Architecture and Standards

Submission for

Technical Security Standard and High Level Architecture for Wireless Local Area Network Connectivity

November 6, 2008
DRAFT v0.2

Copyright notice

Table of Contents

1 Foreword

Wireless standards to support Hospital PharmaNet Access were developed in the summer of 2008. The wireless standard was presented to the Architecture and Standards Review Board for recommendation for approval as a government standard.

As per the July 4, 2008 memo "Security Requirements for Wireless Connectivity" from the CIO (see Annex C), this standard was to be used as a guideline pending modified adoption as a broader standard of government. It currently serves as the wireless standards for Hospital Access to PharmaNet developed by the Ministry of Health Services. These standards were designed to be extended in the development of governemnt (SPAN connectivity) wireless local area network standards.

This package has the new high level (conceptual) architecture for Wireless Local Area Networks and well as an updated Wireless Local Area Networks Security Standard.

2 Introduction

The standard being proposed was jointly developed by Workplace Technology Services (WTS) and the Office of the Chief Information Officer (OCIO). It has been developed to accommodate transmission the most sensitive types of information of government.

A set of security control objectives and security controls for Secure Wireless Local Area Networks (WLANs) were developed with the PharmaNet wireless project and comprise the Secure WLAN Process standard.

In order to simplify and streamline the threat and vulnerability analysis process, the Process standard has been constructed in the format of the Information Security Forum Healthcheck. The standard takes the form of “answers” to each of the relevant Healthcheck questions.

This approach eliminates the need for implementers and security analysts to translate between different formats when conducting threat and vulnerability analysis using the ISF Information Risk Analysis Method (ISF IRAM) tool. The approach will lead to greater certainty and consistency in risk analysis.

The format of this standard has been carefully constructed to streamline and simplify compliance verification and security threat and vulnerability analysis.

The standards writers selected the subset of ISF Healthcheck questions that are relevant directly to WLAN. For each question, the control standard is stated in the form of the answer that is expected of the in-scope organization. When using this standard for compliance checking, documented evidence is required as indicated within the answer text.

This standard represents one of potentially several secure standards. Other standards may be developed and approved, as long as they meet the control objectives set out in the Process Standard.

The intent of this standard is for devices that connect within SPAN/BC. Devices that are part of a public sector organization or public sector service provider but outside of SPAN/BC (due to connectivity requirements to access systems within SPAN/BC) must also comply with this standard.

Non-public sector devices, such as access from home wireless systems, hotspots or kiosks are not covered by this standard. Extensions will be provided at a later date to address this type of wireless access.

The Secure WLAN standard is comprised of a Technical and Process standard.

Variations to the standard as proposed may require the Treat Risk Analysis being redone, depending on the changes being made.

2.1 Classification

The proposed standard and architecture is classified as follows:

Standard	Type	Nature	Review	Scope
Technical Security Standard for WLANs	Technical	Strategic	Annual	Laptops, tablets and desktops NOTE: Updated to reflect LEAP known vulnerabilities.
High Level Architecture for WLANs	Technical	Strategic	Annual	Laptops, tablets and desktops

3 Scope

This document applies to Ministries and WTS. It:

1. Specifies security controls configuration standards and high level architecture for Secure Wireless Local Area Networks (WLAN) that accommodates connectivity of public sector end user laptops, tablets and desktops on the SPAN/BC network; and
2. Describes the security controls in a format that is directly compatible with the Information Security Forum HealthCheck and Information Risk Analysis Method tools.

The standard does not apply to:

1. Ultra mobile devices such as PDAs and cell phones with wireless capability.
2. Connection of Non-public sector end user devices (guest networks).
3. Wireless Wide Area Network (WWAN) connectivity.
4. Printers, scanners and projectors.

