Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2019/43

Application CPS2ter v1.12, adossée à l'application IAS ECC v1.3, en composition sur la plateforme ID-One Cosmo v8.2 (Identification 01 12)

Paris, le 22 novembre 2019

Le directeur général de l'agence nationale de la sécurité des systèmes d'information

Guillaume POUPARD
[ORIGINAL SIGNÉ]

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2019/43

Nom du produit

Application CPS2ter v1.12, adossée à l'application IAS ECC v1.3, en composition sur la plateforme ID-One Cosmo v8.2

Référence/version du produit

Identification 01 12

Conformité à un profil de protection

Néant

Critères d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 4 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

Idemia **2 place Samuel de Champlain,** **92400 Courbevoie, France**	**NXP Semiconductors GmbH** **Troplowitzstrasse 20,** **22529 Hamburg, Allemagne**

Commanditaire

Idemia
2 place Samuel de Champlain,
92400 Courbevoie, France

Centre d'évaluation

CEA - LETI
17 avenue des martyrs, 38054 Grenoble Cedex 9, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Ce certificat est reconnu au niveau EAL2.

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est l'« Application CPS2ter v1.12, adossée à l'application IAS ECC v1.3, en composition sur la plateforme ID-One Cosmo v8.2, Identification 01 12 » développée par Idemia et masquée sur le composant NXP P60D145 développé par *NXP SEMICONDUCTORS GMBH*.

Ce produit est une carte à puce disposant d'une interface contact et d'une interface sans contact qui propose les services IAS et CPS2ter sur le même circuit. Le but est de permettre une transition de la technologie CPS2ter actuellement utilisée par l'Agence des Systèmes d'Information Partagés de Santé (ASIP Santé) vers la technologie CPS3 basée sur le standard IAS.

Ainsi ce produit est destiné à être utilisé comme dispositif de stockage sécurisé de données médicales avec accès à des services distants sensibles. Il est livré en configuration fermée et ne permet pas le chargement d'application en *post-issuance*.

1.2. Description du produit

1.2.1. Introduction

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit et décrits dans [ST] sont :

- l'import de code PIN et de clés ;
- l'authentification via le code PIN de l'utilisateur ;
- l'export de données de l'utilisateur ;
- la génération de nombre aléatoire ;
- la vérification de l'authenticité des commandes entrantes via un cryptogramme, appelée « PRO mode » ;
- l'authentification externe d'entités distantes pour l'accès aux données de l'utilisateur ;
- la personnalisation sécurisée via un canal de confiance.

1.2.3. Architecture

Le produit, dont l'architecture est décrite au chapitre 2 de la cible de sécurité [ST], est constitué :

- du microcontrôleur NXP P60D145 certifié sous la référence [CER-IC] ;
- de la plateforme *Java Card* ouverte « ID-One Cosmo V8.2 », certifiée sous la référence [CER-PTF], avec le code optionnel «R1.0 Appli Deselection before DESFire » ;
- de l'application « IAS ECC v2 version 1.3 » en configuration #1, #2, #3 ou #4, certifiée sous les références ANSSI-CC-2019/33, ANSSI-CC-2019/34, ANSSI-CC-

2019/35 et ANSSI-CC-2019/36 (voir [CER-IAS]), fonctionnant à travers les interfaces contact et sans contact ;
- de l'application « CPS2ter, version 1.12 », fonctionnant seulement via l'interface contact avec le code optionnel « R2.0 GIP-CPS supporting SCP03 ».

Tous ces éléments font partie de la cible d'évaluation (TOE[1]).

1.2.4. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La présence des applications peut être vérifiée par la commande GET STATUS, qui renvoie l'AID des applications et packages présents dans le produit. Le tableau ci-dessous liste ces AID.

Nom de l'aplet	AID (valeur en hexadécimal)	Correspondance
IAS ECC V2 version 1.3	A0000000770108000710000000000000B A0000000770108000710000000000000D A000000077010800071000000000013 A0000000770108000710000010000000E	*Package* Interface *Package* : API *Package* : Add-On *Applet*
CPS2ter version 1.12	A0000000770108000710000010000000C A0000000770108000710000000000000C	*Package* : CPS2ter *Applet*

La version certifiée du produit est identifiable par les éléments des tableaux ci-après, Ces éléments sont détaillés dans la cible de sécurité [ST] et dans les [GUIDES].

