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-2016/02

MetaCRYPT-API

Version 1.2.1

Paris, le 17 février 2016

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

Guillaume POUPARD
[ORIGINAL SIGNE]

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-2016/02

Nom du produit

MetaCRYPT-API

Référence/version du produit

Version 1.2.1

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 3 augmenté

ALC_FLR.3, AVA_VAN.3

Développeur

Bull SAS (Groupe Atos)

rue Jean Jaurès, 78340 Les Clayes sous-bois, France

Commanditaire

Bull SAS (Groupe Atos)

rue Jean Jaurès, 78340 Les Clayes sous-bois, France

Centre d'évaluation

Oppida

4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit 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 la bibliothèque « MetaCRYPT-API » développée par *BULL SAS* (Groupe *ATOS*).

Ce produit est destiné à être intégré dans des applications nécessitant du chiffrement.

1.2. Description du produit

Le produit est une bibliothèque fournissant des services de chiffrement et de déchiffrement de fichiers ou données aux formats CMS ou XML-Enc. .

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. Identification du produit

La version du produit évaluée est la suivante : **MetaCRYPT version 1.2.1.**

Le numéro de version apparait :
- sur le support CD-ROM contenant le produit évalué ;
- dans le fichier MANIFEST.MF présent sur le CD-ROM contenant également le fichier metacrypt-api.jar.

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF]. Ces éléments sont des fichiers au format *bytecode* interprétable par une machine virtuelle Java. Chacun des fichiers est signé afin de pouvoir en vérifier l'intégrité.

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :
- le chiffrement de données (fichiers, flux) et de clés secrètes ;
- le déchiffrement de données (fichiers, flux) et de clés secrètes.

Cette bibliothèque permet d'offrir des services de chiffrement et déchiffrement selon deux modes :
- *Enveloped Data Mode* : dans ce mode MetaCRYPT-API génère une clé secrète pour le document à chiffrer puis chiffre cette clé avec la clé publique de tous les destinataires (voir figure 1).