4 Normative references

International Standards

- IEEE 802.11i - Reference standard for WLAN
- NIST SP800-97 - Establishing Wireless Robust Security Networks: A guide to IEEE 802.11i - Guidance for implementing secure WLAN

Standards Manual

- 6.0 Information Technology Security (CPPM 12.3.6)
- 6.4 Interim Standards for Information Systems Security and Network Connectivity

Information Management Standards

- Ministries must ensure all government information is managed in line with Government Core Policy Manual Chapter 12 Information Management and Information Technology Management 12.3.2 Information Management, http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm#1232. This includes Recorded Information Management, Information Utilization, Data Management and Forms Management.
- A proposed solution must meet the privacy requirements of the *Freedom of Information and Protection of Privacy Act* and Proponents must address any privacy concerns or impacts that are identified in the Privacy Impact Assessment.
- As part of the policy compliance, the province requires the solution provider to agree to meet the Province's security requirements as set out in 7.3 Security Clauses.

Normative references may be undated unless it is considered that future editions will not be applicable.

5 Terms and Definitions

Definitions may be found in NIST SP800-97 *Establishing Wireless Robust Security Networks: A guide to IEEE 802.11i*

For the purposes of this document, following acronyms apply.

RSN	Robust Security Network
RSNA	Robust Security Network Association
AP	Access Point
STA	Station (a wireless endpoint device)
AS	Authentication Server
EAP	Extensible Authentication Protocol
TLS	Transport Layer Security
BSS	Basic Service Set (infrastructure mode, where one or more STA's connects to an AP)
ESS	Extended Service Set (infrastructure mode, consisting of multiple BSS)
IBSS	Independent basic service set (ad hoc mode, allowing STA to STA networks)
AES	Advanced Encryption Standard
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
TKIP	Temporal Key Integrity Protocol
PMK	Pairwise Master Key
GMK	Group Master Key

6 Requirements

Wireless Local Area Networking standards formalization: Published Reference Standards do not exist for WLAN, affecting implementation of WLAN segments within SPAN/BC.

7 General characteristics

Only IEEE 802.11 Robust Security Networks (RSN) are permitted within SPAN/BC.

This generally means that WPA2-Enterprise WLAN deployments, using an EAP-TLS authentication method and 802.1x port-based network access control are required.

Note that a Certificate Authority or PKI infrastructure may be required in order to support manageable deployment of Station (device/client) certificates and Access Point certificates for mutual authentication.

Note that this Secure WLAN standard does not constrain the radio types (a/b/g/n) or other wireless technical options (site surveys) that are unrelated to security.

7.1 WLAN Characteristics and Technical Standard

Key elements for Secure WLAN are listed below:

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 PMK's, establish temporal keys and select cipher suites.
	Protocol	WPA2-Enterprise	WPA-Enterprise with TKIP may be permitted through the standards exception process until hardware can be upgraded to support WPA2 with AES encryption.
	Protocol	WEP protocol must be disabled on AP's and STA's	WEP is not a secure wireless protocol
	Network architecture	Access points configured as Extended Service Sets or Basic Service Sets (i.e. Infrastructure mode mandatory)	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 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 • PEAP **Not-Preferred** • LEAP (pending vendor resolution of security issues)	EAP-TLS methods require the use of a Certificate Authority or 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 RSNA's
	Mutual Authentication	Mutual authentication between STA and AP	Mutual authentication is used to minimize 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	

7.2 Security Control Objectives and Process Standard

A set of security control objectives and security controls for Secure WLAN have been developed and comprise the Secure WLAN Process standard.

In order to simplify and streamline the threat and vulnerability analysis process, the Process standard has been constructed in the format of the Information Security Forum Healthcheck. The standard takes the form of “answers” to each of the relevant Healthcheck questions.

This approach eliminates the need for implementers and security analysts to translate between different formats when conducting threat and vulnerability analysis using the ISF Information Risk Analysis Method (ISF IRAM) tool. The approach will lead to greater certainty and consistency in risk analysis.

The security control objectives that must be met by Secure WLAN security controls are:

