



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-CSPN-2011/06

Middleware IAS ECC
Version 2.08 pour MacOS

Paris, le 30 mai 2011

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

Patrick Pailloux
[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 présumées 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

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification	ANSSI-CSPN-2011/06
Nom du produit	Middleware IAS ECC
Référence/version du produit	Version 2.0 révision 8 pour MacOS
Critères d'évaluation et version	CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN, Phase expérimentale)
Développeur(s)	Gemalto S.A. Avenue du Pic de Bertagne BP100 13881 Gémenos Cedex France Dictao S.A. 152, avenue de Malakoff 75116 Paris France
Commanditaire	Agence Nationale des Titres Sécurisés 5 rue de l'Eglise 08000 Charleville-Mézières France
Centre d'évaluation	Thales Security Systems and Services SAS 18, avenue Edouard Belin BPI 1414 31401 Toulouse Cedex 9 Tél : 562882801, mél : nathalie.feyt@thalesgroup.com

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	6
1.1. PRESENTATION DU PRODUIT	6
1.2. DESCRIPTION DU PRODUIT EVALUE	7
1.2.1. <i>Catégorie du produit</i>	7
1.2.2. <i>Identification du produit</i>	7
1.2.3. <i>Services de sécurité</i>	7
1.2.4. <i>Configuration évaluée</i>	8
2. L’EVALUATION	9
2.1. REFERENTIELS D’EVALUATION	9
2.2. CHARGE DE TRAVAIL PREVUE ET DUREE DE L’EVALUATION	9
2.3. TRAVAUX D’EVALUATION	9
2.3.1. <i>Fonctionnalités, environnement d’utilisation et de sécurité</i>	9
2.3.1.1. Spécification de besoin du produit	9
2.3.1.2. Biens sensibles manipulés par le produit	9
2.3.1.3. Description des menaces contre lesquelles le produit apporte une protection	9
2.3.1.4. Fonctions de sécurité	9
2.3.1.5. Utilisateurs typiques	9
2.3.2. <i>Installation du produit</i>	10
2.3.2.1. Plate-forme de test	10
2.3.2.2. Particularités de paramétrage de l’environnement	10
2.3.2.3. Options d’installation retenues pour le produit	10
2.3.2.4. Description de l’installation et des non-conformités éventuelles	10
2.3.2.5. Durée de l’installation	10
2.3.2.6. Notes et remarques diverses	10
2.3.3. <i>Analyse de la documentation</i>	10
2.3.4. <i>Revue du code source (facultative)</i>	10
2.3.5. <i>Fonctionnalités testées</i>	11
2.3.6. <i>Fonctionnalités non testées</i>	11
2.3.7. <i>Synthèses des fonctionnalités testées / non testées et des non -conformités</i>	11
2.3.8. <i>Avis d’expert sur le produit</i>	11
2.3.9. <i>Analyse de la résistance des mécanismes et des fonctions</i>	12
2.3.9.1. Liste des fonctions et des mécanismes testés - résistance	12
2.3.9.2. Avis d’expert sur la résistance des mécanismes	12
2.3.10. <i>Analyse des vulnérabilités (conception, construction...)</i>	12
2.3.10.1. Liste des vulnérabilités connues	12
2.3.10.2. Liste des vulnérabilités découvertes lors de l’évaluation et avis d’expert	12
2.3.11. <i>Accès aux développeurs</i>	12
2.3.12. <i>Analyse de la facilité d’emploi et préconisations</i>	13
2.3.12.1. Cas où la sécurité est remise en cause	13
2.3.12.2. Recommandations pour une utilisation sûre du produit	13
2.3.12.3. Avis d’expert sur la facilité d’emploi	13
2.3.12.4. Notes et remarques diverses	13
2.4. ANALYSE DE LA RESISTANCE DES MECANISMES CRYPTOGRAPHIQUES	14
2.5. ANALYSE DU GENERATEUR D’ALEAS	14
3. LA CERTIFICATION	15
3.1. CONCLUSION	15
3.2. RESTRICTIONS D’USAGE	15

1. Le produit

1.1. Présentation du produit

Le produit évalué est « Middleware IAS ECC, version 2.0 révision 8 pour MacOS » (ci-après, *Middleware IAS-ECC*, IAS-ECC étant les acronymes pour Identification, Authentification, Signature – *European Card Citizen*) développé par les sociétés DICTAO et GEMALTO.

