



## A006 – Carte à puce

Classification :	non classifié
Type :	norme informatique
Date d'édition :	1 <sup>er</sup> décembre 2024
Version :	4.0.0
Statut :	approuvé
Version précédente :	3.0.2
Caractère contraignant :	directive
Approuvé par :	secteur Transformation numérique et gouvernance de l'informatique (TNI), le 19 novembre 2024
Vérifié par :	- FUB Krypt - SG PKI, Identity & Trust / IDT - OFCL
Annexes :	- annexe 1 de la norme A006 : spécifications de l'OFIT - annexe 2 de la norme A006 : spécifications de l'OFCL

## Table des matières

<b>1</b>	<b>Domaine d'application .....</b>	<b>3</b>
<b>2</b>	<b>Champ d'application .....</b>	<b>3</b>
<b>3</b>	<b>Caractère contraignant .....</b>	<b>3</b>
<b>4</b>	<b>Définitions .....</b>	<b>3</b>
<b>5</b>	<b>Acquisition, confection, commande .....</b>	<b>4</b>
<b>6</b>	<b>Composants et interfaces nécessaires .....</b>	<b>4</b>
<b>6.1</b>	<b>Puce cryptographique .....</b>	<b>4</b>
<b>6.2</b>	<b>Lecteur de carte à puce .....</b>	<b>5</b>
<b>6.3</b>	<b>Carte à puce (vue physique).....</b>	<b>5</b>
<b>6.4</b>	<b>Accès à la carte à puce.....</b>	<b>5</b>
<b>7</b>	<b>Dispositions générales .....</b>	<b>5</b>
<b>8</b>	<b>Dispositions finales.....</b>	<b>6</b>
<b>8.1</b>	<b>Abrogation.....</b>	<b>6</b>
<b>8.2</b>	<b>Entrée en vigueur.....</b>	<b>6</b>
	<b>Annexes .....</b>	<b>7</b>
<b>A.</b>	<b>Modifications par rapport à la version précédente .....</b>	<b>7</b>
<b>B.</b>	<b>Signification des mots-clés déterminant le degré du caractère contraignant...</b>	<b>7</b>
<b>C.</b>	<b>Abréviations .....</b>	<b>7</b>
<b>D.</b>	<b>Références.....</b>	<b>9</b>

Le secteur Transformation numérique et gouvernance de l'informatique (TNI) édicte la directive ci-après en vertu de l'art. 17, al. 1, de l'ordonnance du 25 novembre 2020 sur la coordination de la transformation numérique et la gouvernance de l'informatique dans l'administration fédérale (OTNI) [OTNI].

## 1 Domaine d'application

La présente directive définit les prescriptions applicables aux cartes à puce (*smartcards*) et aux puces cryptographiques utilisées par l'administration fédérale ainsi qu'aux éléments logiciels et matériels nécessaires à leur utilisation.

## 2 Champ d'application

La présente directive s'applique lorsque des certificats de la Swiss Government PKI figurant sur une carte à puce sont impérativement requis par l'autorité fédérale compétente pour la collaboration et l'accomplissement des tâches des autorités.

## 3 Caractère contraignant

Le degré du caractère contraignant des différentes prescriptions est indiqué au moyen de mots-clés en majuscules rassemblés à l'annexe B.

## 4 Définitions

Poste de travail sécurisé (*secure desktop*) : écran qui s'affiche lorsqu'on appuie simultanément sur les touches Ctrl+Alt+Del.

Confection : intégration de la puce cryptographique dans la carte en plastique et autres étapes de traitement en vue de la finalisation de la carte à puce physique (par ex. impression, laminage, programmation). Le résultat de la confection est appelé carte à puce.

Injection de clé sécurisée (*Secure Key Injection* [SKI]) : méthode permettant d'envoyer en toute sécurité des clés secrètes d'une application serveur vers la carte à puce via un PC client non sécurisé [SKI].

