2900-1 (DDCEI 3-5-4)

24 février 1999

SPÉCIFICATIONS POUR CARTE À PUCE ET LECTEUR DE CARTE À PUCE

À JETON ENTRUST POUR LE GOUVERNEMENT DU CANADA

Préparé par : CR Clupp
Capitaine
DDCEI 3-5-4
996-6203

1. Généralités

Le gouvernement du Canada a choisi la famille de produits de chiffrement Entrust pour les services d'identification et d'authentification, de confidentialité et de signature électronique (non répudiable) offerts par son infrastructure de technologies de l'information (ITI). Le gouvernement doit doter son architecture de sécurité d'un système offrant un niveau élevé de sécurité pour le traitement et le stockage de renseignements permettant aux utilisateurs de prouver électroniquement leur identité lorsqu'ils utilisent les services de l'ITI. Des cartes à puce, des lecteurs de carte à puce et des dispositifs d'interface seront utilisés pour assurer la protection des renseignements confidentiels du système Entrust, des signatures numériques, des clés de déchiffrement et des processus de chiffrement et de déchiffrement qui seront utilisés par les employés des divers ministères. Les cartes à puces mettront les données confidentielles Entrust propres à chaque employé à l'abri des altérations, des fraudes et des utilisations illicites. . La clé de chiffrement de la signature numérique sera générée à partir du jeton, y sera conservée et ne pourra être utilisée qu'à partir de celui-ci (la clé de chiffrement de la signature électronique ne pourra donc j**amais** être utilisée sans le jeton). La clé privée de déchiffrement de clé sera conservée sur le jeton. Toutes les opérations de déchiffrement faisant appel à la clé de déchiffrement seront effectuées à partir du jeton. Les normes et caractéristiques auxquelles les cartes à puce et les lecteurs de cartes à puce doivent se conformer pour respecter les exigences gouvernementales sont décrites dans les spécifications indiquées ci-dessous.

2. Normes et spécifications applicables

Les normes et spécifications citées ci-dessous renvoient à leur plus récente version au 24 février 1999.