Il s'agit d'un *package* logiciel composé :

- du *middleware IAS-ECC*, logiciel d'interface, aussi appelé API (*Application Programming Interface*), qui permet à des applications d'accéder aux services cryptographiques et aux différentes fonctionnalités d'une carte à puce de type IAS (conforme à [GIXEL]) ;
- des outils connexes, directement utilisables par les utilisateurs finaux utilisant l'API *middleware IAS-ECC*, permettant aux utilisateurs de :
 - changer leur code personnel (PIN) si le profil le permet ;
 - lire le contenu de sa carte ;
 - diagnostiquer la bonne installation et le bon fonctionnement du *middleware IAS-ECC* en générant un rapport technique d'installation et d'analyse du fonctionnement.

Le *middleware IAS-ECC* implémente les normes **PKCS11** [PKCS] et **TokenD** pour le traitement des demandes de services cryptographiques de la part du logiciel. Il offre en plus une bibliothèque spécifique « **IAS-API** » [IAS-API] qui permet d'effectuer via un « *secure messaging* » des opérations d'accès en lecture à la structure de la carte, d'administration du contenu de la carte, et de signature qualifiée.

1.2. Description du produit évalué

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

1.2.1. Catégorie du produit

<input type="checkbox"/>	1 - détection d'intrusions
<input type="checkbox"/>	2 - anti-virus, protection contre les codes malicieux
<input type="checkbox"/>	3 - firewall
<input type="checkbox"/>	4 - effacement de données
<input type="checkbox"/>	5 - administration et supervision de la sécurité
<input checked="" type="checkbox"/>	6 - identification, authentification et contrôle d'accès
<input type="checkbox"/>	7 - communication sécurisée
<input type="checkbox"/>	8 - messagerie sécurisée
<input type="checkbox"/>	9 - stockage sécurisé
<input type="checkbox"/>	10 - matériel et logiciel embarqué
<input type="checkbox"/>	99- Autres

1.2.2. Identification du produit

La version du produit est précisée à la première ligne du fichier « ReadMe_Fr.txt » présent au niveau du dossier racine de l'installation (Applications/IAS ECC Middleware).

Afin d'assurer l'intégrité du package d'installation (cf. §2.3.12.2), il est recommandé de vérifier que le haché du package d'installation correspond à celui présent dans le guide d'installation [GUIDES].

Voici les valeurs contenues dans le guide d'installation pour MAC :

- le sha256 calculé sur le fichier IAS_ECC_Middleware_Leopard.zip est :
85ddaa8e0f1b673160904977af8db84bd8eb31c23e9506dadec2f82d0e34b93f
- le sha256 calculé sur le fichier IAS_ECC_Middleware_SnowLeopard.zip est :
d440b9fb0da67a9b632e9059f7f6a78f5f4d351546920eb8d0dd5bec0cb7af2f

1.2.3. Services de sécurité

Les fonctions de sécurité concernent la protection du PIN (code PIN global d'authentification et code PIN pour la signature qualifiée). Il s'agit des fonctions suivantes :

1. Protection du PIN en mémoire lors de sa saisie via l'interface propre du *middleware*.
2. Protection du PIN en mémoire lors de son traitement par le *middleware* et sa transmission au lecteur de carte à puce.
3. Protection du PIN en mémoire lors de sa saisie via l'outil de management de code secret.
4. Protection du PIN en mémoire lors de la lecture des informations sur la carte à puce IAS.

On distingue trois cas de figure en fonction du mode de saisie du PIN.

Le PIN est saisi par un *PINpad* (clavier de saisie du PIN) associé à un lecteur de carte : la saisie est donc garantie par le matériel lecteur de la carte.

Le PIN est saisi via un logiciel utilisateur : la saisie doit être garantie par le logiciel utilisateur. Le logiciel transmet le PIN à l'interface PKCS11 du *middleware* IAS-ECC (ou à l'interface TokenD pour les applications spécifiques de MacOS (Safari)). C'est typiquement le cas lors de la saisie du PIN global d'authentification d'une carte. Le *middleware* n'est alors responsable de la protection du PIN que lors de son traitement et de sa transmission au matériel lecteur de carte à puce.

Le PIN est saisi via le *middleware* IAS-ECC lui-même : la saisie est alors effectuée grâce aux fonctions spécifiques du *middleware*. Dans ce cas, le *middleware* est responsable de la confidentialité et de l'intégrité du PIN lors de sa saisie, de son traitement et jusqu'au moment de sa transmission au logiciel de contrôle du lecteur de la carte à puce.