## 5 Acquisition, confection, commande

1. La puce cryptographique DOIT être acquise par l'Office fédéral de l'armement (armasuisse).
2. Le processus de fabrication (confection) de la carte à puce DOIT être effectué ou commandé par l'Office fédéral des constructions et de la logistique (OFCL).
3. La traçabilité DOIT être garantie pour le processus d'acquisition, de livraison et de confection de chaque carte à puce et de chaque puce cryptographique.
4. La commande de cartes à puce DOIT être effectuée par l'intermédiaire de l'OFCL.
5. Toute puce cryptographique acquise de manière autonome par des cantons, des entreprises liées à la Confédération ou des tiers DOIT répondre aux spécifications figurant au chap. 6.1 « Puce cryptographique ».
6. Toute carte à puce acquise, confectionnée et commandée de manière autonome par des cantons, des entreprises liées à la Confédération ou des tiers DOIT être préinstallée par la Swiss Government PKI avant son utilisation.

## 6 Composants et interfaces nécessaires

### 6.1 Puce cryptographique

1. La puce cryptographique DOIT prendre en charge la méthode asymétrique ECC (avec 256, 384 et 512 bits, par ex. Brainpool et Curve25519).
2. La puce cryptographique DOIT prendre en charge la méthode asymétrique RSA (avec 2048 et 4096 bits).
3. La puce cryptographique DOIT EN PRINCIPE prendre en charge la méthode symétrique AES avec 256 bits.
4. La puce cryptographique DOIT avoir au moins une mémoire pour 15 paires de clés asymétriques RSA-4096, y compris les certificats.
5. La puce cryptographique DOIT avoir au moins une certification FIPS 140-2 de niveau 2 (ou une certification équivalente).
6. La puce cryptographique DOIT disposer au minimum d'une certification EAL5+.
7. La puce cryptographique DOIT fournir une implémentation, avec accélération matérielle, des procédures cryptographiques (AES, RSA et ECC).
8. La puce cryptographique DOIT être prise en charge au minimum par les systèmes d'exploitation Windows suivants : Microsoft Windows 10 32/64-BIT et Windows Server à partir de 2012.
9. La puce cryptographique DOIT prendre en charge les interfaces Microsoft CryptoAPI (CSP, mini-lecteur ou CNG) et PKCS#11. Chaque interface DOIT être transparente pour les autres.
10. La puce cryptographique DOIT être prise en charge par au moins une distribution Debian récente.
11. Les spécifications et le code source du générateur de nombres aléatoires (Random Number Generator [RNG]) figurant sur la puce cryptographique DOIVENT pouvoir être consultés, le cas échéant dans le cadre d'un accord de non-divulgence (Non-Disclosure Agreement [NDA]).
12. Les spécifications et le code source de la génération de clés figurant sur la puce cryptographique DOIVENT pouvoir être consultés, le cas échéant dans le cadre d'un accord de non-divulgence.
13. La description et les spécifications détaillées des applications/logiciels installés sur la puce cryptographique DOIVENT être mises à disposition.

14. Il DOIT être possible de définir à la fois un code NIP et un code PUK.
15. Lors de l'initialisation de la puce, il DOIT être possible de définir une politique pour le code NIP et le code PUK. Cette politique définit la longueur minimale et la complexité de ces valeurs.
16. La puce cryptographique DOIT disposer des fonctions de changement du code NIP et de déverrouillage de ce dernier. Ces fonctions doivent pouvoir être appelées dans Windows.
17. La puce cryptographique DOIT prendre en charge la fonction d'injection de clé sécurisée (SKI).
18. La puce cryptographique DOIT EN PRINCIPE prendre en charge une interface sans contact conforme à la norme ISO 14443-A ou ISO 14443-B.

