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-2015/33

# eTravel Essential 1.0, avec BAC, AA et EAC activés, sur composant M7794 A12/G12

*Paris, le 10 septembre 2015*

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

Guillaume POUPARD
[ORIGINAL SIGNE]

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.anssi@ssi.gouv.fr

*Référence du rapport de certification*

# ANSSI-CC-2015/33

*Nom du produit*

## eTravel Essential 1.0, avec BAC, AA et EAC activés, sur composant M7794 A12/G12

*Référence/version du produit*

## Version 1.0

*Conformité à un profil de protection*

**Machine Readable Travel Document with „ICAO Application", Extended Access Control (EAC)**

**Version 1.10, BSI-PP-0056**

*Critères d'évaluation et version*

## Critères Communs version 3.1 révision 4

*Niveau d'évaluation*

## EAL 5 augmenté

**ALC_DVS.2, AVA_VAN.5**

*Développeurs*

**Gemalto**

**6 rue de la verrerie,**
**92197 Meudon, France**

**Infineon Technologies AG**

**AIM CC SM PS – Am Campeon 1-12,**
**85579 Neubiberg, Allemagne**

*Commanditaire*

**Gemalto**

**6 rue de la verrerie, 92197 Meudon, France**

*Centre d'évaluation*

**Serma technologies**

**14 rue Galilée, CS – 10055, 33615 PESSAC Cedex, France**

*Accords de reconnaissance applicables*

**CCRA**

**SOG-IS**

**Le produit est reconnu au niveau EAL4.**

# 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 carte à puce fermée « eTravel Essential 1.0, avec BAC, AA et EAC activés, sur composant M7794 A12/G12 ». Le produit est développé par la société *GEMALTO* et embarqué sur le microcontrôleur M7794 A12/G12 de la société *INFINEON TECHNOLOGIES*.

Le produit évalué est de type « carte à puce » avec et sans contact. Il implémente les fonctions de document de voyage électronique conformément aux spécifications de l'organisation de l'aviation civile internationale (OACI[1]). Ce produit est destiné à permettre la vérification de l'authenticité du document de voyage et à identifier son porteur lors d'un contrôle frontalier, à l'aide d'un système d'inspection.

Ce microcontrôleur et son logiciel embarqué ont vocation à être insérés dans la couverture des passeports traditionnels. Ils peuvent être livrés sous forme de module, d'*inlay*, de couverture de passeport ou de passeport. Le produit final peut également être au format carte plastique.

## 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.

Cette cible de sécurité est conforme au profil de protection [PP0056V1]. Il s'agit d'une conformité stricte.

### *1.2.2. Identification du produit*

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

La procédure d'identification est décrite dans [GUIDES]. Le tableau suivant fournit les commandes et réponses permettant d'identifier le produit.

| Commande produit | Réponse | Description |
|---|---|---|
| GET DATA « 0x9F7F » | 40 90 | Identification du fabricant |
| | 77 50 | Identifiant du microcontrôleur |
| | B2 8C 01 | Identification du logiciel embarqué |
| | 01 02 | Identification du logiciel embarqué |

[1] Encore appelé ICAO pour *International Civil Aviation Organization*.

### *1.2.3. Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :

- la protection en intégrité des données du porteur stockées dans la carte : nations ou organisations émettrices, numéro du document de voyage, date d'expiration, nom du porteur, nationalité, date de naissance, sexe, portrait, autres données optionnelles, données biométriques additionnelles et autres données permettant de gérer la sécurité du document de voyage ;
- le contrôle d'accès aux données du porteur stockées dans la carte ;
- l'authentification du microcontrôleur par le mécanisme optionnel AA (*Active Authentication)* ;
- la protection, en intégrité et en confidentialité, à l'aide du mécanisme de *Secure Messaging*, des données lues ;
- l'authentification forte (avec validation de la chaine de certificats) entre le microcontrôleur et le système d'inspection par le mécanisme EAC (*Extended Access Control*) préalablement à tout accès aux données biométriques.

