Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

IT Security Bulletin
Bulletin de sécurité TI

July 2011 **ITSB-79** **Juillet 2011**

Guidance for the Communications Security of SECRET Information

Purpose

The purpose of this bulletin is to inform the Government of Canada (GC) of the Communications Security Establishment Canada's (CSEC) guidance regarding the use of commercial technologies to safeguard the communications of classified information at the level of SECRET within a departmental local enclave.

CSEC has determined that specific Commercial-Off-The-Self (COTS) Virtual Private Network (VPN) devices can provide adequate protection for the communications security of SECRET information being transmitted within the confines of a departmental local enclave.

This technical safeguard should facilitate the implementation of a departmental SECRET network that is based on users operating a thin-client desktop configuration within a departmental unclassified operations zone and connecting to a back-end security zone where the processing and storing of the SECRET information occurs.

Lignes directrices pour la sécurité des communications liées à l'information SECRET

Objet

Le présent bulletin vise à informer les ministères du gouvernement du Canada (GC) sur les lignes directrices du Centre de la sécurité des télécommunications Canada (CSTC) concernant l'utilisation de technologies commerciales pour protéger la communication de l'information classifiée au niveau SECRET à l'intérieur d'une enclave locale ministérielle.

Le CSTC a déterminé que des dispositifs de réseau privé virtuel (RPV) commerciaux peuvent sécuriser adéquatement la communication de l'information SECRET dans les limites d'une enclave locale ministérielle.

Cette mesure de protection technique devrait faciliter la mise en œuvre d'un réseau ministériel SECRET où les utilisateurs se servent d'ordinateurs de bureau client léger dans une zone de travail non classifiée ministérielle et se connectent à une zone de sécurité dorsale pour le traitement et le stockage de l'information SECRET.

Background

CSEC, as the GC lead security agency for developing and promulgating COMSEC related policy for classified information, has recently concluded an analysis regarding the usage of commercial cryptosystems when safeguarding classified information at the SECRET level. Specifically, the use of COTS products were examined in regards to safeguarding the communication of SECRET information within a departmental local enclave.

A departmental local enclave is defined as a site with a single physical perimeter that maintains a common set of security policies (physical, personnel and Information Technology (IT)) under a single authority. External to the enclave represents where communications occur that extend past the perimeter, for example the Secure Channel Network (SC Net).

Secure Platform for Application Delivery

CSEC is partnering with Public Works and Government Services Canada (PWGSC) to deliver cost effective solutions for departmental SECRET networks. PWGSC offers a solution that can be tailored to departmental needs. This offering by PWGSC is titled Secure Platform for Application Delivery (SPAD).

Contexte

À titre de responsable de la sécurité du GC chargé d'élaborer et de promulguer des instruments de politique liés à la COMSEC à l'égard des renseignements classifiés, le CSTC a terminé récemment une analyse de l'utilisation de systèmes cryptographiques commerciaux pour protéger l'information classifiée au niveau SECRET. L'analyse portait plus particulièrement sur l'utilisation de produits commerciaux en ce qui a trait à la protection de la communication de renseignements SECRET à l'intérieur d'une enclave ministérielle locale.

Une enclave ministérielle locale est un site circonscrit par un périmètre physique unique et qui applique un ensemble commun de politiques de sécurité (matérielle, du personnel et des technologies de l'information [TI]) sous une seule et même autorité. L'extérieur de l'enclave représente l'endroit où sont établies les communications qui s'étendent au-delà du périmètre comme, par exemple, le Réseau de la Voie de communication protégée (VCP).

Livraison d’applications par plateforme protégée

Le CSTC travaille en partenariat avec Travaux publics et Services gouvernementaux Canada (TPSGC) pour fournir des solutions rentables pour les réseaux SECRET des ministères. TPSGC offre une solution qui peut être adaptée aux besoins d'un ministère, soit la Livraison d’applications par plateforme protégée (LAPP).

Recommendations

The analysis concluded:

- Communications security external to a local departmental enclave - that departments continue to use the current CSEC approved technical solution, which is a Type 1 cryptographic device.