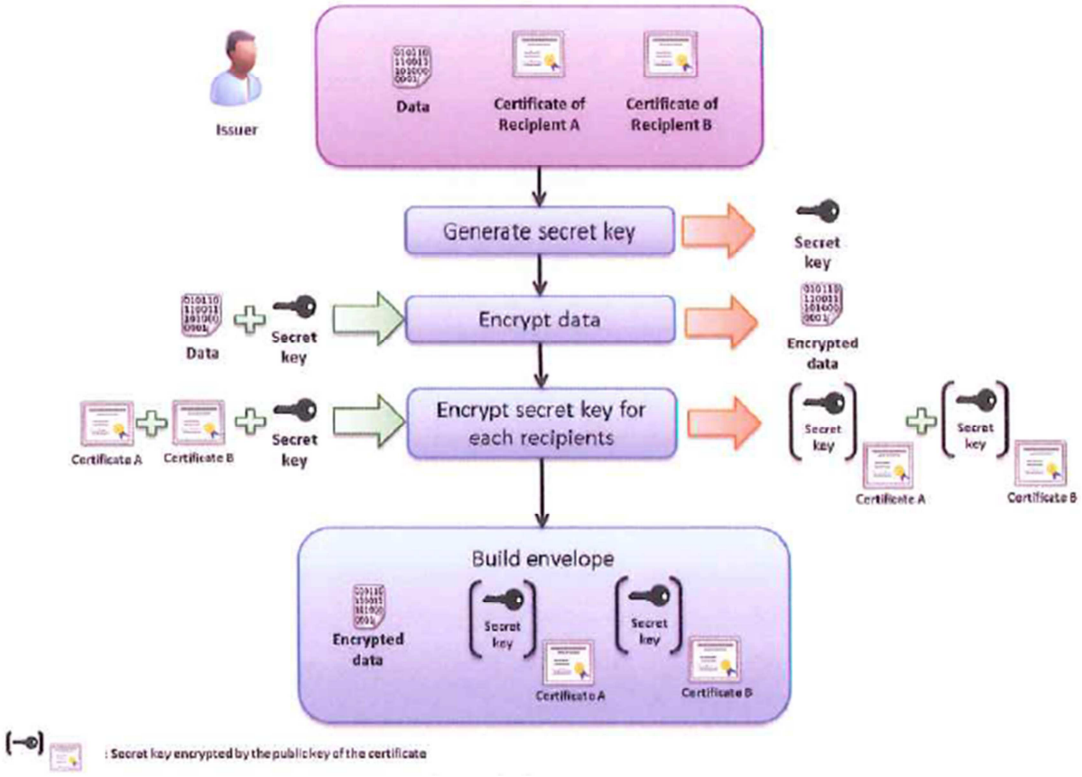

Figure 1 - *Enveloped Data Mode* - Emetteur

Chaque destinataire peut ainsi utiliser sa propre clé privée afin de déchiffrer la clé secrète associée au document envoyé. Une fois cette dernière déchiffrée le document peut être lui-même déchiffré (voir figure 2).

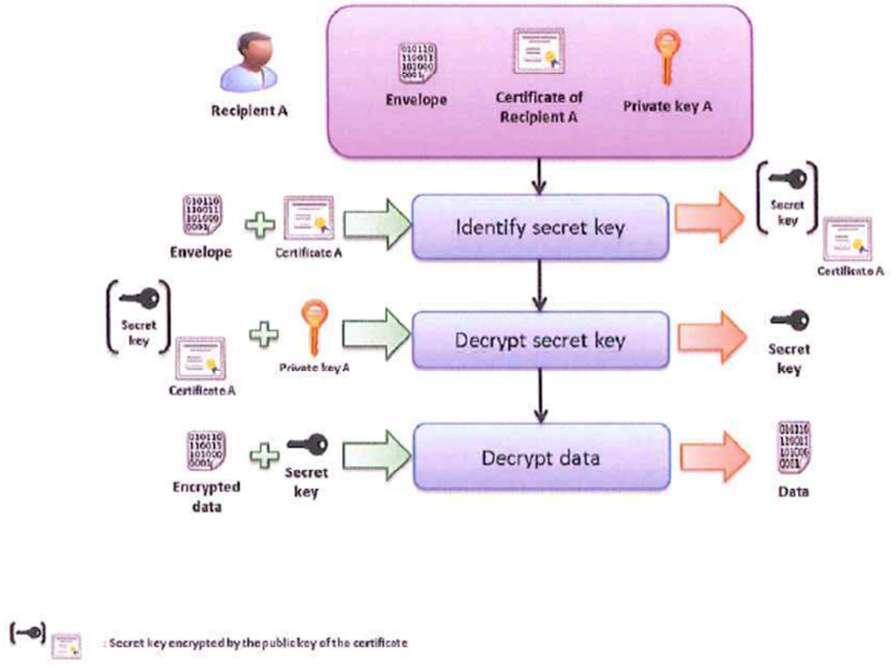

Figure 2 - *Enveloped Data Mode*- Destinataire

- *Encrypted Data Mode* : dans ce mode une clé secrète préalablement partagée entre l'émetteur et le destinataire est utilisée pour le chiffrement et le déchiffrement par les deux entités (voir figure 3).

