ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

(12) BREVET D'INVENTION

(11) N° de publication :
MA 66589 B1

(43) Date de publication :
30.08.2024

(51) Cl. internationale :
B42D 25/24; H04N 1/32; G06Q 10/10

(21) N° Dépôt :
66589

(22) Date de Dépôt :
20.11.2019

(30) Données de Priorité :
21.11.2018 EP 18306538.2

(86) Données relatives à la demande internationale selon le PCT:
PCT/EP2019/081955 20.11.2019

(71) Demandeur(s) :
Thales Dis France SAS, 6, rue de la Verrerie 92190 Meudon (FR)

(72) Inventeur(s) :
CHAPELLIER, Sébastien ; RANTI, Mario-Locas ; WANG-ZW, Jervis ; FOO, Yong Jie

(74) Mandataire :
M. MEHDI SALMOUNI-ZERHOUNI

(86) N° de dépôt auprès de l'organisme de validation : 19804735.9

(54) Titre : **UNE PUCE À CIRCUIT INTÉGRÉ ET SON PROCÉDÉ DE GESTION**

(57) Abrégé : La présente invention concerne une correction de programme sécurisée d'un système d'exploitation de la puce de circuit intégré. Un serveur de correctif crypte un correctif pour le système d'exploitation de la puce de circuit intégré et transmet le correctif crypté à un serveur d'autorité émettrice. Le serveur d'autorité émettrice ajoute le correctif crypté dans un certificat numérique dans une extension au certificat numérique et transmet le certificat numérique comprenant le correctif crypté à un terminal. Le terminal transmet le certificat numérique à la puce de circuit intégré. La puce de circuit intégré récupère l'extension du second certificat numérique et décrypte l'extension à l'aide d'une clé de décryptage du fabricant de la puce de circuit intégré, ce qui permet de récupérer le correctif pour le système d'exploitation de la puce de circuit intégré et installe le correctif dans le système d'exploitation de la puce de circuit intégré.

UNE PUCE À CIRCUIT INTÉGRÉ ET SON PROCÉDÉ DE GESTION

REVENDICATIONS

1. Procédé d'exploitation d'une puce de circuit intégré (203) comprenant un premier certificat numérique d'une autorité émettrice, un serveur de correctifs (501), un serveur de l'autorité émettrice (511) et un terminal (515) pour corriger de manière sécurisée un système d'exploitation (409) de la puce de circuit intégré, le procédé comprenant :

l'exploitation du serveur de correctifs (501) pour chiffrer un correctif (507) vers le système d'exploitation de la puce de circuit intégré ;

l'exploitation du serveur de correctifs pour transmettre le correctif chiffré (509) au serveur de l'autorité émettrice ;

dans lequel le procédé est **caractérisé en ce que**

l'exploitation du serveur de l'autorité émettrice pour ajouter le correctif chiffré dans un second certificat numérique (513) de l'autorité émettrice dans une extension du second certificat numérique ;

l'exploitation du serveur de l'autorité émettrice pour transmettre le second certificat numérique, y compris le correctif chiffré, au terminal ;

l'exploitation du terminal pour communiquer avec la puce de circuit intégré sur présentation de la puce de circuit intégré au terminal ;

l'exploitation du terminal pour transmettre le second certificat numérique, y compris le correctif chiffré, à la puce de circuit intégré ;

l'exploitation de la puce de circuit intégré pour décompresser le second certificat numérique, y compris le correctif chiffré, afin de récupérer l'extension du second certificat numérique ; et

l'exploitation de la puce de circuit intégré pour vérifier que l'extension du second certificat numérique correspond au système d'exploitation de la puce de circuit intégré ; et s'il est vérifié que l'extension correspond au système

d'exploitation de la puce de circuit intégré, pour déchiffrer l'extension du second certificat numérique, permettant ainsi la récupération du correctif pour le système d'exploitation de la puce de circuit intégré, et l'installation du correctif dans le système d'exploitation de la puce de circuit intégré,

l'exploitation du serveur de correctifs pour signer numériquement le correctif chiffré ; et

l'exploitation de la puce de circuit intégré pour vérifier la signature numérique du correctif chiffré avant l'installation du correctif dans le système d'exploitation de la puce de circuit intégré.

2. Procédé selon la revendication 1, comprenant en outre une étape préliminaire d'installation d'une clé privée du fabricant de la puce de circuit intégré dans la puce de circuit intégré ; et dans lequel le serveur de correctifs chiffre le correctif à l'aide de la clé publique correspondant à la clé privée du fabricant de la puce de circuit intégré, et dans lequel la puce de circuit intégré déchiffre l'extension du certificat numérique à l'aide de la clé privée du fabricant.

