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

DEFENCE R&D DÉFENSE

Securing wireless local area networks with GoC PKI

Addendum to report DRDC Ottawa CR 2007-239

Joe Spagnolo and Derrick Cayer

Defence R&D Canada – Ottawa
CONTRACT REPORT
DRDC Ottawa CR 2008-142
July 2008

Canada

Securing wireless local area networks with GoC PKI

Addendum to report DRDC Ottawa CR 2007-239

Joe Spagnolo
NRNS Incorporated

Derrick Cayer
NRNS Incorporated

Prepared By:
NRNS Incorporated
4043 Carling Avenue
Suite 106
Ottawa, Ontario, K2K 2A3
Contract Project Manager: Joe Spagnolo, 613-599-7860
DRDC Ottawa CR 2008-142
CSA: Mazda Salmanian, Defence Scientist, 613-998-0649

Defence R&D Canada – Ottawa

Contract Report
DRDC Ottawa CR 2008-142
July 2008

Original signed by Mazda Salmanian

Mazda Salmanian

Scientific Authority

Approved by

Original signed by Julie Lefebvre

Julie Lefebvre

Head, Network Information Operations Section

Approved for release by

Original signed by Pierre Lavoie

Pierre Lavoie

Chairman, Document Review Panel

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

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.

The NIO section sanctioned some initial work to examine the use of Government of Canada (GoC) Public Key Infrastructure (PKI) certificates to regulate user access to the WLAN and to the Internet Protocol Security (IPsec) based VPN. The work focused on the establishment and protection of digital identities, mutual authentication, authorization, data privacy and integrity, as well as wireless network policy management and dissemination. The initial work provided sufficient functionality to demonstrate the feasibility of using GoC PKI issued certificates for WLAN and VPN authentication. However, the initial work concluded that the test bed must undergo several improvements before it can be presented as a completely integrated solution for GoC enterprise network environments. The NIO section approved additional work to address some of the outstanding issues. The results of this latest work are presented in this addendum report.

We conclude that the combination of Wi-Fi Protected Access 2 (WPA2) when operating in enterprise mode, GoC PKI issued and smart card protected user credentials, as well as 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 applying VPN security on top of WPA2 is redundant and adds unnecessary complexity.

Résumé

R & D pour la défense a mené un projet dans le cadre duquel on a constitué une architecture de réseau privé virtuel (RPV) sans fil sur un banc d'essai du laboratoire des Opérations d'information de réseau (OIR) pour effectuer des communications conformes 802.11/a/b/g. L'objectif visé par ces travaux préliminaires était d'aider à l'élaboration d'une politique de sécurité pour les réseaux locaux sans fil (WLAN) dans les réseaux d'entreprise du gouvernement.

La section OIR a commandité certains travaux initiaux pour examiner la possibilité de recourir aux certificats de l'infrastructure à clé publique (ICP) du Gouvernement du Canada (GC) afin de contrôler l'accès à un WLAN et à un RPV fondé sur IPSec (Internet Protocol Security). Les travaux ont été axés sur l'établissement et la protection des identités numériques, l'authentification mutuelle, l'autorisation, la confidentialité et l'intégrité des données, ainsi que la gestion et la diffusion des politiques sur les réseaux sans fil. Les travaux initiaux ont donné lieu à des fonctionnalités suffisantes pour montrer qu'il était possible d'utiliser les certificats fournis par l'ICP de GC pour assurer l'authentification afin d'accéder à un WLAN et un RPV. Les travaux initiaux ont toutefois conclu que plusieurs améliorations doivent être apportées au banc d'essai avant de pouvoir présenter les résultats sous forme d'une solution entièrement intégrée pour les environnements de réseau d'entreprise du GC. La section OIR a approuvé des travaux

additionnels afin de résoudre quelques problèmes qui demeurent. Les résultats de ces travaux plus récents sont présentés dans le présent rapport additionnel.

Nous concluons que la combinaison de l'accès « Wi-Fi Protected Access 2 » (WPA2) en mode entreprise, des justificatifs utilisateur fournis par l'ICP du GC et protégés par une carte à puce, ainsi que d'une politique de réseau sans fil gérée au moyen des politiques de groupe de Windows constitue une solution acceptable pour fournir un accès authentifié et protégé aux environnements protégés du GC par l'intermédiaire d'un WLAN. Nous concluons aussi l'ajout de la sécurité d'une RPV à la technologie WPA2 est redondant et accroît inutilement la complexité.

Executive summary

Securing wireless local area networks with GoC PKI: Addendum to report DRDC Ottawa CR 2007-239

Joe Spagnolo, Derrick Cayer; DRDC Ottawa CR 2008-142; Defence R&D Canada – Ottawa; July 2008.

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.

The NIO section sanctioned some initial work to examine the use of Government of Canada (GoC) Public Key Infrastructure (PKI) certificates to regulate user access to the WLAN and to the Internet Protocol Security (IPsec) based VPN. The work focused on the establishment and protection of digital identities, mutual authentication, authorization, data privacy and integrity, as well as wireless network policy management and dissemination. The initial work provided sufficient functionality to demonstrate the feasibility of using GoC PKI issued certificates for WLAN and VPN authentication. However, the initial work concluded that the test bed must undergo several improvements before it can be presented as a completely integrated solution for GoC enterprise network environments. The NIO section approved additional work to address some of the outstanding issues. The results of this latest work are presented in this addendum report.

Results: We enhanced the secure wireless test bed to better support GoC enterprise network environments. We re-established the Entrust Authority Security Manager with 2048-bit certificate authority (CA) keys and 1024-bit subscriber keys; we issued digital identities consisting of two single-purpose key pairs to better reflect GoC PKI user credentials; we succeeded in storing the user credentials on the smart card; we configured WPA2 as the wireless security protocol; we configured the Protected Extensible Authentication Protocol (PEAP) with the Extensible Authentication Protocol with Transport Layer Security (EAP-TLS) to protect the identities encoded in certificates; we mandated mutual authentication between the wireless client and the wireless authentication server to prevent connections to rogue wireless access points; and we configured a Layer 2 Tunnelling Protocol (L2TP) with IPsec VPN authenticated with both computer and user credentials.

Although we included a VPN component in the solution, we believe that layering VPN security on top of WLAN security is redundant and adds unnecessary complexity. Since we are using the same user credentials to authenticate to both the WLAN and the VPN, an intruder can use the same compromised credentials to impersonate a user to both the WLAN and the VPN authentication servers. If we require VPN security because we do not trust the WLAN security, then we should not incur the expense of securing the WLAN.

We no longer permit the computer to authenticate to the WLAN before the user logs onto the computer. Since Windows does not password protect private keys issued to the computer, we are concerned that the theft of these keys may permit an intruder to gain unauthorized access to the WLAN. Only GoC PKI issued user credentials stored on password protected smart cards should be used to gain access to the WLAN and the protected network. The computer credentials managed by Windows simply ensure that the authorized user makes use of an authorized computer system.

Several key issues remain outstanding that prevent the use of the secure wireless test bed as a model for an integrated solution for GoC enterprise network environments. They include:

1. The 802.1x supplicant and VPN client refuse to use credentials stored on the Datakey 330 Smart Card.

2. The Internet Authentication Server (IAS) does not acknowledge the reduced TLS handle lifetime configuration.

If the VPN forms part of the solution, these issues must also be addressed:

3. The ISA VPN server does not check the revocation status of client certificates.

4. The Windows VPN client does not enforce server authentication for EAP-TLS.

5. The VPN client configuration should be compiled within a group policy.

6. The ISA VPN server should possess the capability to restrict access to the protected network based on the supplied computer and user certificates.

Sommaire

Securing wireless local area networks with GoC PKI: Addendum to report DRDC Ottawa CR 2007-239

Joe Spagnolo, Derrick Cayer; DRDC Ottawa CR 2008-142; R & D pour la défense Canada – Ottawa; Juillet 2008.

Introduction ou contexte: R & D pour la défense a mené un projet dans le cadre duquel on a constitué une architecture de réseau privé virtuel (RPV) sans fil sur un banc d'essai du laboratoire des Opérations d'information de réseau (OIR) pour effectuer des communications conformes 802.11/a/b/g. L'objectif visé par ces travaux préliminaires était d'aider à l'élaboration d'une politique de sécurité pour les réseaux locaux sans fil (WLAN) dans les réseaux d'entreprise du gouvernement.

La section OIR a commandité certains travaux initiaux pour examiner la possibilité de recourir aux certificats de l'infrastructure à clé publique (ICP) du Gouvernement du Canada (GC) afin de contrôler l'accès à un WLAN et à un RPV fondé sur IPSec (Internet Protocol Security). Les travaux ont été axés sur l'établissement et la protection des identités numériques, l'authentification mutuelle, l'autorisation, la confidentialité et l'intégrité des données, ainsi que la gestion et la diffusion des politiques sur les réseaux sans fil. Les travaux initiaux ont donné lieu à des fonctionnalités suffisantes pour montrer qu'il était possible d'utiliser les certificats fournis par l'ICP de GC pour assurer l'authentification afin d'accéder à un WLAN et un RPV. Les travaux initiaux ont toutefois conclu que plusieurs améliorations doivent être apportées au banc d'essai avant de pouvoir présenter les résultats sous forme d'une solution entièrement intégrée pour les environnements de réseau d'entreprise du GC. La section OIR a approuvé des travaux additionnels afin de résoudre quelques problèmes qui demeurent. Les résultats de ces travaux plus récents sont présentés dans le présent rapport additionnel.

