	Descriptif de la carte agent JCOP3
Version :1.2	Note_carte agent JCOP3_17062021
Date :17/06/21	Nom du fichier : Note_carte agent JCOP3_17062021_V1-2.docx

Caractéristiques normatives de la carte Agent JCOP3.

Identification du produit de l'IN GROUP :

ChipDoc P60 on JCOP 3 SECID P60 (OSB) SSCD qualifiée sur le composant P6022J VB version v7b4).

La carte agent de la deuxième génération est une carte JCOP3 (JAVA CARD OPEN PLATFORM 3).

La carte comporte plusieurs applets (CHIPDOC3, AS ECC, DESFIRE EV1). La carte permet des communications en sans contact et en contacts.

Les tests électriques, mécaniques, d'environnement et d'impression ont été réalisés par l'IN GROUP LABORATOIRE.

La carte a été vérifiée en conformité normative par un laboratoire d'essais indépendant et accrédité COFRAC ISO 17025.

Les normes vérifiées sont :

ISO 7816 (1-2-3-4-6-8-9-11-15) (classe A, B et C)

ISO14443-A, ISO10373-6 (rétro-modulations partie haute et partie basse sur l'amplitude, tests de la résonance et du coefficient de surtension, bande passante et PPS des vitesses de communication)


Les normes suivantes ont été qualifiées par des plans de tests associés :

ISO/IEC 9796-2, ISO/IEC 9797-1 -2, ISO/IEC 10116, FIPS PUB 180-1

ISO/IEC 9564-1,

Les normes suivantes ont été qualifiées par des résultats de plans de tests mécaniques associés :

ISO10373-1,-2,-3, ISO/CEI 7810

	Descriptif de la carte agent JCOP3
Version :1.2	Note_carte agent JCOP3_17062021
Date :17/06/21	Nom du fichier : Note_carte agent JCOP3_17062021_V1-2.docx

Les normes suivantes ont été qualifiées par les résultats des plans de tests MRZ associés :

ICAO Doc 9303 part 5, part 6

Les normes suivantes ont été qualifiées par les résultats des plans de tests d'environnement associés :

ISO/CEI 21789-1 : 201, ISO/CEI 21789-2 : 2011,

Les normes suivantes ont été acquises par conception :

ISO 7811 (ISO1, ISO2, ISO3)

ISO/IEC 7812 -1

Les normes sur la cryptographie RSA et signatures sécurisées ont été acquises par vérification avec des vecteurs de tests spécifiques aux normes citées:


PKCS#1 V2.1

PKCS#15

prEN 14890-1 -2

prEN 15890 -1 -2 -3

NIST 800_38B

	Descriptif de la carte agent JCOP3
Version :1.2	Note_carte agent JCOP3_17062021
Date :17/06/21	Nom du fichier : Note_carte agent JCOP3_17062021_V1-2.docx

Spécifications documentaires associées à la conception de la carte agent

Les spécifications suivantes ont été utilisées pour le développement des services JCOP3 :

Service AS ECC (applet) :


- EUROPEAN CARD FOR e-SERVICES AND NATIONAL e-ID APPLICATIONS
AS ECC identification Authentification Signature V2 révision A02
- Profil de personnalisation P145 SPT006 (IN GROUPE)
- Spécifications de gestion des clés P145 SPT 004 (IN GROUPE)
- Spécifications fonctionnelles P145 SPT 001 (IN GROUPE)

Service DESFIRE EV1 (applet):

Base MF3ICD81 de la société NXP

Services Authentification, Signature, confidentialité JCOP3 :

ChipDoc 3.0 de la société NXP

	Descriptif de la carte agent JCOP3
Version :1.2	Note_carte agent JCOP3_17062021
Date :17/06/21	Nom du fichier : Note_carte agent JCOP3_17062021_V1-2.docx

Conformité aux exigences réglementaires, techniques et de sécurité

Rapport de certification et qualification:

ANSSI-CC-2020/48 *ChipDoc V2 on JCOP 3 P60 in*

SSCD configuration (Version v7b4_2)

DECISION DE QUALIFICATION AU NIVEAU RENFORCE : N°1830/ANSII/SDE

Rapport d'évaluation critères communs:

« ChipDoc V2 on JCOP3 P60 » en version v7b4_2 sur composant P6022 Y VB

Certificate number : CC-20-98209 TÜV Rheinland Nederland B.V.


