Defence Research and Development Canada
Recherche et développement pour la défense Canada

# Securing Wireless Local Area Networks with GoC PKI

J. Spagnolo and D. Cayer

The scientific or technical validity of this Contract Report is entirely the responsibility of the contractor and the contents do not necessarily have the approval or endorsement of Defence R&D Canada.

**Defence R&D Canada – Ottawa**
CONTRACT REPORT
DRDC Ottawa CR 2007-239
October 2007

# Securing Wireless Local Area Networks with GoC PKI

J. Spagnolo
D. Cayer

Prepared by:

NRNS Incorporated
4043 Carling Avenue
Suite 106
Ottawa, Ontario, K2K 2A3

Project Manager: Joe Spagnolo, 613-599-7860
Contract number: W7714 – 030800 / 001 / SV
Contract Scientific Authority: Mazda Salmanian, P.Eng., 613-998-0649

The scientific or technical validity of this Contract Report is entirely the responsibility of the contractor and the contents do not necessarily have the approval or endorsement of Defence R&D Canada.

## Defence R&D Canada – Ottawa

Contract Report
DRDC Ottawa CR 2007-239
October 2007

Scientific Authority

*Originally signed by Mazda Salmanian*

Mazda Salmanian
Defence Scientist, Secure Mobile Networking Group

Approved by

*Originally signed by Julie Lefebvre*

Julie Lefebvre
Head, Network Information Operations Section

Approved for release by

*Originally signed by Pierre Lavoie*

Pierre Lavoie
Chairman, Document Review Panel

# Abstract

Defence R&D Canada led a project in which a wireless virtual private networking (VPN) architecture was set up in a test bed in the Network Information Operation (NIO) lab for 802.11/a/b/g communications. The goal of this initial work was to aid in developing a security policy for use of wireless local area networks (WLAN) in government enterprise networks. This report presents the results of follow-on work that leverages the Government of Canada (GoC) Public Key Infrastructure (PKI) technology for strong authentication of wireless users as well VPN users. The solution presented herein relies on the latest wireless security protocols to secure the wireless link and includes an Internet Protocol Security (IPsec) based VPN to achieve a greater level of assurance for more sensitive GoC network environments. The work focuses on the establishment and protection of digital identities, mutual authentication, authorization, data privacy and integrity, as well as wireless network policy management and dissemination.

We conclude that the Wi-Fi Protected Access 2 (WPA2) when operating in enterprise mode and combined with GoC PKI issued certificates and wireless network policy managed through Windows group policies, is an acceptable solution for providing authenticated/secure WLAN access to GoC protected environments. We also conclude that layering IPsec security on top of WPA2 adds complexity without providing additional assurance against unauthorized WLAN access. While testing the proposed solution, difficulties were encountered integrating the IPsec VPN component of the wireless VPN within an enterprise Microsoft Windows environment.

# Résumé

R & D pour la défense a dirigé un projet dans le cadre duquel on a créé une architecture de réseau privé virtuel (RPV) sans fil sur un banc d’essai dans le laboratoire des Opérations d'information de réseau (OIR) pour des communications 802.11/a/b/g. L’objectif visé par ces travaux préliminaires était d’aider à développer une politique de sécurité pour les réseaux locaux sans fil (WLAN) dans les réseaux d’entreprise du gouvernement. Dans ce rapport, on présente les résultats de travaux complémentaires qui tirent profit de la technologie d’infrastructure à clé publique (ICP) du Gouvernement du Canada (GC) pour une authentification forte des utilisateurs d’appareils sans fil, ainsi que les utilisateurs de RPV. La solution présentée ici repose sur les tout derniers protocoles de sécurité sans fil pour protéger la liaison sans fil et elle inclut un RPV basé sur Internet Protocol Security (IPsec) pour obtenir un niveau d’assurance plus élevé pour les environnements de réseau sensibles du GC. Les travaux portent surtout sur l’établissement et la protection des identités numériques, l’authentification mutuelle, l’autorisation, la protection et l’intégrité des données, ainsi que la gestion et la diffusion des politiques sur les réseaux sans fil.

Nous avons conclu que le chiffrement Wi-Fi Protected Access 2 (WPA2) est une solution acceptable pour fournir un accès authentifié/protégé par WLAN aux environnements protégés du GC lorsqu’il fonctionne en mode entreprise et qu’il est combiné à des certificats délivrés par l’ICP du GC et à une politique sur les réseaux sans fil gérée par des politiques de groupe dans Windows. Nous avons aussi conclu que la structuration en couches de la sécurité IPsec sur le chiffrement WPA2 accroît la complexité sans donner d’assurance additionnelle contre l’accès non autorisé aux WLAN. Pendant la mise à l'essai de la solution proposée, nous avons eu des difficultés à intégrer la composante RPV IPsec du RPV sans fil dans un environnement d'entreprise Microsoft Windows.

# Executive summary

## Securing Wireless Local Area Networks with GoC PKI

**Spagnolo, J., Cayer, D.; DRDC Ottawa CR 2007-239; Defence R&D Canada – Ottawa; October 2007.**

## Introduction or background

Defence R&D Canada led a project in which a wireless virtual private networking (VPN) architecture was set up in a test bed in the Network Information Operation (NIO) lab for 802.11/a/b/g communications. The goal of this initial work was to aid in developing a security policy for use of wireless local area networks (WLAN) in government enterprise networks. This report presents the results of follow-on work that leverages the Government of Canada (GoC) Public Key Infrastructure (PKI) technology for strong authentication of wireless users as well VPN users. The solution presented herein relies on the latest wireless security protocols to secure the wireless link and includes an Internet Protocol Security (IPsec) based VPN to achieve a greater level of assurance for more sensitive GoC network environments. The work focuses on the establishment and protection of digital identities, mutual authentication, authorization as well as wireless network policy management and dissemination.

## Results

Wi-Fi Protected Access (WPA and WPA2) provides industry standard means to connect wireless devices to GoC protected network environments. Their underlying cryptographic algorithms exhibit no known vulnerabilities and provide highly effective privacy and data integrity, but WPA2 offers superior cryptographic strength and is better suited for protected GoC networks.

For higher classification environments such as Protected-B, a deployment may layer an IPsec compliant VPN tunnel on the WPA2 secured wireless link. The VPN gateway carries out VPN authentication with the same user certificates used to perform WLAN authentication. In order to permit the computer to log onto to the Windows domain and download group policies, the VPN gateway must be configured to pass non-VPN traffic through a VPN gateway. This lowers the level of assurance associated with the VPN gateway since the VPN gateway must expose parts of the protected network.

We conclude that WPA2 when operating in enterprise mode and combined with GoC PKI issued certificates and wireless network policy managed through Windows group policies, is an acceptable solution for providing authenticated/secure WLAN access to GoC protected environments. We also conclude that layering IPsec security on top of WPA2 adds complexity without providing additional assurance against unauthorized WLAN access – especially if the VPN gateway must pass non-VPN traffic. If the solution relies on WPA2 to protect the VPN gateway from unauthorized access by non-VPN traffic, then the VPN gateway should not form part of the solution.

If IPsec is deemed necessary for higher classification network environments, the final solution could consider the use of the native Windows IPsec implementation to establish an operating system level VPN using computer credentials (issued from the GoC PKI) instead of user credentials. This may permit the computer to establish the VPN prior to attempting the domain logon and the downloading of the group policies.

# Sommaire

## Securing Wireless Local Area Networks with GoC PKI

**Spagnolo, J., Cayer, D.; DRDC Ottawa CR 2007-239; R & D pour la défense Canada – Ottawa; October 2007.**

## Introduction ou contexte

R & D pour la défense a dirigé un projet dans le cadre duquel on a créé une architecture de réseau privé virtuel (RPV) sans fil sur un banc d’essai dans le laboratoire des Opérations d'information de réseau (OIR) pour des communications 802.11/a/b/g. L’objectif visé par ces travaux préliminaires était d’aider à développer une politique de sécurité pour les réseaux locaux sans fil (WLAN) dans les réseaux d’entreprise du gouvernement. Dans ce rapport, on présente les résultats de travaux complémentaires qui tirent profit de la technologie d’infrastructure à clé publique (ICP) du Gouvernement du Canada (GC) pour une authentification forte des utilisateurs d’appareils sans fil, ainsi que les utilisateurs de RPV. La solution présentée ici repose sur les tout derniers protocoles de sécurité sans fil pour protéger la liaison sans fil et elle inclut un RPV basé sur Internet Protocol Security (IPsec) pour obtenir un niveau d’assurance plus élevé pour les environnements de réseau sensibles du GC. Les travaux portent surtout sur l’établissement et la protection des identités numériques, l’authentification mutuelle, l’autorisation, la protection et l’intégrité des données, ainsi que la gestion et la diffusion des politiques sur les réseaux sans fil.

## Résultats

Le chiffrement Wi-Fi Protected Access (WPA et WPA2) est une norme de l’industrie qui permet de relier des appareils sans fil aux environnements de réseau protégés du GC. Leurs algorithmes cryptographiques sous-jacents ne présentent aucune vulnérabilité connue et ils offrent une protection et une intégrité des données très efficaces, mais le chiffrement WPA2 offre une cryptographie plus forte et il convient mieux aux réseaux protégés du GC.

Pour les environnements de classification supérieurs, comme les environnements Protégé B, un déploiement peut ajouter un tunnel RPV IPsec sous forme de couche à la liaison protégée sans fil WPA2. La passerelle RPV effectue l’authentification RPV avec les mêmes certificats d’utilisateurs que ceux utilisés pour l’authentification WLAN. Pour que l’ordinateur puisse ouvrir une session dans le domaine Windows et télécharger les politiques de groupe, il faut configurer la passerelle RPV de façon à ce qu’elle puisse acheminer du trafic non RPV. Cela réduit le niveau d’assurance associé à la passerelle RPV étant donné que cette dernière doit permettre l’accès à des parties du réseau protégé.

Nous avons conclu que le chiffrement WPA2 est une solution acceptable pour fournir un accès authentifié/protégé par WLAN aux environnements protégés du GC lorsqu’il fonctionne en mode entreprise mode et qu’il est combiné à des certificats délivrés par l’ICP du GC et à une politique sur les réseaux sans fil gérée par des politiques de groupe dans Windows. Nous avons aussi conclu que la structuration en couches de la sécurité IPsec sur le chiffrement WPA2 accroît la

complexité sans donner d'assurance additionnelle contre l'accès non autorisé aux WLAN – surtout si la passerelle RPV doit acheminer du trafic non RPV. Si la solution fait appel au chiffrement WPA2 pour protéger la passerelle RPV contre l'accès non autorisé par du trafic non RPV, la passerelle RPV ne doit pas faire partie de la solution.

Si l'on estime que IPsec est nécessaire pour les environnements de réseau à niveau de classification supérieur, il faut envisager, pour la solution finale, l'utilisation de la mise en œuvre native d'IPsec de Windows pour établir un RPV au niveau du système d'exploitation à l'aide de preuves d'identification d'ordinateur (délivrées par l'ICP du GC) au lieu de preuves d'identification d'utilisateur. Cela pourrait permettre à l'ordinateur d'établir le RPV avant d'essayer d'ouvrir une session dans le domaine et de télécharger les politiques de groupe.

# Table of contents

# List of figures

This page intentionally left blank.

# 1. Introduction

Defence R&D Canada (DRDC) led a project in which a wireless virtual private networking (VPN) architecture was set up in a test bed in the Network Information Operation (NIO) lab for 802.11/a/b/g communications. The security of the architecture and the related protocols were analyzed and documented in TM 2006-124 [1]. In an effort to aid in developing a security policy for use of WLANs in government enterprise networks, the NIO section made a formal request to attach the test bed to NIO's live Information Operations Research & Development Network (IORDN) to demonstrate a secure wireless local area networking (WLAN) extension to the wired network. The response from the Defence Research Establishment Network (DREnet) Management was to use the Government of Canada (GoC) approved Entrust public key infrastructure (PKI) technology instead of the Microsoft native PKI for VPN authentication. Furthermore, DREnet Management recommended that the certificates used to authenticate the VPN be tightly bound to a user and possibly stored on a smart card or token instead of loosely bound to a computer system. This recommendation made for a more sound architecture, one that Communications Security Establishment (CSE) potentially may certify for use GoC protected networks.

# 2. Scope of Work

The original requirement was simply to improve Internet Security (IPsec) [2] protocol authentication with the use GoC PKI issued user certificates instead of Microsoft native PKI issued computer certificates. In the process of examining the original architecture described in TM 2006-124 [1], we noted that we could leverage the GoC PKI to authenticate users to the WLAN as well as to the IPsec VPN. After discussion with the Scientific Authority, the scope of the work was expanded to also address WLAN authentication.