### *1.2.4. Architecture*

Le produit est constitué de :

- d'un microcontrôleur *INFINEON* M7794 A12/G12 (par exemple en configuration SLE77CLFX2400P) et du logiciel *Firmware* fournis par *INFINEON* ;
- du logiciel embarqué 'eTravel Essential v1.0 O.S' développé par *GEMALTO* et comprenant :
    - un niveau 'plateforme native' implémentant les services de bas-niveau, communs à plusieurs produits *GEMALTO* ;
    - un niveau 'applications' impléme ntant les fonctionnalités *MRTD*[1] dédiées à ce produit et stockant les données associées.

### *1.2.5. Cycle de vie*

Le cycle de vie du produit est décrit au premier chapitre de la cible de sécurité [ST].

Trois types de cycle de vie sont envisagés pour le produit dans le périmètre de l'évaluation :

- Le cycle de vie 1 est le cas standard. Il correspond au cas où le composant est livré par le fabricant de composants dans un site *GEMALTO* pour initialisation et pré-personnalisation. Les composants sont ensuite livrés au client directement ou après avoir été mis sous *inlays ;*
- Le cycle de vie 2 est une 1ère alternative qui correspond au cas où *GEMALTO* reçoit les composants au format *inlays* pour initialisation et personnalisation. Pour cela, le *INFINEON* a préalablement transmis les modules au fabricant d'*inlays ;*
- Le cycle de vie 3 est une 2nde alternative qui correspond au cas où le client souhaite recevoir des composants directement à *INFINEON*. Dans ce cas les opérations d'initialisation et de pré-personnalisation sont effectuées par *INFINEON*.

Les sites de développement et de production du microcontrôleur sont identifiés dans le rapport de certification [CERT_IC].

[1] *Machine Readable Travel Document.*

La cible d'évaluation *(TOE)* est également développée ou produite sur les sites suivants :

***GEMALTO***
6 Rue de la Verrerie
92190 Meudon
France

***GEMALTO***
12 Ayer Rajah Crescent
Singapor 139941
Singapour

***GEMALTO***
Avenue du Pic de Bertagne
13881 Gémenos
France

***GEMALTO***
Avenue du Jujubier
13705 La Ciotat Cedex
France

***GEMALTO***
Myllynkivenkuja 4
FI-01620 Vantaa
Finlande

***GEMALTO***
Ul. Skarszewska 2
33-110 Tczew
Pologne

### *1.2.6. Configuration évaluée*

Le certificat porte sur la configuration, après personnalisation par l'émetteur, qui inclut les mécanismes suivants :

- *Basic Access Control;*
- *Active Authentication;*
- *Extended Access Control.*

# 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].

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 du logiciel dans le microcontrôleur déjà certifié par ailleurs.

Le microcontrôleur M7794 A12/G12 a été certifié au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5, conformément au profil de protection [PP0035], le 3 février 2014 sous la référence BSI-DSZ-CC-0917-2014. Ce microcontrôleur a été maintenu sous la référence BSI-DSZ-CC-0917-2014-MA-01 le 12 juin 2014.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 24 juin 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 a été réalisée conformément au référentiel technique de l'ANSSI [REF]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Les mécanismes analysés sont conformes aux exigences des référentiels cryptographiques de l'ANSSI sous réserve de prendre en compte les recommandations se trouvant dans les guides (voir [GUIDES]), dont certaines sont rappelées ici :

- Le bit plus significatif de chaque nombre premier p et n utilisé pour la génération de clé doit être fixé à 1 ;
- L'algorithme de hachage doit être choisi en relation avec la taille de clés des courbes elliptiques ou de l'algorithme RSA si applicable. Par exemple, l'utilisation du SHA-256 avec des clés ECC de 256 bits ;

- L'algorithme Diffie-Hellman d'échange de clés et de vérification de signature doit utiliser des clés de longueurs égales à 2048 bits. L'ordre d'un sous-groupe doit être multiple d'un nombre premier d'au moins 200 bits et la conformité des paramètres de domaine avec la RFC 2785 doit être utilisée ;
- Dans le cas des courbes elliptiques, pour une utilisation ne devant pas dépasser 2020, on emploiera des sous-groupes dont l'ordre est multiple d'un nombre premier d'au moins 200 bits (256 bits au-delà de 2020) ;
- L'algorithme TDES (Triple DES) 2 clés est utilisable au plus tard jusqu'en 2015.
- Dans le cas de l'utilisation de l'algorithme TDES, la même clé ne peut être utilisée pour chiffrer plus de $2^{27}$ blocks.