Conformité aux profils de protection :

BSI-CC-PP-0059-2009-MA-01 v2.0.1

BSI-CC-PP-0075-2012 v1.0.2

Cible de sécurité : ANSSI-CIBLE-CC-2017 (ChipDoc P60 on JCOP3 SEDIC

P60(OSB)SSCD)

	Descriptif de la carte agent JCOP3
Version :1.2	Note_carte agent JCOP3_17062021
Date :17/06/21	Nom du fichier : Note_carte agent JCOP3_17062021_V1-2.docx

ANNEXES TECHNIQUES .

I. Descriptifs techniques

La nouvelle carte agent est constituée d'un seul composant de la famille P60 de NXP, d'un logiciel masqué et d'applets chargées. Les références exactes de la carte agent sont :

**ChipDoc P60 on JCOP 3 SECID P60 (OSB) SSCD
qualifiée sur le composant P6022J VB version v7b4).**

La carte JCOP3 est industrialisée par l'IN GROUP pour le Ministère de l'intérieur.

C'est une carte JCOP3 de NXP, dual interfaces, composée d'un service IAS ECC et d'un service DESFIRE EV1 limité par le SHFD en nombre d'AID et en nombre de fichiers.


L'applet IAS ECC peut fonctionner totalement en mode contact mais elle peut aussi fonctionner en partie en mode sans contact explicite. L'applet est gérée comme un service et peut être activée ou désactivée par le « card manager » de la JCOP3

L'applet DESFIRE EV1 fonctionne qu'en mode sans contact implicite. L'applet est gérée comme un service et peut être que désactivée par le « card manager » de la JCOP3.

L'activation est implicite. L'UID de la carte est configuré en random, c'est-à-dire que la valeur de l'UID est différente à chaque mise en utilisation.

RAPPEL : [Ce n'est par une carte DESFIRE.](#)

[C'est une carte java JCOP3 multi-applicatives.](#)

	Descriptif de la carte agent JCOP3
Version :1.2	Note_carte agent JCOP3_17062021
Date :17/06/21	Nom du fichier : Note_carte agent JCOP3_17062021_V1-2.docx

II. Détection hardware de la carte agent en mode contact.

L'ATR indique des informations d'expertise de la carte mais n'indique pas des informations applicatives :

Les octets protocolaires indiquent une carte pouvant travailler en protocole contact T=0, en T=1 et en mode contactless T=15.

Son interface hardware en mode contact indique une possibilité de travailler en bi-tensions soit en 5V soit en 3V (la troisième tension 1,8V fonctionne mais n'est pas utilisée à ce jour. Ce mode est réservé pour une utilisation future avec des produits «nomade low voltage »). La carte ne fonctionne pas entre 5V et 3V (choix configuré en mode step).

Les vitesses de transmission en mode contact dépendent du lecteur. Elles peuvent aller jusqu'à 161290 bits/s si la fréquence du lecteur est de 5 Mhz (valeur maximale indiquée dans la norme ISO7816).

La partie contactless est traitée dans le compte-rendu d'essais et de sa conformité aux tests de la norme ISO10373-6.


La carte accepte une identification SFI (attention seule une partie spécifiée est autorisée) en mode contact et en mode contactless (sauf attribut forçant le mode contact).

La carte ne comporte qu'une voie logique, c'est à dire qu'elle ne peut pas travailler en mode contact et en mode sans contact en même temps. De plus elle n'est pas prévue par sa mono voie à travailler avec une voie SWP.

La détection de la JCOP3 par Windows entraîne une fonction de propagation des certificats de la carte vers les magasins des certificats.

Rappel :

Le service DESFIRE EV1 n'est pas accessible en mode « contact » car les spécifications ne sont pas compatibles avec la norme réservée au mode à contact.