## 6.2 Lecteur de carte à puce

1. Le lecteur de carte à puce DOIT EN PRINCIPE pouvoir être connecté à l'ordinateur par au moins un port USB.
2. Le lecteur sans contact (Bluetooth SC Reader, NFC) A LE DROIT de prendre en charge une interface sans contact conforme à la norme ISO 14443.
3. Le lecteur de carte à puce DOIT être conforme à la norme PC/SC [PC/SC v2.01].
4. Lors de l'acquisition des équipements de bureautique, l'organisme acquéreur DOIT vérifier la compatibilité des équipements à acquérir (par ex. ordinateurs portables, claviers munis d'un lecteur de carte à puce intégré) avec les cartes à puce utilisées dans l'administration fédérale. La procédure de test DOIT être approuvée par la Swiss Government PKI. Le résultat du test DOIT être communiqué à cette dernière.

## 6.3 Carte à puce (vue physique)

1. La carte à puce DOIT avoir une taille de 85,60 mm × 53,98 mm et une épaisseur de 0,76 mm (selon la norme ISO 7810 ID-1).
2. L'OFCL DOIT établir, en accord avec l'OFIT et le secteur TNI, l'annexe 2 de la présente norme, laquelle doit contenir les prescriptions régissant la carte à puce (vue physique).
3. L'OFCL PEUT par ailleurs décrire les composants et interfaces optionnels (par ex. puce de transpondeur, RFID, antennes pour NFC) dans l'annexe 2 de la présente norme.

## 6.4 Accès à la carte à puce

1. Sous Windows, le pilote qui DOIT EN PRINCIPE être utilisé est le mini-lecteur répondant à la spécification relative au mini-lecteur de carte à puce (v7 ou v7.07) [SCM].
2. Sous Linux, il EST PERMIS d'accéder à la puce cryptographique en utilisant PKCS#11 [PKCS#11].

## 7 Dispositions générales

1. La norme A006 - Carte à puce DOIT être publiée sur l'intranet et l'internet de la ChF.
2. L'OFIT DOIT établir l'annexe 1, la tenir à jour et la publier sur l'intranet et l'internet de la ChF.
3. L'OFCL DOIT publier l'annexe 2 sur l'intranet du secteur TNI.
4. La demande d'inscription de cartes à puce non autorisées sur la liste des cartes à puce

autorisées DOIT être adressée au Comité de gestion des services standard de la Confédération (GSS) conformément au règlement de ce dernier.

## **8 Dispositions finales**

### **8.1 Abrogation**

La norme A006, version 3.0.2, est abrogée.

### **8.2 Entrée en vigueur**

La présente norme entre en vigueur à la date de son approbation.

## Annexes

### A. Modifications par rapport à la version précédente

Migration de la norme vers un nouveau modèle.

Complétion du chap. 5, ch. 5 et 6 .

Remaniement du contenu des chap. 2, 6.1, 6.2 et 7, ch. 2 et 3.

### B. Signification des mots-clés déterminant le degré du caractère contraignant

Le degré du caractère contraignant des différentes dispositions de la présente norme est indiqué au moyen des mots suivants écrits en majuscules :

DOIT	La directive doit impérativement être respectée (sauf dérogation).
EST INTERDIT	L'option ne peut pas être choisie.
EST PERMIS / A LE DROIT	L'option est autorisée explicitement. Les utilisateurs décident s'ils veulent l'utiliser. Si la directive concerne une solution informatique, le fournisseur de la solution doit proposer cette option.
DOIT EN PRIN- CIPE	En règle générale, cette option doit être choisie. Il est toutefois possible de s'en écarter sans que le DTI accorde de dérogation, notamment si l'efficacité économique ou la sécurité ne peuvent plus être garanties. Toute dérogation doit toutefois faire l'objet d'une justification écrite.
PEUT	L'option est admise. Si la directive concerne une solution, le fournisseur de cette dernière décide s'il veut prendre en charge cette option.