Résultats: Nous avons amélioré le banc d'essai protégé sans fil afin de mieux prendre en charge les environnements de réseau d'entreprise du GC. Nous avons rétabli le Entrust Authority Security Manager avec des clés d'autorité de certification (AC) de 2048 bits (CA) et des clés d'abonné de 1024 bits; nous avons distribué des identités numériques composées de deux paires de clés à fonction unique afin de mieux reproduire les justificatifs utilisateur de l'ICP du GC; nous avons réussi à stocker les justificatifs utilisateur sur la carte à puce; nous avons configuré WPA2 comme protocole de sécurité sans fil; nous avons configuré le protocole PEAP (Protected Extensible Authentication Protocol) avec le protocole EAP (Extensible Authentication Protocol) et la sécurité de la couche transport (EAP-TLS) afin de protéger les identités codées dans les certificats; nous avons rendu obligatoire l'authentification mutuelle entre le client sans fil et le serveur d'authentification sans fil afin d'empêcher les connexions avec des points d'accès sans fil non autorisés et nous avons configuré un protocole de tunnel au niveau de la couche 2 (L2TP), l'authentification IPsec du VPN étant réalisée au moyen de justificatifs ordinateur et utilisateur.

Bien que nous ayons inclus une composante RPV dans la solution, nous croyons que la superposition de la sécurité RPV sur la sécurité WLAN est redondante et complique inutilement le système. Comme nous utilisons les mêmes justificatifs utilisateur pour le réseau sans fil et le RPV, un intrus peut utiliser les mêmes justificatifs compromis pour usurper l'identité d'un

utilisateur auprès des serveurs d'identification du réseau sans fil et du RPV. Si nous avons besoin de la sécurité du RPV parce que nous ne faisons pas confiance à la sécurité du réseau sans fil, nous ne devrions pas dépenser pour sécuriser le réseau sans fil.

Nous ne permettrons plus aux ordinateurs d'effectuer leur authentification auprès du WLAN avant que l'utilisateur n'ait ouvert une session sur l'ordinateur. Comme Windows ne protège pas les clés privées accordées à l'ordinateur avec un mot de passe, nous craignons que le vol de ces clés puisse permettre à un intrus d'obtenir un accès non autorisé au WLAN. On ne devrait utiliser que des justificatifs fournis par l'ICP du GC et stockés sur une carte à puce protégée par mot de passe pour accéder au WLAN et au réseau protégé. Les justificatifs de l'ordinateur gérés par Windows garantissent seulement qu'un ordinateur est utilisé par un utilisateur autorisé.

Plusieurs problèmes importants non résolus empêchent l'utilisation du banc d'essai de réseau sans fil protégé comme modèle de solution intégrée pour les réseaux d'entreprise du GC. En voici certains :

1. Le supplicant 802.1x et le client RPV refusent d'utiliser les justificatifs stockés sur la carte à puce Datakey 330.

2. Le serveur d'authentification Internet (IAS) ne reconnaît pas la configuration de la durée des handles TLS.

Si le RPV fait partie de la solution, les problèmes suivants doivent aussi être réglés :

3. Le serveur RPV ISA ne vérifie pas s'il y a eu révocation des certificats client.

4. Le client RPV de Windows VPN n'impose pas l'authentification serveur pour EAP-TLS.

5. La configuration du client VPN devrait être compilée dans une politique de groupe.

Le serveur RPV ISA devrait posséder la capacité de restreindre l'accès au réseau protégé en se basant sur les certificats de l'ordinateur et de l'utilisateur.

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 in GoC protected networks.

The NIO section sanctioned some initial work to examine the use of GoC PKI certificates to regulate user access to the WLAN and to the IPsec based VPN. The work focused on the establishment and protection of digital identities, mutual authentication, authorization, data privacy and integrity, as well as wireless network policy management and dissemination. This initial work is described in [2].

2 Scope of Work

The secure wireless test bed implemented as part of the initial work provided sufficient functionality to demonstrate the feasibility of using GoC PKI issued certificates for WLAN and VPN authentication. However, the report recommended that the test bed must undergo several improvements before it can be presented as a completely integrated solution for GoC enterprise network environments. This addendum report outlines the findings of this recent work. It illustrates the current test bed environment; identifies changes to the proposed solution; details configuration changes; discusses outstanding issues and observations; and describes the operation of the current test bed environment.

3 Test Bed Environment

Figure 1 illustrates the modified test bed environment used to enhance the proposed secure WLAN solution. Modifications include:

- We replaced the NORTEL Contivity Extranet Switch VPN gateway with a Microsoft Internet Security and Acceleration (ISA) Server 2006.
- We eliminated the NORTEL Contivity VPN Client software on the wireless computer and replaced it with the standard Windows XP VPN client software.
- We replaced the Cisco AIRONET AIR-AP1231G wireless access point (AP) with a Cisco AIRONET AIR-AP1242AG wireless AP, which includes support for Wi-Fi Protected Access 2 (WPA2) and the Advanced Encryption Standard (AES) encryption algorithm.
- We installed device drivers for the Cisco AIRONET CB21AG wireless adapter on the wireless computer.
- We installed the Cisco AIRONET Desktop Utility (ADU) software version 4.0 on the wireless computer.
- We added a Windows Vista workstation in order to edit wireless network group policy based on the Windows Vista Wireless and Wired Group Policy Enhancements.

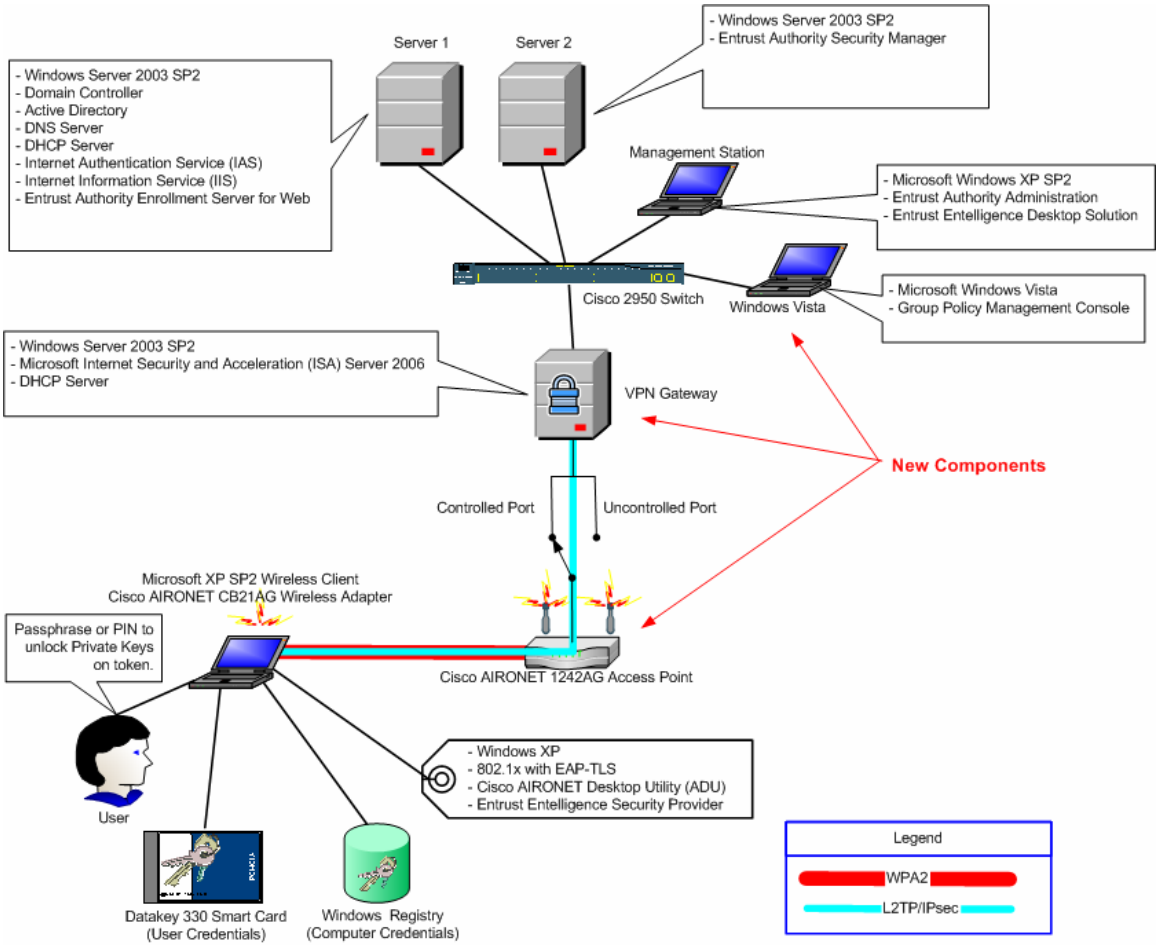

Figure 1- The Lab Environment

4 Solution Modifications

This section outlines the modifications that we introduced to the solution as part of this recent work.

4.1 Computer WLAN Authentication

We removed the computer's Active Directory account from the Active Directory wireless user group since we no longer permit the computer to authenticate to the WLAN before the user logs onto the computer. Computer authentication requires that the computer be issued GoC PKI credentials. Windows stores the corresponding private key in the local key store, which is only accessible by the system. However, Windows does not password protect private keys issued to the computer since the system may perform private key operations before the user logs on. To reduce the risk of theft and/or unauthorized use of the private key, the Entrust CA marks the private key as non-exportable. The Microsoft Internet Authentication Service (IAS) does not differentiate between computer issued certificates and user issued certificates. Theft or compromise of computer issued credentials may permit an attacker to use the computer credentials to authenticate to the WLAN as a user.