#	**Secure WLAN Control Objective**
1	An ‘information security architecture’ should be established, which provides a framework for the application of standard security controls throughout the enterprise.
2	Only software and hardware which has been generally proven to be reliable and robust should be used. All hardware and software must be recorded in an inventory.
3	All buildings within the enterprise that house critical IT facilities (e.g. data centres, network facilities and key user areas) should be physically protected against accident or attack.
4	Critical computer equipment and facilities should be protected against power outages.
5	Computer equipment and facilities should be protected against fire, flood, environmental and other natural hazards.
6	Critical applications should be run on robust, reliable hardware and software, supported by alternative or duplicate facilities.
7	The network should be designed to cope with current and predicted levels of traffic and be protected using a range of in-built security controls.
8	Systems should be configured to provide authorized functionality, and to prevent unauthorised or incorrect updates or elevated access to unauthorized users.
9	Workstations connected to systems within the computer installation should be purchased from a list of approved suppliers, tested prior to use, supported by maintenance arrangements and protected by physical controls.
10	Network devices should be configured to provide authorized functionality, and to prevent unauthorised or incorrect updates.
11	Networks should be supported by accurate, up-to-date documentation.
12	Access control arrangements should be established to restrict access by all types of user to approved system capabilities of the computer installation.
13	All users of the computer installation should be authorised using documented procedures before they are granted access privileges.
14	All users should be authenticated by using UserIDs and passwords or by strong authentication mechanisms (e.g. smartcards or biometric devices, such as fingerprint recognition) before they can gain access to target systems.
15	Logs of all key events within the computer installation should be maintained (preferably using automated tools), reviewed periodically and protected against unauthorised change.
16	Key network activities should be monitored.
17	Virus protection arrangements should be established, and maintained enterprise-wide.

18	Intrusion detection mechanisms should be applied to critical systems and networks.
19	Network traffic should be routed through a firewall, prior to being allowed access to the network.
20	Wireless access should be authorised, authenticated, encrypted and permitted only from approved locations/devices.
21	Cryptographic keys should be managed tightly, in accordance with documented standards/ procedures, and protected against unauthorised access or destruction.
22	Any public key infrastructure (PKI) used by the application should be protected by 'hardening' the underlying operating system(s) and restricting access to Certification Authorities.
23	Sensitive information held on data storage media (including magnetic tapes, disks, printed results and stationery) must be protected against corruption, loss or disclosure.
24	Robust, reliable hardware and software should be acquired, following consideration of security requirements and identification of any security deficiencies.

7.3 High Level Architecture

This architecture describes a design for establishing a Secure Wireless Local Area Network. The model allows for 3 classes of devices to gain access to SPAN wireless services:

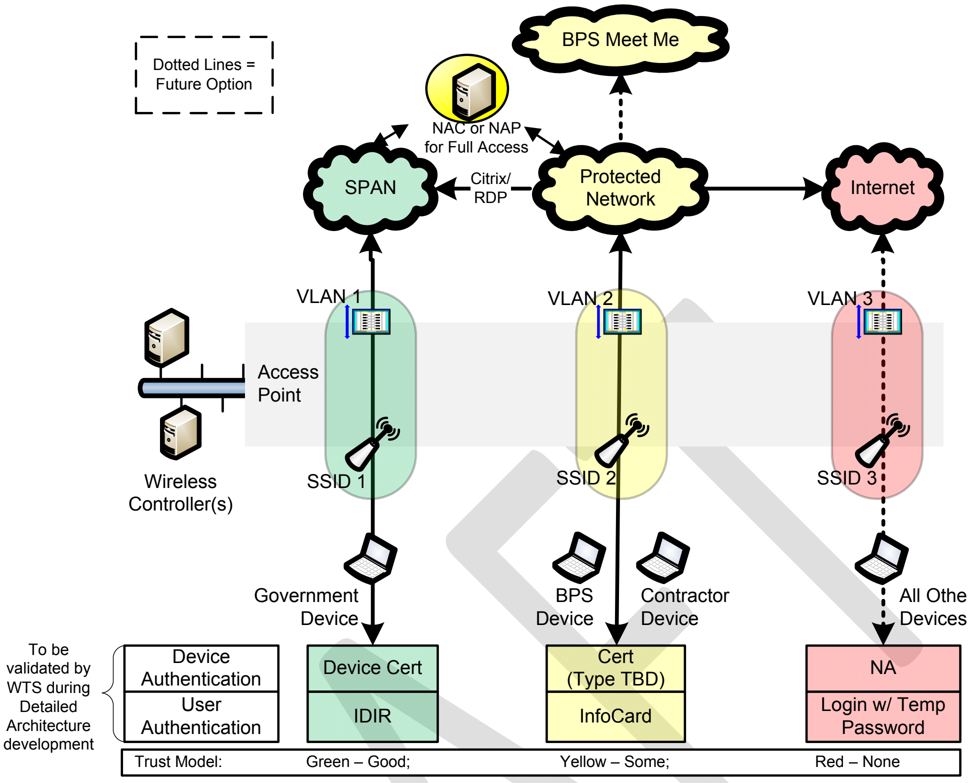
1. **Trusted devices**: Core government managed devices have direct secure access onto the SPAN network (green below).
2. **Semi-Trusted Devices**: Broader public sector devices (as an example), are given access to a protected area, from which they can securely access their own or other private network spaces (yellow below). This may include contractors and consults under contract to the government.
3. **Un-trusted Devices**: Devices which the government cannot exert control (physically or by policy or contract) over or those devices that pose indeterminate risk are given access to the Internet (red below). Example: vendors that require access in order to provide on-site presentations.