1.2.4. ***Configuration évaluée***

Sans objet.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de Sécurité de Premier Niveau en phase expérimentale. Les références des documents se trouvent en annexe 2.

2.2. Charge de travail prévue et durée de l'évaluation

La charge de travail totale a été de 18 h.j au lieu des 25 h.j normalement prévu car l'évaluateur a pu s'appuyer sur les résultats des évaluations des versions Windows [CSPN-2010/02] et Linux [CSPN-2010/04].

2.3. Travaux d'évaluation

Ce paragraphe apporte des précisions sur la cible de sécurité [CDS] fournie en entrée de l'évaluation. Ces précisions sont issues du [RTE] élaboré par l'évaluateur suite à ses travaux.

2.3.1. *Fonctionnalités, environnement d'utilisation et de sécurité*

2.3.1.1. **Spécification de besoin du produit**

Conforme à la cible de sécurité [CDS] (chapitre « Argumentaire (description) du produit »).

2.3.1.2. **Biens sensibles manipulés par le produit**

Conformes à la cible de sécurité [CDS] (chapitre « Description des biens sensibles que le produit doit protéger »).

2.3.1.3. **Description des menaces contre lesquelles le produit apporte une protection**

Conforme à la cible de sécurité [CDS] (Chapitre « Description des menaces »).

2.3.1.4. **Fonctions de sécurité**

Conformes à la cible de sécurité [CDS] (chapitre « Description des fonction de sécurité du produit »).

2.3.1.5. **Utilisateurs typiques**

Conformes à la cible de sécurité [CDS] (chapitre « Description des utilisateurs typiques »).

2.3.2. *Installation du produit*

2.3.2.1. **Plate-forme de test**

Deux Mac ont été utilisés pour faire ces tests, l'un sous l'OS *Leopard* (10.5.8) et l'autre sous *Snow Leopard* (10.6.3) :

- Mac OS X 10.6.3
2.4Ghz Intel Core 2 Duo
2Go de DDR3 (1067MHz)
- Mac OS X 10.5.8
1.83Ghz Intel Core 2 Duo
2Go de DDR2 (667MHz)

Les tests de conformité et de pénétration pouvant avoir un lien avec le système d'exploitation ont été rejoués sur les deux configurations. Les résultats obtenus ont toujours été identiques.

2.3.2.2. **Particularités de paramétrage de l'environnement**

Il faut disposer des droits d'administrateur pour installer le middleware.

Le fonctionnement de celui-ci requiert aussi que le système implémente :

- une interface PC/SC (*Personal Computer/Smart Card*) opérationnelle ;
- un lecteur de cartes à puce correctement installé dans l'environnement PC/SC ;
- une carte à puce IAS émise dans un format compatible avec le *middleware* (Profil « Générique Gemalto » ou profil « CNIe v0.11.1 » (Carte Nationale d'Identité électronique)).

2.3.2.3. **Options d'installation retenues pour le produit**

Aucune option d'installation n'est disponible.

2.3.2.4. **Description de l'installation et des non-conformités éventuelles**

L'installation ajoute une bibliothèque dynamique dans le dossier « /usr/lib », cinq bibliothèques dynamiques dans le dossier « /usr/lib/ClassicClient », ainsi que trois applications connexes aux applications Mac OS X dans le dossier « IAS ECC *Middleware* ».

2.3.2.5. **Durée de l'installation**

L'installation du package se déroule au travers d'une interface conviviale en quelques secondes.

2.3.2.6. **Notes et remarques diverses**

L'installation est simple et ne requiert aucune configuration de la part de l'utilisateur.

2.3.3. *Analyse de la documentation*

L'évaluateur a eu accès à la documentation technique du produit [GUIDES]. La documentation est claire et aucune non-conformité n'a été relevée.

2.3.4. *Revue du code source (facultative)*

Les évaluateurs n'ont pas eu accès au code source.