Dans le cadre du processus de qualification renforcée, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI. Ces 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.

## 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 [CERT_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 « eTravel Essential 1.0, avec BAC, AA et EAC activés, sur composant M7794 A12/G12 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 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], notamment d'utiliser, lors de la personnalisation, les valeurs 'Security Attributes' indiquées afin que les conditions d'accès soient celles recherchées pour une configuration mettant en œuvre les fonctionnalités BAC, AA (optionnel) et EAC.

Reconnaissance du certificat

### *3.2.1. 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 puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

### *3.2.2. 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 EAL4 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, Singapour, 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 5+ | 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** | **5** | Complete semi-formal functional specification with additional error information |
| | ADV_IMP | | | | **1** | 1 | **2** | 2 | **1** | Implementation representation of the TSF |
| | ADV_INT | | | | | **2** | **3** | 3 | **2** | Well-structured internals |
| | ADV_SPM | | | | | | **1** | 1 | | |
| | ADV_TDS | | **1** | **2** | **3** | **4** | **5** | **6** | **4** | Semiformal 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 | **5** | Development tools 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 | **2** | Compliance with implementation standards |
| 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** | **3** | Testing: modular 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 :<br>– eTravel Essential 1.0 EAC on BAC Security Target, D1315456 version 1.2, 26 février 2015, Gemalto.<br><br>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :<br>– Security target Lite eTravel Essential 1.0 EAC on BAC, version 1.2p, référence D1315456, février 2015, Gemalto. |
| [RTE] | Rapport technique d'évaluation :<br>Evaluation Technical Report : ERODIUM Project , référence ERODIUM-FULL-PP56V1_ETR_v1.0/1.0, 24 juin 2015, Serma Technologies. |
| [CERT_IC] | Infineon Technologies Security Controller M7794 A12 and G12 with optional RSA2048/4096 v1.02.013 or v2.00.002, EC v1.02.013 or v2.00.002 and Toolbox v1.02.013 or v2.00.002 libraries and with specific IC-dedicated software.<br>*Certifié par le BSI le 3 février 2014 sous la référence BSI-DSZ-CC-0917-2014, et maintenu le 12 juin 2014 sous la référence BSI-DSZ-CC-0917-2014-MA-01.* |
| [ANA-CRY] | Cryptographic Mechanisms Evaluation Report: ERODIUM Project, ERODIUM_MRTD_cryptography_v1.0/1.0, 6 février 2015, Serma Technologies. |
| [CONF] | Liste de configuration du produit :<br>eTravelEssential10, référence D1388129-LIS-DOC eTravelEssential10, version 1.2, 31 août 2015, Gemalto. |
| [GUIDES] | – eTravel Essential 1.0 AGD_PRE document, référence D1330275, version 1.0, 23 mai 2014, Gemalto ;<br>– eTravel Essential 1.0 Operational User Guide, reference D1330276, version 1.0, 23 mai 2014, Gemalto ;<br>– eTravel Essential 1.0 Reference Manual, reference D1325786, 25 février 2015, Gemalto. |
| [PP0035] | Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.* |
| [PP0056V1] | Protection Profile - Machine Readable Travel Document with "ICAO Application", Extended Access Control, BSI, version 1.10, 25 mars 2009 BSI-PP-0056. |

# 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 :<br>Part 1: Introduction and general model,<br>September 2012, version 3.1, revision 4, ref CCMB-2012-09-001;<br>Part 2: Security functional components,<br>September 2012, version 3.1, revision 4, ref CCMB-2012-09-002;<br>Part 3: Security assurance components,<br>September 2012, version 3.1, revision 4, ref CCMB-2012-09-003. |
| [CEM] | Common Methodology for Information Technology Security Evaluation : Evaluation Methodology,<br>September 2012, version 3.1, révision 4, ref CCMB-2012-09-004. |
| [JIWG IC] * | Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, February 2009. |
| [JIWG AP] * | Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, January 2013. |
| [COMP] * | Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.2, January 2012. |
| [CC RA] | Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, July 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.