This report describes a layered wireless network solution for potential use in GoC protected network environments such as Protected-A or Protected-B. The work examines the use of GoC PKI certificates to regulate user access to the WLAN and to the IPsec based VPN. We focus our attention on the establishment and protection of digital identities, mutual authentication, authorization, data privacy and integrity, as well as wireless network policy management and dissemination. We ignore wireless network availability issues such as denial-of-service attacks against wireless computers.

# 3. Strong Authentication

The GoC PKI[1] binds an entity such as a system, user or an application process to a digital identity in a form of a certificate. In the case of a digital signature certificate, the certificate subscriber possesses the sole copy of the associated private key used to prove the digital identity to another entity such as an authentication server. The GoC approved cryptographic algorithms used to implement digital signatures have been vetted by government organizations and are deemed to be secure. It is practically impossible to impersonate a digital identity without possession of the associated private signing key. However, it is important to note that a PKI's level of assurance is dependent on the processes used to generate, store and manage private keys as well as on the work flows that govern the issuance of certificates associated with those keys. A low assurance PKI may store private keys on disk files protected by weak passwords and may employ a self-serve web application to issue certificates to subscribers based on the requestor's knowledge of easily obtainable information such as a birth date. A high assurance PKI may generate and store private keys on hardware tokens protected by biometrics and may require that the subscriber present herself in person to prove her identity with government issued photo identification.

Organizations follow a well defined registration processes when issuing GoC PKI credentials to users within the organization. The Local Registration Authority (LRA) must verify the identity of the user before the user can enrol in the GoC PKI and acquire digital credentials. When the user leaves the organization or when a private key is lost, stolen or suspected of compromise, the associated public certificate is revoked by the certificate authority. Revocation information informs the relying party that it should no longer trust a previously issued and currently valid certificate.

GoC PKI issued digital credentials deliver strong authentication based on digital signatures or encryption. Authentication is further strengthened when the solution includes a smart card or hardware token that holds and protects the private keys associated with the digital credentials. This stronger two-factor authentication requires that the authenticating entity (i.e. the user) have two components in its possession: physical access to the smart card that holds the private keys; and knowledge of the password that unlocks the smart card in order to perform private key operations. An attacker must acquire possession of both components to steal the digital identity.

The establishment and maintenance of a GoC PKI is very expensive in terms of infrastructure and manpower. To achieve a high return on investment (ROI) for a PKI, the organization must integrate GoC PKI digital credentials within numerous systems and applications instead of maintaining several single-purpose identity management solutions. GoC PKI digital credentials can be used for single sign-on, secure email, file encryption, secure web access, VPN authentication and WLAN authentication.

[1] The GoC PKI is based on PKI software from Entrust Inc.

# 4. Solution Overview

The original solution documented in TM 2006-124 [1] dismissed the wireless link as insecure and instead relied on IPsec based security to establish a secure channel between the wireless computer and the wireless access point (AP), which also included an embedded IPsec based VPN gateway capability. The wireless computer used a Microsoft native PKI issued computer certificate to authenticate the security association between the wireless computer and the AP. The original solution also employed a Layer 2 Tunnelling Protocol (L2TP) Point-to-Point Protocol (PPP) tunnel embedded within the IPsec security association to authenticate the computer user using Active Directory username/password based credentials.

The solution presented in this document uses GoC PKI issued certificates to authenticate computers and users to the WLAN as well as the IPsec VPN. The WLAN authentication portion of the solution is based on an Entrust Integration Guide [3] originally published in 2004. Our solution relies on the latest wireless security protocols to secure the wireless link. The solution also layers an IPsec VPN within the secure wireless link to achieve a greater level of assurance for more sensitive GoC network environments.

## 4.1 Standards

The solution makes extensive use of standards from the Wi-Fi Alliance, the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronic Engineers (IEEE), the International Telecommunication Union (ITU), and the Federal Information Processing Standards (FIPS).

### 4.1.1 Wireless Standards

The wireless products that form part of the solution conform to the IEEE 802.11 [4] wireless local area network (WLAN) standard. 802.11b provides 11 Mbps of shared WLAN access, while the 802.11g provides 54 Mbps of shared WLAN access. Although the 802.11 standard primarily defines a medium access control (MAC) and several physical layer (PHY) specifications for wireless connectivity, it also specifies wireless security protocols. The original wireless security protocol, Wire Equivalent Privacy (WEP), is extremely insecure and provides no privacy whatsoever. IEEE has since defined 802.11i as the new wireless security standard. 802.11i makes use of cryptographic standards such as the Temporal Key Integrity Protocol (TKIP) with Message Integrity Check (MIC), and the counter mode (CTR) with cipher-block chaining message authentication code (CBC-MAC) Protocol (CCMP). CCMP is based on the Advanced Encryption Standard (AES) encryption algorithm.

The Wi-Fi Alliance compiled two wireless security standards that implement a subset of the 802.11i standard. The Wi-Fi Protected Access (WPA) [5] standard augments wireless privacy and integrity with the use of the TKIP with MIC. WPA2 [5] provides superior security with the CCMP and AES. Wireless devices typically can be enhanced to support WPA with a firmware/software upgrade. An upgrade of the wireless hardware is needed to support for WPA2 and its AES based encryption. Unlike WEP, which does not include an authentication mechanism and relies on a single shared static key, WPA and WPA2 include an authentication mechanism and support per-user, per-session, per-packet encryption.

WPA and WPA2 support two modes of operation: Personal Mode and Enterprise Mode. Personal mode makes use of a pre shared key (PSK) to authenticate users. The key is known and shared by all users, which presents management challenges since the wireless configuration must be modified on all devices in order to change the PSK. Enterprise mode leverages the IEEE 802.1X network authentication and access control framework, which uses the Extensible Authentication Protocol (EAP) [8] to implement different types of authentication. The Transport Layer Security EAP type (EAP-TLS) [9] supports certificate based authentication for mutual authentication of the wireless device and the authentication server, and implements TLS standard key exchange methods for establishing the symmetric key material to encrypt and protect the data exchanged between the wireless device and the AP.

WPA and WPA2 enterprise mode requires a back-end authentication service that is typically provided by an implementation of the Remote Authentication Dial-In User Service (RADIUS) [10]. A Wi-Fi certified enterprise access point (AP) operates two logical ports to the wired network. When a wireless node connects to the AP, only the uncontrolled port is active – which only permits communication between the AP and the backend RADIUS server in order to authenticate the wireless node. If the RADIUS server grants WLAN access to the authenticated wireless node, the AP enables the controlled port – which provides the wireless node unrestricted access to the wired network.

WPA and WPA2 employ the same cryptographic algorithms for both personal and enterprise mode. The TKIP-MIC and AES-CCMP algorithms provide strong encryption and integrity and both are free of any known vulnerabilities. However, the effectiveness of the underlying cryptographic algorithms is entirely dependent on the generation and handling of the cryptographic key material. Any static password based scheme dependent on hash-based credential exchange is susceptible to an off-line brute force attack against the captured hash.

### 4.1.2 Public Key Infrastructure Standards

A Certificate Authority (CA) issues X.509 certificates to subscribers, which can be individuals (people) or devices. A certificate contains the public portion of a public/private key pair and can serve as an encryption certificate, verification certificate or both. The verification certificate is used to authenticate entities by verifying the digital signature generated by a corresponding private signing key.

Certificate enrolment protocols provide individuals and devices a means to request certificates from the CA. These protocols include on-line protocols such as the PKIX (Public-Key Infrastructure X.509) Certificate Management Protocol (CMP) [15] and the Simple Certificate Enrollment Protocol (SCEP) [16] as well as off-line schemes such as the exchange of Public Key Cryptography Standard (PKCS) #10 encoded certificate signing requests (CSR) and PKCS #7 encoded certificate chains.

A CA must revoke a certificate when the corresponding private key is lost, stolen, or compromised. The CA stores revocation information within a Certificate Revocation List (CRL) that an entity can retrieve from the certificate repository using a directory access protocol such as the Lightweight Directory Access Protocol (LDAP) [17].

### 4.1.3 Virtual Private Network Standards

The IETF defines a suite of protocols called IPsec [2] for securing Internet Protocol (IP) communications. IPsec specifies both key management protocols and data security protocols.

The Internet Security Association and Key Management Protocol (ISAKMP) [18] provides a framework for authenticating peers and exchanging cryptographic key material. ISAKMP simply defines the framework and is key exchange independent. The Internet Key Exchange (IKE) [19] protocol implements the ISAKMP framework to authenticate peers and obtain dynamic keying material for security associations. IKE supports various form of authentication include pre shared keys (PSK) and digital signatures with the use of digital certificates.

The Encapsulated Security Payload (ESP) [20] protocol provides confidentiality, data origin authentication and data integrity to IP traffic flows. ESP can operate in transport or tunnel mode. Transport mode secures traffic between two IPsec peers but does not conceal the identity of the communicating end-points. Tunnel mode secures traffic between an IPsec end-point and a security gateway or between two security gateways. Tunnel mode wraps the original IP packet within the outer packet used to communicate between the IPsec end-points. The original (inner) IP packet is encrypted to conceal the identity of the communicating end-points and optionally authenticated to ensure the integrity of both the inner IP packet header, which identifies the communicating end-points, and the payload.

## 4.2 Hardware/Software Components

This section describes the hardware and software components that form part of the solution.

### 4.2.1 Microsoft Server 2003 with Active Directory

Microsoft Server 2003 provides the underlying operating system for the Microsoft Domain Controller, Active Directory, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP) services. The Domain Controller provides authentication services necessary for computers and users to perform a Windows domain logon. Active Directory, which uses LDAP as its directory access protocol, stores computer and user account information, public certificates issued to computers and users, as well as group policies established by the Windows domain administrator. A Windows computer logs onto the Windows domain to retrieve group policies, such as wireless network policies, in advance of the user initiated logon. This allows the Windows operating system to acquire and enforce the latest group policies.

**Software Version:** Microsoft Server 2003 SP2.

**Installed Patches:** All patches and updates available from the Windows Update site.

### 4.2.2 Entrust Authority Security Manager

Entrust Authority Security Manager is the CA component of the PKI. This product is used extensively within the Government of Canada (GoC) PKI, which includes the Department of National Defence (DND). Entrust Authority Security Manager provides certificate enrolment services as well as complete certificate and key lifecycle management. It stores public certificates and certificate status information in the Microsoft Active Directory.

**Software Version:** Entrust Authority Security Manager Version 7.1 SP1

**Installed Patches:** 128970

### 4.2.3 Entrust Authority Enrollment Server for Web

Entrust Authority Enrollment Server for Web is the add-on component to Entrust Authority Security Manager that issues digital certificates to applications (web servers) and devices (VPN gateways). Entrust Authority Enrollment Server for Web requires the installation of the Microsoft Internet Information Service (IIS) on the system prior to installing Entrust Authority Enrollment Server for Web. The Microsoft IAS acquires its PKI certificate via the Entrust Authority Enrollment Server for Web through the exchange of PKCS #10 encoded certificate signing request and PKCS #7 encoded certificate chains. The IAS system administrator must initiate the certificate enrolment using a standard web browser such as Internet Explorer.

**Software Version:** Entrust Authority Enrollment Server for Web 7.0 SP1

**Installed Patches:** 131443, 133361

### 4.2.4 Microsoft Internet Authentication Service

The Microsoft Internet Authentication Service (IAS) is the Microsoft implementation of a RADIUS server. IAS performs centralized authentication, authorization, and accounting (AAA) for many types of network access, including WLAN and VPN connections. IAS supports the EAP-TLS authentication type as well as other password based authentication methods. IAS makes use of the Entrust Authority Enrollment Server for Web to enrol in its PKI certificate. It retrieves CRLs from the Active Directory to check the status of certificates used for WLAN authentication.

A shared secret provides privacy and integrity to the RADIUS sessions between the IAS and network devices such as the wireless AP that require AAA services.

**Software Version:** The IAS software version 5.2.3790.3959.

**Installed Patches:** All patches and updates available from the Windows Update site.

### 4.2.5 Microsoft Internet Information Service

The Microsoft Internet Information Service (IIS) is the Microsoft implementation of a Hyper-Text Transfer Protocol (HTTP) web server. This component provides the front-end interface to the Entrust Authority Enrollment Server for Web.