Eléments de configuration		Origine
Nom / Version de la TOE	IAS ECC v2, version 1.3 en configuration #1	*IDEMIA*
Identification interne de l'application « CPS2ter, version 1.12 »	« 01 12 »	
Identification interne de l'application « IAS ECC v2, version 1.3 »	« F0 02 02 13 »	
Référence de la plateforme	ID-One Cosmo v8.2	
Identification de la plateforme	« 6F 01»	
Identification du code optionnel « R1.0 Appli Deselection before DESFire »	« 90 30 82 »	
Identification du code optionnel « R2.0 GIP-CPS supporting SCP03 »	« 90 30 72 »	
Référence du microcontrôleur	NXP P60D145	*NXP SEMICONDUCTORS GMBH*
Identification du composant	« 30 »	

[1] *Target of Evaluation.*

Ces éléments peuvent être vérifiés par les méthodes décrites dans les [GUIDES]. Notamment l'identification s'effectue par l'envoi de la commande GET DATA :

- avec le tag DF 52 pour la plateforme, les codes optionnels « R1.0 Appli Deselection before DESFire » et « R2.0 GIP-CPS supporting SCP03 » et du composant ;
- avec le tag DF 67 pour l'application « IAS ECC v2 » ;
- avec le tag DF 66 pour l'application « CPS2ter v1.12 ».

1.2.5. Cycle de vie

Le cycle de vie du produit est décrit au chapitre 2.3 de [ST]. Il est composé des phases listées dans le tableau suivant, pouvant être regroupées en trois étapes :

- le développement (phases 1 à 3) ;
- la production (phases 4 et 5) ;
- l'état opérationnel (phases 6 et 7).

Le point de livraison de la TOE est en sortie de la phase 3. Après cette phase la TOE est considérée comme auto-protégée.

Phases	Tâches	Couvert par	Acteurs ou Sites
1	Développement des parties logicielles	ALC	*IDEMIA* (Courbevoie et Pessac) Sites audités dans le cadre de [CER-PTF]
2	Développement du microcontrôleur	ALC	Sites audités dans le cadre de [CER-IC]
3	Fabrication	ALC	Sites audités dans le cadre de [CER-IC]
Point de livraison de la TOE			
4	*Packaging* et initialisation	AGD_PRE	Agent de fabrication
5	Pré-personnalisation	AGD_PRE	Agent de fabrication
6	Personnalisation	AGD_PRE	Agent personnalisateur
7	Utilisation	AGD_OPE	Utilisateur final

Le produit a été développé sur les sites suivants d'*IDEMIA* (voir [SITES]) :

***IDEMIA* – Courbevoie** [CRB]	***IDEMIA* – Pessac** [PSC]
2, place Samuel de Champlain 92400 Courbevoie, France	Bâtiment Elnath, 11 avenue de Canteranne, 33600 Pessac, France

Les sites intervenant dans le cycle de vie de la plateforme et du composant sont listés respectivement dans [CER-PTF] et [CER-IC].

1.2.6. Configuration évaluée

Le certificat porte sur le produit tel que décrit au paragraphe 1.2.3 et identifié au paragraphe 1.2.4.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 5** [CC] et à la méthodologie d'évaluation définie dans le manuel [CEM].
Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [JIWG IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

2.2. Travaux d'évaluation

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration de l'application VITALE dans la plateforme déjà certifiée par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation de la plateforme « Plateforme ID-One Cosmo v8.2 masquée sur le composant NXP P60D145 » au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5, conforme au profil de protection [PP JCS-O]. Cette plateforme a été certifiée le 19 juillet 2019 sous la référence ANSSI-CC-2019/28 (voir [CER-PTF]).

L'évaluation s'appuie sur les résultats d'évaluation des produits « IAS ECC V2, version 1.3 sur la plateforme ID-One Cosmo v8.2, en configuration #1, #2, #3 et #4 » certifiés le 17 septembre 2019, respectivement sous les références ANSSI-CC-2019/33, ANSSI-CC-2019/34, ANSSI-CC-2019/35 et ANSSI-CC-2019/36 (voir [CER-IAS]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 7 novembre 2019, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI [REF] n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilité de conception et de construction pour le niveau AVA_VAN.5 visé.

2.4. Analyse du générateur d'aléas

Le générateur de nombres aléatoires, de nature physique, utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur (voir [CER-IC]).