	Descriptif de la carte agent JCOP3
Version :1.2	Note_carte agent JCOP3_17062021
Date :17/06/21	Nom du fichier : Note_carte agent JCOP3_17062021_V1-2.docx

III. Détection hardware de la carte par le lecteur RFID.

La carte agent JCOP3 est une carte JAVA **multi-applicatives** ayant 2 applets actives.

- La carte agent JCOP3 **en mode sans contact** est en mode implicite c'est-à-dire que l'applet DESFIRE EV1 est active dès l'activation du champ magnétique.

Si le **premier octet** émis par le lecteur (octet de CLASS) vers la carte est **un octet de CLASS DESFIRE** alors le « card manager » verrouille l'applet DESFIRE EV1

Si le **premier octet émis** par le lecteur n'est pas une **valeur de CLASS DESFIRE** alors l'applet DESFIRE est désactivée et l'applet IAS ECC est alors activé.

Dans le cas où cette valeur n'est pas comprise comme un octet de CLASS IAS ECC alors le « card manager » désactive également l'applet IAS ECC. N'ayant plus d'autre applet à sélectionner alors la carte se verrouille et répond **un statut d'erreur « 6884 »**.

Une mise en hors champs est alors obligatoire par le logiciel du poste de travail.


Si le **premier octet** émis par le lecteur (octet de CLASS) vers la carte est **un octet de CLASS IAS ECC** alors le « card manager » verrouille l'applet IAS ECC.

Si le **premier octet émis** par le lecteur n'est pas une **valeur de CLASS DESFIRE ni IAS ECC** alors le « card manager » de la carte désactivera aussi l'applet IAS ECC.

N'ayant plus d'applet activée, le « card manager » répondra à toutes les futures APDU reçues avec le statut d'erreur :

SW= 68 84

Une mise en hors champs est alors obligatoire par le logiciel du poste de travail.

	Descriptif de la carte agent JCOP3
Version :1.2	Note_carte agent JCOP3_17062021
Date :17/06/21	Nom du fichier : Note_carte agent JCOP3_17062021_V1-2.docx


IV. Notes techniques sur les dysfonctionnements.

- La plupart des dysfonctionnements vient de lecteurs obsolètes ne pouvant plus être mis à jour.
- De nombreux **lecteurs multi applicatifs** ne respectent pas les séquences de mise en champ et de mise en hors champ entre deux changements de protocole comme le demande la norme ISO 14443. Rappel normatif, le changement de protocole A, B, B' et C est autorisé. Après la sélection d'un protocole ISO (A, B , B') on sélectionne une application. En cas de non réponse, la carte/badge/smartphone est rejetée en coupant le champ puis en réactivant celui-ci afin de détecter une autre application et ainsi de suite afin de trouver la bonne application.

Pour faciliter la détection il est conseillé soit de désactiver la recherche automatique d'un protocole, soit de forcer la priorité sur une application voulue (exemple le service DESFIRE)

- Le fonctionnement non conforme du lecteur avec WINDOWS lors des échanges en trame CCID provoque des arrêts de communication avec la carte agent.

Pour rappel la carte JCOP3 est une carte JAVA avec des certificats et ce n'est pas une carte DESFIRE EV1. Windows va détecter une carte JAVA et via les commandes CCID va demander la propagation des certificats puis va réinitialiser correctement l'environnement du lecteur comme lors de la détection de la carte.

	Descriptif de la carte agent JCOP3
Version :1.2	Note_carte agent JCOP3_17062021
Date :17/06/21	Nom du fichier : Note_carte agent JCOP3_17062021_V1-2.docx

V. Exemples d'anomalies normatives des lecteurs RFID lors d'une connexion à une carte agent JCOP3.

1) Exemple d'un lecteur multi-protocole provoquant **une erreur de communication**

Etape 1 :

Détection de la carte agent JCOP3

Etape 2 :

Activation du champ magnétique du lecteur (La carte est en mode implicite et le service DESFIRE est activé)