**Software Version:** The IIS software that ships with Microsoft Server 2003 SP2.

**Installed Patches:** All patches and updates available from the Windows Update site.

### 4.2.6 Cisco AIRONET 1200 Access Point

The Cisco AIRONET 1200 Access Point is a Wi-Fi certified enterprise AP. The model used in testbed (AIR-AP1231G) supports WPA personal and enterprise mode, but requires a hardware upgrade to support WPA2. The Cisco AIRONET 1200 AP relays EAP messages between the client wireless workstation (the 802.1x supplicant) and the backend authentication service – the IAS. Since the IAS implements a RADIUS server, the Cisco AIRONET 1200 AP wraps EAP messages in RADIUS packets. If the IAS grants WLAN access to the authenticated wireless node, the Cisco AIRONET 1200 AP enables the controlled port – which provides the wireless node unrestricted access to the wired network.

**Software Version:** IOS version 12.3(8)JA with Boot Loader version 2.2(8)JA

### 4.2.7 Entrust Entelligence Security Provider

Entrust Entelligence Security Provider is an enterprise desktop security product that facilitates the deployment of strong PKI based security. It can manage digital identities issued to users as well as computers. Entrust Entelligence Security Provider provides access to Entrust PKI managed digital identities to Windows applications that conform to the Windows Cryptographic Application Programmer's Interface (CryptoAPI) [21]. CryptoAPI provides applications access to public/private key cryptographic operations offered by a Cryptographic Service Provider (CSP) such as Entrust Entelligence Security Provider and the Datakey Smart Card CSP.

The CSP performs all private key operations such as decryption and digital signatures and maintains exclusive control and ownership over the private keys in the associated Key Container. The Key Container may take the form of a smart card or token or may simply be a file based key store such as an Entrust profile. In the case of a smart card or token, the device performs the public/private key cryptographic operation directly on the smart card or token that holds the private key(s). For user certificates protected by a password, the CSP prompts to user to enter the password that unlocks the Key Store before the CSP can undertake public/private key cryptographic operations on the user's behalf. For computer certificates the CSP must operate in silent mode since the computer certificate cannot be password protected.

**Software Version:** Entrust Entelligence Security Provider 8.0

**Installed Patches:** 132192

### 4.2.8 Datakey 330 Smart Card

The Datakey 330 Smart Card stores Entrust credentials in the form of private keys and public certificates. Through the Datakey Smart Card CSP, the card handles all public/private key encryption and digital signature operations associated with the user's Entrust identity. The Datakey 330 Smart Card can store user digital credentials, but cannot store computer digital credentials since computer digital credentials cannot be protected by a password.

**Software Version:** CIP Version 4.7 MU18

### 4.2.9 Windows XP 802.1x Supplicant

Windows XP includes a built-in 802.1x authentication client (supplicant) to gain access to both wired and wireless networks using the EAP, including EAP-TLS. Since the Windows 802.1x supplicant is CryptoAPI aware, Windows XP can perform WLAN authentication based on Entrust managed certificates maintained by the Entrust Entelligence Security Provider or the Datakey Smart Card CSP.

**Software Version:** The 802.1x Supplicant software that ships with Microsoft Windows XP SP2.

**Installed Patches:** All patches and updates available from the Windows Update site.

### 4.2.10 NORTEL Contivity Extranet Switch

The NORTEL Contivity Extranet Switch serves as the VPN gateway that terminates VPN tunnels from client wireless workstations. It supports certificate based authentication, IKE dynamic keying and ESP tunnel mode security associations. The NORTEL Contivity Extranet Switch enrols in its PKI certificate with PKIX-CMP to the Entrust Authority Security Manager. It retrieves CRLs from the Active Directory to check the status of certificates used for IKE authentication.

**Hardware Model:** 1500

**Software Version:** Version 04_55.180

### 4.2.11 NORTEL Contivity VPN Client

The NORTEL Contivity VPN Client is an IKE and IPsec compliant VPN client for Windows operating systems, including Windows XP. Since the NORTEL Contivity VPN Client is CryptoAPI aware, it can perform IKE authentication based on Entrust managed certificates maintained by the Entrust Entelligence Security Provider or the Datakey Smart Card CSP.

**Software Version:** Version 04_65.30 (128-bit) versions

### 4.2.12 Client Wireless Workstation

The client wireless workstation is a Windows XP notebook computer equipped with a Wi-Fi Certified Cisco Air-CB21AG-W-K9 802.11a/b/g wireless cardbus adapter with WPA and WPA2 support. Software included on the wireless client workstation includes the Entrust Entelligence Security Provider, the Windows 802.1x supplicant and the NORTEL Contivity VPN Client.

**Software Version:** Microsoft Windows XP Pro SP2

**Installed Patches:** All patches and updates available from the Windows Update site.

**Cisco Wireless Card Driver:** Version 3.6.0.61

## 4.3 Test Bed Architecture

We established a testbed architecture that includes the software/hardware components described in section 4.2. In this section, we present two solutions. The base solution relies on wireless security protocols to control and secure access to the wired network. The enhanced solution also includes IPsec based security to control and secure access to more sensitive wired environments. However, both solutions utilize Entrust issued credentials to implement strong certificate based mutual authentication and make use of smart cards to achieve two-factor authentication consisting of something the user must possess (the smart card that contains private keys) and something the user must know (the password to access the private keys on the smart card).

### 4.3.1 Base Solution

The base solution relies solely on wireless security protocols to control and secure access to the wired network. The wireless computer and wireless user must possess PKI credentials issued by the Entrust CA and the wireless user must know the password needed to unlock the user credentials stored on the smart card or the Entrust disk-based profile.

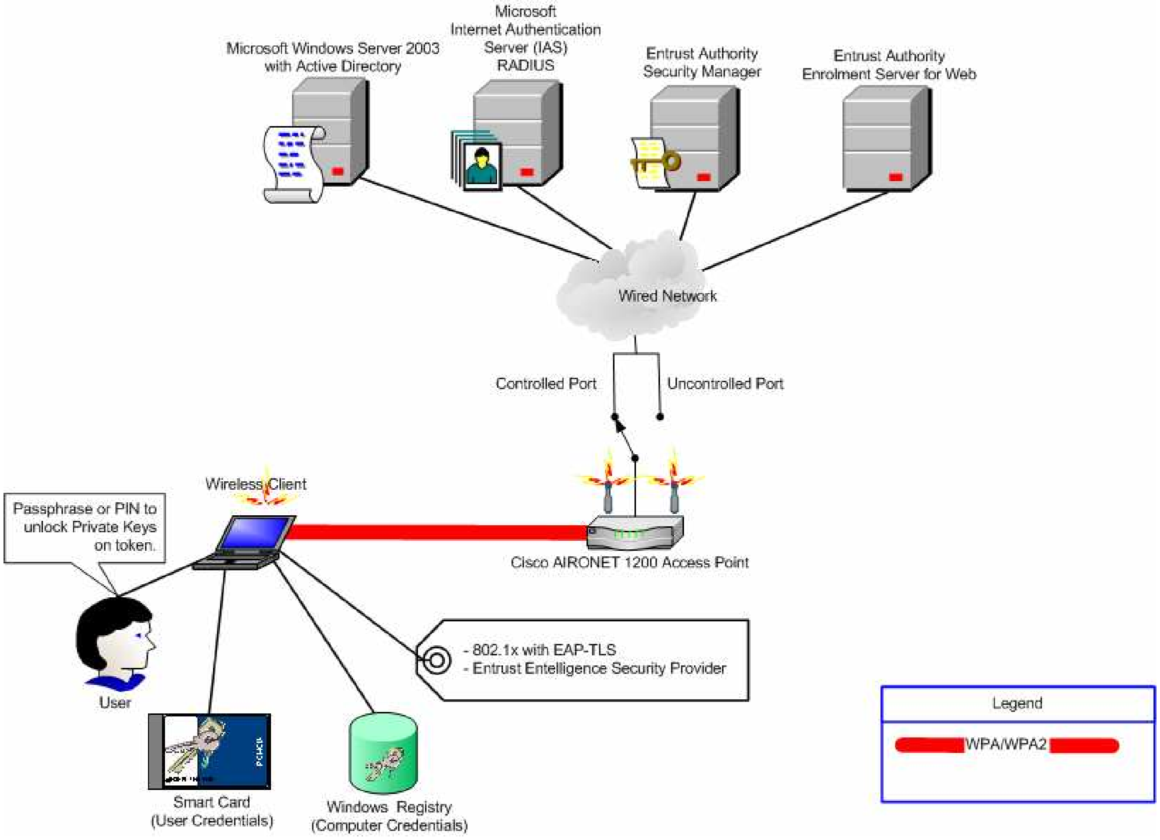


*Figure 1- Base Solution*

WPA/WPA2 secures the wireless link between the wireless computer and the AP. Unique cryptographic key material is generated for each distinct user session as part of the EAP-TLS authentication and key exchange dialogue, which is described in more detail in section 4.6.

The AP bridges DHCP requests from wireless client computers to the DHCP server executing on the Windows Server 2003 system connected to the wired network. The DHCP server assigns IP address leases to wireless computers.

### 4.3.2 Enhanced Solution

The enhanced solution layers IPsec based security on top of the wireless security protocols. The user must first authenticate to the WLAN before the user can establish a VPN tunnel to the VPN gateway.

After the user authenticates to the AP and gains access to the wired network, the user must start an IPsec compliant VPN client to establish a secure IPsec tunnel to NORTEL Contivity Extranet Switch VPN gateway. As with the base solution, the user must possess PKI credentials issued by the Entrust CA and must know the password needed to unlock the credentials stored on the smart card or the Entrust disk-based profile. The Entrust PKI credentials authenticate the user to both the wireless AP as well as the VPN gateway. Since the wireless security protocols secure the link layer, they also encrypt all IKE and ESP packets exchanged between the Wireless Client workstation and the VPN gateway – which results in double encryption over the wireless link.

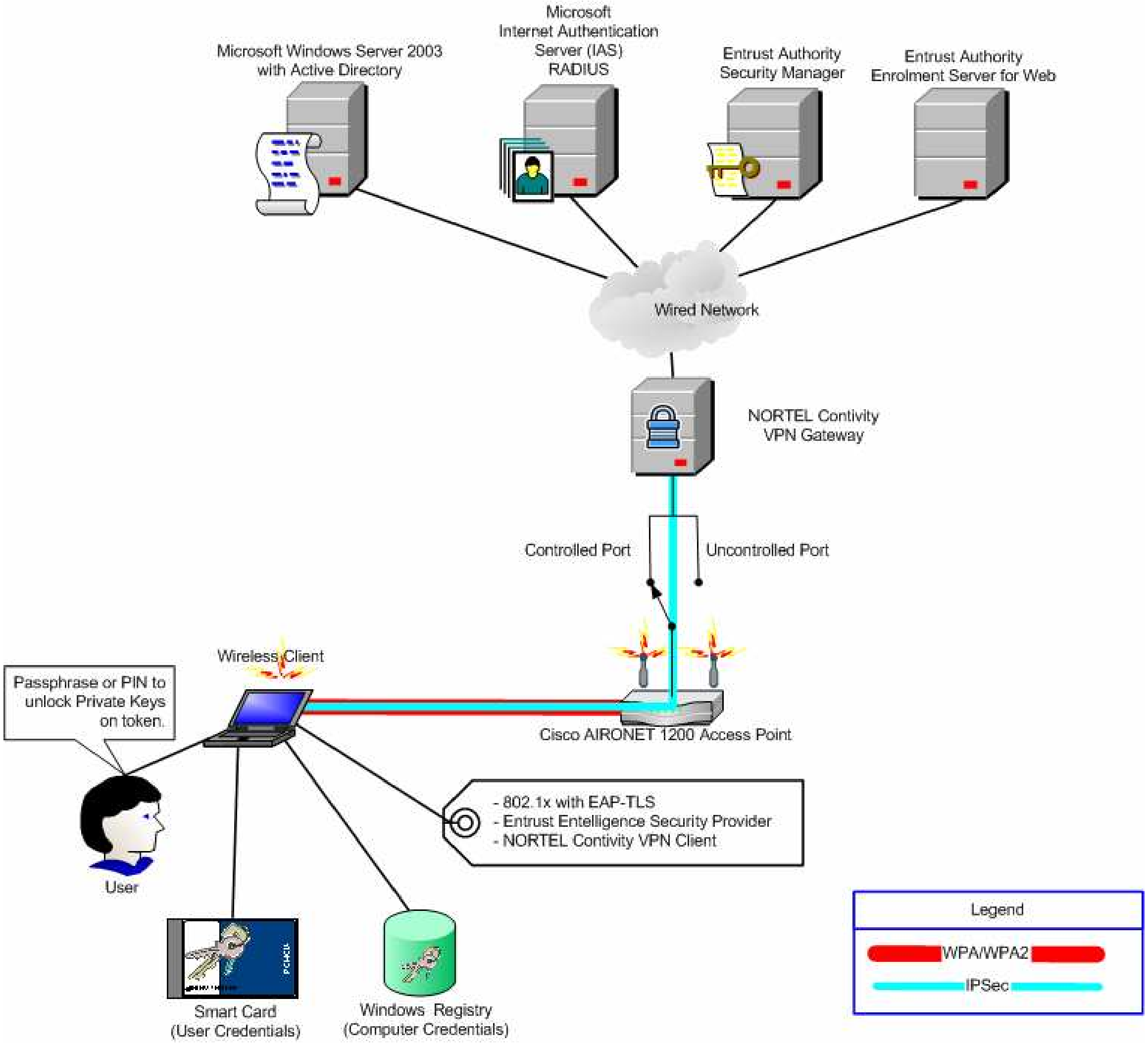


*Figure 2- Enhanced Solution*

The enhanced solution requires that the VPN gateway forward (pass-through) certain non-VPN traffic between the AP and wireless computers and the wired network. Although this traffic is not encrypted by the IPsec VPN, it is WPA/WPA2 encrypted on the wireless link. This traffic includes:

- RADIUS traffic between the AP and the IAS RADIUS server.

