**Dossier d’évaluation en vue d’une   
certification Critères communs**

***Application form   
for a Common criteria evaluation***

Rappel

*Reminder*

Extrait du Décret 2002-535 modifié :

*Courtesy translation of an Extract of modified Decree 2002-535*

Art. 2. - Une évaluation en vue de la certification prévue à l'article 1er est effectuée à la demande d'un commanditaire qui adresse à l’Agence nationale de la sécurité des systèmes d'information un dossier d'évaluation. Le dossier comporte notamment la description du système de sécurité à évaluer, les dispositions prévues pour lui conférer sa pleine efficacité ainsi que le programme de travail prévisionnel permettant une évaluation.

Dès réception de ce dossier, l’Agence nationale de la sécurité des systèmes d'information si elle estime que les objectifs de sécurité ne sont pas définis de manière pertinente au regard des normes, prescriptions techniques ou règles de bonne pratique applicables au moment où commence l'évaluation, notifie au commanditaire qu'elle ne pourra pas en l'état du dossier procéder à la certification envisagée.

*Art. 2. - An evaluation in the goal of a certification as defined in article 1 is performed at the request of a sponsor who sends to ANSSI (Agence nationale de la sécurité des systèmes d’information) an application form. The form comprises a description of the security system to be evaluated, the measures taken to achieve its full efficiency, and the provisional evaluation work plan.*

*Upon reception of the application form, if it is considered that the security objectives are not commensurate with respect to the standards, technical requirements or rules of good practice at the time of the beginning of the evaluation, ANSSI notifies the sponsor that the expected certification cannot be carried out in compliance with the present application form.*

Le présent dossier est destiné à permettre l’enregistrement d’un projet d’évaluation et de certification selon le référentiel Critères communs par l’Agence nationale de la sécurité des systèmes d'information.

*This file is intended to allow the registration of an evaluation and certification project according to the Common criteria standard by ANSSI.*

Il doit être renseigné et adressé :

*It has to be fulfilled and sent:*

* Par courriel (pour un pré-enregistrement), à [certification@ssi.gouv.fr](mailto:certification.anssi@ssi.gouv.fr) en indiquant dans l’objet du message [Nouvelle demande d’évaluation] (le scan signé de cette demande, et la ou les cibles de sécurité doivent être joints au courriel)

*By e-mail (for a pre-registration), to* [certification@ssi.gouv.fr](mailto:certification@ssi.gouv.fr%0d) *with* [Nouvelle demande d’évaluation] *in the e-mail subject field (the scanned version of this current application form signed and the Security Target as attachments of this e-mail).*

**Et / *And***

* Par courrier postal, à :

*To be sent to :*

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 07 SP

France

**L’enregistrement de la demande sera effectif lorsque l’intégralité des documents demandés sera parvenue notamment la demande originale signée par les deux parties.**

***The registration of the request will be validated upon reception by ANSSI of the signed paper version by both parties and all the requested documents.***

Conditions générales de la certification

*General conditions for 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.

*Decree 2002-535 of April 18, 2002 modified, about the evaluation and certification of the security provided by products and systems of information technologies.*

* Portée du certificat / *Scope of certificate*

Le certificat atteste que l'exemplaire du produit, du système, du profil de protection ou du site considéré[[1]](#footnote-2) soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées. Il atteste également que l'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises. Il n’a pas valeur de recommandation de l’objet évalué.

Un certificat de produit ne garantit pas que le produit certifié soit totalement exempt de vulnérabilité exploitable. En effet, il existe toujours une probabilité résiduelle que des vulnérabilités exploitables n’aient pas été découvertes. Cette probabilité est cependant d’autant plus faible que le niveau d’évaluation est élevé.

L’attribution d’un certificat ne permet à elle seule en aucune façon au fabricant ou au vendeur du produit ou à l’exploitant du site de dégager sa responsabilité légale en cas de dommages résultant de l’utilisation de l’objet concerné.

Par ailleurs, la sécurité offerte par un objet certifié n’est valable que dans le cas d’une utilisation de l’objet considéré conforme aux recommandations figurant dans le rapport de certification.

*The certificate testifies that the product, the system, the protection profile or the site considered[[2]](#footnote-3) submitted to evaluation fulfils the specified security characteristics. It also testifies that the evaluation has been performed in compliance to the current rules and standards, and with the required competence and impartiality. This is not a recommendation for the use of the target of evaluation.*

*A product certificate does not guarantee that the certified product is totally free of any exploitable vulnerability. Indeed, there is always a residual probability that exploitable vulnerabilities have not been discovered. This probability is however as low as the evaluation assurance level is high.*

*The awarding of the certificate does not free in any way the manufacturer or the seller of a product or the site manager from its legal responsibility in case of damage resulting from use of the target.*

*In addition, the security provided by the certified target is valid only in the case of a usage in compliance with the recommendations stated in the certification report.*

* Droits et obligations des commanditaires et des développeurs / *Sponsors and developers’ rights and obligations*

Les commanditaires et les développeurs doivent se conformer aux dispositions du 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. Ils doivent se conformer également aux dispositions de la politique de certification, aux règles et normes définies par l’ANSSI pour les procédures d'évaluation et de certification et aux guides techniques mis à la disposition du public (disponible soit sur le site institutionnel de l’ANSSI, [www.ssi.gouv*.fr*](http://www.ssi.gouv.fr)*,* soit sur demande au centre de certification).