Par ailleurs, comme requis dans le référentiel cryptographique de l'ANSSI [REF], la sortie du générateur physique d'aléas subit un retraitement de nature cryptographique.
Les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.5 visé.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit « Application CPS2ter v1.12, adossée à l'application IAS ECC v1.3, en composition sur la plateforme ID-One Cosmo v8.2, Identification 01 12» soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté des composants ALC_DVS.2 et AVA_VAN.5.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[1], des certificats Critères Communs.
La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 ainsi qu'à la famille ALC_FLR.
Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4+	Intitulé du composant
ADV Développement	ADV_ARC		1	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	**4**	Complete functional specification
	ADV_IMP				1	1	2	2	**1**	Implementation representation of TSF
	ADV_INT					2	3	3		
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	**3**	Basic modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	**1**	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	**4**	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	**4**	Problem tracking CM coverage
	ALC_DEL		1	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			1	1	1	2	2	**2**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD			1	1	1	1	2	**1**	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	**1**	Well-defined development tools
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	**2**	Analysis of coverage
	ATE_DPT			1	1	3	3	4	**1**	Testing: basic design
	ATE_FUN		1	1	1	1	2	2	**1**	Functional testing
	ATE_IND	1	2	2	2	2	2	3	**2**	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	**5**	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Security Target CPS2ter Application on ID-One Cosmo v8.2, référence FQR 110 9044, version 3 du 03/10/2019. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Security Target Lite CPS2ter Application on ID-One Cosmo v8.2, référence FQR 110 9201, version 1 du 03/10/2019.
[RTE]	Rapport technique d'évaluation : - LAKSHMI, Rapport Technique d'Evaluation, référence LETI.CESTI.LAK.ETR.001, version 1.3 du 07/11/2019.
[CONF]	Liste de configuration du produit : - LAKSHMI Configuration List, référence FQR 110 9090, version 2 du 03/10/2019.
[GUIDES]	Guide d'installation et d'administration du produit : - GIP-CPS on ID-One Cosmo v8.2 – AGD_PRE – Pre-Personalization Guide, référence 110 8975, version 3 du 03/10/2019. Guide d'utilisation du produit : - GIP-CPS on ID-One Cosmo v8.2 – AGD_OPE – Reference Guide, référence FQR 110 8976, version 1 du 23/10/2018 ; - CPS3ter Java Applet – SOFTWARE REQUIREMENTS SPECIFICATIONS, référence 0708037 00 SRS, version 7-AA du 31/01/2019 ; - Optional code R1.0 GIP-CPS suppporting SCP03, référence FQR 110 9105, version 2 du 02/04/2019. Guides d'installation, d'administration et de développement d'applications sécurisées sur la plateforme : - ID-One Cosmo V8.2 Pre-Perso Guide, référence FQR 110 8875 version 3, 13/03/2019 ; - ID-One Cosmo V8.2 Reference Guide, référence FQR 110 8885, version 3, 06/03/2019 ; - ID-One Cosmo V8.2 on P60D145 - Applet Security Recommandations, référence FQR 110 8963, version 4, 18/03/2019 ; - ID-One Cosmo V8.1-n Application Loading Protection Guidance, référence FQR 110 8001, version 1, 11/10/2016 ; - Optional code R1.0 Appli Deselection defore DESFire, référence FQR 110 9106, version 2 du 02/04/2019.

[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - [CRB] o IDEMIA Development Environment ALC Class Evaluation Report (Generic Documentary activities, reference IDEMIA R&D site 2018_GEN_v1.1, 19 juin 2019 *;* o Site Technical Audit Report CRB, référence IDEMIA R&D site 2018_CRB_STAR_v1.3, 26/06/2019. - [PSC] o IDEMIA Development Environment ALC Class Evaluation Report (Generic Documentary activities, reference IDEMIA R&D site 2018_GEN_v1.0, 29 novembre 2018 *;* o Site Technical Audit Report PSC, reference IDEMIA R&D site 2018_PSC_STAR_v1.1, 22/05/2019.
[CER-IC]	Certification Report for NXP Secure Smart Card Controller P6022y VB* including IC Dedicated Software from NXP Semiconductors Germany GmbH. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 18 mai 2018, sous la référence BSI-DSZ-CC-1059-2018.*
[CER-PTF]	Rapport de certification pour la « Plateforme ID-One Cosmo v8.2 masquée sur le composant NXP P60D145 ». *Certifié par l'ANSSI le 19 juillet 2019 sous la référence ANSSI-CC-2019/28.*
[CER-IAS]	Rapports de certification de: - « IAS ECC V2, version 1.3 en configuration #1 sur la plateforme ID-One Cosmo v8.2 » *;* *Certifié par l'ANSSI le 17 juillet 2019 sous la référence ANSSI-CC-2019/33 ;* - « IAS ECC V2, version 1.3 en configuration #2 sur la plateforme ID-One Cosmo v8.2 » ; *Certifié par l'ANSSI le 17 juillet 2019 sous la référence ANSSI-CC-2019/34 ;* - « IAS ECC V2, version 1.3 en configuration #3 sur la plateforme ID-One Cosmo v8.2 » ; *Certifié par l'ANSSI le 17 juillet 2019 sous la référence ANSSI-CC-2019/35 ;* - « IAS ECC V2, version 1.3 en configuration #4 sur la plateforme ID-One Cosmo v8.2 » ; *Certifié par l'ANSSI le 17 juillet 2019 sous la référence ANSSI-CC-2019/36. ;*

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure ANSSI-CC-CER-P-01 Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : - Part 1: Introduction and general model, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001; - Part 2: Security functional components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002; - Part 3: Security assurance components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, février 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 3.0, avril 2019.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.5.1, mai 2018.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.