- DNS requests, responses and updates between wireless client computers and the DNS server.
- DHCP requests/replies between wireless client computers and the DHCP server.
- Active Directory queries/responses between wireless client computers and the Active Directory server.
- Naming Service queries/responses between wireless client computers and the Domain Controller.
- Session Service queries/responses between wireless client computers and the Domain Controller.
- Server Message Block dialogue between wireless client computers and the Domain Controller.
- Kerberos dialogue between wireless client computers and the Domain Controller.

## 4.4 Actual Lab Setup

The actual lab setup illustrated in Figure 3 consists of two server systems instead of the four servers shown in Figure 1 and Figure 2. Server 1 houses the required Microsoft software as well as the Entrust Authority Enrollment Server for Web. Server 2 provides an exclusive Windows Server 2003 server platform for the Entrust Authority Security Manager software. The actual lab setup also includes a management workstation to manage CA policies as well as add, recover and revoke user and machine PKI credentials.

## 4.5 Enabling a New Wireless Computer and User

The solution herein provides controlled access to a protected network environment to select users on select wireless computers. The new wireless computer and new wireless user must be provided with Active Directory accounts and Entrust digital identities; they both must be added to the Active Directory wireless user group; and a property must be included in their Active Directory accounts to recognize the entity's enrolled Entrust PKI certificate as an alternate authentication method. To gain access through the VPN gateway in the enhanced solution environment, the new wireless user must also be configured as an authorized VPN user within the VPN gateway. Annex A identifies the necessary steps to enable a new wireless computer and new wireless user. Annex B identifies the necessary steps to enable a new wireless VPN user.

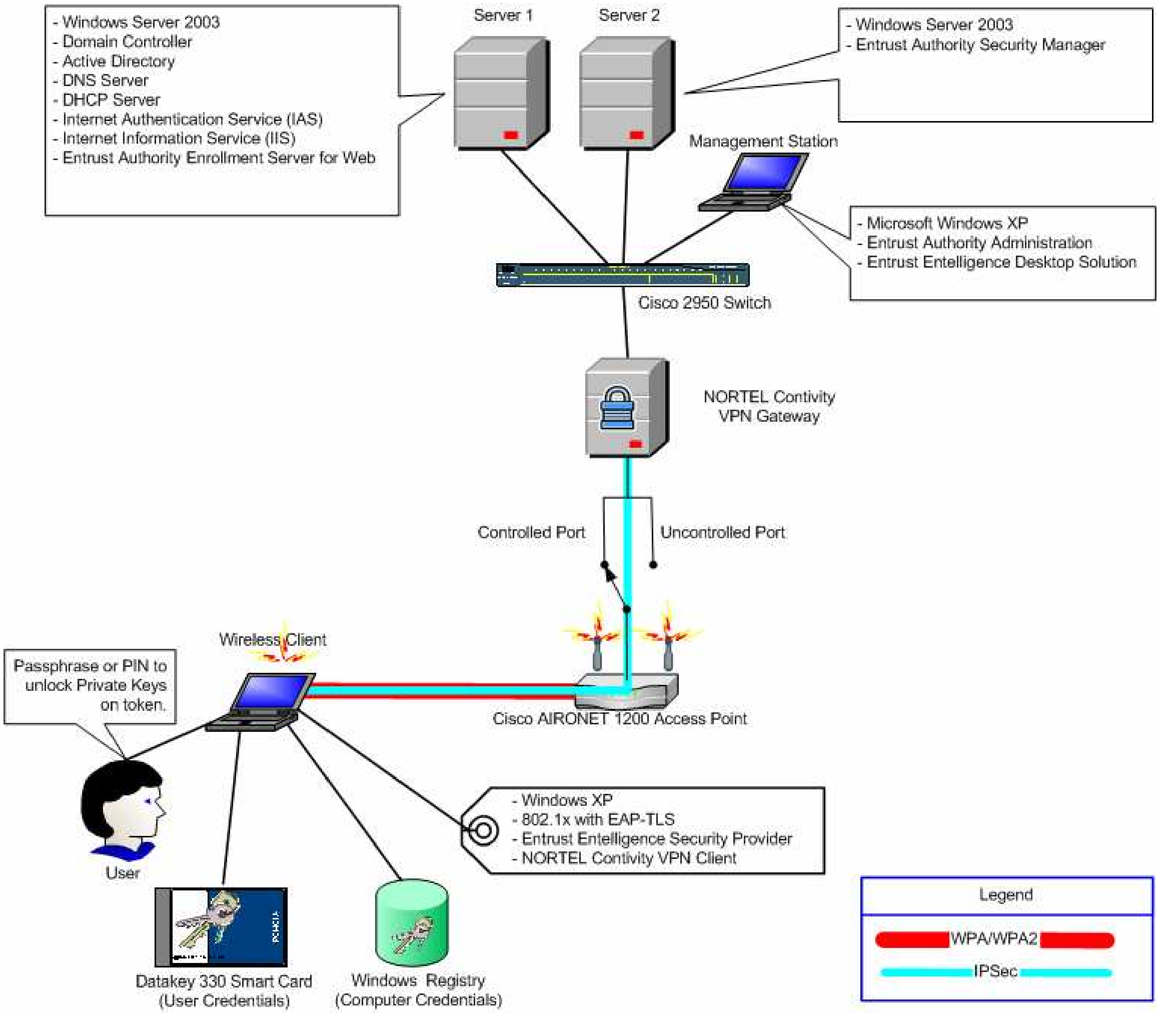


*Figure 3- Actual Lab Setup*

Figure 3 illustrates the enhanced solution configuration, which includes the VPN gateway. The basic solution configuration excludes the VPN gateway and connects the Cisco AIRONET 1200 AP directly to the Cisco 2950 switch.

## 4.6 WLAN Authentication

The wireless computer and wireless user authenticate to the WLAN with their Entrust PKI issued credentials. Figure 4 illustrates a high-level description of the dialogue between the various software/hardware components when a wireless user attempts to authenticate to the WLAN. The dialogue is identical for a wireless computer.

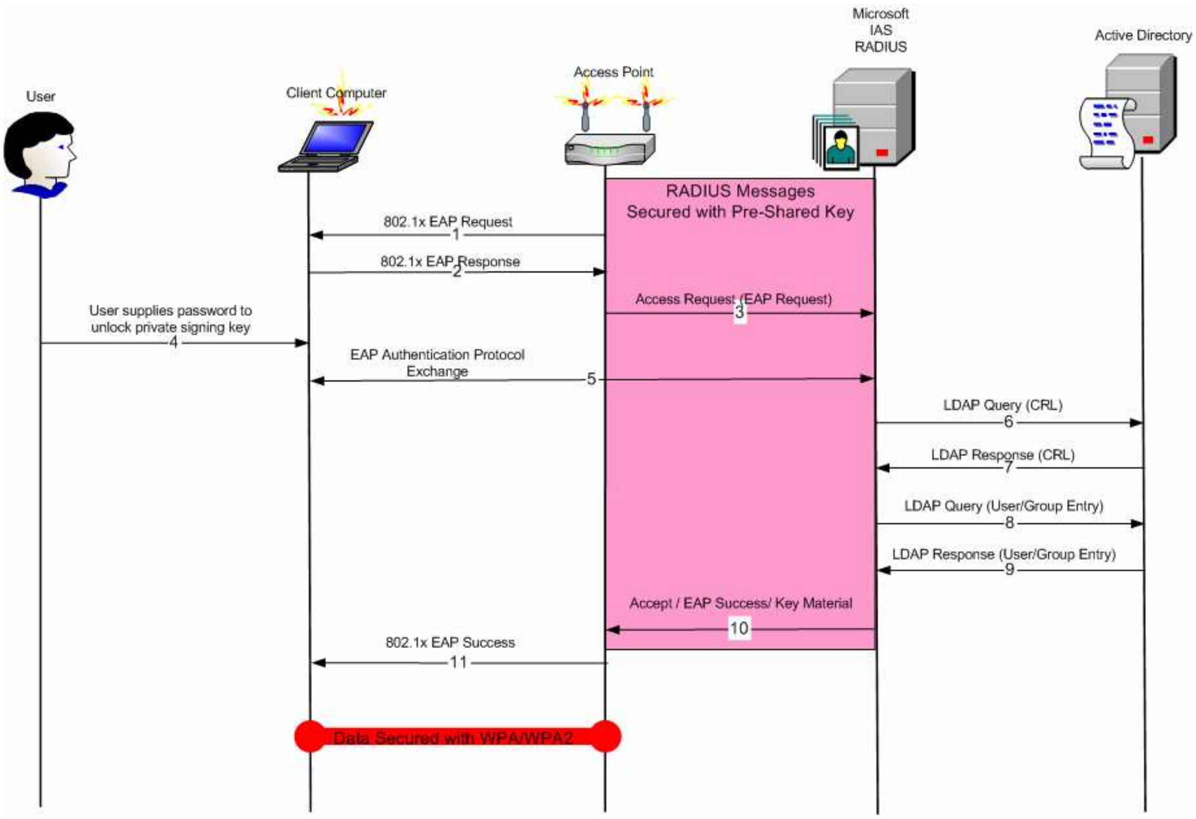

User
Client Computer
Access Point
Microsoft IAS RADIUS
Active Directory
RADIUS Messages Secured with Pre-Shared Key
802.1x EAP Request
1
802.1x EAP Response
2
Access Request (EAP Request)
3
User supplies password to unlock private signing key
4
EAP Authentication Protocol Exchange
5
LDAP Query (CRL)
6
LDAP Response (CRL)
7
LDAP Query (User/Group Entry)
8
LDAP Response (User/Group Entry)
9
Accept / EAP Success/ Key Material
10
802.1x EAP Success
11
Data Secured with WPA/WPA2

*Figure 4-WLAN Authentication*

1. After the Client Computer establishes an 802.11 association with the AP, the AP issues an EAP Request message to the Client Computer. The EAP Request message identifies the authentication type requested by the AP. In this case the authentication type is EAP-TLS.

2. The Client Computer responds an EAP Response message, which initiates the EAP-TLS authentication.

3. The AP engages the RADIUS server to complete the EAP-TLS authentication sequence on behalf of the AP. It does so with a RADIUS Access Request message that includes information contained in the EAP Response message (i.e. peer identification).

4. Since the user must use his Entrust PKI credentials to authenticate to the WLAN, the user is prompted to enter the password that unlocks his private signing key. This occurs when the Windows XP 802.1x supplicant invokes CryptoAPI methods to have data digitally signed.[2]

[2] Currently, the user is not prompted to unlock the Entrust PKI credentials. We configured Entrust Entelligence Security Provider to initiate an Entrust logon after the user logs into Windows.

5. The Windows XP 802.1x supplicant and the IAS complete the EAP-TLS mutual authentication and key generation dialogue. The AP is now acting as a pass-through for EAP-TLS messages and does not participate directly in the EAP-TLS authentication dialogue. The EAP-TLS authentication dialogue includes a 4-way handshake to generate the necessary cryptographic key material that will be used by the Client Computer and the AP to secure the wireless link. WPA/WPA2 Enterprise mode generates unique cryptographic key material for each distinct user session[3].

6. The IAS queries the Active Directory to retrieve CRL that contains the revocation status for the certificate presented by the authenticated User.

7. The Active Directory responds with the requested CRL, which the IAS uses to ensure that the user certificate has not been revoked and remains valid.

