Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

IT Security Alert
Alerte de sécurité TI

January 2009 **ITSA-52** **Janvier 2009**

Procedures for Zeroization and Handling of Key Storage Devices (KSD-64)

Purpose

The purpose of this Alert is to provide Government of Canada (GC) COMSEC accounts with procedures for zeroization and handling of Key Storage Devices (KSD-64).

ITSA-52 supercedes the bulletin *Updated Procedures on the Handling, Transportation and Zeroization of KSD-64 Devices* (ITSB-44), September 24, 2007.

Background

The KSD-64 is one of the delivery mechanisms from which GC COMSEC accounts receive keys for most of the Secure Communications Interoperability Protocol (SCIP) devices, and for GC COMSEC accounts with STU-III waivers, their keys for STU-III terminals.

The KSD-64 will be used to key SCIP devices until such time as all Secure Data Network System (SDNS) keys can be distributed to GC COMSEC accounts electronically.

The KSD-64 is currently loaded onto SCIP devices using the DataKey Electronics PKS-703 Parallel Key Reader/Writer (PKS-703).

Unlike the STU-III terminal, which zeroizes the

Procédures de mise à zéro et de manutention des dispositifs de stockage de clés (KSD-64)

Objet

La présente alerte a pour objet de transmettre aux comptes COMSEC du gouvernement du Canada (GC) les procédures de mise à zéro et de manutention des dispositifs de stockage de clés (KSD-64).

L'ITSA-52 vient remplacer le bulletin *Mise à jour des procédures relatives à la manutention, au transport et à la mise à zéro des dispositifs KSD-64* (ITSB-44) publié le 24 septembre 2007.

Contexte

Le KSD-64 est l'un des mécanismes de livraison par lesquels les comptes COMSEC du GC reçoivent des clés pour la plupart de leurs dispositifs compatibles au protocole d'interopérabilité des communications sécurisées (SCIP pour *Secure Communications Interoperability Protocol*) et, dans le cas des comptes COMSEC du GC qui ont une dispense liée aux STU-III, des clés pour leurs terminaux STU-III.

Le KSD-64 servira à mettre à la clé les dispositifs SCIP jusqu'au moment où toutes les clés *Secure Data Network System* (SDNS) peuvent être distribuées électroniquement aux comptes COMSEC du GC.

Le contenu du KSD-64 est chargé dans un dispositif SCIP par l'intermédiaire du dispositif PKS-703 Parallel Key Reader/Writer (le PKS-703) de DataKey

Canada

KSD-64 during the load process as well as being capable of zeroizing the KSD-64 as one of its functions, the PKS-703 overwrites the KSD-64 content at the end of the load process. This overwrite process is not approved as a method of destruction by Communications Security Establishment Canada (CSEC); therefore the KSD-64 retains the same classification and handling as before the key loading process began.

Initially, GC COMSEC accounts using the PKS-703 to load keys on SCIP devices, were authorized to utilize the STU-III terminal or the Local Management Devices/Key Processor (LMD/KP) platform to zeroize the KSD-64. However, GC COMSEC accounts were advised that the use of STU-III after 30 September 2007 was no longer approved (see reference D). As a result, unless granted a STU-III waiver, the use of a STU-III terminal to zeroize the KSD-64 is no longer authorized.

Find below the procedures applicable to your COMSEC account.

Procedures

If your COMSEC account has been granted a STU-III waiver or manages a LMD/KP platform follow procedure "1"; otherwise follow procedure "2".

1. GC COMSEC Accounts Authorized to Zeroize the KSD-64

A. **GC COMSEC accounts with STU-III Waiver**:
GC COMSEC accounts that have been granted a STU-III waiver allowing them to use STU-III terminals for secure communications may continue to zeroize the KSD-64 using STU-III. Once zeroized, the KSD-64 is UNCLASSIFIED and should be returned to Electronics.

Contrairement au STU-III, qui met à zéro le KSD-64 durant le processus de chargement et qui offre également cette fonction dans une option de menu, le PKS-703 écrase le contenu du KSD-64 à la fin du chargement. Ce processus n'est pas approuvé comme méthode de destruction par le Centre de la sécurité des télécommunications Canada; par conséquent, la classification et la manutention du KSD-64 demeurent inchangées une fois le processus de chargement terminé.

Au départ, les comptes COMSEC du GC qui utilisaient le PKS-703 pour charger des clés dans les dispositifs SCIP étaient autorisés à utiliser le STU-III ou la plateforme du dispositif de gestion locale/processeur de clés (LMD/PK pour *Local Management Devices/Key Processor*) pour mettre à zéro les KSD-64. Or, les comptes COMSEC du GC ont été informés que l'utilisation du STU-III n'était plus autorisée après le 30 septembre 2007 (référence D plus bas). Par conséquent, à moins d'une dispense liée à l'utilisation du STU-III, il est désormais interdit d'utiliser ce terminal pour mettre à zéro un KSD-64.