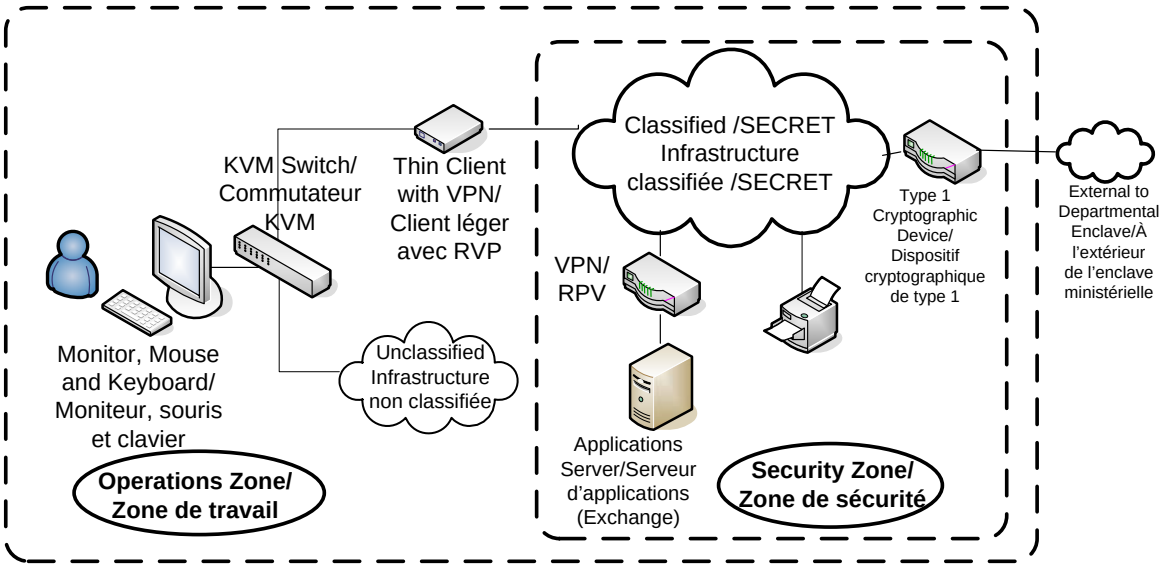
- Communications security within a local departmental enclave – with the maturity and capability of available commercial technologies, specific commercially available VPN solutions can be used to adequately secure the communications of SECRET information.

Recommandations

Conclusions de l'analyse :

- Sécurité des communications à l'extérieur d'une enclave ministérielle locale – Les ministères continuent d'utiliser la solution technique approuvée par le CSTC à l'heure actuelle, soit un dispositif cryptographique de type 1.

- Sécurité des communications à l'intérieur d'une enclave ministérielle locale – Les technologies disponibles sur le marché ont atteint un niveau de maturité et de capacité tel, qu'il est possible d'utiliser certaines solutions RPV commerciales pour sécuriser adéquatement la communication de l'information SECRET.



Description of Alternative Technical Solution for Departmental Enclaves

Departments who plan to deploy a SECRET network are advised to begin their Threat and Risk Assessments (TRA) early in the

Description de solutions techniques de rechange pour les enclaves ministérielles

On recommande aux ministères qui prévoient déployer un réseau SECRET d'entreprendre leur évaluation des menaces et des risques (EMR) tôt au

Requirements stage. The appropriate steps to conduct for the TRA are described in the *Harmonized TRA Methodology*, available on the CSEC website. Subject to the findings of the TRA, CSEC specified COTS VPN devices may be used.

Departments are advised to use CSEC recommended COTS VPN solutions available from CSEC upon request. COTS VPN solutions are also available through PWGSC's SPAD offering for departmental Secret networks. Any COTS VPN solutions will need to be configured, operated, and maintained according to CSEC guidance.

moment de la définition des besoins. La marche à suivre appropriée est donnée dans la *Méthodologie harmonisée d'EMR* disponible sur le site du CSTC. Les résultats de l'EMR détermineront s'il est possible d'utiliser des dispositifs RPV commerciaux approuvés par le CSTC.

Il est conseillé aux ministères d'utiliser les solutions RPV commerciales qui sont recommandées par le CSTC. On peut se procurer une liste des produits disponibles auprès de celui-ci. Des solutions RPV commerciales sont également disponibles par l'intermédiaire du programme LAPP de TPSGC pour les réseaux SECRET ministériels. Il faudra configurer, exploiter et maintenir la solution RPV commerciale sélectionnée conformément aux lignes directrices du CSTC.

Contacts and Assistance

IT Security Client Services
Communications Security Establishment Canada

PO Box 9703, Terminal
Ottawa, ON K1G 3Z4
By email: itsclientservices@cse-cst.gc.ca
Telephone: 613-991-7654

Aide et renseignements

Services à la clientèle de la Sécurité des TI
Centre de la sécurité des télécommunications Canada
C.P. 9703, Terminus
Ottawa (Ontario) K1G 3Z4
Courriel : itsclientservices@cse-cst.gc.ca
Téléphone : 613-991-7654

La chef adjointe de la Sécurité des TI,

Originally signed by /
Signé initialement par

Toni Moffa

Deputy Chief, IT Security

2011-07-07
Date