Les commanditaires doivent prendre toutes les dispositions nécessaires en vue de la conduite de l’évaluation, à savoir :

* choisir et définir l’objet à évaluer ;
* définir des objectifs de sécurité de l’objet à évaluer (cible de sécurité) ;
* fournir à l’ANSSI le dossier d'évaluation ;
* mettre à disposition les fournitures requises pour l’évaluation ;
* autoriser la participation d’observateurs de l’ANSSI externes au centre de certification soumis aux mêmes contraintes de confidentialité et d’impartialité que les membres du centre ;
* transmettre au centre d’évaluation et à l’ANSSI des informations réputées fiables et qui ne risqueraient pas de fausser leur jugement ;
* permettre à l’ANSSI l’accès aux sites du cycle de vie du produit évalué ;
* permettre à l’ANSSI l’accès aux zones de production durant l’audit de site ;
* permettre la rencontre des personnes souhaitées par l’ANSSI durant l’audit de site ;
* effectuer les démarches nécessaires pour permettre à l’ANSSI de rencontrer les éventuels sous-traitants ;
* effectuer les démarches nécessaires pour permettre aux auditeurs habilités du COFRAC :
  + de rencontrer le personnel impliqué dans la fabrication du produit ;
  + d’accéder aux zones de production.

Si l’évaluation du produit nécessite l’accès à des documents payants (comme par exemple un profil de protection ou une norme), le commanditaire s’engage à les fournir au centre de certification à sa demande. Les éventuels coûts associés à cette mise à disposition sont à la charge du commanditaire.

**Au cours de l’évaluation, si une vulnérabilité est découverte susceptible d’impacter une ou des versions déjà déployées, il est de la responsabilité des commanditaires ou des développeurs d’informer ses utilisateurs.**

Les commanditaires et les développeurs ne peuvent annoncer qu’un objet est certifié que sur la base d’un certificat valide, c’est-à-dire :

* ne pas déclarer que l’objet est certifié alors qu’il est en cours d'évaluation ;
* déclarer que l’objet est certifié uniquement pour le périmètre de la certification octroyée ;
* cesser immédiatement d’utiliser tout matériel publicitaire faisant état de la certification en cas de suspension ou de retrait de la certification.

Toute communication relative au certificat doit préciser les caractéristiques de sécurité auxquelles l’objet a été certifié conforme.

Une fois la certification prononcée, les commanditaires et développeurs doivent :

* s’assurer que les produits fabriqués en série et vendus en lien avec le certificat délivré sont strictement identiques au produit qui a fait l’objet de la certification. A cet égard, des exemplaires de produits fabriqués répondant au certificat délivré devront être fournis à l’ANSSI sur simple demande ;
* utiliser le certificat de manière non frauduleuse, non erronée et non abusive ;
* utiliser le certificat sans nuire à l’ANSSI ;
* se conformer aux exigences de la certification pour faire de la publicité, éditer des brochures et des documents ;
* respecter scrupuleusement les règles d’usage des marques associées à la certification ;
* prendre toutes les dispositions nécessaires pour instruire les réclamations, relatives aux produits certifiés, exprimées par ses clients ;
* notifier l’ANSSI sans délai des changements affectant soit le commanditaire, soit le développeur ou l’un de ses fournisseurs, soit son produit certifié qui peuvent avoir des conséquences sur le certificat ;
* respecter toutes les procédures auditées au titre des tâches ALC[[3]](#footnote-4) ;
* reproduire dans leur intégralité ou tel que spécifié par le programme de certification tout document remis à autrui concernant la certification ;
* aviser sans délai le centre de certification d’une plainte concernant la conformité de l’objet certifié aux exigences listées dans la cible de sécurité ;
* conserver les enregistrements de toutes les réclamations dont il a eu connaissance concernant la conformité aux exigences de certification et placer ces enregistrements à la disposition de l’ANSSI ;
* prendre les actions adéquates en cas de réclamation ou d’imperfection constatée dans ses produits certifiés et documenter les actions prises ;
* respecter scrupuleusement les exigences prévues en cas de suspension ou de retrait du certificat ;
* mener une veille sur les vulnérabilités qui seraient de nature à affecter la sécurité du produit ;
* signifier systématiquement et sans délai à l’ANSSI (CERT-FR[[4]](#footnote-5)), avec en copie le centre de certification, toute vulnérabilité avec son analyse d’impact associée afin de permettre leur instruction et l’établissement d’un message vers les utilisateurs des produits certifiés ;
* obtenir l’accord explicite du centre d’évaluation et du centre de certification préalablement à toute diffusion du rapport d’évaluation à un tiers.