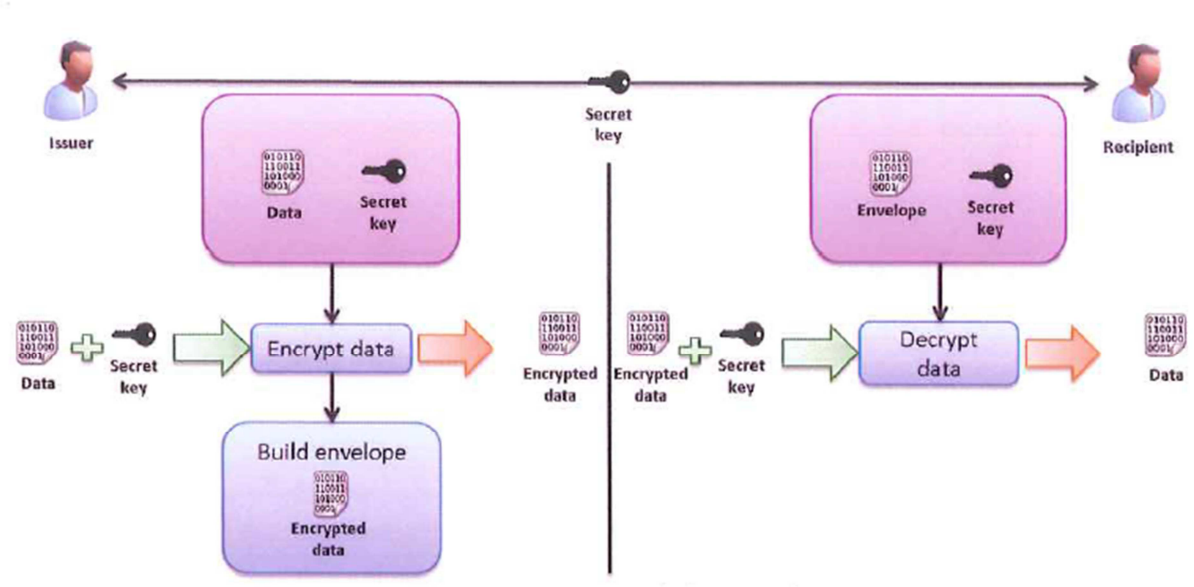

Figure 3 - *Encrypted Data Mode*

1.2.4. Architecture

L'évaluation portera sur l'ensemble de la bibliothèque MetaCRYPT-API dont le périmètre est représenté (en rose) sur le schéma suivant :