Since we no longer permit the computer to authenticate to the WLAN before the user logs onto the computer, we eliminated the need for the VPN gateway to pass non-VPN traffic required by the computer to complete a Windows domain logon and download group policies.

4.2 Certificate Enrolment

We no longer make use of the Entrust Enrolment Server for Web to issue credentials to the IAS server. Instead we defined an enterprise certificate type and installed Entrust Entelligence Security Provider on the IAS system and used it to acquire the computer certificate from the Entrust CA. We used the same approach for installing a computer certificate on the ISA VPN server.

4.3 VPN Configuration

Microsoft Windows XP includes support for two flavours of VPN: the Point-to-Point Tunnelling Protocol (PPTP) [19] as well as the Layer 2 Tunnelling Protocol (L2TP) [20] combined with IPsec [21]. We configured the VPN using L2TP/IPsec.

5 Configuration Changes

This section describes the configuration changes needed to implement the current solution.

5.1 Key Lengths

We re-initialized the Entrust Certificate Authority (CA) with 2048-bit CA keys and 1024-bit subscriber keys. We chose these settings to reflect the current configuration of the Department of National Defence (DND) certificate authority (CA).

5.2 Smart Cards

We were successful in storing Entrust PKI credentials on the Datakey 330 Smart Card with the use of the Entrust Entelligence Security Provider. We employed Microsoft Internet Explorer (IE) to confirm the correct operation of the Datakey Smart Card. When IE accessed a secure web site that required certificate based client authentication, we were prompted for the personal identification number (PIN) to unlock the smart card. This permitted the smart card to execute the cryptographic operations required to authenticate to the secure web site.

5.3 WPA2

Windows XP SP2 requires a software update to support WPA2. We installed the KB917021 update [3] on the Windows XP wireless client computers. This update also enables WPA2 support in wireless network group policies (see section 5.6).

We were successful in establishing a WPA2 secured wireless link between the Windows XP wireless computer and the AIRONET AIR-AP1242AG wireless AP.

5.4 Certificate Types

As part of the initial work, we issued single key-pair digital identities to users. As part of this recent work, we issued digital identities consisting of two single-purpose key pairs (one for digital signatures and one for encryption) to better reflect GoC PKI user credentials. We created new certificate types based on the Entrust default enterprise certificate type. The relevant portions of the Entrust certificate specification file that describe these certificate types are included in Annex C.

The “ent_wireless_default” certificate type permits a user to authenticate to the WLAN using credentials stored on a smart card. It generates two single-use key pairs and issues two public certificates – one for verification and one for encryption. It includes the required Extended Key Usage (EKU) extension in the verification certificate.

The “ent_wireless_epf” certificate type is similar to the “ent_wireless_default” certificate type but stores the user credentials in an Entrust disk based profile.

The "ent_vpn_computer" certificate type permits a computer to authenticate to the VPN. It generates a single dual-use key pair and issues a single verification/encryption certificate. It includes the required EKU extension in the sole dual-purpose certificate.

The "wireless_auth_server" certificate type is issued to the IAS and ISA servers to enable them to serve as an authentication server. It generates a single dual-use key pair and issues a single verification/encryption certificate. It includes the required EKU extension in the sole dual-purpose certificate.

5.5 Dynamic Host Configuration

We configured the Microsoft ISA VPN server to act as a Dynamic Host Configuration Protocol (DHCP) server for wireless computers. As part of the initial work we were forced to assign a static network address to the wireless computer since the NORTEL VPN gateway did not include a DHCP server and did not relay DHCP requests to an internal DHCP server.

5.6 Wireless Network Group Policy

Windows Server 2003 does not support the inclusion of WPA2 settings in its wireless network group policy. Wireless clients running Windows Vista can support WPA2 configured through a wireless network group policy obtained from the new Windows Server 2008 operating system. However, the Windows Vista Group Policy Management Console may be used to compile a WPA2 compliant wireless network group policy for a Windows 2003 Server.

After we applied the required Active Directory schema extensions [4], we were able to compile WPA2 compliant wireless network group policy on the Windows 2003 Server using the Windows Vista Group Policy Management Console [5]. This required the deployment of a Windows Vista computer within the Windows domain and the use of a domain administrator account on the Windows Vista system to edit the wireless network group policy. After we applied the Active Directory schema extensions and altered the wireless network group policy using the Windows Vista system, we could no longer edit the wireless network group policy on the Windows Server 2003 system. The Windows Server 2003 group policy editor could only view the read-only wireless network group policy.

We enhanced the wireless network group policy to use the Protected Extensible Authentication Protocol (PEAP) in conjunction with the Extensible Authentication Protocol (EAP) with Transport Layer Security EAP type (EAP-TLS). PEAP encrypts the user's public certificate, which contains a distinguished name as well as other information that identifies the owner of the certificate. Unlike the TLS session established for EAP-TLS, which delivers mutual authentication between the client and the server, the PEAP TLS session does not require client authentication and only authenticates the server to the client. Mutual authentication for the PEAP TLS session would require that the client expose its public certificate, which defeats the purpose of layering PEAP over EAP-TLS.

The following diagrams display screen shots from the Windows Vista Group Policy Management Console and illustrate the compiled wireless network group policy.

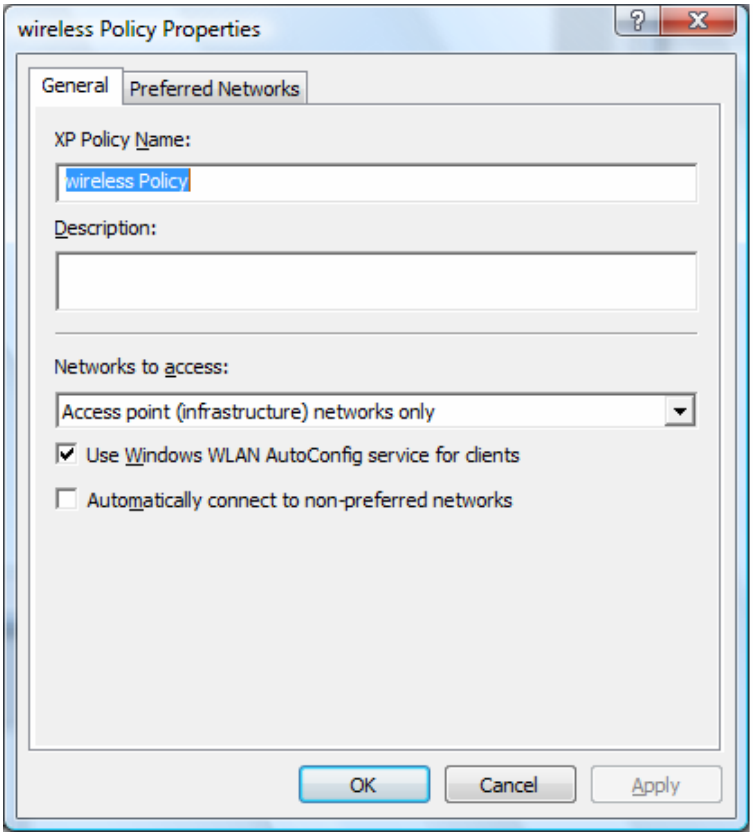

Figure 2 – Windows XP Wireless Network Policy

Figure 2 illustrates the creation of a Windows XP wireless network policy using the Windows Vista Group Policy Management Console.

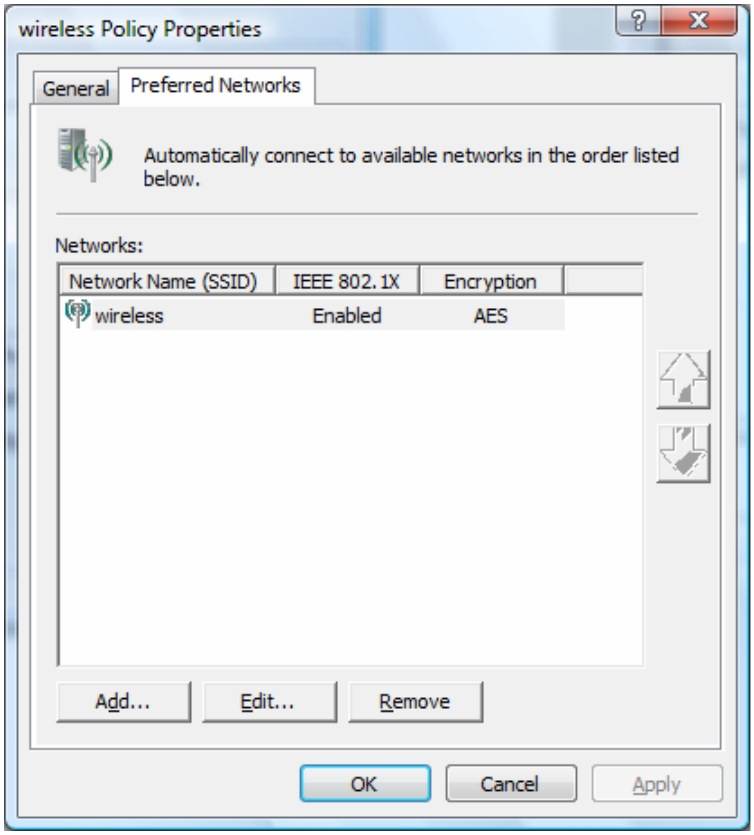

Figure 3 - Preferred Networks

Figure 3 illustrates the definition of the preferred network called "wireless".