Etape 3

Test 1^{er} protocole : exemple recherche de CALYPSO

SELECT MF CALYPSO

➤ 94 A4 00 00 02 3F 00 00

< 6E 00

L'APDU n'est pas reconnu par DESFIRE actif, le premier octet **94** reçu par la carte provoque une désactivation du service DESFIRE et une activation du service IAS ECC. Celui-ci traite ce premier octet **94** et n'est pas reconnu par l'IAS ECC provoquant également la désactivation du service IAS ECC. Le « card manager » de la carte JAVA va refuser cette APDU en répondant par un statut 6E 00. **A partir de cette étape la carte n'a plus d'applet activé et pourra répondre que par un statut d'erreur.** Seule une réinitialisation du champ (donc de la carte pourrait débloquer cet état)

Le lecteur va poursuivre sa recherche de protocole sans réinitialiser le champ magnétique (erreur ISO14443)

Test 2eme protocole : exemple recherche iCLASS


Select MF iCLASS

➤ 80 A6 00 00 03 00 00 00

< 68 84

Le « card manager » n'ayant plus d'applet active va répondre à toutes les APDUs reçues par le statut « 68 84 ».

Conclusion : impossible de sortir de la boucle sans une coupure du champ.

	Descriptif de la carte agent JCOP3
Version :1.2	Note_carte agent JCOP3_17062021
Date :17/06/21	Nom du fichier : Note_carte agent JCOP3_17062021_V1-2.docx

2) Exemple d'un lecteur multi-protocole **sans erreur de communication** :

Etape 1 :

Détection de la carte agent JCOP3

Etape 2 :

Activation du champ magnétique du lecteur (La carte est en mode implicite et le service DESFIRE est activé)

Etape 3

Test 1^{er} protocole : exemple recherche de CALYPSO

SELECT MF CALYPSO

➤ **94** A4 00 00 02 3F 00 00

< **6E 00**

L'APDU n'est pas reconnu par DESFIRE actif, le premier octet **94** reçu par la carte provoque une désactivation du service DESFIRE et une activation du service IAS ECC. Celui-ci traite ce premier octet **94** et n'est pas reconnu par l'IAS ECC provoquant également la désactivation du service IAS ECC. Le « card manager » de la carte JAVA va refuser cette APDU en répondant par un statut 6E 00

Etape 4 :

Le lecteur coupe alors le champ magnétique, puis le réactive.

Le lecteur va poursuivre sa recherche de protocole

Test 2eme protocole : recherche iCLASS

Select MF iCLASS

➤ 80 A6 00 00 03 00 00 00 00

< **6E 00**

Etape 5 :

Le lecteur coupe le champ magnétique puis le réactive

Le lecteur va poursuivre sa recherche de protocole


Test 3eme protocole : recherche DESFIRE

SELECT MF DESFIRE

➤ 90 5A 00 00 03 00 00 00 00

< **91 00**

L'APDU est reconnue par le service DESFIRE actif (mode implicite), le premier octet **90** reçu par la carte provoque un verrouillage du service DESFIRE par le « card manager » et poursuit l'analyse de l'APDU. L'APDU SELECT MF est décodée et exécutée correctement par le service DESFIRE permettant l'émission du statut OK soit **91 00**.

	Descriptif de la carte agent JCOP3
Version :1.2	Note_carte agent JCOP3_17062021
Date :17/06/21	Nom du fichier : Note_carte agent JCOP3_17062021_V1-2.docx

VI. CONCLUSION

La carte agent émule exactement une carte DESFIRE EV1 si le lecteur émet toujours le premier octet CLASS de l'APDU des spécifications DESFIRE dès l'activation du champ magnétique de celui-ci.

A partir de cette étape, le lecteur est conforme et les travaux d'intégration de la carte agent peuvent être réalisés par une simple carte DESFIRE EV1 par un industriel en la configurant avec un UID à valeur aléatoire par la commande décrite dans les spécifications DESFIRE EV1. Le nombre de clés et leurs valeurs ainsi que les keysetting sont paramétrés en fonction d'un usage spécifique (AID défini avec le MI).