Under all scenarios access is controlled. This may be through by either device certificates and/or user passwords. Smart Cards may also be a future option for authentication.

Access from the protected network back into SPAN will be through Citrix or RDP. Upon the availability of a Network Access Protection/Network Access Control capability, direct access may be allowed.

The lower section of the diagram will be finalized once detailed architectural design and vendor select is complete, as some capabilities may vary with the final vendor solution.

A complete description can be found in Annex B – WLAN High Level Architecture.



To be validated by WTS during Detailed Architecture development

Device Authentication	Device Cert	Cert (Type TBD)	NA
User Authentication	IDIR	InfoCard	Login w/ Temp Password
Trust Model:	Green – Good;	Yellow – Some;	Red – None

7.4 Information characteristics

In all cases WLAN implementations must assume that information being transmitted on the WLAN is of the highest security classification. Implementers cannot assume that compensating controls are in place to protect the information. For example, do not assume that the transmitted information is encrypted by the originator.

8 Evaluation criteria

This technical, process and reference standard set for secure WLAN makes assumptions regarding the existence of certain technologies such as WPA2-Enterprise certified equipment, enterprise PKI infrastructure, and inclusion of the WLAN in the non-public side of the SPAN/BC network.

During the Wireless Hospital Access to PharmaNet project, an efficient, standards based, evaluation approach was developed, and is described below. The evaluation approach is used for evaluating implementations for compliance to the standard, and for determination of the impacts of variances.

The objective of the evaluation approach was to eliminate the need to conduct a full IRAM for each wireless implementation, since IRAM is comprehensive and requires much work. This approach shifts the effort from intensive analysis to simple compliance checking.

The wireless standard has been written in the format of the ISF Healthcheck tool, in order to allow assessors to quickly check for conformance. If specific non-conformant items are found, these items can be traced directly through the IRAM tool to determine any impacts on overall risk.

Note: this evaluation approach may be replaced with processes developed by the OCIO Architecture and Standards Review Board.

Step	Process	Decision
1. OCIO publishes Secure WLAN Standard, consisting of Technical and Process standards	• Technical standard is a set of configuration items • Process standard is a set of "Expected Answers" to ISF Healthcheck questions	n/a
2. Organization compares actual implementation to standard	• Compare proposed implementation to Secure WLAN Process Standard to determine points of variance • Compare proposed implementation to Secure WLAN Technical Standard to determine points of variance	Determine if variances are material. Note that variance may be due to implementation of stronger controls or compensating controls. If no variance, implementation is compliant.
3. Conduct full IRAM if material variances found in step 2	• Conduct a full IRAM process to determine risks • Submit STRA report for approval	Treat risks as determined by IRAM STRA

8.1 Enquiry Scope

Extensive consultation and collaboration has been undertaken between the Ministry of Health, Vancouver Island Health Authority, the OCIO Information Security Branch and the OCIO Architecture & Standards Branch in the development of this standard. Since the wireless end user device connections are not within SPAN/BC, WTS was not directly involved but were advised of the project and provided with updates as made available.

8.2 Analysis/Acceptance

The OCIO Information Security Branch and Architecture and Standards Branch are in agreement with the contents of this document. Additionally the Ministry of Health is in acceptance with the contents.

8.3 Response

The inclusion of ISO as a standards basis was positively accepted.