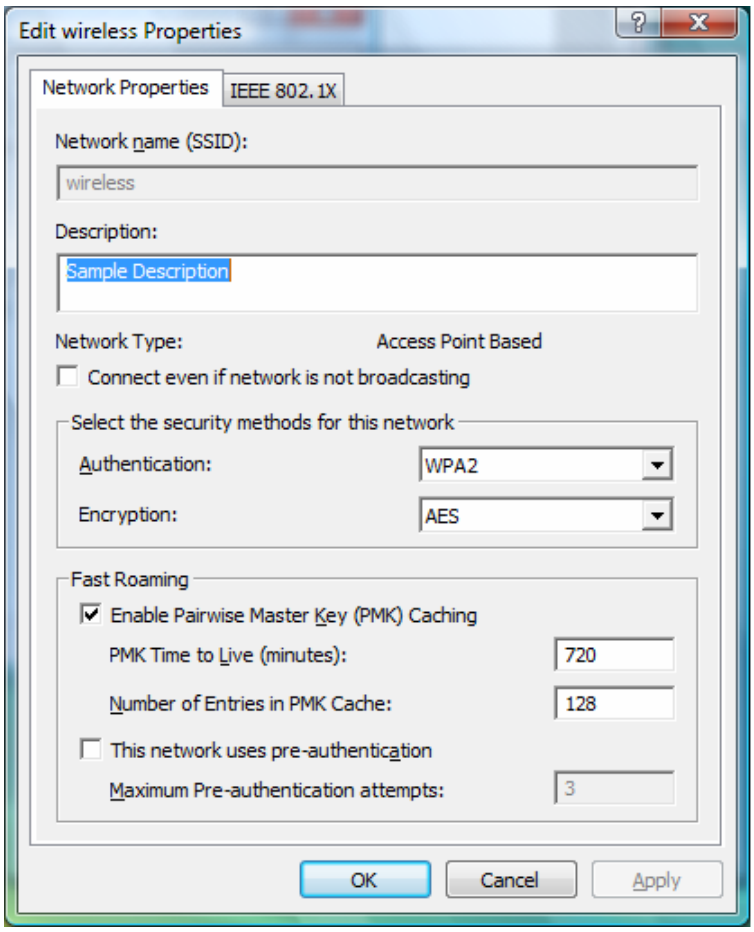

Figure 4 - Wireless Network Properties

Figure 4 illustrates the wireless network properties for the "wireless" network. We selected "WPA2" as the authentication method and "AES" as the encryption algorithm.

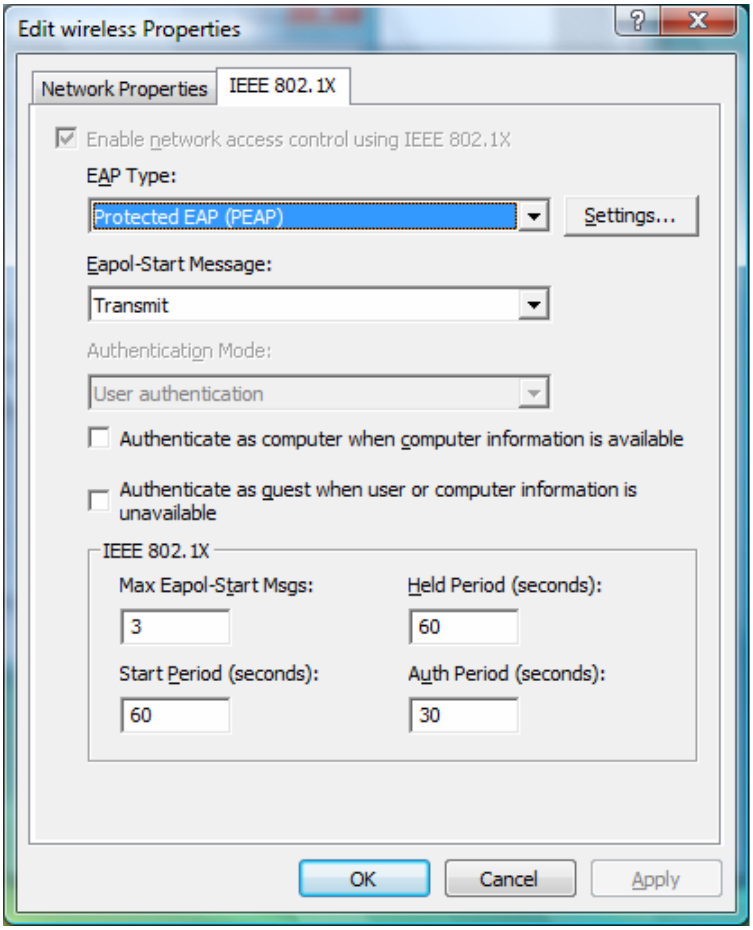

Figure 5 – IEEE 802.1x Settings

Figure 5 shows the wireless properties required to enable PEAP instead of EAP-TLS. We selected "Protected EAP (PEAP)" as the "EAP type". Since we no longer permit the computer to authenticate to the WLAN before the user logs onto the computer, we unchecked the "Authenticate as computer when computer information is available" option.

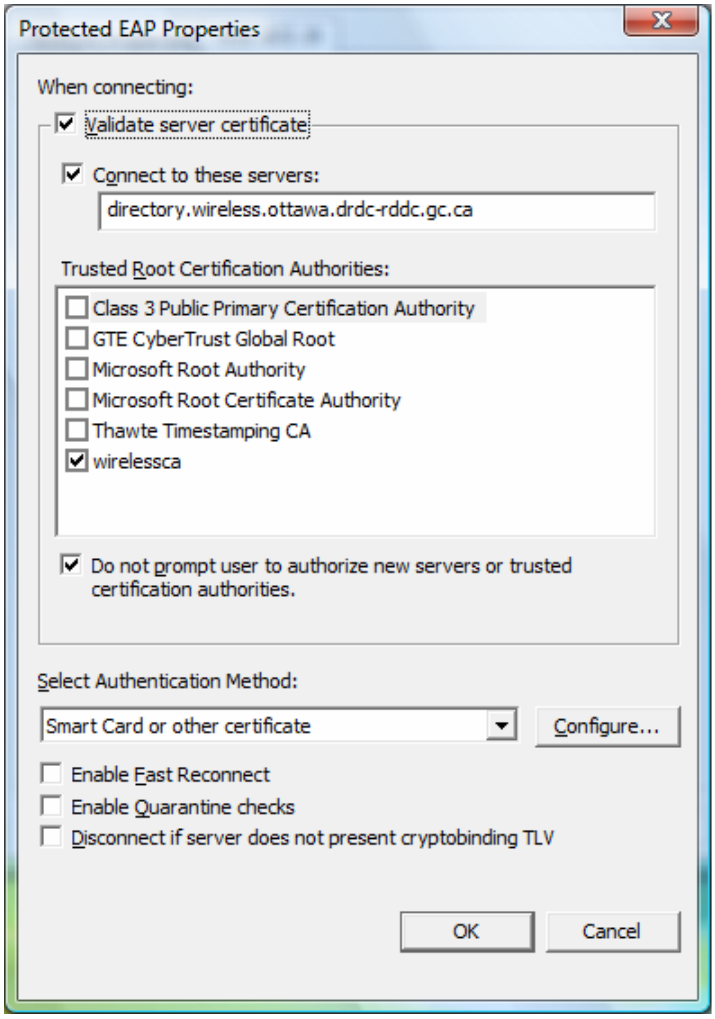

Figure 6- Protected EAP Properties

Figure 6 illustrates the PEAP configuration properties. Selecting "Smart card or other certificate" as the authentication method enables EAP-TLS as the secondary authentication method. As with EAP-TLS, we want the PEAP client to authenticate the server so we identified the authorized authentication server. In this case, the authentication server must present the "directory.wireless.ottawa.drdc-rddc.gc.ca" certificate issued by the "wirelessca". We issued the "directory.wireless.ottawa.drdc-rddc.gc.ca" certificate to the IAS RADIUS server. This is the IAS RADIUS server computer certificate that the IAS RADIUS server stores in its local key store. The policy does not allow the system to prompt the user to authorize new servers or trusted certification authorities, which is an absolute requirement for guaranteeing server authentication.

