mobility Technology Profile

Advances in secured wireless communications have improved the usability of this technology and the potential application of the technology is promising, there are also some important challenges that need to be addressed to fully take advantage of the technology. These ideas are explored in this profile developed by the Office of the Corporate Chief Technology Officer (OCCTO), Ministry of Government Services - http://intra.occto.mbs.gov.on.ca/occtoservices/tfs

A.3.2 Other GO-ITS Related to WLANs

A.3.2.1 GO-ITS 25.5 Security Standard - Requirements for Wireless Local Area Networks

A.3.2.2 GO-ITS 25.5.1 Security Standard - Best Practices for Wireless Local Area Networks

Both Security Standards are available at http://www.itstandards.gov.on.ca

A.3.3 Wi-Fi Alliance White Paper

A.3.3.1 Title: 'Deploying Wi-Fi Protected Access WPA and WPA2 in the Enterprise'

This white paper is structured to provide a practical hands-on guide for deploying WPA and WPA2 in the enterprise. Source and copyright is with the Wi-Fi Alliance. The white paper is available for download at http://www.wi-fi.org