8. The IAS queries the Active Directory to retrieve user/group information associated with the authenticated User.

9. The Active Directory responds with the requested user/group information, which the IAS uses to ensure that the authenticated User is authorized as a wireless user.

10. The IAS issues a RADIUS Accept message to the AP. The RADIUS Accept message contains an EAP Success message as well as the generated cryptographic key material that the AP requires to encrypt the wireless link between the AP and the Client Computer. The generated cryptographic keys are protected by the secure session between the AP and the IAS, which is encrypted using a pre shared key configured in both devices. Alternatively, the IAS may respond with a RADIUS Reject message (EAP Failure) if the user failed to authenticate, if the user was not authorized to access the WLAN, or if the user presented a revoked certificate.

11. The AP forwards the EAP Success message to the Client Computer.

## 4.7 VPN Authentication

The user authenticates to the VPN gateway with his Entrust PKI issued credentials. Figure 5 illustrates a high-level description of the dialogue between the various software/hardware components when a user attempts to authenticate to the VPN.

[3] If the same user authenticates to the wireless network concurrently on two separate computers, unique cryptographic keys will be generated for each session.

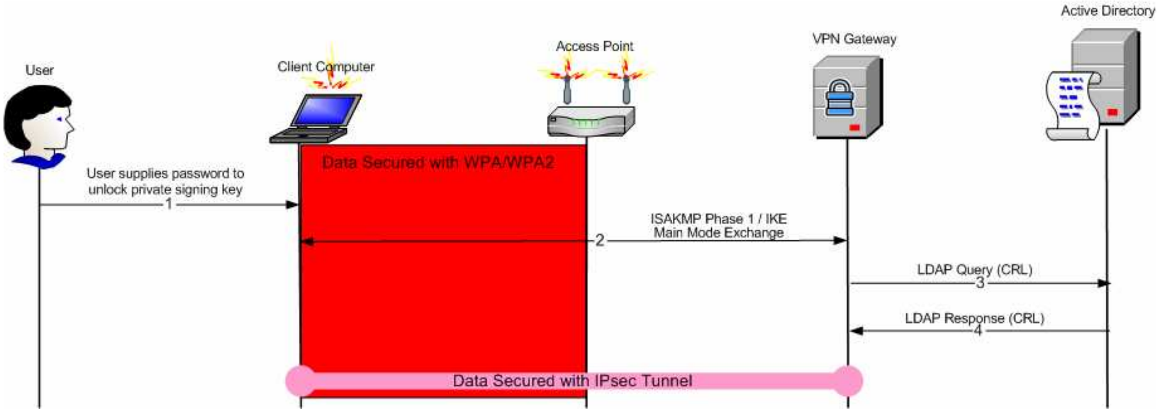

User
Client Computer
Access Point
VPN Gateway
Active Directory
Data Secured with WPA/WPA2
User supplies password to unlock private signing key
1
ISAKMP Phase 1 / IKE Main Mode Exchange
2
LDAP Query (CRL)
3
LDAP Response (CRL)
4
Data Secured with IPsec Tunnel

*Figure 5-VPN Authentication*

1. After the Client Computer gains access to the wired network through the AP, the Client Computer must initiate an ISAKMP Phase 1 / IKE Main Mode exchange with the VPN Gateway. Since the user must use his Entrust PKI credentials to authenticate to the VPN Gateway, the user is prompted to enter the password that unlocks his private signing key. This occurs when the NORTEL Contivity VPN client software invokes CryptoAPI methods to have data digitally signed. [4]

2. The ISAKMP Phase 1 / IKE Main Mode exchange establishes cryptographic key material for the ISAKMP security association and validates the identity of the peers (the client and the VPN gateway). IKE makes use of Diffie-Hellman as its key establishment protocol.The peers exchange digitally signed data and their public certificates to establish and validate their identities.

3. The VPN gateway queries the Active Directory to retrieve CRL that contains the revocation status for the certificate presented by the authenticated User.[5]

4. The Active Directory responds with the requested CRL, which the VPN gateway uses to ensure that the User certificate has not been revoked and remains valid.

Although Figure 5 contains the wireless AP, it is important to note that the wireless AP does not participate in any aspect of the IPsec authentication. The wireless AP simply bridges the communication between the wireless link and the wired network.

[4] The system prompts the user to unlock the Entrust credentials when the user connects using the NORTEL Contivity VPN gateway. The system does not prompt the user if the user recently unlocked the Entrust credentials.

[5] The NORTEL VPN gateway periodically polls the LDAP server at configurable intervals to retrieve new CRLs.

# 5. Known Issues and Observations

This section outlines known issues as well as other observations that were noted during our installation and testing.

## 5.1 Key Lengths

The Entrust CA was originally configured with 2048-bit CA keys as well as 2048-bit subscriber (user) keys. We encountered problems storing 2048-bit keys and certificates on the Datakey 330 Smart Card. As a result, we downgraded the CA and subscriber key lengths to 1024-bit keys.

## 5.2 Smart Cards

After we downgraded the CA and subscriber key lengths to 1024-bit keys, we were still unable to store Entrust PKI credentials on the Datakey 330 Smart Card. The DND PKI engineering group supplied new software drivers for the Datakey 330 Smart Card but we did not have time to test the new drivers. As a result we did not use the Datakey 330 Smart cards and instead stored Entrust PKI credentials on disk based Entrust Profile files.

## 5.3 WPA2

The Cisco AIRONET 1200 AP (AIR-AP1231G) requires a hardware upgrade in order to support WPA2. The hardware upgrade was not made available in time to incorporate WPA2 in the testbed environment. As a result, we only tested with WPA.

## 5.4 Certificate Types and Extended Key Usage

Certificates issued to the IAS, wireless client computers as well as wireless users must contain an Extended Key Usage (EKU) extension. Microsoft requires the following object identifiers (OID):

| | |
|---|---|
| IAS Server: | 1.3.6.1.5.5.7.3.1 |
| Wireless Client Computer: | 1.3.6.1.5.5.7.3.2 |
| Wireless User: | 1.3.6.1.5.5.7.3.2 |

The organization must issue certificates with the proper EKU extensions to the IAS as well as each wireless computer and wireless user authorized to connect to the WLAN. The organization must also re-issue certificates to wireless users if the existing certificates do not contain the required EKU extension.

We used the Entrust pre-defined “MS VPN Client User” certificate specification to issue certificates to wireless users. This certificate type contains the required EKU extension but the resulting digital identity includes only a single dual-purpose key-pair. The GoC PKI usually issues digital identities consisting of two single-purpose key pairs: one for digital signatures and one for encryption. Wireless users should make use of their standard GoC PKI digital identity to authenticate to the WLAN and not be issued special purpose WLAN authentication certificates. The final solution should define a new certificate specification that is based on the standard dual key pair GoC PKI certificate specification.

We defined a new certificate type called “MS Client Machine” to issue certificates to wireless computers. We based this new certificate type on the Entrust pre-defined “MS VPN Client Machine” certificate type, which includes two key pairs. Since WLAN authentication only requires a signing certificate, the final solution could include one single-purpose key pair in the wireless computer digital identity.

## 5.5 Authentication, Trust and Authorization

In addition to performing authentication, a software component must also determine if it trusts the authenticated entity and if the authenticated entity has the authorization to perform the requested function.

### 5.5.1 IAS RADIUS Server

When authenticating to the WLAN, the computer and user present a public certificate issued by the Entrust PKI CA, which the IAS recognizes as a trusted CA. However, the IAS must also associate the machine and user certificate to the associated Active Directory account. Active Directory includes mechanisms that permit security applications such as the IAS to authenticate to Active Directory accounts through alternate methods such as the X.509 certificates issued from the Entrust PKI. After the Domain Administrator creates the computer and user Active Directory account and the computer and user enrol in their Entrust PKI credentials, the Domain Administrator must define an *altSecurityIdentities* property to map the entity’s enrolled Entrust PKI certificate to the entity’s Active Directory account.

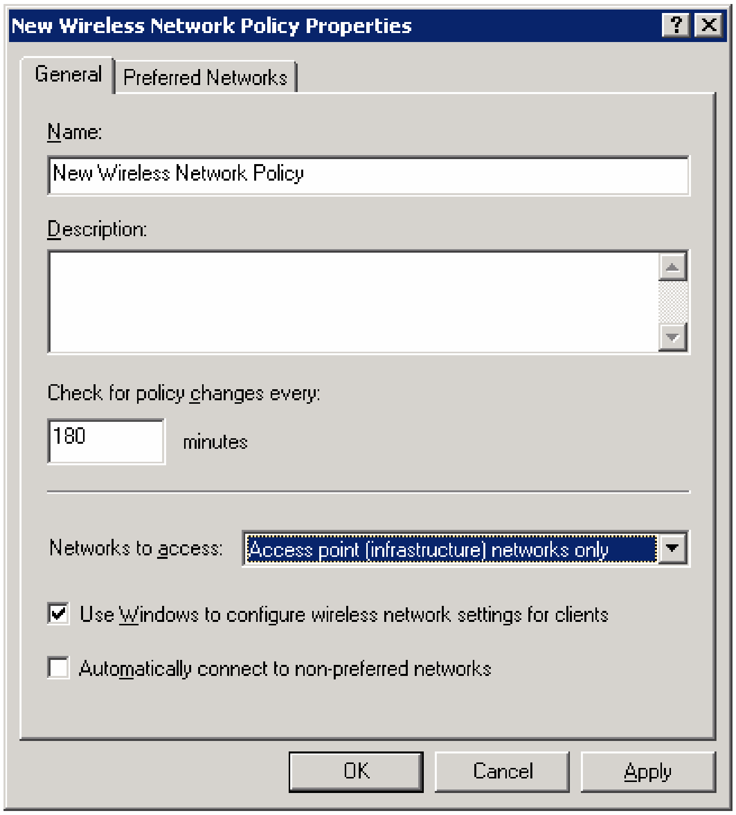
It is important that the system maintains the *altSecurityIdentities* property throughout the lifetime of the wireless computer and wireless user account. The System Administrator must modify the mapping when the entity undergoes a Distinguished Name (DN) Change operation or when the entity is removed from the Entrust PKI. We established this mapping manually in the test bed environment. Maintaining this property manually will likely result in erroneous data within the Active Directory. Instead, this information should be managed automatically using Active Directory Services Interface (ADSI) scripts.

As discussed in section 4.6, the IAS retrieves the appropriate CRL from the Active Directory to determine the revocation status of the computer or user certificate. If the Entrust PKI CA revokes the certificate, the IAS does not trust the presented certificate and does not permit access to the WLAN.

After the IAS positively identifies the computer or user and determines that the entity has not been revoked, the IAS retrieves group information from the Active Directory to determine if the computer or user forms part of the wireless group. If the computer or user does not form part of the wireless group, regardless of the fact that the entity possesses valid Entrust PKI credentials and certificate can be mapped to a valid Active Directory account, the IAS does not permit access to the WLAN.

### 5.5.2 Wireless Network Policy

The wireless network properties control how the wireless computer accesses the WLAN. The wireless properties can be specified on the local machine but can also be compiled within a Windows domain group policy. We created a wireless network policy within Active Directory that gets disseminated to client computers when the client computer connects to the domain on both wired and wireless networks. Figure 6 illustrates the creation of the "New Wireless Network Policy".



Name:
New Wireless Network Policy

Description:

Check for policy changes every:
180 minutes

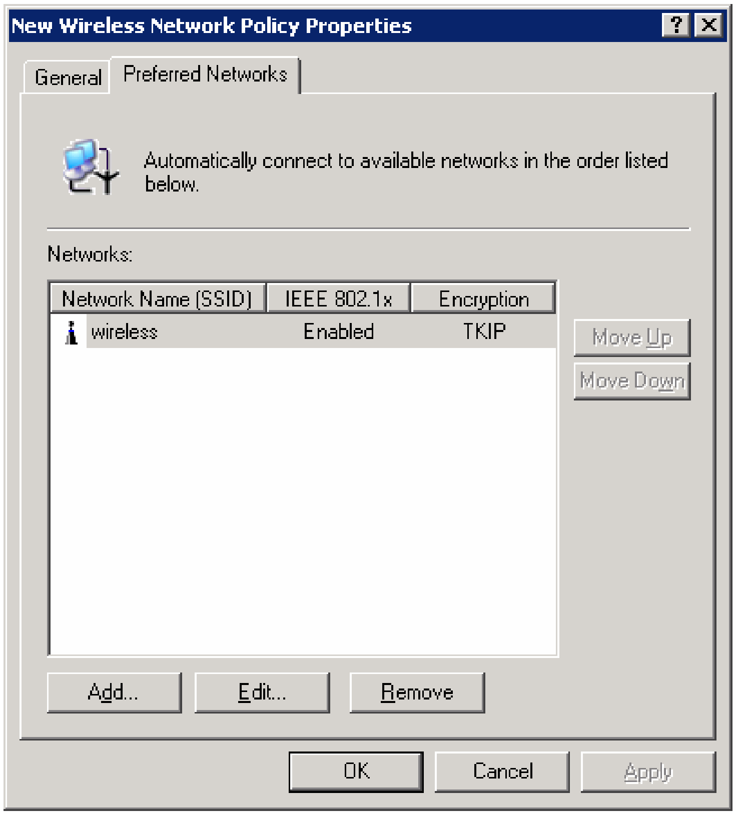
Networks to access: Access point (infrastructure) networks only

☑ Use Windows to configure wireless network settings for clients

☐ Automatically connect to non-preferred networks

*Figure 6- Wireless Network Policy Properties*

Figure 7 identifies the preferred wireless networks for the domain. We created a wireless network called “wireless”.