2.1. ISO/IEC 7810: Cartes d'identification – Caractéristiques physiques

2.2. ISO/IEC 7811: Cartes d'identification – Techniques d'enregistrement

2.2.1 ISO/IEC 7811-1 Partie 1 : Estampage

2.2.2 ISO/IEC 7811-1 Partie 2 : Raie magnétique

2.2.3 ISO/IEC 7811-1 Partie 3 : Position des caractères estampés sur les cartes ID-1

2.2.4 ISO/IEC 7811-1 Partie 4 : Position des pistes magnétiques pour lecture uniquement – Pistes 1 et 2

2.2.5 ISO/IEC 7811-1 Partie 5 : Position de la piste magnétique enregistrement-lecture – Piste 3

2.2.6 ISO/IEC 7811-1 Partie 6 : Bandeau magnétique – Haute coercitivité

2.3. ISO/IEC 7812 : Système de numérotation et procédures de demande pour l'identification des émetteurs

2.4. ISO/IEC 7813 : Cartes d'identification – Cartes de transactions financières

2.5. ISO/IEC 10373 : Cartes d'identification – Méthodes d'essai

2.6. ISO/IEC 7816 : Cartes d'identification – Cartes à circuits intégrés à contact

2.6.1 ISO/IEC 7816-1 : Caractéristiques physiques

2.6.2 ISO/IEC 7816-2 : Dimensions et emplacement des contacts

2.6.3 ISO/IEC 7816-3 : Signaux électroniques et protocoles de transmission

2.6.4 ISO/IEC 7816-4 : Commandes intersectorielles pour les échanges

2.6.5 ISO/IEC 7816-5 : Système de numérotation et procédures d'enregistrement d'identificateurs d'applications

2.6.6 ISO/IEC 7816-6 : Éléments de données intersectoriels

2.7. Normes Federal Information Processing Standard (FIPS) du National Institute of Standards and Technology (NIST)

2.7.1 FIPS140-1 : Security Requirements for Cryptographic Modules

2.7.2 FIPS 186 : Digital Signature Standard (DSS)

2.8. Normes relatives à la cryptographie à clé publique (PKCS)

2.8.1 PKCS#1 : RSA Encryption Standard (version 1.5)

2.8.2 PKCS#11 : Cryptographic Token Interface Standard (version 1.0)

2.9. Spécifications relatives aux cartes à puces pour ordinateurs personnels (PC/SC)

3. Spécifications relatives aux cartes à puce

3.1 Caractéristiques physiques :

Les caractéristiques physiques des cartes à puce doivent être conformes à la norme ISO/IEC 7816-1 et doivent respecter les exigences des normes ISO/IEC 7810, ISO/IEC 7811 (parties 1 à 5), ISO/IEC 7812 et ISO/IEC 7813.

3.1.1 Les cartes à puce doivent être soumises à des essais conformément aux recommandations de la norme ISO/IEC 10373 pour vérifier leurs propriétés :

a. en flexion;

b. en torsion.

3.1.2 Les méthodes d'essai pour cartes à puce décrites dans l'annexe à la norme ISO/IEC 7816-1 doivent être appliquées et respectées, dans la mesure où elles sont pertinentes.

3.2 Dimensions et emplacement des contacts :

Les dimensions et l'emplacement des contacts doivent être conformes à la figure 2 de la norme ISO/IEC 7816-2.

3.2.1 Les contacts doivent être placés au recto de la carte (sur la face opposée à celle où se trouve le bandeau magnétique), tel qu'illustré à l'annexe A de la norme ISO/IEC 7816-2 et conformément aux critères énoncés dans les normes ISO/IEC 7811-1 et 7811-2.

3.2.2 Les contacts doivent être isolés conformément aux recommandations contenues dans l'annexe B de la norme ISO/IEC 7816-2.

3.3 Signaux électriques et protocoles de transmission :

Les signaux électriques et les protocoles de transmission doivent être conformes à la norme ISO/IEC 7816-3.

3.3.1 Les cartes à puce doivent être utilisées avec des dispositifs d'interface provenant de divers fabricants :

a. La conception des cartes à puce doit faire en sorte que l'insertion d'une carte à puce de classe A ou B dans un dispositif d'interface de classe A, B ou AB n'endommage ni la carte ni le dispositif (par exemple, l'insertion d'une carte à puce de classe B, dont la tension de fonctionnement est de 3 V c.c., dans un dispositif d'interface de classe A, qui fonctionne sur une tension de 5 V c.c., ne doit causer aucun dommage à la carte ou au dispositif).

3.3.2 Les cartes à puce doivent être compatibles avec les protocoles asynchrones semi-duplex de types " T=0 " ou " T=1 ". Le protocole " T=14 " ne doit pas être utilisé.

3.4 Commandes intersectorielles pour les échanges :

La structure de fichiers, les jeux de commandes et l'architecture de sécurité des cartes à puce doivent être conformes à la norme ISO/IEC 7816-4 et ne doivent pas permettre d'accéder à des commandes permettant de contourner les contrôles de sécurité Entrust.

3.5 Procédures et algorithmes cryptographiques :

3.5.1 Le jeu d'algorithmes cryptographiques asymétriques mis en œuvre dans les cartes à puce doit inclure les algorithmes suivants, utilisés par le gouvernement du Canada et supportés par Entrust :

a. RSA – Conformément à la norme PKCS#1 [avec clé d'au moins 1 024 bits];

b. DSA –Conformément à la norme FIPS 186 [avec clé d'au moins 1 024 bits].