*The sponsors and the developers must conform to the provisions of modified Decree 2002-535 of April 18th, 2002, about the evaluation and certification of the security provided by products or systems of information technologies. They must also conform to the dispositions of certification policy, to the rules and standards defined by ANSSI for the evaluation and certification procedures, and to the technical guides publicly available (See ANSSI institutional website*, [www.ssi.gouv.fr](http://www.ssi.gouv.fr) *or ask the certification body).*

*The sponsors must take all the arrangements for the evaluation, he is required to:*

* Choose and define the object to be evaluated.
* Define the security objectives of the object (Security Target of evaluation).
* Supply ANSSI with the application form.
* Provide the elements required for the evaluation.
* Transmit information to evaluation facility and ANSSI deemed reliable and that would not risk falsifying their judgment.
* Allow ANSSI access to the sites of the life cycle of the product evaluated.
* Allow ANSSI access to the production areas during the site audit.
* Allow to meeting of the staff desired by ANSSI during the site audit.
* Take the necessary steps to enable ANSSI to meet potential subcontractor.
* Allow empowered COFRAC auditors to:
  + Meet the people involved in product manufacturing.
  + Access the production area.

*Should the evaluation of the product require access to non-free documents (such as, but not limited to, a protection profile or a standard), the sponsor has to ensure all said documents are available to the certification body upon request. The eventual costs will be borne by the sponsor and therefore the documents will be made available free of charge to ANSSI.*

***Important point: during evaluation, if a vulnerability is discovered that could have an impact on one or more versions already deployed, it’s the responsibility of the sponsor or developer to inform its users.***

*The sponsors and the developers can advertise that an object is certified only based on a valid certificate, i.e. they shall:*

* Not declare an object as certified while the evaluation is still undergoing.
* Declare an object as certified only for the scope specified in the certificate.
* Stop immediately the use of any advertisement mentioning the certification in the event of suspension or withdrawal of the certification.

*Any communication on the certificate must mention the security characteristics the object has been certified compliant to.*

*Once the certificate is issued the sponsors and the developers have to:*

* Make sure that products manufactured in series and sold in link with the issued certificate are strictly identical to the one which was the object of certification. In this respect, copies of manufactured products corresponding to the certificate issued must be provided to ANSSI on request.
* Use the certificate in a non-fraudulent, non-erroneous and non-abusive manner.
* Use the certificate without harming the ANSSI.
* Comply with the requirements of the certificate to advertise, publish brochures and documents.
* Commit himself to scrupulously respecting the rule of use of trade mark logos associated to certification.
* Take all the necessary measures to address the complaint relating to the certified products, expressed by its customers.
* Notify ANSSI without delay of the changes affecting either the sponsor or the developers or one of his suppliers, or his certified product which can have consequences on the certificate.
* Respect all the audited procedures during the ALC tasks.
* Reproduce in their entirety or as specified by the certification program, any document given to others concerning the certification.
* Notify the certification body without delay of any complaint about the compliance of a certified product with the requirements listed in the security target document.
* Keep records of all claims of which it is aware concerning compliance with the certification requirements and make these recordings available to ANSSI.
* Take appropriate action in case of complaint or imperfection found in its certified products and document them.
* Comply strictly with the requirements in the event of suspension or withdrawal of the certificate.
* Monitor vulnerabilities that could affect the security of the product.
* Systematically notify without delay ANSSI (CERT-FR) with a copy to the certification body, of any vulnerability with its associated impact analysis in order to enable their instruction and the establishment of a message toward the users of the certified products.
* Obtain the explicit agreement of the evaluation laboratory and the certification centre prior to any distribution of the evaluation report to a third party.
* Droits et obligations du centre d’évaluation / *Evaluation facility ’ rights and obligations*

Le centre d’évaluation :

* s’engage à ne pas faire intervenir du personnel qui aurait, au préalable, donné des conseils en lien avec le produit objet de l’évaluation ;
* s’assure de l’indépendance et de l’impartialité de son personnel vis-à-vis des commanditaires ou des développeurs ;
* s’est assuré que les travaux objet de l’évaluation correspondent totalement à ses portées d’accréditation et d’agrément ;
* s’engage à prendre toutes les dispositions nécessaires pour permettre aux auditeurs habilités du COFRAC :
  + de rencontrer le personnel impliqué dans les évaluations de produit ;
  + d’assister à une évaluation en cours.

*The evaluation facility:*

* Is committed not to involve staff who have previously provided advice related to the product being evaluated.
* Ensures that staff involved in the project has no connection with the sponsor/ developer.
* Ensures that the evaluation work fully corresponds to its accreditation and license ranges.
* Commits itself to allow empowered COFRAC auditors to:
  + Meet the people involved in product evaluations.
  + Observe a current evaluation.
* Frais liés à la certification / *Fees for certification*

Conformément à l’article 3 du décret 2002-535 modifié, le commanditaire détermine avec le centre d'évaluation en charge de l'évaluation, avant le début des travaux, le coût et les modalités de paiement de l'évaluation.