8.4 Packaging

The standard as proposed for the Standard Manual is contained in Annex A and Annex B.

9 Bibliography

CORE POLICY MANUAL 12 Information Management and Information Technology Management, http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm#1234 .

Annex A. Technical Security Standard for Wireless Local Area Networks

IM/IT Standards Manual	**Effective Date**: **Scheduled Review**:
Office of the Chief Information Officer **Province of British Columbia**	**Type:** Technical Standard
5.0 Information Technology Management (CPPM 12.3.5)	
5.1 Technical Security Standard for Wireless Local Area Networks	

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 PSN/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 PMK's, 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 AP's 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 mandatory)	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** **Minimal** • EAP-TLS • LEAP* • EAP-TTLS • 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 RSNA's
	Mutual Authentication	Mutual authentication between STA and AP	Mutual authentication is used to minimize 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 be only 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 Standard is Used

The standard is meant for WTS, 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 Exceptions

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 is a compelling business reason wireless networks should not or could not make use of this standard, the information systems director must address his or her concerns to the OCIO through a Request for Exception.

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

The OCIO is the owner of this standard. Its website is located at www.cio.gov.bc.ca .

Contact

Architecture and Standards Branch, OCIO

Annex B. High Level Architecture for Wireless Local Area Networks

IM/IT Standards Manual	**Effective Date**: January 2009 **Scheduled Review**: TBD
Office of the Chief Information Officer **Province of British Columbia**	**Tags:** Architecture, Technical, Wireless, Conceptual, Mobility, WLAN
5.0 Information Technology Management (CPPM 12.3.5)	
5.x High Level Architecture for Wireless Local Area Networks	

Summary

The architecture presented in this document is classified as technical. It is conceptual in nature and vendor agnostic. Being vendor agnostic this model can be implemented under a variety of vendor solutions. It is meant to provide guidance in the downstream development of detailed architectures and the selection of vendor solutions.

Authorship

This architecture was developed by the OCIO (owner) in consultation with WTS.

The OCIO is responsible for its content.

Business Context

The purpose of this architecture is to provide a conceptual view of core government wireless services and supports further development of detailed architecture. It supports IMIT strategies for information sharing, improved secured access for a variety of client types and support for an increasing mobile workforce. Similar design has been implemented in other jurisdictions and proven to be effective. The risks associated with this design are minimal.

ASDLC Requirements

This architecture should be reviewed upon completion of detailed architectural design and solution selection, and every 3 years thereafter. The OCIO or WTS may both request update to this architecture.

Viewpoint

The viewpoint is “strategic planner”. It is long term and conceptual. Related projects include the WTS Wi-Building project. The design aligns with existing security policy.

State

There is no preceding conceptual architecture. This model will be used in the WTS Wi-Building Service which should be available in the 2009/10 fiscal year.

Description of the Architecture

This architecture describes a design for establishing a Secure Wireless Local Area Network. The model allows for 3 classes of devices to gain access to SPAN wireless services:

4. **Trusted devices**: Core government managed devices have direct secure access onto the SPAN network (green below).