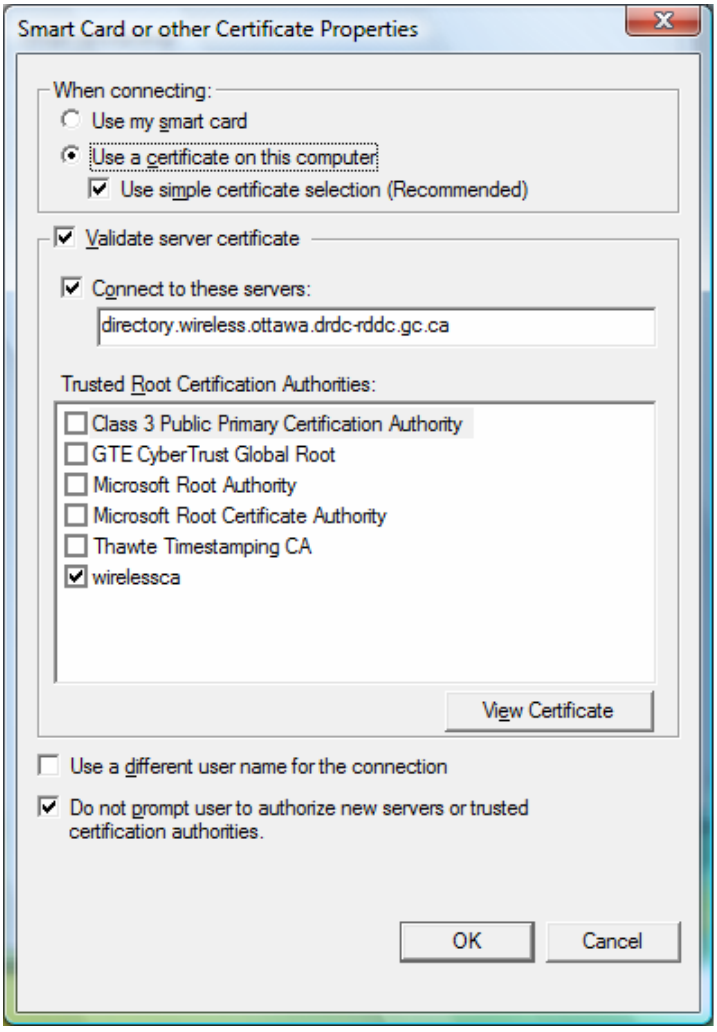

Figure 7- EAP Certificate Properties

Figure 7 illustrates the EAP-TLS configuration properties. These are the exact same settings as we configured for EAP-TLS as part of the initial work. Since we require mutual authentication between the client and the server, we again identified the authorized authentication server. The authentication server must present the "directory.wireless.ottawa.drdc-rddc.gc.ca" certificate issued by the "wirelessca". Like the PEAP properties, the EAP-TLS properties include the "Do not prompt user to authorize new servers or trusted certification authorities" option, which is an absolute requirement for guaranteeing mutual client/server authentication. This option was not present using the Windows Server 2003 group policy editor.

5.7 VPN Client Configuration

We configured L2TP/IPsec to establish a VPN between the wireless computer and the Microsoft ISA VPN server. L2TP/IPsec includes two levels of authentication. IPsec requires computer credentials to authenticate the physical computer to the VPN gateway and L2TP requires user credentials to authenticate the user to the VPN gateway. Our solution mandates the use of GoC

PKI certificates for both IPsec and L2TP authentication. This section describes the configuration settings required on each Windows XP wireless computer to establish an L2TP/IPsec VPN between the wireless computer and the ISA VPN server.

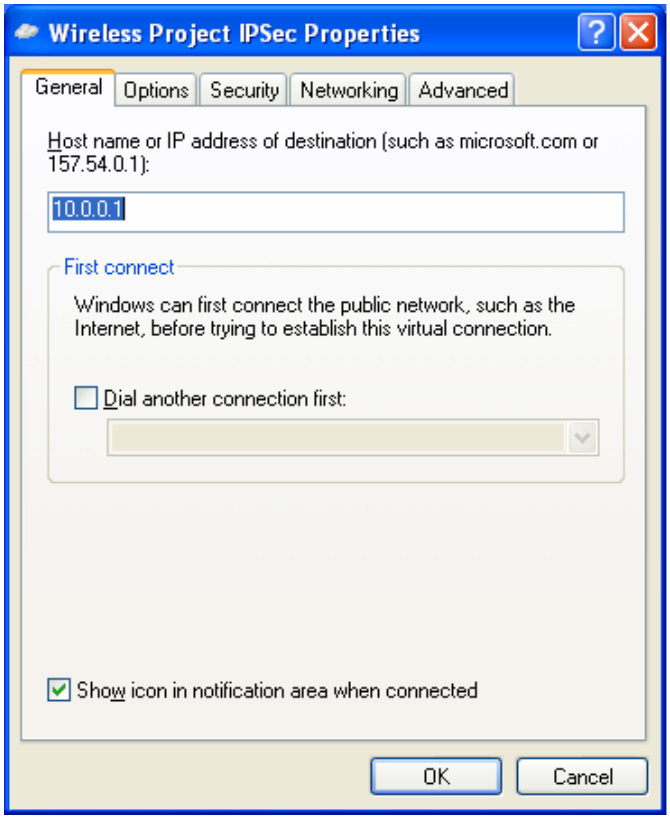

Figure 8 - VPN Client General Settings

Figure 8 illustrates the general settings for the VPN client. This configuration pane simply identifies the IP address of the ISA VPN server.

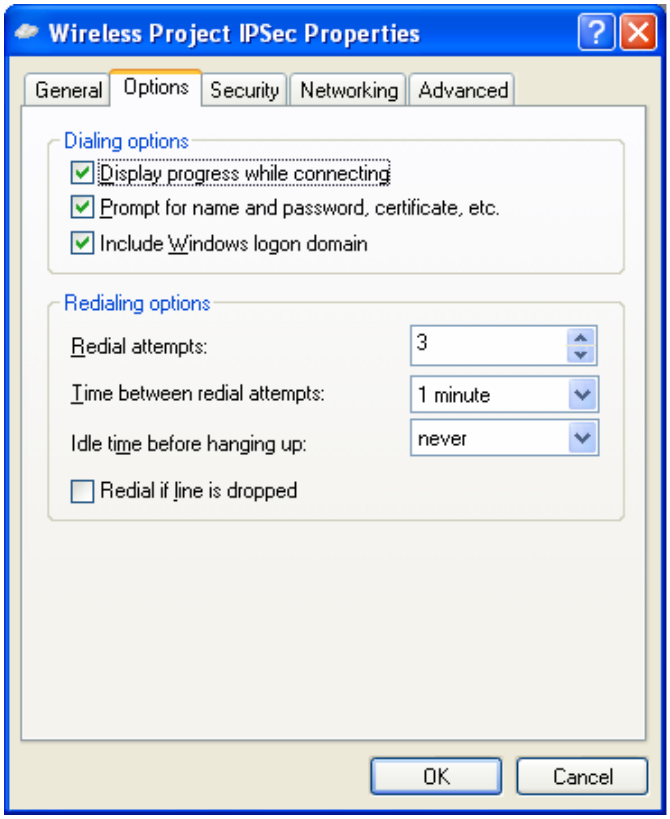

Figure 9 - VPN Client Options

Figure 9 illustrates the VPN client options. We selected the "Include Windows logon domain" option to initiate a Windows domain logon after the VPN establishes itself.

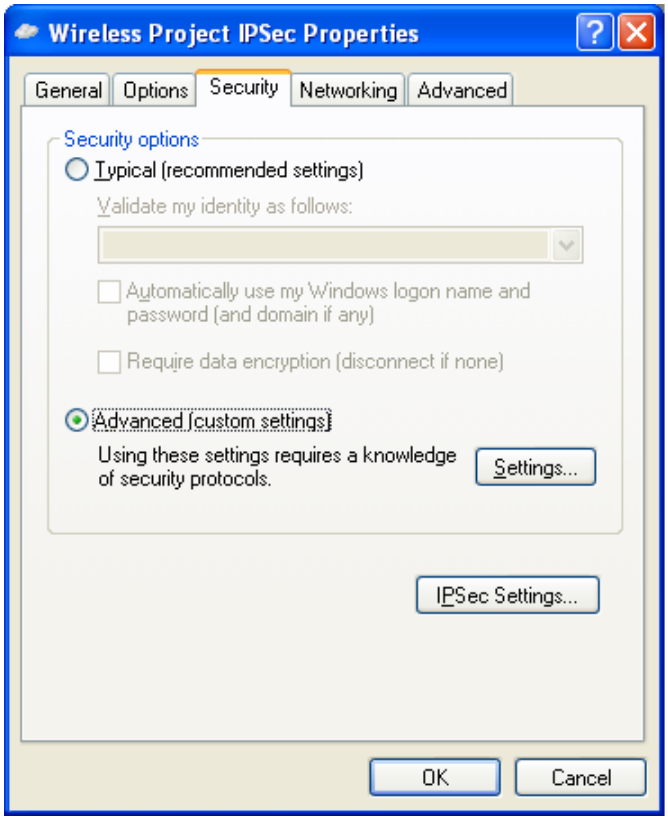

Figure 10 - VPN Client Security Settings

Figure 10 illustrates the VPN client security settings. We selected "Advanced [custom settings]". The "Settings" button accesses the advanced settings.