La certification n’est pas soumise à paiement.

*In compliance to article 3 of modified Decree 2002-535, before the start of the evaluation tasks the sponsor must define with the evaluation facility the cost and rules of invoicing for the evaluation.*

*The certification is free of charge.*

* Confidentialité / *Confidentiality*

Conformément à la loi n° 83-634 du 13 juillet 1983 et au décret n°86-83 du 17 janvier 1986, les agents de l’ANSSI sont tenus au secret professionnel dans le cadre des règles instituées dans le Code pénal et notamment l’article 226-13 (La révélation d’une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d’une fonction ou d’une mission temporaire, est punie d’un an d’emprisonnement et de 15000 euros d’amende).

A ce titre, aucun accord de confidentialité (*Non Disclosure Agreement*) ne peut être invoqué par des commanditaires, des développeurs ou des centres d’évaluation pour déroger à ses engagements.

*In accordance with law n° 83-634 dated July 13th, 1983 and decree n° 86-83 dated January 17th, 1986, ANSSI agents are subject to professional secrecy within the rules established in the penal code of French law especially article 226-13. (The disclosure of an confidential information by a person entrusted to it either from his or her status or occupation, or because of his or her temporary function or mission, is punished by a year of imprisonment and a 15 000 euros fine).*

*No confidentiality agreement (Non Disclosure Agreement) can be invoked by sponsors, developers or evaluation facilities to derogate from its commitments.*

**Commanditaire de l’évaluation / *Sponsor of the evaluation***

Nom, titre et société / *Name, title and company,*

atteste avoir pris connaissance des conditions générales et demande l’enregistrement de ce dossier d’évaluation en vue de la certification de l’objet identifié.

*attests to having read the general conditions for certification and requests the registration of this evaluation form for the certification of the identified object.*

|  |  |  |  |
| --- | --- | --- | --- |
| A/*At* |  | , le*/the* |  |

**[Signature de la personne habilitée à engager la société,**

**ou du mandataire social de la société]**

***[Signature of the person authorized to commit the company   
or the Company Executive officer]***

**Centre d’évaluation en charge de l’évaluation / *Evaluation facility responsible for the evaluation***

Nom, titre et société / *Name, title and company,*

atteste avoir pris connaissance des conditions générales et demande l’enregistrement de ce dossier d’évaluation en vue de la certification de l’objet identifié.

*attests to having read the general conditions for certification and requests the registration of this evaluation form for the certification of the identified object.*

|  |  |  |  |
| --- | --- | --- | --- |
| A/*At* |  | , le*/the* |  |

**[Signature de la personne habilitée à engager la société,**

**ou du mandataire social de la société]**

***[Signature of the person authorized to commit the company   
or the Company Executive officer]***

# Portée de l’évaluation/ *Scope of the evaluation*

### Type de certification / *Type of certification*

|  |  |
| --- | --- |
| Certification de produit / *Product certification* | OUI / NON  *YES / NO* |
| Certification de profil de protection / *Protection Profile certification* | OUI / NON  *YES / NO* |
| Certification de site / *Site certification* | OUI / NON  *YES / NO* |
| Certification de composants d’assurance ALC génériques[[5]](#footnote-6)  *ALC generic components certification[[6]](#footnote-7)* | OUI / NON  *YES / NO* |

### Critères d’évaluation / *Evaluation Criteria*

|  |  |  |  |
| --- | --- | --- | --- |
| Critères d’évaluation de la sécurité informatique [ITSEC], juin 1991  + ITSEC Joint Interpretation Library version 2.0, novembre 1998  *Information Technology Security Evaluation Criteria [ITSEC], June 1991*  *+ ITSEC Joint Interpretation Library version 2.0, November 1998* | | |  |
| Common Criteria for Information Technology Security Evaluation  + interprétations finales ([*www.commoncriteriaportal.org*](http://www.commoncriteriaportal.org/))  *Common Criteria for Information Technology Security Evaluation*  *+ final interpretations (*[*www.commoncriteriaportal.org*](http://www.commoncriteriaportal.org/)*)* | Version  Révision |  |  | |
| Niveau d’évaluation visé / *Targeted evaluation level* |  | | | |

### Description de l’objet à évaluer / *Description of the object to evaluate*

|  |  |
| --- | --- |
| Nom de l’objet à évaluer  *Name of the object to be evaluated* |  |
| Référence / *Reference* |  |
| Version soumise à évaluation  *Version submitted for evaluation* |  |
| Développeur(s) / *Developer(s)* |  |
| Description succincte de l’objet à évaluer *Short description of the object to be evaluated* |  |

### Référence de la cible de sécurité / *Reference of the Security Target*

|  |  |
| --- | --- |
| Titre de la cible de sécurité  *Security Target title* |  |
| Référence / *Reference* |  |
| Version / *Version* |  |

(Joindre cette cible de sécurité au dossier / *Provide the security target with the application form*)