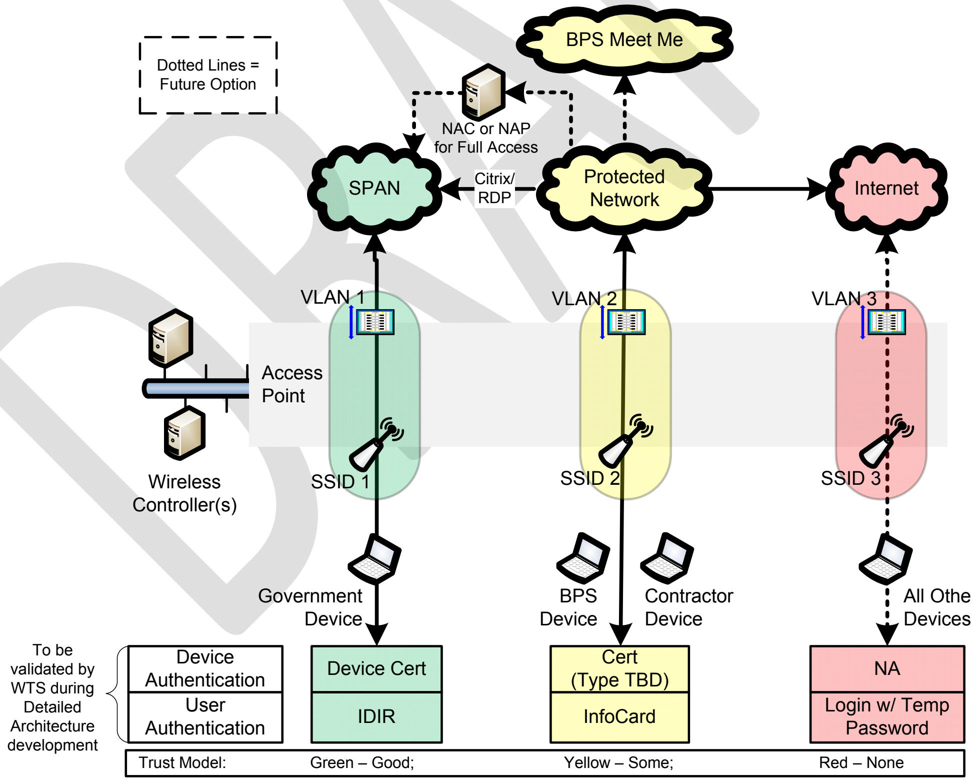
5. **Semi-Trusted Devices**: Broader public sector devices (as an example), are given access to a protected area, from which they can securely access their own or other private network spaces (yellow below). This may include contractors and consults under contract to the government.

6. **Un-trusted Devices**: Devices which the government cannot exert control (physically or by policy or contract) over or those devices that pose indeterminate risk are given access to the Internet (red below). Example: vendors that require access in order to provide on-site presentations.

Under all scenarios access is controlled. This may be through by either device certificates and/or user passwords. Smart Cards may also be a future option for authentication.

Access from the protected network back into SPAN will be through Citrix or RDP. Upon the availability of a Network Access Protection/Network Access Control capability, direct access may be allowed.

The lower section of the diagram will be finalized once detailed architectural design and vendor select is complete, as some capabilities may vary with the final vendor solution.



Annex C. Memo - Security Requirements for Wireless Connectivity

Ref: 51876

Date: July 4, 2008

To: Chief Information Officer Council

Re: **Security Requirements for Wireless Connectivity**

During the past few months, the Office of the Auditor General carried out a review of wireless network security within the government. The findings revealed a number of unsecured wireless access points in or near the Province of British Columbia (Province) government offices. The field work was done by scanning the areas surrounding government buildings in "war driving" mode as close as possible to the location on roads, parking lots and at a one block radius around each site. Wireless access points with weak encryption or no encryption at all were detected.

Although the report does not specify whether the identified unsecured wireless access points are connected to the government network, I am requesting that each ministry take necessary steps to secure all wireless networks they have across the Province and report back to the Office of the Chief Information Officer when this task is complete. The Office of the Auditor General will be conducting a more thorough and in-depth scan of wireless connectivity in various areas of the Province in six months and preparing a report for the Legislative Assembly on the assessment of wireless security of the government network.

The protection of the information held by government is of utmost importance to us. It is also our duty to ensure that appropriate security controls and safeguards are in place to protect government information. Chapter 6.6.1 d) in the Information Security Policy lists the controls required for wireless local area networks:

- Strong link layer encryption, such as Wi-Fi Protected Access;
- User and device network access controlled by government authentication services;
- The use of strong, frequently changed, automatically expiring encryption keys and passwords;
- Segregation of wireless networks from wired networks by the use of filters, firewalls or proxies; and,
- Port-based access control, for example use of 802.1x technology.

Unsecured wireless access points are in violation of this policy and pose a risk to the security of government information. The Architecture and Standards Branch of the Office of the Chief Information Officer is developing a standard for wireless local area networks that will address security related issues. In the interim, the wireless standard for Hospital Access to Pharmanet developed by the Ministry of Health Services, can be used as a guideline. This standard will be available mid-July of 2008.

Thank you for your cooperation and immediate attention to this important matter.

"Original signed by"

Dave Nikolejsin

Chief Information Officer