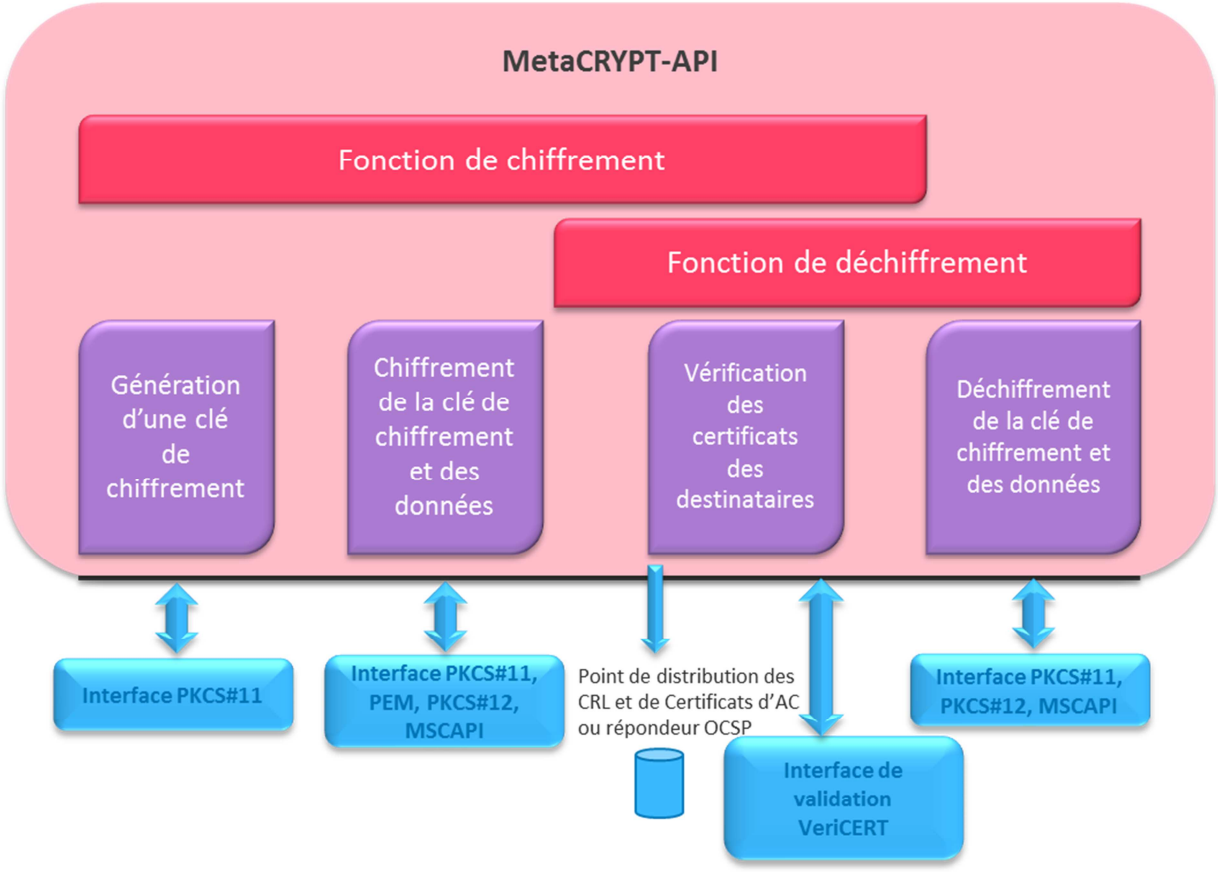

Figure 4 - Architecture et périmètre de la cible d'évaluation

La liste détaillée des composants de la TOE est décrite dans le §1.5 de la cible de sécurité [ST].

1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :

- la définition du besoin ;
- la spécification (documentation) et l'implémentation de la solution retenue ;
- la validation de la solution ;
- l'intégration de la solution sur les projets clients ;
- la diffusion de la solution chez le client ;
- la maintenance corrective.

Le produit a été développé sur le site suivant :

BULL SAS (Groupe *ATOS*)

Rue Jean Jaurès
78340 Les Clayes sous-bois
France

La bibliothèque MetaCRYPT-API est destinée à être intégrée dans des applications cryptographiques. Ainsi, pour l'évaluation, le développement des applications appelantes est considéré en tant que phase d'utilisation du produit au sens des [CC].

1.2.6. Configuration évaluée

La bibliothèque MetaCRYPT-API a été évaluée par le CESTI avec une application appelante s'appuyant sur la configuration d'évaluation suivante :

- le système d'exploitation Microsoft Windows7 Enterprise 64 bits ;
- l'environnement *ORACLE* Java Runtime Environment 8 update 45 (32 bits) ;
- des certificats et clés stockés dans un fichier PKCS#12 protégé par un mot de passe ou dans un support cryptographique *GEMALTO* Multiapp ID IAS ECC ;
- des certificats téléchargés via un annuaire OpenLDAP 2.4.39 en LDAP/LDAPS, via un serveur *TOMCAT* avec les protocoles HTTP/HTTPS ou dans un fichier local ;
- la validation des certificats via le répondeur Bull MetaPKI v9.5.8 OCSP (*Online Certificate Status Protocol*) ou via un magasin de CRLs (*Certificate Revocation Lists*).

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs version 3.1 révision 4 [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 10 novembre 2015 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 vulnérabilités de conception et de construction pour le niveau AVA_ VAN.3 visé.

Il est à préciser que les algorithmes présents dans la bibliothèque sont conformes au référentiel technique de l'ANSSI [REF] avec :

- pour les algorithmes symétriques, la possibilité d'utilisation jusqu'en 2020 (triple DES) ;
- pour les algorithmes asymétriques, seul le RSA est présent avec la recommandation dans les guides [GUIDES] de n'utiliser que des clés de taille supérieure à 2048 bits.

Il n'est pas mentionné dans les guides [GUIDES] la possibilité d'emploi d'algorithmes non conformes au référentiel [REF].

2.4. Analyse du générateur d'aléas

Le produit ne comporte pas de générateur d'aléas entrant dans le périmètre d'évaluation. Il est fait l'hypothèse lors de l'évaluation que le chiffrement mis en œuvre (vecteurs d'initialisation, génération de clés) s'appuie sur un générateur d'aléas conforme au référentiel technique de l'ANSSI [REF].

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 « MetaCRYPT-API » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 3 augmenté des composants ALC_FLR.3 et AVA_VAN.3.

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], notamment :

- *les recommandations sur la configuration de MetaCRYPT-API :*
  - les tailles de clés RSA pouvant être utilisées sont : 2048 bits et 4096 bits ;
  - la récupération des politiques de chiffrement, des CRLs et des certificats d'Autorités de Certification depuis un point de distribution distant doit s'effectuer avec l'utilisation du protocole de communication sécurisé TLS ;
  - l'utilisation uniquement de son propre mécanisme interne de vérification des certificats pouvant faire toutefois appel à la collecte externe de CRL (*Certificate Revocation Lists*) ou à un répondeur OCSP (*Online Certificate Status Protoco*l) ;
  - l'utilisation des moyens de stockage sécurisés pour la récupération de la clé privée afin de garantir son intégrité et sa confidentialité (exemple : conteneur PKCS#12, carte à puce via le protocole PKCS#11...) ;
  - MetaCRYPT-API ne doit pas utiliser de transformation (XSLT/XPATH) dans sa configuration lors de la réalisation d'une opération de chiffrement.