Si la cible de sécurité est conforme à un profil de protection / *If the Security Target is compliant with a Protection Profile*

|  |  |
| --- | --- |
| Titre du profil de protection  *Protection Profile title* |  |
| Référence / *Reference* |  |
| Version / *Version* |  |
| Le profil de protection est-il certifié ?  *Is the protection profile certified?* | OUI / NON  *YES / NO* |

### Cas d’une réévaluation / *Case of a re-evaluation*

Les travaux d’évaluation peuvent être réduits en utilisant les résultats d’un projet antérieur. Il est dans ce cas nécessaire de fournir une analyse d’impact sur les changements entre les versions (cette analyse d’impact peut être réalisée selon le modèle proposé dans le document [AC] [*Assurance Continuity: CCRA requirements*](http://www.commoncriteriaportal.org/files/supplements/2004-02-009.pdf) *chap. 5 Impact Analysis Report*).

*The evaluation tasks can be reduced in reusing previous evaluated evidences. It is necessary in this case to provide an impact analysis on the changes between product versions (this impact analysis can be established on the basis proposed in the document: [AC]* [*Assurance Continuity: CCRA requirements*](http://www.commoncriteriaportal.org/files/supplements/2004-02-009.pdf) *chap. 5 Impact Analysis Report).*

|  |  |  |  |
| --- | --- | --- | --- |
| Nom de code du projet antérieur  *Code name of previous project* |  | | |
| Référence et date du certificat  *Reference and date of the certificate* |  |  | |
| Titre de l’analyse d’impact  *Title of the impact analysis report* |  | | |
| Si l’évaluation confirme que le produit à certifier n’a pas évolué depuis la précédente certification (évolutions mineures du produit conformément aux définitions de [AC] [*Assurance Continuity: CCRA requirements*](http://www.commoncriteriaportal.org/files/supplements/2004-02-009.pdf)), indiquer si la référence du nouveau certificat doit être liée à l’ancienne (format ANSSi-CC-20xx/yy-Rn)]  *If evaluation process confirms that the product to be certified has not changed since the previous certification (minors changes of the product according to [2012-06-01]* [*Assurance Continuity: CCRA requirements*](http://www.commoncriteriaportal.org/files/supplements/2004-02-009.pdf)*]definitions), state if the reference of the new certificate should be linked to the previous one (ANSSi-CC-20xx/yy-Rn format)]* | | | OUI / NON  *YES / NO* |

### Cas d’une composition / *Case of a composition*

L’évaluation du produit, objet de la demande peut être réalisée en se basant sur les résultats de l’évaluation d’un produit sous-jacent, réalisée indépendamment. Ce mode d’évaluation, définit par la JIL et les CC ([*Composite product evaluation for Smartcards and similar devices*](http://www.sogis.eu/documents/cc/domains/sc/JIL-Composite-product-evaluation-for-Smart-Cards-and-similar-devices-v1.5.1.pdf)) pour les cartes à puce, nécessite la fourniture de certains documents. Le certificat ou la dernière analyse de vulnérabilité du produit sous-jacent doit dater de moins d’un an et demi à la date de fin de l’évaluation du produit, objet de cette demande.

*The evaluation of the product, subject of the application form, can be done by taking into account the independent evaluation results from the underlying product. This evaluation mode is defined by the JIL and CC (*[*Composite product evaluation for Smartcards and similar devices*](http://www.sogis.eu/documents/cc/domains/sc/JIL-Composite-product-evaluation-for-Smart-Cards-and-similar-devices-v1.5.1.pdf)*) for smart cards, and requires documents to be provided. The certificate or the last vulnerability assessment of the underlying product must be less than a year and a half old at the date of the end of the evaluation of the product, subject of this request.*

|  |  |
| --- | --- |
| Référence et date\* de la certification du produit sous-jacent  *Reference and date*\* *of certification of underlying product* |  |

\*ou date prévisionnelle / *or expected date*

|  |  |
| --- | --- |
| Evaluation ou expertise réalisée antérieurement par le centre d’évaluation sur ce micro-circuit  *Evaluation or expertise made previously by the evaluation facility on this integrated circuit* | OUI / NON  *YES / NO* |

### Analyse cryptographique / Cryptographic analysis

|  |  |  |  |
| --- | --- | --- | --- |
| Les fonctions de sécurité de la TOE[[7]](#footnote-8) mettent-elles en œuvre des mécanismes cryptographiques ?  *Do the TOE security functions implement cryptographic mechanisms?*  L’efficacité des mécanismes cryptographiques doit le cas échéant être analysée conformément à ANSSI-CC-CRY-P-01. Joindre au dossier les spécifications cryptographiques rédigées conformément aux prescriptions du document « Fournitures nécessaires à l’analyse de mécanismes cryptographiques », voir [www.ssi.gouv.fr](http://www.ssi.gouv.fr) et renseigner les tableaux suivants.  *The efficiency of cryptographic mechanisms shall be analyzed in accordance with ANSSI-CC-CRY-P-01. Provide with the application form the cryptographic specification written according to the document « Fournitures nécessaires à l’analyse de mécanismes cryptographiques », see* [*www.ssi.gouv.fr*](http://www.ssi.gouv.fr) *and fill in the following table.* | | OUI / NON  *YES / NO* | |
| Titre du document de spécifications cryptographiques :  *Cryptographic specification document title* |  | |
| Référence/ *Reference* |  | |
| Version/ *Version* |  | |
| Le produit met-il en œuvre des mécanismes cryptographiques propriétaires ou non standards ?  *Does the TOE implement proprietary or non-standard cryptographic mechanisms?* | | OUI / NON  *YES / NO* |