Vous trouverez ci-après les procédures qui s'appliquent à votre compte COMSEC.

Procédures

Si votre compte COMSEC a reçu une dispense liée aux STU-III ou dispose d'une plateforme LMD/KP, suivez la procédure 1, sinon suivez la procédure 2.

1. Comptes COMSEC du GC autorisés à mettre à zéro les KSD-64

A. **Comptes COMSEC du GC ayant reçu une dispense liée aux STU-III :**
Les comptes COMSEC du GC qui ont reçu une dispense liée aux STU-III les autorisant à utiliser des STU-III pour les communications sécurisées peuvent continuer de mettre à zéro les KSD-64 à l'aide du STU-III. Une fois mis à zéro, les KSD-64 sont NON CLASSIFIÉ et devraient être retournés à

the CSEC National Distribution Authority (NDA) unless it is to be retained and used as a user Crypto-Ignition Key (CIK).

B. **GC COMSEC accounts with Local Management Devices/Key Processor (LMD/KP) platform**:
GC COMSEC accounts that manage a LMD/KP platform shall utilize the KP to zeroize the KSD-64. Once zeroized the KSD-64 is UNCLASSIFIED and should be returned to the CSEC NDA unless it is to be retained and used as a user CIK.

Note 1: GC COMSEC accounts with a STU-III waiver and a LMD/KP platform may choose option 1 or 2 to zeroize the KSD-64.

Note 2: A blank or zeroized KSD-64 does not have to be shipped through COMSEC channels.

Note 3: GC COMSEC accounts located in the Ottawa area may contact the CSEC NDA at (613) 991-8822 to coordinate the pickup of the KSD-64 by CSEC NDA staff during routine courier runs.

2. GC COMSEC Accounts Not Authorized to Zeroize KSD-64

GC COMSEC accounts which have not been granted a STU-III waiver allowing them to use STU-III terminals for secure communications and do not manage a LMD/KP platform must follow these procedures:

A. When ordering SDNS keys on KSD-64s:
GC COMSEC accounts should keep to a minimum the number of operational keys ordered. KSD-64s loaded with operational keys must be handled in accordance with the classification (up to and including TOP SECRET Compartmented Information [CI]) of

l'Agence nationale de distribution (AND) du CSTC à moins que l'on ne souhaite les conserver en vue de les utiliser comme clés de contact cryptographique (CIK pour *Crypto-Ignition Key*) utilisateur.

B. **Comptes COMSEC du GC munis d'une plateforme LMD/KP :**
Les comptes COMSEC du GC qui disposent d'une plateforme LMD/KP doivent utiliser le KP pour mettre à zéro leurs KSD-64. Une fois mis à zéro, les KSD-64 sont NON CLASSIFIÉ et devraient être retournés à l'AND du CSTC à moins que l'on ne souhaite les conserver en vue de les utiliser comme CIK utilisateur.

Nota 1 : Les comptes COMSEC du GC ayant une dispense liée aux STU-III et une plateforme LMD/KP peuvent choisir l'option 1 ou 2 pour mettre à zéro les KSD-64.

Nota 2 : Nul n'est besoin d'expédier un KSD-64 vierge ou mis à zéro par les voies COMSEC.

Nota 3 : Les comptes COMSEC du GC situés dans la région d'Ottawa peuvent communiquer directement avec l'AND du CSTC au 613-991-8822 pour coordonner la collecte du KSD-64 par le personnel de l'AND du CSTC durant leur tournée régulière.

2. Comptes COMSEC du GC non autorisés à mettre à zéro les KSD-64

Les comptes COMSEC du GC qui n'ont pas reçu de dispense liée aux STU-III les autorisant à utiliser un STU-III pour les communications sécurisées et qui n'ont pas de plateforme LMD/KP doivent suivre les procédures ci-après :

A. Au moment de commander des clés SDNS sur KSD-64, les comptes COMSEC du GC devraient garder le nombre de clés opérationnelles à un minimum. Les KSD-64 dans lesquels ont été chargées des clés opérationnelles doivent être manutentionnées conformément au niveau de classification (allant jusqu'au niveau TRÈS SECRET/ Informations cloisonnées [TS/IC],

the key it contains. For example, if the KSD-64 is loaded with operational TOP SECRET key, storage and handling must meet Two person Integrity [TPI] compliance until the KSD-64 has been zeroized). GC COMSEC accounts should opt to order seed keys on their KSD-64s. The KSD-64 loaded with seed key is at the PROTECTED A level, facilitating the handling of the KSD-64 throughout its life cycle.

B. When keying SCIP devices, using the KSD-64 and the PKS-703, GC COMSEC accounts shall apply these interim procedures:

1. The COMSEC Custodian shall prepare a GC-223 Transfer Report Initiating (TRI), instead of Destruction Report (DR) (as instructed in the ITSG-10), to transfer the KSD-64 to CSEC NDA which is authorized to zeroize the KDS-64. When preparing the GC-223, GC COMSEC accounts shall record, in the remarks column, the serial number of the PKS-703 and of the SCIP device on which the SDNS key will be loaded.
2. Once the COMSEC Custodian has loaded the SDNS key on the SCIP device, he/she shall sign the TRI, package the KSD-64 with its identification tag and the TRI according to ITSG-10 (Chapter 6, Section 6) and transfer the package to the CSEC NDA where it is authorized for destruction.