3..5.2 La conception de tous les modules cryptographiques doit être conforme au niveau 2 de la norme FIPS 140-1 concernant les caractéristiques physiques :

a. Les mécanismes de sécurité physique doivent être conçus de façon à ce qu'il existe une probabilité élevée que les tentatives d'utilisation, de modification ou d'accès à la carte puissent être détectées par des traces visibles.

b. Les microcircuits inclus aux cartes doivent être de qualité grande série, doivent comprendre des mesures de protection passive (ils doivent être recouverts d'un enduit qui les protège des risques environnementaux et d'autres dommages matériels).

c. Les microcircuits doivent comporter un revêtement opaque révélant les tentatives d'altération (un revêtement de protection passive opaque révélant les tentatives d'altération, ou un revêtement opaque révélant les tentatives d'altération, appliqué sur l'enduit de protection passive).

d. Les microcircuits doivent être accompagnés d'une documentation comprenant les spécifications complètes des mesures de protection physiques dont ils font l'objet et du niveau de sécurité correspondant à ces mesures de protection.

3.5.3 Les interfaces API qui fournissent des services cryptographiques doivent être conformes à la mise en œuvre des normes PKCS#11 dans les produits Entrust.

3.5.4 Le fournisseur de cartes à puce doit démontrer leur compatibilité avec la famille de produits de chiffrement d'Entrust Technologies pour l'exécution des fonctions suivantes :

a. génération d'une paire de clés pour signature sur la carte à puce au cours du processus normal d'initialisation de l'entité Entrust;

b. stockage des éléments d'identification de l'utilisateur sur la carte à puce, notamment :

i) clé de signature privée;

ii) clé de déchiffrement de clé privée;

iii) certificat de vérification de la signature publique de l'autorité de certification;

iv) certificat de vérification de la signature publique;

v) historique de la clé.

c. Le code d'utilisateur et le mot de passe Entrust sont utilisés pour l'identification et l'authentification.

d. La carte à puce doit effectuer des opérations de hachage du message à l'aide de la clé de signature privée d'Entrust.

3.5.5 La carte à puce doit effectuer la signature du hachage sur le jeton en moins de 3 secondes. La période de 3 secondes comprend les délais d'entrée-sortie, la récupération de la clé et la signature elle-même.

3.5.6 La clé de signature privée doit toujours demeurer sur le jeton.

3.5.7 La carte à puce doit utiliser un algorithme de génération de nombres aléatoires conforme aux spécifications de l'annexe 3 de la norme FIPS 186.

3.5.8 Les algorithmes cryptographiques symétriques utilisés par les cartes à puce pour la protection des mots de passe, des NIP, des données d'identification Entrust et d'autres données confidentielles doivent appliquer l'algorithme de chiffrement 3DES à au moins 168 bits, ou l'algorithme de chiffrement CAST à au moins 128 bits. L'utilisation d'autres algorithmes doit être approuvée par le gouvernement du Canada.

3.6 Architecture des cartes à puce

L'architecture des cartes à puce doit satisfaire aux exigences suivantes ou les dépasser :

3.6.1 Les cartes à puce doivent être dotées d'une capacité mémoire minimale de 8 ko pour l'enregistrement des données d'identification d'utilisateur Entrust, dont les clés privées pour le chiffrement et le déchiffrement.

3.6.2 Les cartes à puce doivent disposer d'une mémoire vive (RAM) d'une capacité minimale de 240 octets.

3.6.3 Les cartes à puce doivent disposer d'une mémoire morte (ROM) d'une capacité minimale de 13 ko.

3.6.4 Les cartes à puce doivent être dotées d'une UCT fonctionnant à au moins 8 bits.

3.6.5 La fréquence de l'horloge interne des cartes à puce doit être d'au moins 3 MHz.

3.6.6 La mémoire permanente des cartes à puces doit pouvoir être soumise à un minimum de 100 000 cycles d'écriture-effacement.