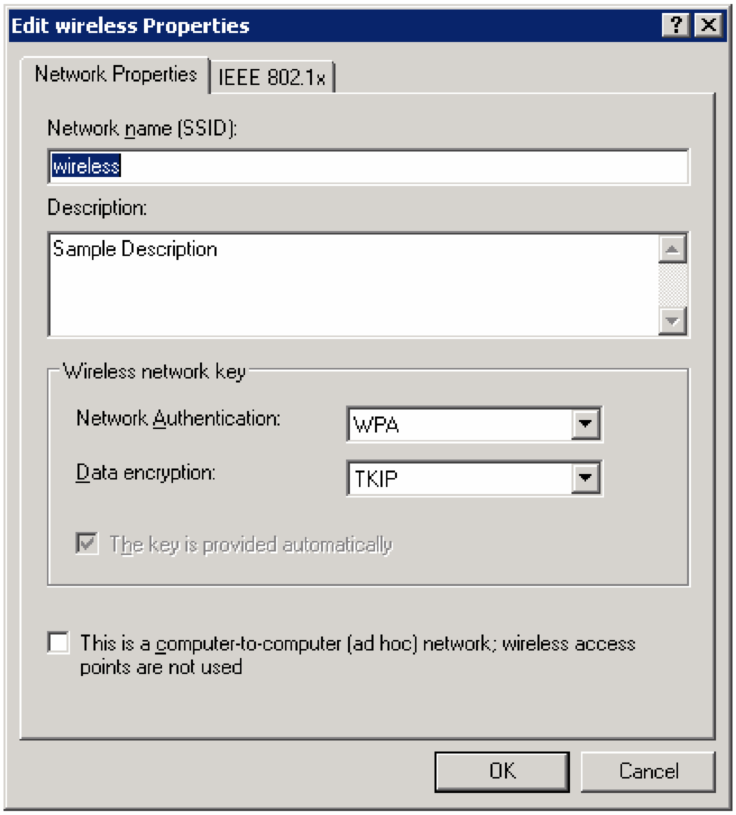
Automatically connect to available networks in the order listed below.

Networks:

| Network Name (SSID) | IEEE 802.1x | Encryption |
|---|---|---|
| wireless | Enabled | TKIP |

*Figure 7- Preferred Networks*

Figure 8 shows the network properties for the “wireless” network. The network properties specify WPA as the wireless security protocol and TKIP for privacy and data integrity. We chose these settings to match the current capability of the Cisco AIRONET 1200 AP. These settings should specify WPA2 and AES when the AP includes support for WPA2.



Network name (SSID): wireless

Description: Sample Description

Network Authentication: WPA

Data encryption: TKIP

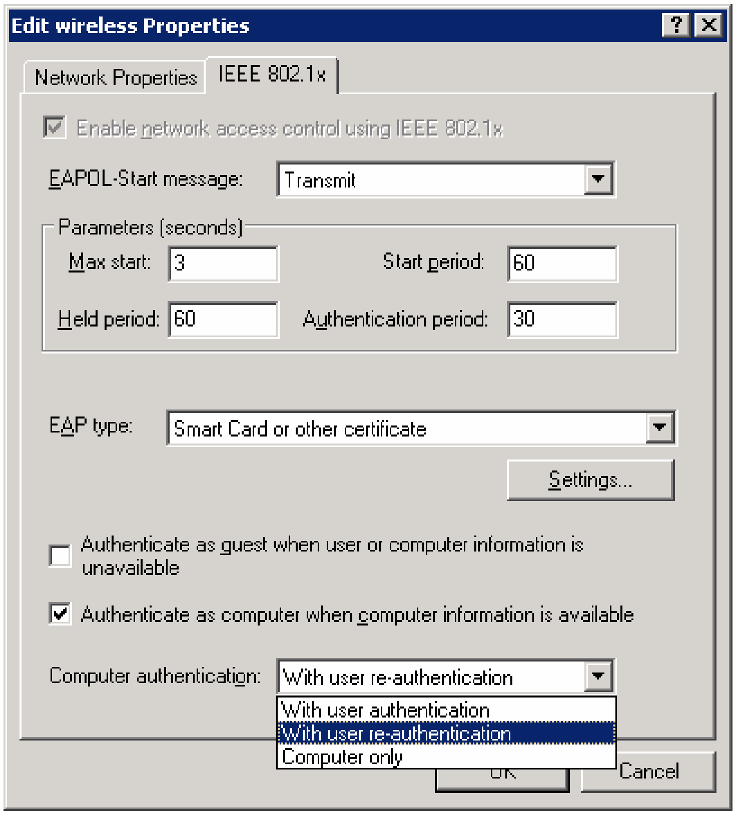
☑ The key is provided automatically

☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

*Figure 8- Network Properties*

When WPA or WPA2 (without PSK) is selected as the Network Authentication protocol for a wireless network, Windows automatically enables 802.1x authentication for the wireless network. Figure 9 shows the IEEE 802.1x properties which indirectly enable EAP-TLS by requesting “Smart Card or other certificate” based authentication.

The IEEE 802.1x properties specify that the computer should authenticate to the WLAN using computer credentials when available, but the computer should re-authenticate to the WLAN using user credentials after the user logs in. When a computer is powered on in the proximity of the wireless AP, the computer authenticates to the WLAN using the Entrust PKI credentials issued to the computer and retrieves group policies from the Active Directory. After a user logs on to the computer, the computer re-authenticates to the WLAN using the Entrust PKI credentials issued to the user.



Edit wireless Properties

☑ Enable network access control using IEEE 802.1x

EAPOL-Start message: Transmit

Parameters (seconds)

Max start: 3

Start period: 60

Held period: 60

Authentication period: 30

EAP type: Smart Card or other certificate

□ Authenticate as guest when user or computer information is unavailable

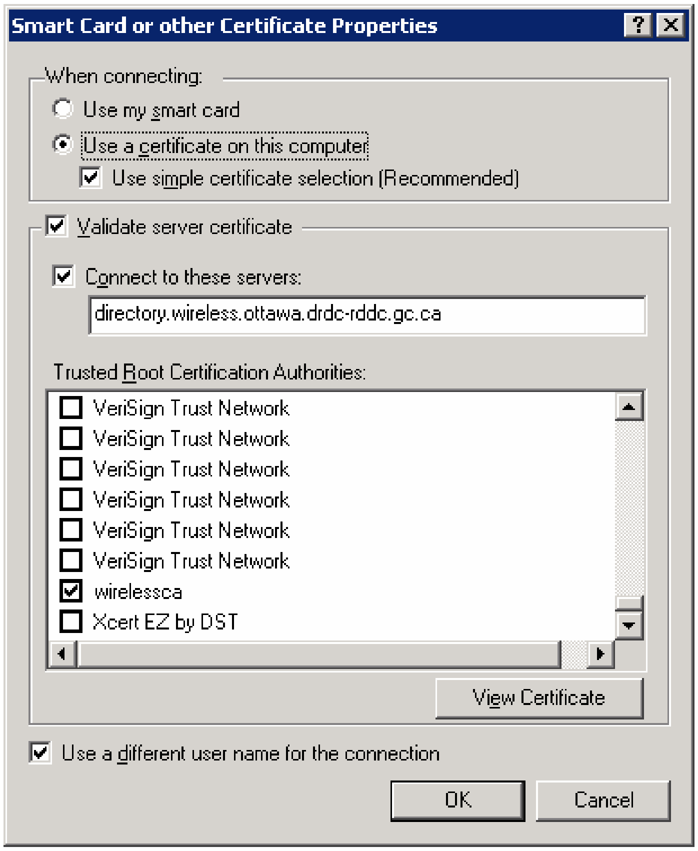
☑ Authenticate as computer when computer information is available

Computer authentication: With user re-authentication

*Figure 9- IEEE 802.1x Properties*

Clicking on the "Settings" buttons displays the "Smart Card or other Certificates" pane. Figure 10 illustrates the certificate properties for the authentication server certificate. The certificate presented by the authentication server must be valid; the authentication server certificate must contain "directory.wireless.ottawa.drdc-rddc.gc.ca" as the SubjectName or SubjectAltName; and the authentication server certificate must have been issued by the trusted certificate authority called "wirelessca". This information allows the 802.1x supplicant to detect rogue or unauthorized authentication servers. If the policy does not identify a trusted authentication server, an attacker could deploy an unauthorized authentication server and rogue AP using other credentials issued by the trusted CA.[6]

[6] The other certificate must contain the correct Extended Key Usage attribute as described in section 5.4.



Smart Card or other Certificate Properties

When connecting:

○ Use my smart card

● Use a certificate on this computer

☑ Use simple certificate selection (Recommended)

☑ Validate server certificate

☑ Connect to these servers:

directory.wireless.ottawa.drdc-rddc.gc.ca

Trusted Root Certification Authorities:

- □ VeriSign Trust Network
- □ VeriSign Trust Network
- □ VeriSign Trust Network
- □ VeriSign Trust Network
- □ VeriSign Trust Network
- □ VeriSign Trust Network
- ☑ wirelessca
- □ Xcert EZ by DST

☑ Use a different user name for the connection

*Figure 10 - Certificate Properties*

The Windows XP 802.1x supplicant does not check the revocation status of the certificate issued to the IAS. If an IAS is compromised and the associated private keys are stolen, the thieves obtain the ability to establish a rogue authentication server using the same compromised certificates. Since the Windows XP 802.1x supplicant does do not perform certificate status checking, the wireless network group policy must be modified to no longer validate the compromised IAS certificate. Moreover the compromised IAS must be re-established with a different name than the name encoded in the compromised certificate.

### 5.5.3 VPN Gateway

The NORTEL Contivity Extranet Switch performs its own authentication and authorization functions. The Contivity administrator identifies a trusted CA by importing the public CA certificate. Authorized users must present a public certificate issued by the trusted CA. The Contivity administrator can define distinct user groups based on the distinguished name encoded in subscriber certificates[7]. If the organization requires a more refined VPN user authentication mechanism, the Contivity administrator may establish groups based on individual users identifiable by the full distinguished name encoded in their certificates. The Contivity

[7] This requires that entities have been previously grouped together in distinct branches of the directory information tree (DIT) and that their distinguished name includes an identifiable portion of the DIT.

administrator may then apply different network filters to different groups or may assign internal IP addresses from distinct address pools to different groups.

As discussed in section 4.7, the Contivity Extranet Switch retrieves the appropriate CRL from the Active Directory to determine the revocation status of the user certificate. If the Entrust PKI CA revoked the user certificate, the Contivity Extranet Switch does not trust the presented user certificate and does not permit the user access to the VPN.

### 5.5.4 VPN Client

The user must configure the Contivity VPN Client to use an Entrust PKI issued certificate to authenticate to the VPN gateway. The Contivity VPN Client does permit the user to specify additional parameters to validate the VPN gateway certificate to explicitly identify an authorized VPN gateway. The Contivity VPN Client accepts any valid public certificate issued by the same CA that issued the user's certificate. Furthermore, the Contivity VPN Client does not check the revocation status of the certificate presented by the VPN gateway.

The inability of the Contivity VPN Client to recognize an authorized VPN gateway allows any user with valid Entrust PKI certificate to establish a rogue VPN gateway. The inability of the Contivity VPN Client to check the revocation status of the VPN gateway certificate allows an intruder to establish a rogue VPN gateway using a previously compromised and revoked Entrust PKI certificate. We recognize however that it is much more difficult to establish a rogue VPN gateway than it is to establish a wireless rogue AP that is accessible over public air ways.