- *les recommandations sur l'application utilisatrice de MetaCRYPT-API :*
  - l'application appelante doit utiliser le fichier MetaCRYPT-API et les bibliothèques associées qui ont été signés par le certificat de BULL afin d'en garantir la provenance et l'intégrité ;
  - l'application appelante de MetaCRYPT-API doit s'assurer de l'authenticité de l'origine des politiques de chiffrement avant qu'elles ne soient utilisées par MetaCRYPT-API. Lorsque la récupération de ces politiques est effectuée par la fonction de MetaCRYPT-API sur un service distant alors la communication doit être sécurisée en utilisant le protocole de communication HTTPS sécurisé par un protocole TLS ;

- l'environnement d'utilisation de MetaCRYPT-API doit fournir à l'application appelante les moyens de contrôler l'intégrité des services et des paramètres de MetaCRYPT-API ;
- l'application utilisatrice ne doit pas être utilisée ou exécutée en mode « administrateur » sur le poste de travail afin de garantir l'interdiction d'écriture et de lecture de fichiers sur les répertoires non accessibles par l'utilisateur de l'application ;
- lors de l'utilisation du format de chiffrement avec transport de clé, la politique de chiffrement doit forcer la vérification de la présence de l'usage de clé « *keyEncipherment* » dans les certificats des destinataires ;
- lorsqu'une instance de l'objet « *RecipientManager* » n'est plus utile, il est nécessaire de supprimer sa référence. Ainsi, les éléments sensibles de l'objet (comme la clé privée) seront supprimés au passage du « *garbage collector » ;*
- lors de l'utilisation d'un chiffrement ou déchiffrement au format « *Encrypteddata* », il est nécessaire de supprimer la référence de clé secrète utilisée au passage du « *garbage collector* ».

- *les recommandations sur la machine hôte*

  La machine hôte sur laquelle MetaCRYPT-API s'exécute doit être sous la responsabilité d'une personne morale ou physique qui garantit que les mesures ci-après sont bien appliquées. Le système d'exploitation de la machine hôte doit offrir des contextes d'exécution séparés pour les différentes tâches qu'il exécute.

  De plus, les mesures suivantes doivent être appliquées:
  - la machine hôte est protégée contre les virus ;
  - les échanges entre la machine hôte et d'autres machines via un réseau ouvert sont contrôlés par un pare feu contrôlant et limitant les échanges ;
  - l'accès aux fonctions d'administration de la machine hôte est restreint aux seuls administrateurs de celle-ci ;
  - l'installation et la mise à jour de logiciels sur la machine hôte est sous le contrôle de l'administrateur ;
  - le système d'exploitation de la machine hôte refuse l'exécution d'applications téléchargées ne provenant pas de sources sûres.

3.3. Reconaissance 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 jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4. 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].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], 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] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.
[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, la Suède et la Turquie.

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 3+	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**	**3**	Functional specification with complete summary
	ADV_IMP				**1**	1	**2**	2		
	ADV_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**2**	Architectural 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	**3**	Authorisation controls
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**3**	Implementation representation CM coverage
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**1**	Identification of security measures
	ALC_FLR								**3**	Systematic flaw remediation
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3		
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	**3**	Focused vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Cible de sécurité METACRYPT-API, référence EVALCC-MCRYPT-ST-01-v1.5 du 6 mai 2015.
[RTE]	Rapport technique d'évaluation : - METACRYPT-API v1.0, référence OPPIDA/CESTI/METACRYPT-API/RTE du 16 octobre 2015.
[CONF]	Liste de configuration du produit : - Liste de configuration, référence configurationList du 17 septembre 2015.
[GUIDES]	Guides d'utilisation du produit : - MetaCRYPT-API, référence MetaCRYPT_API_Guide_Programmation-v1.6, version 1.6 du 25/08/2015 ; - MetaCRYPT - Guide des Codes d'erreurs, référence MetaCRYPT_API_Guide_Codes_Erreurs-v1.1, version 1.1 du 13/05/2015.

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 CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; Part 2: Security functional components, Septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[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.
[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.