2.3.5. *Fonctionnalités testées*

Fonctionnalité	Profil de la carte	Résultat
Saisie du code secret et connexion à la carte à puce par l'intermédiaire de Firefox.	Générique Gemalto	Réussite
Saisie du code secret et connexion à la carte à puce par l'intermédiaire du trousseau d'accès (TokenD).	Générique Gemalto	Réussite
Saisie du code secret et connexion à la carte à puce par l'intermédiaire de l'application IAS_Diag.	Générique Gemalto	Réussite (Voir le 1 du §2.3.7)
Interface du middleware avec un PINPad	Tous	Réussite partielle (Voir le 2 du §2.3.7)
Accès aux fichiers grâce au trousseau d'accès (TokenD).	Tous	Réussite
Accès aux certificats via Firefox	Tous	Réussite
Utilisation des bibliothèques tierces	-	Réussite

2.3.6. *Fonctionnalités non testées*

Sans objet.

2.3.7. *Synthèses des fonctionnalités testées / non testées et des non -conformités*

1 - L'applicatif ne précise pas le nombre d'essais effectués ou restants ni l'état de la carte (bloquée ou non).

2 - L'utilisation d'un PINPad permet d'utiliser l'application de changement de code et l'application de diagnostic pour saisir le PIN de signature. Il n'est en revanche pas possible d'utiliser le PINPad sous Firefox ou Safari pour saisir le PIN global dans l'application de diagnostic. Enfin, il n'est pas possible de retaper un code PIN sur certains modèles de PINPad si le premier était erroné.

2.3.8. *Avis d'expert sur le produit*

Le produit est conforme à ses spécifications.

2.3.9. *Analyse de la résistance des mécanismes et des fonctions*

2.3.9.1. **Liste des fonctions et des mécanismes testés - résistance**

L'avis sur la résistance des mécanismes est donné au §2.3.9.3.

Fonction et mécanisme
Test de l'outil de diagnostique du <i>middleware</i> IAS
Test de l'outil de consultation du contenu des cartes du <i>middleware</i> IAS
Test de l'outil de changement du code secret du <i>middleware</i> IAS
Protection du code PIN en mémoire
Protection du code PIN global en mémoire cache
Effacement du code PIN en mémoire
Effacement du code PIN global en mémoire cache

2.3.9.2. **Avis d'expert sur la résistance des mécanismes**

Hors utilisation (utilisateur non authentifié), le *middleware* IAS-ECC ne compromet pas les biens sensibles qu'il est censé protéger (PIN).

En utilisation (utilisateur authentifié, *middleware* IAS-ECC en exécution), le *middleware* traite correctement les biens sensibles qu'il manipule afin d'éviter leur compromission ultérieure. On notera que les mécanismes de sécurité mis en œuvre pour atteindre ces objectifs étant tous implantés en logiciel, ils sont tous potentiellement vulnérables si les précautions d'emploi et les hypothèses d'environnement ne sont pas respectées (cf. §2.3.12.2.).

Enfin, l'évaluateur n'a pas identifié de cas où le *middleware* dégraderait la sécurité du poste de travail sur lequel il s'exécute.

2.3.10. *Analyse des vulnérabilités (conception, construction...)*

2.3.10.1. **Liste des vulnérabilités connues**

Il n'a pas été identifié de vulnérabilités connues sur ce produit particulier. Par contre, le produit peut être sensible à des vulnérabilités existantes dans les environnements sur lesquels il s'appuie (MacOS, Safari, TokenD, etc.).

2.3.10.2. **Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert**

Une vulnérabilité résiduelle a été découverte lors de l'évaluation : un attaquant qui cible le circuit d'approvisionnement du *middleware* peut remplacer le package par une version illégitime du logiciel (menace identifiée dans la cible de sécurité [CDS]).

Il est donc nécessaire de vérifier l'intégrité du package d'installation avant de l'installer (cf. §2.3.12.2.).

2.3.11. *Accès aux développeurs*

Au cours de l'évaluation, les évaluateurs ont eu accès au développeur du produit. Au cours des échanges techniques qui ont eu lieu, le développeur a fait preuve d'une très bonne maîtrise de son produit et a été en mesure de répondre rapidement et efficacement aux questions posées.

2.3.12. *Analyse de la facilité d'emploi et préconisations*

2.3.12.1. **Cas où la sécurité est remise en cause**

Néant.

2.3.12.2. **Recommandations pour une utilisation sûre du produit**

Intégrité du package d'installation

L'administrateur doit vérifier l'intégrité du package d'installation avant d'installer le *middleware*. Les hachés sha256 des packages sont disponibles dans le guide d'installation [GUIDES] et dans le paragraphe 1.2.2 du présent document.