## 5.6 Private Key Access

When the wireless user attempts to connect to the WLAN, the CSP associated with the public certificate (Entrust Entelligence Security Provider) should prompt the user to enter the password to unlock the wireless user's credentials if the credentials remain locked. Unfortunately, the 802.1x supplicant does not appear to engage the CSP and the Entrust Entelligence Security Provider does not prompt for the password. Instead, Entrust Entelligence Security Provider could be configured to unlock the credentials immediately after the user logs on to the computer.

We did note that the NORTEL VPN Client does cause the CSP to prompt the user to unlock the user's Entrust credentials.

## 5.7 TLS Handle Caching

Client computers and the IAS cache the TLS handle after a successful WLAN authentication exchange. The TLS handle contains a portion of the TLS connection properties and allows the re-authentication process between the client computer and the IAS to occur more rapidly at the expense of security. For instance the presence of a cached TLS handle may permit a user with an expired or revoked certificate to gain access to the WLAN. Since the default TLS handle cache lifetime on client computers and the IAS is 10 hours, this introduces a serious weakness in the WLAN authentication process. Microsoft operating systems include a registry entry that defines the TLS handle cache lifetime. That registry entry should be modified on both client computers and IAS to either prevent TLS handle caching or to reduce the TLS handle cache lifetime to a value deemed acceptable by the organization's security policy[8]. Alternatively Microsoft suggest that the organization can mitigate the effects of TLS handle caching by removing the Active Directory account of a revoked user; by eliminating the alternate security identity mapping in the revoked user's Active Directory entry; or by rescinding a revoked user's wireless group membership. We did not test these alternative methods and do not recommend their use since we believe that applications should reference the CRL to determine the certificate revocation status.

## 5.8 Computer Authentication

Computers running Windows operating systems connect to the network using computer credentials in order to retrieve group policy updates prior to the user logon. Since our secure WLAN solution mandates authentication based on Entrust PKI issued certificates, only wireless computers seeded with an authorized digital identity can connect to the WLAN prior to user logon. If the computer cannot authenticate to the WLAN and log onto the Windows domain, the user may not be able to log onto the Windows domain[9]. If the user logs on the local computer instead of the Windows domain, the user may still have access to domain resources but the user must supply domain credentials before the server grants access to the requested domain resources. To support Windows domain logon by users, the computer must first authenticate to the WLAN and log onto the Windows domain.

The wireless network policy outlined in section 5.5.2 specified an authentication policy of "Computer authentication with User re-authentication". This permits the computer to connect to the WLAN and download group policy and forces the user to re-authenticate to the WLAN after the user logs onto the computer. However, this setting does not mandate computer authentication prior to user authentication and permits users to connect unauthorized computers to the WLAN by simply moving their Entrust issued user credentials to a personally owned computer. The "Computer only" authentication policy setting restricts WLAN access to corporate owned computers but does not permit user authentication.

## 5.9 User Switching

Windows XP includes support for switching between users without logging off the idle user. We did not test the impact of switching from a WLAN and VPN authenticated user to a user that has yet to authenticate to the WLAN and VPN. The computer should re-authenticate to the WLAN and VPN using the Entrust PKI certificate issued to the active user. Regardless, the Windows XP user switching capability presents a serious security challenge and should be disabled.

## 5.10 VPN Pass-Through and DHCP Relay

We configured extremely liberal filters within the NORTEL Contivity Extranet Switch to permit non-VPN communication between the AP and wireless computers and the wired network. This is needed to permit the computer to log onto the Windows domain, download group policies, and facilitate the subsequent domain logon by the user.

[8] TLS Handle Caching should be enforced with a Windows domain group policy.

[9] The user may achieve domain logon with cached domain credentials stored on the wireless computer.

The pass-through configuration lowers the level of assurance associated with the VPN gateway since it may permit an attacker to gain unauthenticated and unauthorized access to the protected network. This risk is mitigated by the fact that the attacker must first present strong credentials before being granted access to the WLAN. However it is possible that an attacker can bypass the WLAN and initiate the attack from the wired network between the AP and the unprotected side of the VPN gateway. This risk can be mitigated my co-locating the AP and the VPN gateway in a secure location.

We also configured DHCP relay to enable the wireless workstation to acquire an IP address and network information dynamically from the DHCP server executing on the Windows Domain Controller. However, the NORTEL Contivity Extranet Switch does not relay DHCP requests from a non-secure network to the internal secure network. Since the Cisco AIRONET 1200 AP does not include a DHCP server (it simply acts as a DHCP relay), we were forced to configure static network information within the wireless computer. The final solution should include a DHCP server on the AP or the VPN gateway to issue IP address leases to wireless computers.

## 5.11 Consistent Client Configuration to Prevent Spoofing

Section 5.5.2 outlines the Windows XP client configuration required to validate the IAS authentication server. The 802.1x supplicant can only be assured that it is authenticating to an authorized authentication server when the client configuration correctly identifies the IAS certificates and the associated issuing CA.  Section 5.5.4 also discusses the NORTEL VPN Client's inability to accept configuration parameters used to identify authorized VPN gateways and to detect rogue VPN gateways.

Client configuration for both the WLAN and the VPN must provide the ability to positively identify authorized authentication servers and VPN gateways. Improperly configured client workstations may experience authentication failures or may unknowingly interact with rogue authentication servers or VPN gateways. Fortunately, Windows manages WLAN client configuration centrally within a group policy and pushes the policy to client computers when client computers connect to the Windows domain through wired or wireless networks. The NORTEL VPN Client requires that computers be individually configured with new client configuration such as the IP address of the VPN gateway.

## 5.12 Client Certificate Status Checking

The Windows 802.1x supplicant does not check the status of the certificate supplied by the IAS RADIUS server as part of the WLAN authentication. We revoked the IAS certificate, but it did not prevent the client computer from authenticating with the IAS and gaining access to the WLAN. The client computer cannot retrieve the CRL until it gains access to the wired network and it can only gain access to the wired network if it completes the WLAN authentication process. For this reason, we can understand why the client computer does not check the status of the IAS certificate during the WLAN authentication process. However, the 802.1x supplicant should defer the certificate status check after the client computer gains access to the wired network and it should disconnect from the wireless network if it discovers a revoked IAS certificate. Section 5.5.2 previously discussed approaches for dealing with compromised IAS certificates.

Similarly, the NORTEL VPN Client does not check the status of the certificate supplied by the VPN gateway server as part of the VPN authentication. We revoked the VPN gateway certificate, but it did not prevent the client computer from authenticating with the VPN Gateway and gaining access to the protected network.

## 5.13 Protection of Identity Information

EAP-TLS uses certificates to achieve mutual authentication between the wireless computer/user and the authentication server. The wireless computer/user and the authentication server exchange the public certificates as part of the TLS handshake. A public certificate contains a distinguished name as well as other information that identifies the owner of the certificate. Although the certificates carry the "public" label, their content may be considered sensitive by certain organizations. An eavesdropper cannot use a public certificate to gain unauthorized access to the WLAN, but the eavesdropper can learn the names of individuals within the organization or determine when a member of the organization connects or disconnects to/from the WLAN.

Protected EAP (PEAP) [23] uses TLS to hide the identity of the client entity. PEAP uses a TLS channel to protect the inner EAP exchange. The Microsoft 802.1x supplicant supports PEAP to protect the inner EAP-TLS exchange, which prevents eavesdroppers from extracting the identity information encoded in public certificates. We did not enable PEAP in the testbed environment.

# 6. Conclusions

Wireless security protocols such as WPA and WPA2 provide industry standard means to connect wireless devices to computer networks that contain sensitive or protected information. The underlying cryptographic algorithms (TKIP-MIC for WPA and AES-CCMP for WPA2) exhibit no known vulnerabilities[10] and provide highly effective privacy and data integrity, but WPA2 offers superior cryptographic strength and is better suited for protected GoC networks. TKIP-MIC and AES-CCMP are symmetric algorithms that require the secure generation and injection of cryptographic keys. WPA and WPA2 enterprise mode leverage the IEEE 802.1x network authentication and access control framework that uses EAP to implement different types of authentication. Enterprise mode allocates per-user, per-session cryptographic keys to authorized computers and users.

Secure WLAN deployments should make use of the strong authentication capability of the existing GoC PKI, which allocates digital credentials to systems, application processes and users. The use of the Microsoft IAS as the backend RADIUS authentication server requires the establishment of an explicit mapping between the GoC PKI issued certificates and an alternate security identity within the entity's (i.e. computer and user) Active Directory entry. In an enterprise environment, these mappings should be established and maintained automatically using ADSI scripts.

The EAP-TLS authentication method supports certificate based authentication and is compatible with GoC PKI issued and managed certificates. Authentication is further strengthened when a smart card holds and protects the private keys associated with the digital credentials to implement a stronger two-factor authentication scheme. Since the TLS handshake exposes the identities encoded within certificates, higher classification environments should consider deploying PEAP to protect identity information.

Microsoft Windows group policies permit the compilation and management of wireless network policy and facilitate the propagation of any changes to the wireless network policy to authorized wireless computers. Wireless network policy selects the wireless security protocol, defines cryptographic algorithms, and identifies the digital identity of the authentication server. Without group policies, the wireless network settings must be managed separately on individual computers – an error prone process that provides an unacceptable level of assurance in protected network environments.

For higher classification environments such as Protected-B, a deployment may layer an IPsec compliant VPN tunnel on the WPA2 secured wireless link. The VPN gateway carries out VPN authentication with the same user certificates used to perform WLAN authentication. In order to permit the computer to log onto the Windows domain and download group policies, the VPN gateway must be configured to pass non-VPN traffic through a VPN gateway. This lowers the level of assurance associated with the VPN gateway since the VPN gateway must expose parts of the protected network.

[10] The Personal mode of both WPA and WPA2 is vulnerable to brute force on-line attacks against weak pre-shared keys. The use of a long and complex pre-shared key mitigates this vulnerability.

We believe WPA2 enterprise mode, when combined with GoC PKI issued certificates and wireless network policy managed through Windows group policies, is an acceptable solution for providing authenticated/secure WLAN access to GoC protected environments. We also conclude that layering IPsec security on top of WPA2 adds complexity without providing any significant additional assurance against unauthorized WLAN access – especially if the VPN gateway must pass non-VPN traffic. If the solution relies on WPA2 to protect the VPN gateway from unauthorized access by non-VPN traffic, then the VPN gateway should not form part of the solution.

If IPsec is deemed necessary for higher classification network environments, the final solution could consider the approach described in TM 2006-124 [1] that employs the native Windows IPsec implementation to establish an operating system level VPN using computer credentials (issued from the Entrust PKI in this scenario) instead of user credentials. This may permit the computer to establish the VPN prior to attempting the domain logon and the downloading of the group policies.

# 7. Future Work

The secure wireless testbed provides sufficient functionality to demonstrate the feasibility of using GoC PKI issued certificates for WLAN and VPN authentication. However, we believe that the testbed must undergo several improvements before it can be presented as a completely integrated solution for GoC enterprise network environments. These improvements include:

1. Re-establish the Entrust Authority Security Manager with 2048-bit CA keys and 2048-bit subscriber keys. The number of key pairs in a subscriber digital identity should be compatible with the GoC PKI.
2. Install and test the new Datakey 330 Smart Card drivers and store 2048-bit user digital credentials on the smart card.
3. Upgrade the Cisco AIRONET 1200 AP hardware/software to support WPA2.
4. Investigate why the 802.1x supplicant does not activate the Entrust Entelligence Security Provider to initiate an Entrust logon when the user attempts to authenticate to the WLAN.
5. Develop ADSI scripts to automatically establish GoC PKI issued certificates as alternate security identities within Active Directory.
6. Investigate the use of PEAP with EAP-TLS to prevent the disclosure of identities encoded in GoC PKI issued certificates.
7. Investigate GoC PKI based authentication with roaming wireless nodes to ensure proper handoff from one AP to another.
8. Investigate the possibility of establishing an operating system level VPN using Entrust PKI issued computer credentials to permit the computer to establish the VPN prior to attempting the domain logon and the downloading of the group policies.