Sélectionner le référentiel pour l’analyse théorique des mécanismes cryptographiques

*Select the basis for the theoretical analysis of the cryptographic mechanisms*

|  |  |
| --- | --- |
| Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version en vigueur. | OUI / NON  *YES / NO* |
| SOG-IS *Crypto Evaluation Scheme Agreed Cryptographic Mechanisms*, version en vigueur. | OUI / NON  *YES / NO* |

### Méthodes spécifiques à l’évaluation de l’objet / *Evaluation specific methods of the target*

Ne peuvent être sélectionnés ici que les documents supports à caractère facultatif

*Only optional supporting documents may be selected.*

|  |  |  |
| --- | --- | --- |
| [AIS 31] Functionality classes and evaluation methodology for physical random number generator, BSI (*Bundesamt für Sicherheit in der Informationstechnik*),  version courante / current version | | OUI / NON  *YES / NO* |
| [COLL] Collection of Developer Evidence, [www.commoncriteriaportal.org](http://www.commoncriteriaportal.org), version courante / current version | | OUI / NON  *YES / NO* |
| Autres / *Others* | | OUI / NON  *YES / NO* |
| Si oui, préciser / *If yes, specif*y |  | |

### Eventuel objectif réglementaire / *Product Qualification process*

|  |  |  |
| --- | --- | --- |
| Cette évaluation entre dans le cadre d’une qualification standard ANSSI ?  *This evaluation takes part of a ANSSI’s standard qualification?* | | OUI / NON  *YES / NO* |
| Cette évaluation entre dans le cadre d’une qualification renforcée ANSSI ?  *This evaluation takes part of a ANSSI’s reinforced qualification?* | | OUI / NON  *YES / NO* |
| Cette évaluation entre dans le cadre d’une certification de conformité eIDAS ?  *This evaluation takes part of a eIDAS conformity?* | | OUI / NON  *YES / NO* |
| Cette évaluation entre dans le cadre d’une qualification LPM ?  *This evaluation takes part of a LPM qualification?* | | OUI / NON  *YES / NO* |
| Autres / *Others* | | OUI / NON  *YES / NO* |
| Si oui, préciser / *If yes, specif*y |  | |

Dans le cadre d’une procédure de qualification de produit, les commanditaires et les centres d’évaluation autorisent le Centre de certification à transmettre au bureau Qualification et Agrément de l’ANSSI tout document nécessaire à l’instruction du dossier.

*In the context of the product qualification process, the sponsor and the evaluation facilitiesauthorize the certification body to transmit to the qualification team of ANSSI, any document necessary for the investigation of the project.*

### Confidentialité du projet d’évaluation / *Confidentiality of the evaluation project*

|  |  |
| --- | --- |
| L’existence du projet d’évaluation est-elle confidentielle ?  *Is the existence of this evaluation project confidential?* | OUI / NON  YES / *NO* |

### Nom de code proposé pour l’évaluation / *Code name suggested for the evaluation*

|  |  |
| --- | --- |
| Nom de code proposé pour l’évaluation  *Suggested code name for the evaluation* |  |

Il est suggéré d’adopter le nom de l’objet lorsque l’existence de l’évaluation n’est pas confidentielle. Le centre de certification proposera un autre nom en cas de collision avec un projet existant.

*It is suggested to adopt the object name when the existence of the evaluation is not confidential. The certification body will propose another name if the product name is the same as an existing evaluation project.*

### Format des rapports d’évaluation / *Format of evaluation reports*

|  |  |
| --- | --- |
| Langue utilisée dans les rapports d’évaluation  *Language to be used in the evaluation reports* | Français / Anglais *French / English* |

### Publication du certificat / *Certificate Publication*

Une fois l’objet certifié, l’ANSSI propose au commanditaire que le rapport de certification soit publié sur son site Web.

*Once the object to be evaluated is certified, ANSSI proposes to the sponsor that the certification report be published on its Website.*

|  |  |
| --- | --- |
| Souhaitez-vous que le rapport de certification issu de cette évaluation soit publié ?  *Would you like to have the certification report of this evaluation published?* | OUI / NON  YES */ NO* |

### Reconnaissance internationale du certificat / *International recognition of the certificate*

La reconnaissance internationale du certificat (de produit et de profil de protection) implique que soient publiés la version finale de la cible de sécurité (ou du profil de protection) et le rapport de certification.