3.7 Mesures de sécurité logiques pour cartes à puce

Le système d'exploitation du microcontrôleur des cartes à puce doit comporter des mesures de sécurité logiques pour assurer l'intégrité et la confidentialité des données. Les cartes à puces doivent être dotées des caractéristiques suivantes :

3.7.1 Codes de transport protégeant les cartes en transit entre le fabricant et l'émetteur des cartes. Ces codes sont destinés à prévenir le chargement de données dans les cartes à l'insu de l'émetteur. La méthode utilisée pour la

transmission des codes du fabricant à l'émetteur doit être approuvée par le gouvernement du Canada.

3.7.2 Système de numérotation et procédures de demande pour l'identification des émetteurs conformes à la norme ISO/IEC 7812.

3.7.3 Zones confidentielles ou secrètes, accessibles seulement à partir du système d'exploitation des cartes et à l'aide de codes d'autorisations appropriés. Ces zones sont destinées à protéger les renseignements confidentiels, tels que les NIP ou les clés de chiffrement privées, de tentatives d'accès externes. L'accès à ces zones doit pouvoir être configuré par les utilisateurs à l'aide de mécanismes de contrôle d'accès définis par le gouvernement du Canada.

3.7.4 Fichiers protégés en écriture pour prévenir la modification de leur contenu (les données d'identifications Entrust, par exemple) sans l'autorisation du système d'exploitation.

3.7.5 Les opérations suivantes doivent être exécutées par le microprocesseur des cartes :

(a) génération de la clé de signature;

(b) signature numérique des documents;

(c) vérification et authentification des messages externes;

(d) chiffrements des mots de passe enregistrés;

(e) chiffrement des autres données sauvegardées dans le microprocesseur.

3.8 Mesures de sécurité physiques pour cartes à puce

Les cartes à puces doivent être dotées de mécanismes de sécurité physiques conformes aux spécifications de niveau 2 de la norme FIPS 140-1, afin de protéger leur microcontrôleur des altérations.

4. Spécifications des lecteurs et dispositifs d'interface pour cartes à puce

4.1 Spécifications relatives à l'interopérabilité des cartes à puce et des ordinateurs personnels (spécifications PC/SC)

Les dispositifs d'interface pour cartes à puce doivent être conformes à l'ensemble des spécifications PC/SC et doivent être dotés des mécanismes décrits aux sous-

sections 4.2 et 4.3. Les fournisseurs doivent présenter une documentation détaillée attestant que ces exigences sont respectées.

4.2 Exigences physiques relatives aux dispositifs d'interface

4.2.1 Le retrait et l'insertion des cartes dans les dispositifs doivent se faire manuellement.

4.2.2 La carte doit être placée dans le dispositif d'interface de façon à demeurer accessible à son titulaire en tout temps.

4.2.3 Le dispositif d'interface doit être doté d'un logement qui retient la carte en position stationnaire, et non d'une fente de balayage.

4.2.4 Le dispositif d'interface doit être conçu pour éviter tout dommage à la carte causé par des guides, des pinces, des rouleaux et d'autres mécanismes, particulièrement aux zones réservées au bandeau magnétique optionnel et aux caractères estampés.

4.2.5 La détection de l'insertion d'une carte dans le dispositif d'interface doit être effectuée à l'aide d'un microcontact, plutôt qu'avec un interrupteur à lame.

4.2.6 Le dispositif d'interface doit supporter les protocoles de caractères T=0 et T=1 définis dans la norme ISO/IEC 7816-3.