Recommandations pour le poste

Le produit doit être utilisé sur un Mac hébergeant un système d'exploitation correctement administré et à jour de ses correctifs de sécurité. Il doit être au minimum protégé par un produit anti-virus (avec bases d'information à jour et proposant des fonctions de détection des infections informatiques furtives - *anti-spyware*, *anti-rootkit*, etc.) et par un pare-feu correctement configuré.

Le produit ne devrait pas être utilisé en cas de doute sur la sécurité du système.

Recommandations générales

L'utilisateur doit porter une attention particulière à la confidentialité du PIN de sa carte. Pour prendre une référence connue, il devrait attacher une même importance à la sécurité de sa carte IAS qu'à celle de sa carte bancaire.

En cas de perte ou de vol du support, l'utilisateur doit avertir l'opérateur du service sécurisé associé à son support afin que le certificat correspondant au support soit révoqué.

L'utilisateur doit veiller à ne pas quitter son poste en ayant une procédure de changement de mot de passe en cours.

2.3.12.3. **Avis d'expert sur la facilité d'emploi**

Le *middleware* IAS-ECC n'est pas à proprement dit un logiciel destiné à un utilisateur final. Il est d'abord destiné à fournir une interface de « haut-niveau » à des applications informatiques. Néanmoins, l'utilisateur est susceptible d'interagir directement avec le produit dans certains cas :

- lors de l'installation ;
- lors de la saisie d'un PIN ;
- lorsqu'il utilise les outils associés.

Notes et remarques diverses

Néant.

2.4. Analyse de la résistance des mécanismes cryptographiques

Sans objet.

2.5. Analyse du générateur d'aléas

Sans objet.

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.

Ce certificat atteste que le produit « Middleware IAS ECC, version 2.0 révision 8 pour MacOS » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS].

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 spécifiés dans la cible de sécurité [CDS] et suivre les recommandations énoncées dans le présent rapport.

Annexe 1. Références documentaires du produit évalué

[CDS]	<i>Cible de sécurité CSPN - Middleware IAS-ECC V2.0 pour environnement MAC OS ; Date : 07/10/2010</i>
[RTE]	<i>Rapport d'évaluation CSPN, Projet : CSPN_IAS ; Référence : CIS_CSPN ; Date : 13/12/2010</i>
[GUIDES]	<u>Guide d'installation</u> : <i>MW IAS ECC - Guide d'installation MAC ; Référence : MW IAS ECC ; Date : 26/11/2010</i> <u>Guide d'administration</u> : <i>MW IAS ECC Setup ; Référence : MW IAS ECC Setup ; Date : 08/11/2010</i>
[CONF]	<i>MW IAS CardBrowser - Spécifications fonctionnelles ; Référence : MW IAS Card Browser ; Date : 27/07/2010</i>
[GIXEL]	<i>European Card for e-Services and National e-ID applications - Technical Specifications; IAS ECC, Revision: 1.01 [http://www.gixel.fr/accesCAT.asp?cat_id=44]</i>
[PKCS]	<i>Additional PKCS#11 Mechanisms; PKCS #11 v2.01 Cryptographic Token Interface Standard; PKCS #11 v2.01</i>
[IAS-API]	<i>Middleware IAS - PKCS#11 - Crypto API - Guide de programmation</i>
[CSPN-2010/02]	<i>Rapport de certification ANSSI-CSPN-2010/02 – Middleware IAS-ECC V.2.0.12 pour Windows Date : 07/05/2010 [http://www.ssi.gouv.fr/site_rubrique54_certificat_cspn_2010_02.html]</i>
[CSPN-2010/04]	<i>Rapport de certification ANSSI-CSPN-2010/04 – Middleware IAS-ECC V.2.0 pour Linux Date : 22/10/2010 [http://www.ssi.gouv.fr/site_rubrique54_certificat_cspn_2010_04.html]</i>

Annexe 2. Références 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.

[CSPN]

Certification de sécurité de premier niveau (CSPN) des technologies de l'information, version 2. 4, phase expérimentale, n° 915/SGDN/DCSSI/SDR/CCN du 25 avril 2008.

Critères pour l'évaluation de sécurité de premier niveau des technologies de l'information, phase expérimentale, version 1. 4.

Méthodologie d'évaluation en vue de la CSPN et contenu attendu du RTE, phase expérimentale, version 1. 3.

Documents disponibles sur www.ssi.gouv.fr