L’accord du CCRA permet au certificat issu d’une évaluation Critères communs d’être reconnu par plus d’une vingtaine de pays dans le monde. Cette reconnaissance est limitée :

* au niveau EAL2 si aucun cPP[[8]](#footnote-9) n’est utilisé dans le cadre de l’évaluation de produit ;
* au niveau d’évaluation identifié dans le cPP sinon.

L’accord du SOG-IS permet au certificat issu d’une évaluation réalisée en utilisant les [ITSEC] ou les [CC] d’être reconnu par une quinzaine de pays en Europe.

*International recognition of the certificate (of the product or the protection profile) requires the final version of the security target (or the protection profile) to be published with the certification report.*

*With the CCRA recognition arrangement, Common Criteria certificates can be recognised by more than 20 countries in the world. This recognition is limited:*

* At the level EAL2 if no cPP[[9]](#footnote-10) is used by the product evaluation.
* Otherwise at the evaluation level identified by the cPP.

*With the SOG-IS recognition arrangement, [ITSEC] and [CC] certificates can be recognised by around fifteen countries in Europe.*

|  |  |
| --- | --- |
| Souhaitez-vous que le certificat issu de cette évaluation entre dans le cadre des accords de reconnaissance mutuelle ?  *Do you want the certificate edited for this evaluation to be under mutual recognition agreement?* | OUI / NON  YES */ NO* |

# **Constitution du comité de pilotage de l’évaluation / Constitution of an Evaluation Steering**Committee

Le comité de pilotage est constitué au minimum d’un représentant du commanditaire, du centre d’évaluation et du centre de certification. Des représentants des développeurs peuvent également participer au comité de pilotage. Des observateurs peuvent être invités aux réunions du comité de pilotage sur invitation du commanditaire.

*The Evaluation Steering Committee comprises at least a representative from the sponsor, one from the evaluation facility and one from the certification body. Representatives from the developers may also participate to the steering committee. Observers can be invited to the meetings by the sponsor.*

### Commanditaire /*Sponsor*

Le commanditaire est l’organisme ou la personne qui commande l’évaluation et qui la finance.

Le commanditaire est responsable de :

* la définition de la cible de sécurité qui précise le périmètre de l’évaluation ;
* la mise à disposition des fournitures requises pour l’évaluation ;
* des moyens de tests nécessaires à la réalisation de l’évaluation lorsque ceux-ci sont spécifiques.

*The sponsor is the organization or the person which applies and funds the evaluation.*

*The sponsor is responsible for:*

* Defining the Security Target which defines the scope of the evaluation.
* Providing the deliverables required for the evaluation.
* The means of testing necessary to carry out the evaluation when these are specific.

|  |  |
| --- | --- |
| **Nom et/ou raison sociale**  ***Company name*** |  |
| **Nom du contact**  ***Point of contact*** |  |
| **Adresse / *Address*** |  |
| **Tél. / *Tel*** |  |
| **Fax/ *Fax*** |  |
| **Courriel / *E-mail*** |  |

### Centre d’évaluation /*Evaluation facility*

Le centre d’évaluation réalise l’évaluation. Il agit en tant que tierce partie indépendante des développeurs de produits, des exploitants des sites et des commanditaires. Il est agréé par l’ANSSI et est à ce titre tenu de respecter toutes les règles du schéma.

Pour mener à bien ses travaux, le centre d’évaluation doit avoir accès à des informations et à des biens sensibles, définis comme tels par le commanditaire ou le(s) développeur(s).

*The evaluator performs the evaluation. It acts as a third party independent from the developers of the products, the sites managers and from the sponsors. The evaluation facility is licensed by ANSSI and therefore must follow all the rules from the French scheme.*

*To perform its tasks, the evaluator could need to have access to sensitive information and assets defined as such by the sponsor or the developer(s).*

|  |  |
| --- | --- |
| **Nom et/ou raison sociale**  ***Company name*** |  |
| **Nom du contact**  ***Point of contact*** |  |
| **Adresse / *Address*** |  |
| **Tél. / *Tel*** |  |
| **Fax / *Fax*** |  |
| **Courriel / *E-mail*** |  |
| **Liste des évaluateurs qui interviendront sur le projet / *List of the evaluators involved in the evaluation*** |  |

### Organisme de certification / *Certification body*

L’organisme de certification est le centre de certification de l’ANSSI. Il met en œuvre le schéma d’évaluation et de certification. Son rôle essentiel est d’apporter une confirmation indépendante que les évaluations ont été correctement effectuées, conformément aux critères, méthodes et procédures du schéma et que les conclusions de ces évaluations sont fondées.

*The certification body, whose role is taken by ANSSI, manages the evaluation and certification scheme. Its essential role is to independently confirm that the evaluations have been correctly performed, in accordance with the criteria, methods and procedures of the scheme, and that the results of the evaluations are relevant.*

|  |  |
| --- | --- |
| Nom / *Name* | ANSSI – Centre de Certification |
| **Adresse / *Address*** | SGDSN, 51 boulevard de La Tour-Maubourg, 75700 Paris 07 SP, France |
| **Tél. / *Tel*** | +33 (0)1.71.75.82.82 |
| **Fax / *Fax*** | +33 (0)1.84.82.40.60 |
| **Courriel / *E-mail*** | certification@ssi.gouv.fr |

### Développeur(s) / *Developer(s)*

Le développeur désigne l’organisation qui spécifie, élabore, gère ou maintient l’objet à évaluer ou certains de ses composants.