# References

[1] Lynne Genik, Matthew Kellett, Peter C. Mason, Mazda Salmanian and Vahid Aftahi, “Virtual Private Wireless Local Area Networking”, (DRDC Ottawa TM 2006-124), Defence R&D Canada – Ottawa, 2006

[2] Kent, S., Atkinson, R., “Security Architecture for the Internet Protocol”, IETF Request For Comment 2401, November 1998

[3] “Integration Guide – Entrust Wireless Security Using Microsoft 802.1x Authentication Client and Cisco Aironet Access Points”, Document Issue 1.0, Entrust Inc., April 2004

[4] “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”, IEEE

[5] “WPA and WPA2 Implementation White Paper - Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise”, Wi-Fi Alliance, March 2005

[6] "Wi-Fi Protected Access: Strong, standards-based, interoperable security for today’s Wi-Fi networks", Wi-Fi Alliance, April 2003

[7] "Securing Wi-Fi Wireless Networks with Today’s Technologies", Wi-Fi Alliance, February 2003

[8] B. Aboba, L. Blunk, J Vollbrecht, J. Carlson, H. Levkowetz, “Extensible Authentication Protocol (EAP)”, IETF Request For Comment 3748, June 2004

[9] B. Aboba, D. Simon, “PPP EAP TLS Authentication Protocol”, IETF Request For Comment 2716, October 1999

[10] C. Rigney, S. Willens, A. Rubens, W. Simpson, “Remote Authentication Dial In User Service (RADIUS)”, IETF Request For Comment 3748, June 2000

[11] “Deployment of Protected 802.11 Networks Using Microsoft Windows”, Microsoft Corporation, February 2007

[12] "IEEE 802.1X for Wired Networks and Internet Protocol Security with Microsoft Windows", Microsoft Corporation, November 2005

[13] Mick Bauer, “Securing WLANs with WPA and FreeRADIUS”, Paranoid Penguin

[14] “Internet Authentication Service (IAS) Operations Guide”, Microsoft Corporation

[15] C. Adams, S. Farrell, T. Kause, T. Mononen, "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)", IETF Request For Comment 4210, September 2005

[16] A. Nourse, C. Madson, D. McGrew, X. Liu, "Cisco Systems' Simple Certificate Enrollment Protocol(SCEP)", IETF Internet Draft, June 2007

[17] K. Zeilenga, "Lightweight Directory Access Protocol version 3 (LDAPv3)", IETF Request For Comment 3673, December 2003

[18] D. Maughan, M. Schertler, M. Schneider, J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)" IETF Request For Comment 2408, November 1998

[19] D. Harkins, D. Carrel, "The Internet Key Exchange (IKE)", IETF Request For Comment 2409, November 1998

[20] S. Kent, R. Atkinson, "IP Encapsulating Security Payload (ESP)", IETF Request For Comment 2406, November 1998

[21] "The Smart Card Cryptographic Service Provider Cookbook", Microsoft Corporation, October 2002

[22] “Entrust Entelligence™ Security Provider 8.0 for Windows® Administration Guide”, Document issue: 2.0, Entrust Inc., August 2007

[23] A. Palekar, D. Simon, J. Salowey, H. Zhou, G. Zorn, S. Josefsson, “Protected EAP Protocol (PEAP) Version 2“, Internet Draft, October 2004

[24] “Certificate requirements when you use EAP-TLS or PEAP with EAP-TLS”, Microsoft

[25] “Configuring the Contivity VPN Client”, Version 4.10, NORTEL Networks

# Annex A Enabling a New Wireless User

The solution herein provides controlled access to a protected network environment to select users on select wireless computers. This section outlines the procedure for enabling a new wireless computer and a new wireless user.

1. Connect the new wireless computer to the wired network.
2. On the wireless client computer and logged on as the local administrator, install the Entrust Entelligence Security Provider software.
3. On the wireless client computer and logged on as the local administrator, join the computer to the Windows domain. This step must be completed by a Domain Administrator. This creates a computer account in the Active Directory for the new wireless computer.
4. On the Domain Controller, create a user account for the new wireless user in the Active Directory.
5. On the Domain Controller, create a user account for the new wireless computer in the Active Directory. Set the “Full name” of the account to the fully qualified domain name of the new wireless computer. Set the “User login name” to the fully qualified domain name of the new wireless computer. Do not supply a password and disable the account.
6. Use the Entrust Authority Administration tool to add the new wireless user to Entrust. Set the certificate SubjectAltName to the User Principle Name (UPN) associated to the user entry in the Active Directory – (i.e. wirelessuser1@wireless.ottawa.drdc-rddc.gc.ca). Change the certificate type for the new wireless user to “MS VPN Client User”. This ensures the certificate receives the correct Extended Key Usage attribute. Record the reference number and authorization code as they will be needed to enrol the new wireless user in its digital identity.
7. Use the Entrust Authority Administration tool to add the new wireless computer to Entrust. Change the certificate type for the new Wireless computer to “MS Client Machine”.[11] This ensures the certificate receives the correct Extended Key Usage attribute. Record the reference number and authorization code as they will be needed to enrol the new wireless computer in its digital identity.
8. On the wireless client computer and logged on as the local administrator, use the “Entrust Computer Digital ID” snap-in component of the Microsoft Management Console (mmc) to “Enrol Computer for Entrust Digital ID”. Type the reference number and authorization code recorded in step #7 to create the computer digital identity. The Entrust computer identity is stored in the Windows registry and does not require a password for protection.
9. On the wireless client computer, log off as the local administrator and perform a domain logon as the new wireless user.
10. On the wireless client computer and logged on as the new wireless user, use Entrust Entelligence Security Provider to enrol the new wireless user in its digital identity. Select “Enrol for Entrust Digital ID…”. Type the reference number and authorization code recorded in step #6 to create the user digital identity. Select the Entrust disk based profile to store the digital identity and supply a password to protect the digital identity.
11. On the Domain Controller, add the new wireless user Active Directory user account created in step 4 to the “WirelessUsers” group.

[11] We created this certificate type. It was not part of the standard Entrust master.certspec file.

12. On the Domain Controller, check “Allow access” for “Remote Access Permission (Dial-in or VPN)” in the new wireless user’s Active Directory user account created in step #4.
13. On the Domain Controller, establish a mapping between the new wireless user certificate and the new wireless user Active Directory user account created in step 4. Select the new wireless user’s Entrust certificate and save the certificate to a file. Select “Name Mappings” and “Add” a mapping for the certificate by selecting file.
14. On the Domain Controller, select the certificate from the new wireless computer’s Active Directory user account created in step #2 and save it to a file.
15. On the Domain Controller, select the new wireless computer Active Directory computer account created in step #2 and add the entry to the “WirelessUsers” Group.
16. On the Domain Controller, check “Allow access” for “Remote Access Permission (Dial-in or VPN)” in the new wireless computer’s Active Directory computer account created in step #2.
17. On the Domain Controller, establish a mapping between the new wireless computer certificate and the new wireless computer Active Directory computer account created in step #2. Select “Name Mappings” and “Add” a mapping for the certificate by selecting file created in step # 14.
18. On the wireless client computer, log off as the new wireless user, shutdown the new wireless computer, and disconnect the new wireless computer from the wired network.
19. Restart the new wireless computer. The new wireless computer authenticates to the WLAN using computer credentials.
20. On the wireless client computer, perform a domain logon as the new wireless user and log in to Entrust Entelligence Security Provider using the password specified in step #10. After a brief pause, the new wireless computer authenticates to the WLAN using user credentials.

# Annex B Enabling a New VPN User

The solution herein provides controlled access to a protected network environment to select wireless users. This section outlines the procedure for enabling a new wireless VPN user.

1. Connect the new wireless computer to the wired network.
2. On the wireless client computer and logged on as the local administrator, install the NORTEL VPN Client software.
3. On the wireless client computer, log off as the local administrator, shutdown the new wireless computer, and disconnect the new wireless computer from the wired network.
4. Using the NORTEL Contivity Extranet Switch management interface, add a new VPN user to the Base group. Select “Full Distinguished Name” as the “Subject Distinguished Name” and enter the full distinguished name as it appears in the previously issued wireless user certificate.
5. Restart the new wireless computer. The new wireless computer authenticates to the WLAN using computer credentials.
6. On the wireless client computer, perform a domain logon as the new wireless user and log in to Entrust Entelligence Security Provider. The new wireless computer authenticates to the WLAN using user credentials.
7. On the wireless client computer, start the NORTEL VPN Client and create a “New Connection Profile” using the “Connection Wizard”. Select “Digital Certificate or Smartcard” as the “Authentication Type”, select “Microsoft Stored Certificate” as the “Digital Certificate Type” and select the public signature verification certificate (Client Authentication) issued by the Entrust CA. Finally, enter the IP address of the VPN gateway.

# List of symbols/abbreviations/acronyms/initialisms

| | |
|---|---|
| ADSI | Active Directory Script Interface |
| AES | Advanced Encryption Standard |
| CCMP | Cipher-Block Chaining Message Authentication Code Protocol |
| CMP | Certificate Management Protocol |
| CRL | Certificate Revocation List |
| CSE | Communications Security Establishment |
| CSP | Cryptographic Security Provider |
| CSR | Certificate Signing Request |
| DHCP | Dynamic Host Configuration Protocol |
| DIT | Directory Information Tree |
| DN | Distinguished Name |
| DND | Department of National Defence |
| DNS | Domain Name System |
| DRDC | Defence Research and Development Canada |
| DREnet | Defence Research Establishment Network |
| EAP | Extensible Authentication Protocol |
| EKU | Extended Key Usage |
| FIPS | Federal Information Processing Standards |
| GoC | Government of Canada |
| IAS | Internet Authentication Service |
| IETF | Internet Engineering Task Force |
| IIS | Internet Information Service |
| IORDN | Information Operations Research and Development Network |
| IP | Internet Protocol |
| IPsec | Internet Security Protocol |
| ISAKMP | Internet Security Association and Key Management Protocol |
| ITU | International Telecommunication Union |
| LDAP | Lightweight Directory Access Protocol |
| LRA | Local Registration Authority |
| NIO | Network Information Operations |

| | |
|---|---|
| OID | Object Identifier |
| PEAP | Protected Extensible Authentication Protocol |
| PKCS | Public Key Cryptography Standard |
| PKI | Public Key Infrastructure |
| PKIX | Public Key Infrastructure (X.509) |
| PPP | Point-to-Point Protocol |
| PSK | Pre-Shared Key |
| SCEP | Simple Certificate Enrollment Protocol |
| TKIP | Temporal Key Integrity Protocol |

This page intentionally left blank.

This page intentionally left blank.

## DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

| | |
|---|---|
| 1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)<br>NRNS Inc.<br>4043 Carling Avenue, Suite 106<br>Ottawa, Ontario K2K 2A3 | 2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)<br>UNCLASSIFIED |

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C, R or U) in parentheses after the title.)

Securing Wireless Local Area Networks with GoC PKI

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

Spagnolo, J., Cayer, D.

| | | |
|---|---|---|
| 5. DATE OF PUBLICATION (Month and year of publication of document.)<br>October 2007 | 6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)<br>39 | 6b. NO. OF REFS (Total cited in document.)<br>25 |

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Contract Report

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

Secure Mobile Networking Group, Network Information Operations Section, DRDC Ottawa

| | |
|---|---|
| 9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)<br>15BR02 | 9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)<br>W7714 – 030800 / 001 / SV |
| 10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.) | 10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)<br>DRDC Ottawa CR 2007-239 |

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

(X ) Unlimited distribution
( ) Defence departments and defence contractors; further distribution only as approved
( ) Defence departments and Canadian defence contractors; further distribution only as approved
( ) Government departments and agencies; further distribution only as approved
( ) Defence departments; further distribution only as approved
( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

UNLIMITED

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

Defence R&D Canada led a project in which a wireless virtual private networking (VPN) architecture was set up in a test bed in the Network Information Operation (NIO) lab for 802.11/a/b/g communications. The goal of this initial work was to aid in developing a security policy for use of wireless local area networks (WLAN) in government enterprise networks. This report presents the results of follow-on work that leverages the Government of Canada (GoC) Public Key Infrastructure (PKI) technology for strong authentication of wireless users as well VPN users. The solution presented herein relies on the latest wireless security protocols to secure the wireless link and includes an Internet Protocol Security (IPsec) based VPN to achieve a greater level of assurance for more sensitive GoC network environments. The work focuses on the establishment and protection of digital identities, mutual authentication, authorization, data privacy and integrity, as well as wireless network policy management and dissemination.

We conclude that the Wi-Fi Protected Access 2 (WPA2) when operating in enterprise mode and combined with GoC PKI issued certificates and wireless network policy managed through Windows group policies, is an acceptable solution for providing authenticated/secure WLAN access to GoC protected environments. We also conclude that layering IPsec security on top of WPA2 adds complexity without providing additional assurance against unauthorized WLAN access. While testing the proposed solution, difficulties were encountered integrating the IPsec VPN component of the wireless VPN within an enterprise Microsoft Windows environment.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Wireless, WLAN, PKI, Security, VPN, IEEE 802.11, Wi-Fi Protected Access, WPA, WPA2