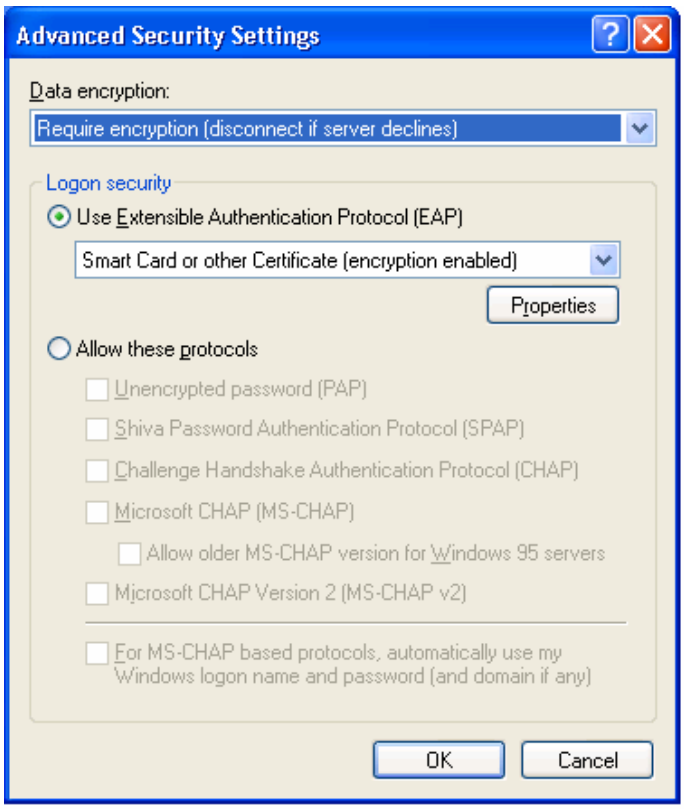

Figure 11 - VPN Client Advanced Security Settings

Figure 11 illustrates the VPN client advanced security settings. We mandated the use of encryption and selected EAP with smart cards or certificates as the authentication method.

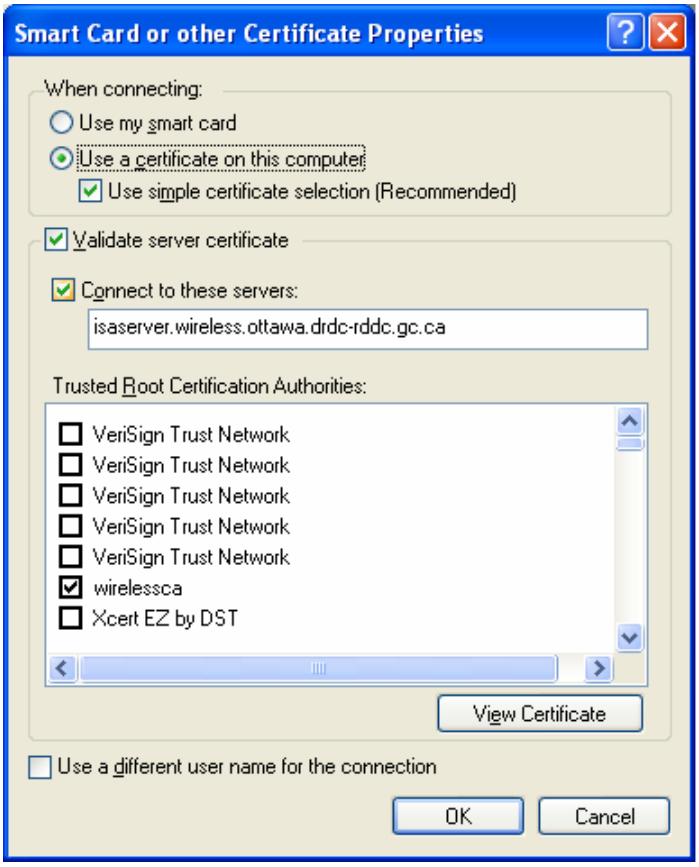

Figure 12 - VPN Gateway Certificate Properties

Figure 12 illustrates the certificate properties for the VPN gateway certificate. Since we require mutual authentication between the client and the server, we again identified the authorized authentication server. The certificate presented by the VPN gateway must be valid; the VPN gateway certificate must contain "isaserver.wireless.ottawa.drdc-rddc.gc.ca" as the SubjectName or SubjectAltName; and the VPN gateway certificate must have been issued by the trusted certificate authority called "wirelessca". We issued the "isaserver.wireless.ottawa.drdc-rddc.gc.ca" certificate to the ISA VPN server. This is the ISA VPN server computer certificate that the ISA VPN server stores in its local key store. These settings permit the VPN client to detect rogue or unauthorized VPN gateways. If the configuration does not identify a trusted VPN gateway, an attacker could deploy an unauthorized VPN gateway using other credentials issued by the trusted CA.

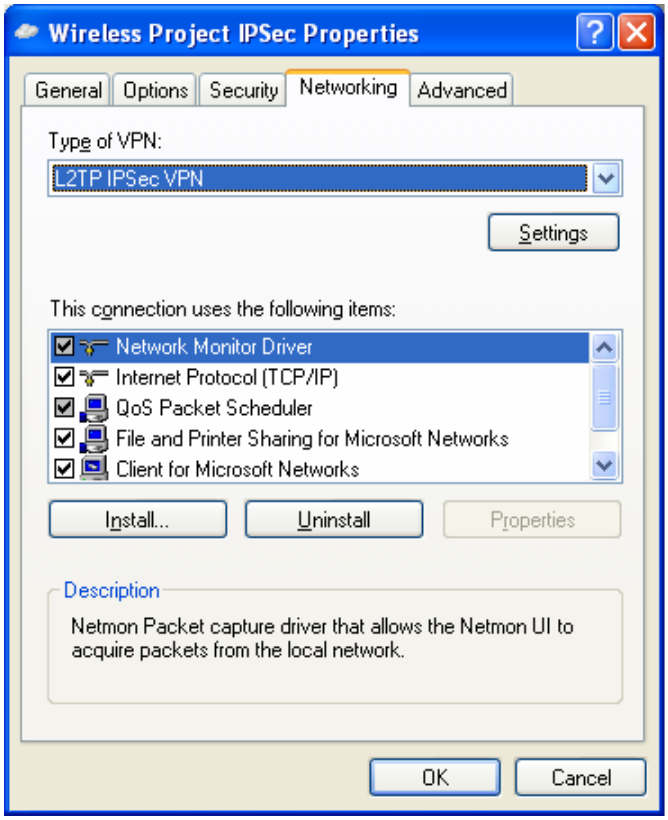

Figure 13 - VPN Client Networking Settings

Figure 13 illustrates the VPN client networking settings. We specified "L2TP IPSec VPN" as the VPN type.

6 Outstanding Issues and Observations

This section outlines outstanding issues as well as other observations that we noted during our configuration and testing activities.

6.1 Smart Cards

We were unsuccessful in using the Datakey 330 Smart Card to authenticate to the wireless network. The Windows 802.1x supplicant reported that "The card is available for use. However the card is not the one being requested and cannot be used for the current operation". We opened a service request with Microsoft support who concluded that the card ATR[1] was not saved in the registry and linked to a Cryptographic Security Provider (CSP). We opened a service request with Entrust to report this problem.

6.2 Certificate Selection

The Windows 802.1x supplicant can use either the encryption or the verification certificate to authenticate to the WLAN. However the certificate selection process appears to be non-deterministic. Initially the 802.1x supplicant selected the encryption certificate, but the WLAN authentication failed since the encryption certificate did not contain the required client authentication Extended Key Usage (EKU) extension. We responded by adding the required EKU extension to the encryption certificate as well as the verification certificate and re-issued the user credentials. The 802.1x supplicant then selected the verification certificate, which allowed the user to authenticate to the WLAN. We proceeded to remove the client authentication EKU extension from the encryption certificate and re-issued the user credentials. The 802.1x supplicant again selected the verification certificate, which allowed the user to authenticate to the WLAN.

We were unable to identify the algorithm used by the Windows 802.1x supplicant to select the certificate for WLAN authentication.

6.3 Windows Domain Logon

When the wireless computer is connected to the wired network and the user logs into the Windows domain, Windows caches the user's domain credentials on the wireless computer. This permits the user to complete a Windows Domain logon before the user authenticates and gains access to the WLAN. After the wireless user establishes the L2TP/IPsec VPN (authenticated with the user certificate), Windows initiates a domain logon with the username/password credentials supplied by the user when the user performed the initial computer logon (refer to Figure 9). This allows the user to access domain resources such as file servers without repeatedly having to furnish the same Windows Domain credentials that the user supplied when the user logged onto the computer.

[1] A sequence of bytes returned from a smart card when it is turned on. These bytes are used to identify the card to the system. This definition was acquired from the Microsoft Developer Network.

6.4 Private Key Access

In the initial report, we described how the 802.1x supplicant does not invoke the Entrust Entelligence Security Provider to prompt the user for the password to unlock the Entrust based profile. This issue may be related to the problem described in Section 6.1 whereby the 802.1x supplicant is unable to access the Datakey 330 Smart Card. We included this issue in the service request to Microsoft and Entrust.

6.5 IAS Server Authentication

The wireless network group policy presented section 5.6 includes a check box labelled "Do not prompt user to authorize new servers or trusted certification authorities" for both the PEAP and EAP-TLS settings. We noted that PEAP enforces server authentication on the wireless computer. If the certificate presented by the authentication server does not match the identity configured in the group policy (as described in Figure 6 in section 5.6), the 802.1x supplicant blocks the connection to the WLAN. The 802.1x supplicant does not allow the user to authorize new servers or trusted certification authorities. We also noted that EAP-TLS as the secondary authentication method also enforces server authentication on the wireless computer. When the certificate presented by the authentication server does not match the identity configured in the group policy (as described in Figure 7 in section 5.6), the 802.1x supplicant blocks the connection to the WLAN. This enforces server authentication and prevents the user from connecting to rogue wireless access points.

