IM/IT Architecture & Standards Manual **STANDARD** **Office of the Chief Information Officer** **Province of British Columbia**	**Effective Date:** 2009-02-19 **Scheduled Review: Annual** **Last Updated:** 2012-03-01 **Last Reviewed:** 2012-03-01 **Type:** Technical

5.0 Information Technology Management (CPPM 12.3.5)

5.9 Technical Security Standard for Wireless Local Area Networks

Keywords: Standard, Technical, Wireless, Conceptual, Mobility, WLAN

Description of Standard

This standard describes the configuration parameters required for establishing a Secure Wireless Local Area Network, whether or not a device is directly connected to the SPAN/BC network.

The specifications documented here should be considered as Minimum Standards. If an implementer chooses a stronger option, it is permitted, but should be clearly noted in system documentation.

The National Institute of Standards and Technology Special Publication SP800-97, *Establishing Wireless Robust Security Networks: A guide to IEEE 802.11i*, has been used extensively in development of this technical specification document.

Group	**Topic**	**Current Standard**	**Comments / Rationale**
Wireless Network Architecture	Robust Security Network (RSN)	IEEE 802.11 RSN consisting of only RSN Associations established using the 4-way handshake.	Only Robust Security Networks, which consist of only RSN Associations, are permitted. No Pre-RSN configurations are permitted. The 4-way handshake is used to validate possession of PMKs, establish temporal keys and select cipher suites.
	Protocol	WPA2-Enterprise	WPA is only permitted until hardware can be upgraded to support WPA2 with AES encryption.
	Protocol	WEP protocol must be disabled on APs and STAs.	WEP is not a secure wireless protocol.
	Network architecture	Access points configured as Extended Service Sets or Basic Service Sets. (i.e., infrastructure mode mandaory)	Independent Basic Service Sets (Ad-hoc mode) must be disabled on stations and access points.
	Network architecture	Must use an Authentication Server for keys.	Pre-shared keys must not be used for authentication due to significant management overhead in complex

Group	Topic	Current Standard	Comments / Rationale
			deployments.
	Network architecture	Detection of Rogue APs mandatory	Implementation must be able to detect and disable unapproved APs.
	Network architecture	Connection between AP and AS must be encrypted.	To prevent interception or manipulation of keys
	Station configuration	STAs must be configured such that they authenticate to named servers only, and only accept certificates from the CA that signed the server certificates.	To prevent uncontrolled acceptance of invalid certificates
Access Control	Authentication	Station authentication using an Extensible Authentication Protocol (EAP) method based on Transport Layer Security (TLS), one of: **Preferred** • EAP-TLS • EAP-TTLS **Minimal** • LEAP* • PEAP	EAP-TLS methods require the use of an enterprise PKI, with certificates deployed to each STA. STAs should be configured to only allow approved EAP methods.
	Access control	IEEE 802.1x port-based access control	The combination of EAP and 802.1x together support the establishment of RSNAs.
	Mutual Authentication	Mutual authentication between STA and AP	Mutual authentication is used to minimize the risk of masquerading access points.
Cryptography & Key Management	Master Session Key / AAA key	MSK ≥ 256 bits	
	Pairwise Master Key	Maximum lifetime ≤8 hours PMK ≥ 256 bits	
	Group Master Key	Maximum lifetime ≤24 hours	
		GMK ≥ 128 bits (CCMP) GMK ≥ 256 bits (if using TKIP)	
	Transmission encryption	CCMP (with AES) Key ≥ 128 bits	

- There are known vulnerabilities related to LEAP.

Assumptions

- This standard applies to end-user devices, such as laptops, tablets and desktop workstations. This standard does not apply to ultra-mobile devices, such as PDAs and cell phones with wireless capability.
- This standard applies to wireless end-user devices that access information held within SPAN/BC.
- End-user and device-based authentication to the wireless network will be used (not user-based).
- The wireless network standard described here will only be used for known devices and users. Extensions may be developed and approved to accommodate guests, anonymous or public access.

- WPA using TKIP encryption is not permitted under the proposed standard. Organizations wishing to use WPA-Enterprise with TKIP must apply for an exception, using the process established by the GCIO.

Where to Apply This Standard

The standard is meant for SSBC, any ministry, other public agency or external service provider that is considering implementing a Secure Wireless Local Area Network that requires access to the SPAN/BC network.

Authority and Exemptions

This standard has been issued by the Office of the Chief Information Officer (OCIO) to minimize security exposures and maximize the privacy information traveling across the connected networks.

If there are compelling business reasons why an organization is unable to comply with this architecture or standard, the organization's CIO may authorize a submission for exemption through the ASB.

Metrics and Enforcement

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout Government. However, in order to effectively manage information security, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard. The OCIO Information Security Branch will also monitor for compliance.

Terms and Definitions

Any IM/IT security and network terminology found in this standard will be included in a consolidated Glossary, which is currently under development by the OCIO.

References

Information Security Policy

6.6 Communications and Operations Management – Network security management

6.6.1 A range of controls must be implemented to achieve and maintain security within the government network.

7.4 Access Control – Network access control

7.4.5 Groups of information services, users and information systems must be segregated on networks.

Additional Information

1. The OCIO is the owner of this standard. Its website is located at www.cio.gov.bc.ca
2. The full Architecture and Standard documentation can be found at: www.cio.gov.bc.ca/local/cio/standards/documents/standards/wlan_connectivity.pdf.
3. For wireless network security guidelines for non-government entities, please use the following guidelines:

   Wireless Local Area Network Assessment Checklist for Non-Government Entities Accessing Government Information which can be located at:

http://www.cio.gov.bc.ca/cio/standards/standards_manual.page

Contact

Architecture and Standards, OCIO

email: ASB.CIO@gov.bc.ca