4.2.7 Le dispositif d'interface doit appliquer les " règles de fonctionnement sans erreur " suivantes, énoncées au paragraphe 4.9.2.2 de la partie 2 des spécifications PC/SC :

a. Une fois l'ATR complétée, le dispositif transmet un bloc S ou un bloc I.

b. Après avoir complété la transmission d'un bloc, l'unité qui transmet passe en mode de réception et attend la transmission d'un bloc par l'autre unité. Quand l'unité en mode de réception a complété la lecture d'un bloc, dont la fin est signalée par le champ LEN, elle peut passer en mode de transmission.

c. Si on utilise l'adressage de nœud, la valeur désignant le nœud doit être incluse au premier bloc transmis par le dispositif d'interface. Cette valeur doit être utilisée pour tous les échanges ultérieurs pendant la session logique entre le fournisseur de services et la carte à puce.

d. Si le dispositif d'interface veut utiliser une valeur IFSD différente de 32 (valeur initiale), il doit transmettre un bloc S (demande IFS). Il est

recommandé d'utiliser la valeur 254 et d'inclure cette donnée au premier bloc transmis à la carte à puce par le dispositif d'interface. Le dispositif peut exécuter cette opération de façon indépendante, mais devrait attendre que le fournisseur de services ait lancé une session logique afin d'établir correctement le mode d'adressage de nœud.

e. L'unité réceptrice doit accuser réception de tous les blocs I en transmettant un bloc I ou un bloc R approprié. Les blocs R sont utilisés en mode de chaînage.

f. Les blocs S sont toujours échangés en paires : un bloc S de demande est toujours suivi par un bloc S de réponse.

4.2.8 Tous les lecteurs doivent être compatibles avec l'interface entre le pilote de dispositif d'interface et le gestionnaire de ressources de carte à puce.

4.2.9 Les soumissions pour dispositifs d'interface doivent inclure tous les logiciels nécessaires à l'interface avec les PC et les cartes à puce. Le gouvernement ne doit pas être dans l'obligation d'acquérir des logiciels supplémentaires pour effectuer la mise en œuvre des dispositifs d'interface.

4.3 Exigences relatives aux fonctionnalités

4.3.1 Le dispositif d'interface doit permettre la sélection du protocole et la définition des paramètres associés afin de maximiser les performances lors de l'utilisation de l'application prévue. Le dispositif d'interface doit faire l'analyse de l'ATR (code de réponse à une réinitialisation transmis par la carte à puce au dispositif d'interface) conformément aux recommandations de la norme ISO/IEC 7816-3. Cette opération a pour but de déterminer quelles options offertes par la carte à puce sont supportées par le dispositif d'interface. Celui-ci doit attendre la connexion de la première application avant de déterminer les paramètres du protocole.

4.3.2 Lorsqu'une carte à puce est insérée pendant une longue période dans un dispositif d'interface, mais n'est utilisée qu'occasionnellement, le dispositif d'interface doit pouvoir activer et désactiver la carte au besoin pour réduire la consommation de courant. Cette opération doit être contrôlée par le fournisseur de services de carte à puce. Une demande d'activation de la carte à puce provoquera l'activation des contacts, une réinitialisation à froid et le traitement de la séquence ATR.

4.3.3 Le dispositif d'interface doit être alimenté par le PC et ne doit pas comporter de bloc d'alimentation externe.

4.4 Facteur de forme

Le matériel proposé doit être offert en plusieurs facteurs de forme, dont :

4.4.1 PS/2

4.4.2 RS 232

4.4.3 Carte PC

4.5 Compatibilité avec les systèmes d'exploitation Microsoft

Tous les dispositifs d'interface proposés doivent avoir réussi les essais du programme Microsoft Windows Hardware Quality Labs (WHQL), doivent faire l'objet d'un rapport d'essai officiel et leur utilisation doit être sanctionnée par l'une des licences de Microsoft suivantes :

4.5.1 Logo "Designed for Microsoft Windows 95".

4.5.2 Logo "Designed for Microsoft Windows NT"

4.6 Support de la plateforme Unix

Le jeton pour carte à puce Entrust doit respecter les exigences gouvernementales en matière de sécurité classifiée dans l'environnement Unix. À ces fins, les dispositifs d'interface doivent être compatibles avec les versions suivantes du systèmes d'exploitation Unix :

4.6.1 Solaris de Sun

4.6.2 HP/UX