When configured with the basic Windows Server 2003 wireless network group policy[2], EAP-TLS as the secondary authentication method does not enforce server authentication on the wireless computer. When the certificate presented by the authentication server does not match the identity configured in the group policy, the 802.1x supplicant prompts the user to authorize the unknown authentication server. This defeats server authentication and permits the user to override the wireless network group policy and connect to a rogue wireless access point. Please note that unlike the EAP-TLS configuration shown in Figure 7, the EAP-TLS configuration presented by the Windows Server 2003 group policy editor does not include a check box labelled "Do not prompt user to authorize new servers or trusted certification authorities". Furthermore, EAP-TLS exhibits the same behaviour when configured as the primary authentication method.

6.6 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. By default the IAS server caches a TLS handle for 10 hours [6]. When a wireless client reconnects, the IAS server does not check the revocation status of the wireless

[2] Before the Active Directory schema was extended and the wireless network group policy was created using the Windows Vista Group Policy Management Console.

client certificate. Furthermore, the IAS server[3] only retrieves a new Certificate Revocation List (CRL) when the current CRL expires[4] [7].

As illustrated in Figure 14, the IAS server caches the TLS handle after the wireless user connects successfully to the WLAN. If the wireless user attempts to reconnect to the WLAN with a revoked certificate, the IAS server grants access to the WLAN based on the cached TLS handle without checking the revocation status of the certificate. If the revoked wireless user attempts to reconnect to the WLAN after the TLS handle expires and the IAS server retrieves the new CRL, the IAS server consults the new CRL and rejects access to the WLAN.

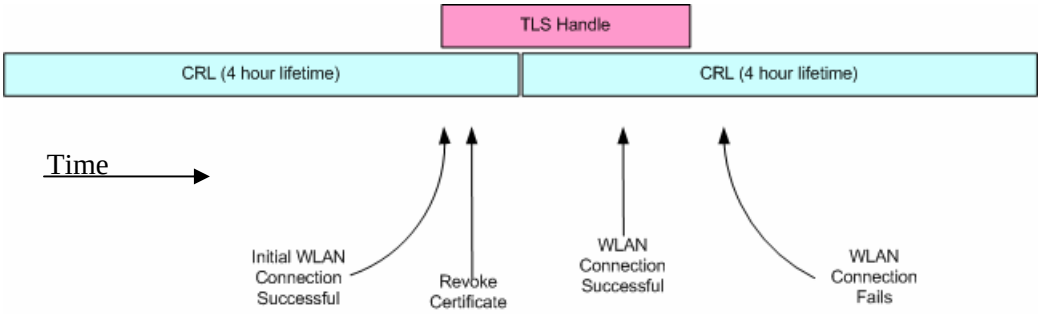

Figure 14 - TLS Handle Caching

As part of the initial work we modified Windows registry settings within the IAS server to limit the lifetime of a cached TLS handle to 300,000 milliseconds or 5 minutes. Although that appeared to prevent the use of recently revoked certificates for WLAN authentication, we were unable to reproduce that behaviour as part of the most recent work.

6.7 VPN Group Policies

Ideally a domain administrator should compile the VPN client settings presented in section 5.7 within a group policy that is acquired by all wireless computers. We did not have sufficient time to experiment with group policies for VPN access.

6.8 VPN Access Control

The IAS Server ensures that all certificates presented by wireless clients form part of the wireless group. The ISA VPN server should also possess this capability so that it may restrict access to the protected network based on the supplied computer and user certificates and only grant access to computers and users that were deemed to require VPN access. Ideally, the ISA VPN server should differentiate between computer certificates for IPsec authentication and user certificates for L2TP authentication. We did not have sufficient time to experiment with VPN access control in the ISA VPN server.

[3] The CRL cache is maintained by the underlying Windows 2003 Server.
[4] The CRL lifetime is 4 hours as determined by the Entrust Security Manager

6.9 ISA VPN Server Authentication

We noted that EAP-TLS does not enforce server authentication for the VPN client. When the certificate presented by the VPN gateway does not match the identity configured in the VPN client configuration (as described in Figure 12 in section 5.7), the VPN client prompts the user to authorize the unknown VPN gateway. This defeats server authentication and permits the user to override the VPN settings and connect to a rogue VPN gateway. Figure 12 does not include a check box labelled "Do not prompt user to authorize new servers or trusted certification authorities".

6.10 VPN Client Certificate Status Checking

We configured CRL checking within the ISA VPN server but the ISA VPN server could not detect revoked certificates. There was no evidence that the ISA VPN server attempted to retrieve the CRL from the Active Directory.

7 Test Bed Operation

The test bed environment allows an authorized wireless user to authenticate to the WLAN and the L2TP/IPsec VPN using GoC PKI issued credentials. The scenario described below assumes that the user credentials are stored in an Entrust disk based profile maintained by Entrust Security Provider and stored not on a smart card (see section 6.1).

1. The user logs into the wireless computer using her domain username/password credentials. The wireless computer verifies the credentials against cached domain credentials present on the wireless computer.

2. The wireless computer attempts to connect to the authorized WLAN.

3. The system warns the user that Windows was not able to find a certificate to log on to the WLAN.

4. The user logs into Entrust Entelligence Security Provider and unlocks her GoC PKI credentials.

5. The system prompts the user to select a certificate to authenticate the user to the WLAN.

6. The user selects her GoC PKI certificate.

7. The 802.1x supplicant employs the selected user certificate and associated credentials to authenticate the wireless computer with the IAS.

8. The wireless AP grants the wireless computer access to the WLAN.

9. The system caches the selected certificate when the user successfully authenticates to the WLAN. As such, future WLAN connection attempts may omit steps 5 and 6.

The remaining steps are not required in deployments that exclude the VPN gateway. Once the user authenticates to the IAS server and the wireless AP grants the wireless computer access to the WLAN, the computer acquires access to the wired network.

10. The user initiates the L2TP/IPsec VPN to the ISA VPN server.

11. Assuming that the user's GoC PKI credentials remain unlocked, the system prompts the user to select a certificate to authenticate the user to the L2TP/IPsec VPN.

12. The user selects her GoC PKI certificate.

13. The L2TP/IPsec VPN client employs the computer certificate (for IPsec) and the selected user certificate (for L2TP) to authenticate the wireless computer with the ISA VPN server.

14. The ISA VPN server grants the wireless computer access to the VPN and logs the user into the Windows domain.

15. The system caches the selected certificate when the user successfully authenticates to the VPN. As such, future VPN connection attempts may omit steps 11 and 12.

16. The wireless computer gains access to the wired protected network.

17. The user can access domain resources such as file servers without the need to supply additional credentials.

Annex A identifies the necessary steps to enable a new wireless user. Annex B identifies the necessary steps to enable a new wireless VPN user.

8 Conclusions

We enhanced the secure wireless test bed to better support GoC enterprise network environments. We re-established the Entrust Authority Security Manager with 2048-bit CA keys and 1024-bit subscriber keys; we issued digital identities consisting of two single-purpose key pairs to better reflect GoC PKI user credentials; we succeeded in storing the user credentials on the smart card; we configured WPA2 as the wireless security protocol; we configured PEAP with EAP-TLS to protect the identities encoded in certificates; we mandated mutual authentication between the wireless client and the IAS RADIUS server to prevent connections to rogue wireless access points; and we configured a L2TP/IPsec VPN authenticated with both computer and user credentials.

Although we included a VPN component in the test bed, we believe that layering VPN security on top of WLAN security is redundant and adds unnecessary complexity. Since we are using the same user credentials to authenticate to both the WLAN and the VPN, an intruder can use the same compromised credentials to impersonate a user to both the WLAN and the VPN authentication servers. If we require VPN security because we do not trust the WLAN security, then we should not incur the expense of securing the WLAN.

We no longer permit the computer to authenticate to the WLAN before the user logs onto the computer. Since Windows does not password protect private keys issued to the computer, we are concerned that the theft of these keys may permit an intruder to gain unauthorized access to the WLAN. Only GoC PKI issued user credentials stored on password protected smart cards should be used to gain access to the WLAN and the protected network. The computer credentials managed by Windows simply ensure that the authorized user makes use of an authorized computer system.

Several key issues remain outstanding that prevent the use of the secure wireless test bed as a model for an integrated solution for GoC enterprise network environments. They include:

18. The 802.1x supplicant refuses to use credentials stored on the Datakey 330 Smart Card to authenticate a user to the WLAN. Although the system sees the smart card in the reader, the system does not recognize the card and refuses to use it. Microsoft support concluded that the card ATR is not saved in the registry and linked to a CSP. We raised this issue in a service request to Entrust. This problem appears to be localized to the 802.1x supplicant and the Windows VPN client since we were able to use the credentials stored on the Datakey 330 Smart Card to authenticate to a secure web server.

19. The IAS server does not acknowledge the reduced TLS handle lifetime configuration. The IAS server permits a revoked user to access the WLAN based on the availability of a cached TLS handle. This issue needs to be raised with Microsoft.

If the VPN forms part of the solution, these issues must also be addressed:

20. The ISA VPN server does not check the revocation status of client certificates. We believe that this issue can be resolved if the device is properly configured. We did not have sufficient time to examine this issue in detail.

21. The Windows VPN client does not enforce VPN gateway authentication for EAP-TLS. When the VPN gateway presents a certificate different than the certificate described in the VPN client settings, the system allows the user to override the VPN settings and connect to an unauthorized VPN gateway.

22. The VPN client configuration should be compiled within a group policy that is acquired by all wireless computers instead of being created and managed independently on numerous computers.

23. The ISA VPN server should possess the capability to restrict access to the protected network based on the supplied computer and user certificates and only grant access to computers and users that were deemed to require VPN access.