### C. Abréviations

<b>Abréviation</b>	<b>Signification</b>
armasuisse	Office fédéral de l'armement (fait partie du Département fédéral de la défense, de la protection de la population et des sports)
OFCL	Office fédéral des constructions et de la logistique (fait partie du Département fédéral des finances)
OTNI	Ordonnance du 25 novembre 2020 sur la transformation numérique et la gouvernance de l'informatique dans l'administration fédérale
OFIT	Office fédéral de l'informatique et de la télécommunication
CNG	<u>Cryptography Next Generation</u> : introduite avec la version 7 de Windows, elle permet d'utiliser les algorithmes définis par le NIST dans la suite B.

<b>Abréviation</b>	<b>Signification</b>
CNG/CSP	Le <u>C</u> rypto <u>N</u> ext <u>G</u> eneration Key Storage Provider (KSP) et le Micro-soft Smart Card Base <u>C</u> ryptographic <u>S</u> ervice <u>P</u> rovider peuvent accéder à la carte à puce à l'aide du mini-lecteur [SCM] fourni par le fabricant de la carte.
DH	Diffie Hellmann, protocole d'échange de clés
GSS	Comité de gestion des services standard de la Confédération
TNI	Secteur Transformation numérique et gouvernance de l'informatique
ISO	Organisation internationale de normalisation
NDA	Accord de non-divulgence (Non-Disclosure Agreement)
NFC	Near Field Communication
PC/SC	Personal Computer – Smartcard Interface (ordinateur personnel - interface de carte à puce)
NIP	Numéro d'identification personnel
PKCS#11	Public Key Cryptographic Standard Number 11, norme créée par RSA LABORATORIES, voir [PKCS#11]. La version actuelle est la 2.20.
PUK	Clé personnelle de déverrouillage (Personal Unblocking Key)
RNG	Générateur de nombres aléatoires (Random Number Generator)
RSA	Système cryptographique nommé d'après ses inventeurs, à savoir Rivest, Shamir et Adleman
SKI	Injection de clé sécurisée (Secure Key Injection)
RS	Recueil systématique du droit fédéral
PTA	Prescriptions techniques et administratives concernant les services de certification dans le domaine de la signature électronique, annexe de l'ordonnance portant le numéro RS <a href="#">943.032.1</a>

## D. Références

- [OTNI] Ordonnance du 25 novembre 2020 sur la coordination de la transformation numérique et la gouvernance de l'informatique dans l'administration fédérale (état le 1<sup>er</sup> janvier 2022) ; RS 172.010.58 – <https://www.fedlex.admin.ch/eli/cc/2020/988/fr>
- [OMETA] Ordonnance sur l'utilisation de moyens électroniques pour l'exécution des tâches des autorités ; RS 172.019.1 – <https://www.fedlex.admin.ch/eli/cc/2023/754/fr>
- [PC/SC v2.01] PC/SC Workgroup Specifications Overview  
[PC/SC Workgroup – We set the standard for integrating smart cards and smart card readers into the mainstream computing environment. \(pcscworkgroup.com\)](https://www.pcscworkgroup.com/)
- [PKCS#11] Cryptographic Token Interface Standard  
<https://www.cryptsoft.com/pkcs11doc/STANDARD/pkcs-11v2-20.pdf>
- [SCM] Smart Card Minidriver Versions (versions du mini-lecteur de carte à puce)  
<https://msdn.microsoft.com/en-us/library/windows/hardware/dn631754><https://learn.microsoft.com/en-us/windows-hardware/drivers/smartcard/smart-card-minidriver-versions>
- [SKI] Secure Key Injection (injection de clé sécurisée)  
[https://msdn.microsoft.com/en-us/library/windows/hardware/dn468772\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/hardware/dn468772(v=vs.85).aspx)<https://learn.microsoft.com/en-us/windows-hardware/drivers/smartcard/secure-key-injection>
- [PTA] Prescriptions techniques et administratives concernant les services de certification dans le domaine de la signature électronique  
<https://www.bakom.admin.ch/bakom/fr/page-daccueil/l-ofcom/organisation/bases-legales/pratique-en-matiere-d-execution/prescriptions-techniques-et-administratives/rs-943-032-1.html>