3. Procédé selon la revendication 1, comprenant en outre une étape préliminaire d'installation d'une clé secrète du fabricant de la puce de circuit intégré dans la puce de circuit intégré ; et dans lequel le serveur de correctifs chiffre le correctif à l'aide de la clé secrète correspondant à la clé secrète du fabricant de la puce de circuit intégré, et dans lequel la puce de circuit intégré déchiffre l'extension du certificat numérique à l'aide de la clé secrète du fabricant.

4. Procédé selon l'une quelconque des revendications précédentes, dans lequel le second certificat numérique de l'autorité émettrice est un certificat de lien qui renvoie au premier certificat de l'autorité de certification stocké sur la puce de circuit intégré.

5. Procédé selon l'une quelconque des revendications précédentes, dans lequel le certificat de lien est un certificat de lien de l'autorité de certification vérifiant le pays et l'extension du lien du certificat de lien contient un identificateur d'objet indiquant que le fabricant de la puce de circuit intégré est à l'origine de l'extension du certificat de lien.

6. Procédé selon l'une quelconque des revendications précédentes, dans lequel la puce de circuit intégré est incorporée dans un document de sécurité électronique.

7. Procédé selon l'une quelconque des revendications précédentes, dans lequel le document de sécurité électronique est un document de voyage lisible par machine.

8. Puce de circuit intégré (203) comprenant :

un processeur (301) ; et

une mémoire (303) connectée au processeur et contenant des instructions exécutables par le processeur, y compris un système d'exploitation ; et

dans laquelle la puce de circuit intégré est **caractérisée en ce que** les instructions permettent au processeur de :

recevoir un certificat numérique (513) provenant d'un serveur de correctifs (501) par l'intermédiaire d'un terminal de vérification (515), le certificat numérique comportant une extension contenant un correctif chiffré (509) pour le système d'exploitation (409) ;

décompresser le certificat numérique, permettant ainsi la récupération de l'extension du certificat numérique ;

vérifier que l'extension du certificat numérique correspond au système d'exploitation de la puce de circuit intégré ; et s'il est vérifié que l'extension correspond au système d'exploitation de la puce de circuit intégré, pour déchiffrer l'extension du certificat numérique, permettant ainsi la récupération du correctif pour le système d'exploitation de la puce de circuit intégré, et l'installation du correctif dans le système d'exploitation de la puce de circuit intégré ;

dans laquelle les instructions du chargeur de correctifs comprennent en outre des instructions permettant au processeur de vérifier la signature numérique du correctif chiffré avant l'installation du correctif dans le système d'exploitation de la puce de circuit intégré.

9. Puce de circuit intégré selon la revendication 8, dans laquelle la mémoire comporte en outre une clé privée du fabricant de la puce de circuit intégré ; et

dans laquelle le correctif est chiffré à l'aide de la clé publique correspondant à la clé privée du fabricant de la puce de circuit intégré, et dans laquelle les instructions comprennent en outre des instructions permettant au processeur de déchiffrer l'extension du certificat numérique à l'aide de la clé privée du fabricant.

10. Puce de circuit intégré selon la revendication 8, dans laquelle la mémoire comporte en outre une clé secrète du fabricant de la puce de circuit intégré ; et dans laquelle le correctif est chiffré à l'aide de la clé secrète partagée ; et dans laquelle les instructions comprennent en outre des instructions permettant au processeur de déchiffrer l'extension du certificat numérique à l'aide de la clé secrète partagée du fabricant.

11. Puce de circuit intégré selon l'une quelconque des revendications 8 à 10, dans laquelle le second certificat numérique de l'autorité émettrice est un certificat de lien qui renvoie au premier certificat de l'autorité de certification stocké sur la puce de circuit intégré.

12. Puce de circuit intégré selon la revendication 11, dans laquelle le certificat de lien est un certificat de lien de l'autorité de certification vérifiant le pays et l'extension du certificat de lien contient un identificateur d'objet indiquant que le fabricant de la puce de circuit intégré est à l'origine de l'extension du certificat de lien.

13. Puce de circuit intégré selon l'une quelconque des revendications 8 à 12, dans laquelle la puce de circuit intégré est incorporée dans un document de sécurité électronique.

14. Puce de circuit intégré selon l'une quelconque des revendications 8 à 13, dans laquelle le document de sécurité électronique est un document de voyage lisible par machine.