Note 1: GC COMSEC accounts located in the Ottawa area may contact the CSEC NDA at (613) 991-8822 to coordinate the pickup of KSD-64s by CSEC NDA staff during routine courier runs.

Note 2: GC COMSEC accounts located

inclusivement) de ces clés. Par exemple, si un KSD-64 contient des clés opérationnelles TRÈS SECRET, l'entreposage et la manutention du KSD-64 doivent respecter le principe de l'intégrité par deux personnes (TPI pour *Two Person Integrity*) jusqu'à ce que le KSD-64 soit mis à zéro. Les comptes COMSEC du GC devraient plutôt commander des clés de diversification sur leurs KSD-64. Un KSD-64 comportant des clés de diversification est PROTÉGÉ A, ce qui facilite sa manutention durant toute la durée de son cycle de vie.

B. Au moment de mettre à la clé leurs dispositifs SCIP à l'aide d'un KSD-64 et d'un PKS-703, les comptes COMSEC du GC doivent appliquer les procédures provisoires suivantes :

1. Le gardien COMSEC doit préparer un rapport GC-223 de lancement de rapport de transfert (TRI pour *Transfer Report Initiating*) au lieu d'un rapport de destruction (DR pour *Destruction Report*) (comme il est indiqué dans l'ITSG-10), pour transférer le KSD-64 à l'AND du CSTC, qui est autorisée à mettre à zéro les KDS-64. Au moment de préparer le GC-223, les comptes COMSEC du GC doivent inscrire dans la colonne *Remarques* le numéro de série du PKS-703 et du dispositif SCIP dans lequel la clé SDNS sera chargée.
2. Une fois qu'il a chargé la clé SDNS dans le dispositif SCIP, le gardien COMSEC doit signer le TRI, emballer le KSD-64 avec son étiquette d'identification et le TRI conformément aux instructions données dans l'ITSG-10 (chapitre 6, section 6) et transférer le tout à l'AND du CSTC qui est autorisée à effectuer la destruction.

Nota 1 : Les comptes COMSEC du GC situés dans la région d'Ottawa peuvent communiquer directement avec l'AND du CSTC au 613-991-8822 pour coordonner la collecte du KSD-64 par le personnel de l'AND du CSTC durant leur tournée régulière.

Nota 2 : Les comptes COMSEC du GC situées à

outside the Ottawa area shall courier the package(s) according to ITSG-10 (Chapter 6, Section 7)

References

A. *Canadian Cryptographic Doctrine for the DataKey Electronics PKS-703 Parallel Key Reader/Writer and PK64KC and KSD-64A* (CCD-26), January 2004

B. *CSEC, Approval For Use Datakey Electronics PKS-703 Parallel Memory Key ReaderWriter and PK64KC and KSD-64 A Key Storage Device*, 2 February 2004

C. *COMSEC Material Control Manual* (ITSG-10), July 2006

D. *STU-III Technology No Longer Approved for Use in Canada* (ITSA-43), 25 October 2007

Contacts and Assistance

Head, IT Security Client Services
Communications Security Establishment Canada
PO Box 9703, Terminal
Ottawa, Ont K1G 3Z4

Telephone: (613) 991-8744
e-mail : itsclientservices@cse-cst.gc.ca

l'extérieur de la région d'Ottawa doivent envoyer leur(s) colis conformément à l'ITSG-10 (chapitre 6, section 7).

Références

A. *Doctrine canadienne en matière de cryptographie visant le PKS-703 Parallel Key Reader/Writer et les dispositifs de stockage de clés PK64KC et KSD-64A de DataKey Electronics* (CCD-26), Janvier 2004

B. *CSTC, Approbation d'utilisation, Lecteur-enregistreur de clé à mémoire parallèle PKS-703 et dispositifs de stockage de clé PK64KC et KSD-64A de Datakey Electronics*, 2 février 2004

C. *Manuel de contrôle du matériel COMSEC* (ITSG-10), juillet 2006

D. *Utilisation de la technologie STU-III dorénavant non autorisée au Canada STU-III* (ITSA-43), 25 octobre 2007

Aide et renseignements

Chef, Services à la clientèle de la Sécurité des TI
Centre de la sécurité des télécommunications Canada
C.P. 9703, Terminus
Ottawa (Ontario) K1G 3Z4

Téléphone : 613-991-8744
Courriel : itsclientservices@cse-cst.gc.ca

La directrice par intérim de la Gestion de la mission de la Sécurité des TI,

Originally signed by /
Signé initialement par

Christine Rainville
Acting Director, IT Security Mission Management