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] Joe Spagnolo, D. Cayer, “Securing Wireless Local Area Networks with GoC PKI”, (DRDC Ottawa CR 2007-239), Defence R&D Canada – Ottawa, 2007

[3] “Description of the Wireless Client Update for Windows XP with Service Pack 2”, Article ID 917021, Revision 5.1, Microsoft Corporate, August 2007

[4] “Active Directory Schema Extensions for Windows Vista Wireless and Wired Group Policy Enhancements”, Microsoft Corporation, May 2006

[5] “Windows Vista Wireless Networking Evaluation Guide”, Microsoft Corporation

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

[7] “Certificate Revocation and Status Checking”, Microsoft Corporation, January 2006

[8] “Protected Extensible Authentication Protocol”, Microsoft Corporation, January 2005

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

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

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

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

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

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

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

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

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

[18] “Basic L2TP/IPsec Toubleshooting in Windows XP”, Microsoft Corporation

[19] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, G. Zorn, "Point-to-Point Tunneling Protocol (PPTP)", IETF Request For Comment 2637, July 1999

[20] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, B. Palter, "Layer Two Tunneling Protocol "L2TP"", IETF Request For Comment 2661, August 1999

[21] B. Patel, B. Aboba, W. Dixon, G. Zorn, S. Booth, "Securing L2TP using IPsec", IETF Request For Comment 3193, November 2001

This page intentionally left blank.

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. 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 "Default Wireless EPF"[5]. 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.

6. On the wireless client computer, log off as the local administrator and perform a domain logon as the new wireless user.

7. 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 #5 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.

8. On the Domain Controller, add the new wireless user Active Directory user account created in step 4 to the "WirelessUsers" group.

9. 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.

10. 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.

[5] When the Entrust credentials are stored on the smart card, use "Default Wireless".

11. 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.

12. Restart the new wireless computer.

13. 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 #7. 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 configuring a new wireless VPN user. The following steps are best performed between step 3 and step 4 of the "Enabling a New Wireless User" procedure described in Annex A.

1. Use the Entrust Authority Administration tool to add the new wireless computer to Entrust. Change the certificate type for the new Wireless computer to "VPN Computer". 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.

2. 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 #1 to create the computer digital identity. The Entrust computer identity is stored in the Windows registry and does not require a password for protection.

3. On the wireless client computer, configure the L2TP/IPsec VPN connection as described in 5.7. Create a new VPN connection via "Start→Control Panel→Network Connections".

To connect to the VPN, simply double click on the VPN connection after the wireless computer completes the WLAN authentication (step 13 of the "Enabling a New Wireless User" procedure described in Annex A) and achieves connectivity to the WLAN.

Annex C Certificate Specifications

```
; -------------------------------------------------------------------
; Default Enterprise Wireless Certificate Type
;
; For authenticating to the WLAN with credentials stored on a
; smart card.
; -------------------------------------------------------------------
ent_wireless_default=enterprise,Default Wireless,Default Wireless
Enterprise Certificates
;-------------------------------------------------------------------
;- Enterprise Default Wireless Certificate Type                    -
;-                                                                 -
;- This certificate type defines two key pairs                     -
;- Encryption:     has keyEncipherment key usage bit set           -
;- Verification:   has digitalSignature key usage bit set          -
;-                 has client authentication enhanced key usage set -
;-------------------------------------------------------------------
[ent_wireless_default Certificate Definitions]
1=Encryption
2=Verification

[ent_wireless_default Encryption Extensions]
keyusage=2.5.29.15,n,m,BitString,001

[ent_wireless_default Verification Extensions]
keyusage=2.5.29.15,n,m,BitString,1
extkeyusage=2.5.29.37,n,m,SeqOfObjectIdentifier,1.3.6.1.5.5.7.3.2


; -------------------------------------------------------------------
; EPF Enterprise Wireless Certificate Type
;
; For authenticating to the WLAN with credentials stored in an Entrust
; disk based profile.
; -------------------------------------------------------------------
ent_wireless_epf=enterprise,Default Wireless EPF,Default Wireless EPF
Enterprise Certificates
;-------------------------------------------------------------------
;- Enterprise Wireless EPF Certificate Type                        -
;-                                                                 -
;- This certificate type defines two key pairs                     -
;- Encryption:     has keyEncipherment key usage bit set           -
;- Verification:   has digitalSignature key usage bit set          -
;-                 has client authentication enhanced key usage set -
;-------------------------------------------------------------------
[ent_wireless_epf Certificate Definitions]
1=Encryption
2=Verification

[ent_wireless_epf Encryption Extensions]
keyusage=2.5.29.15,n,m,BitString,001
```

```
[ent_wireless_epf Verification Extensions]
keyusage=2.5.29.15,n,m,BitString,1
extkeyusage=2.5.29.37,n,m,SeqOfObjectIdentifier,1.3.6.1.5.5.7.3.2

; ------------------------------------------------------------------------
; Enterprise VPN Computer Certificate Type
;
; For authenticating a computer to the VPN with computer credentials
; stored in the Windows certificate store.
; ------------------------------------------------------------------------
ent_vpn_computer=enterprise,VPN Computer,VPN Enterprise Computer
Certificates
;------------------------------------------------------------------------
;- Enterprise VPN Computer Certificate Type                             -
;-                                                                      -
;- This certificate type defines a single key pair                      -
;- Dual Usage:     has keyEncipherment key usage bit set                -
;-                 has digitalSignature key usage bit set               -
;-                 has client authentication enhanced key usage set     -
;------------------------------------------------------------------------
[ent_VPN_computer Certificate Definitions]
1=Dual Usage

[ent_VPN_computer Dual Usage Extensions]
keyusage=2.5.29.15,n,m,BitString,101
extkeyusage=2.5.29.37,n,m,SeqOfObjectIdentifier,1.3.6.1.5.5.7.3.2

; ------------------------------------------------------------------------
; Enterprise Authentication Server Certificate Type
;
; For authenticating an authentication server to wireless and VPN
; clients computer credentials stored in the Windows certificate store.
; ------------------------------------------------------------------------
wireless_auth_server=enterprise,Wireless Auth Server,Wireless Auth
Server Enterprise Certificates
;------------------------------------------------------------------------
;- Wireless Authentication Server Computer Certificate Type             -
;-                                                                      -
;- This certificate type defines a single key pair                      -
;- Dual Usage:     has keyEncipherment key usage bit set                -
;-                 has digitalSignature key usage bit set               -
;-                 has server authentication enhanced key usage set     -
;------------------------------------------------------------------------
[wireless_auth_server Certificate Definitions]
1=Dual Usage

[wireless_auth_server Dual Usage Extensions]
keyusage=2.5.29.15,n,m,BitString,101
extkeyusage=2.5.29.37,n,m,SeqOfObjectIdentifier,1.3.6.1.5.5.7.3.1
```

This page intentionally left blank.

List of symbols/abbreviations/acronyms/initialisms

AES	Advanced Encryption Standard
AP	Access Point
CRL	Certificate Revocation List
CSE	Communications Security Establishment
CSP	Cryptographic Security Provider
DHCP	Dynamic Host Configuration Protocol
DND	Department of National Defence
DRDC	Defence Research and Development Canada
DREnet	Defence Research Establishment Network
EAP	Extensible Authentication Protocol
EKU	Extended Key Usage
GoC	Government of Canada
IAS	Internet Authentication Service
IETF	Internet Engineering Task Force
IORDN	Information Operations Research and Development Network
IP	Internet Protocol
IPsec	Internet Security Protocol
ISA	Internet Security and Acceleration (Server)
L2TP	Layer 2 Tunnelling Protocol
NIO	Network Information Operations
PEAP	Protected Extensible Authentication Protocol
PKI	Public Key Infrastructure
PPTP	Point-to-Point Tunnelling Protocol
PSK	Pre-Shared Key
TKIP	Temporal Key Integrity Protocol

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.)

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

2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

UNCLASSIFIED

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

Securing wireless local area networks with GoC PKI: Addendum to report DRDC Ottawa CR 2007-239

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.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
July 2008	38	21

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.)

Defence R&D Canada – Ottawa
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4

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.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
15BR02	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.)
	DRDC Ottawa CR 2008-142

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

Unlimited

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.

The NIO section sanctioned some initial work to examine the use of Government of Canada (GoC) Public Key Infrastructure (PKI) certificates to regulate user access to the WLAN and to the Internet Protocol Security (IPsec) based VPN. The work focused on the establishment and protection of digital identities, mutual authentication, authorization, data privacy and integrity, as well as wireless network policy management and dissemination. The initial work provided sufficient functionality to demonstrate the feasibility of using GoC PKI issued certificates for WLAN and VPN authentication. However, the initial work concluded that the test bed must undergo several improvements before it can be presented as a completely integrated solution for GoC enterprise network environments. The NIO section approved additional work to address some of the outstanding issues. The results of this latest work are presented in this addendum report.

We conclude that the combination of Wi-Fi Protected Access 2 (WPA2) when operating in enterprise mode, GoC PKI issued and smart card protected user credentials, as well as 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 applying VPN security on top of WPA2 is redundant and adds unnecessary complexity.

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

Defence R&D Canada

Canada's leader in Defence
and National Security
Science and Technology

R & D pour la défense Canada

Chef de file au Canada en matière
de science et de technologie pour
la défense et la sécurité nationale

www.drdc-rddc.gc.ca