Le développeur est responsable de :

* l’élaboration de la plupart des fournitures ;
* l’assistance technique aux évaluateurs si nécessaire (formation, passage de tests, mise à disposition d’une plate-forme d’évaluation, accès à l’environnement de développement, de production du produit en évaluation).

*The developer is the organization which designs, manufactures, manages or maintains the object to evaluate or some of its components.*

*The developer is responsible for:*

* Generating most of the elements of evidence.
* Technically assisting the evaluator if needed (training, testing, access to development and production environments of the evaluated product).

|  |  |
| --- | --- |
| **Nom et/ou raison sociale**  ***Company name*** |  |
| **Nom du contact**  ***Point of contact*** |  |
| **Adresse / *Address*** |  |
| **Tél. / *Tel*** |  |
| **Fax / *Fax*** |  |
| **Courriel / *E-mail*** |  |

### Observateur(s) (facultatif) / *Observer(s) (optional)*

Le commanditaire peut proposer la présence d’un (ou plusieurs) observateur associé au suivi de la certification. L’observateur est soumis à l’acceptation de l’ANSSI et est tenu informé du démarrage de l’évaluation ainsi que des résultats obtenus. Les éléments précis auxquels auront accès le ou les observateurs seront déterminés avec le Centre de Certification, le centre d’évaluation et le commanditaire lors de la réunion de démarrage.

*The sponsor may suggest participation of one (or several) observer(s) in the certification follow up. The observer shall be approved by ANSSI and will be informed of the evaluation kick off and outcomes. Specific details that observer(s) will have access to will be decided during the kick off meeting by the Certification Body, the Information Technology Security Evaluation Facility and the sponsor.*

|  |  |
| --- | --- |
| **Nom et/ou raison sociale**  ***Company name*** |  |
| **Nom du contact**  ***Point of contact*** |  |
| **Adresse / *Address*** |  |
| **Tél. / *Tel*** |  |
| **Courriel / *E-mail*** |  |

# Programme de travail prévisionnel pour l’évaluation / *Provisional Evaluation Work Program*

Les informations suivantes doivent être fournies en même temps que ce dossier d’évaluation :

* la description du cycle de vie du produit évalué, définissant les activités ayant un impact sur la sécurité du produit évalué et sur la charge d’évaluation[[10]](#footnote-11);
* et pour chaque tâche d’évaluation :
  + l’élément de preuve à fournir (ou fourniture) et sa date de disponibilité ;
  + la charge d’évaluation prévue ;
  + une description succincte des travaux d’évaluation à mener (permettant d’argumenter la charge d’évaluation) et précisant si des résultats d’évaluations précédentes sont réutilisés ou si des travaux doivent être réalisés sur site.

*The following information must be provided at the same time as this application form for evaluation:*

* The description of the product workflow, defining the activities having a security impact on the evaluated product and on the evaluation workload[[11]](#footnote-12).
* And, for each evaluation task:
  + The element of evidence to be supplied and its date of delivery.
  + The provisional workload for the evaluation.
  + A short description of the evaluation work to be done (justifying the evaluation workload) and indicating whether results from previous evaluations can be re-used or whether on-site activities must be performed.

**NB** : L’ensemble des éléments de preuve fourni par le commanditaire ou le développeur doit par défaut être mis à disposition dans les locaux du centre d’évaluation. Toute éventuelle demande de dérogation à cette règle doit être portée à la connaissance du Centre de certification et dûment justifiée. Le Centre de certification peut l’accepter ou non suivant les motivations fournies. En cas d’acceptation, une provision sur la charge d’évaluation doit être prévue qui pourra être réajustée au fur et à mesure de l’avancement des travaux en fonction des besoins exprimés par le centre d’évaluation.

***NB****: By default, the set of evidences provided by either the sponsor or the developer must be available in the evaluation facilities. Any exception request must be justified and notified to the certification body, which can decide to accept or deny it base on the provided justification. If accepted, the evaluation facility must define a provisional workload. That provisional workload could be readjusted according to the evaluation progress and the evaluation facility needs.*

Les pages suivantes donnent des exemples :

* de description des processus intervenant dans la fabrication du produit évalué ;
* de présentation du programme de travail pour :
  + une évaluation de produit au niveau EAL3 + ALC\_FLR.3 (avec la composition et l’analyse de la cryptographie) suivant les Critères Communs version 3.1 révision 5 ;
  + une évaluation de profil de protection (PP) suivant les Critères Communs version 3.1 révision 5 ;
  + une évaluation de site au niveau AST + ALC\_CMC.3 + ALC\_CMS.3 + ALC\_DEL.1 + ALC\_FLR.3 + ALC\_LCD.1.

*The following pages give examples of,* ***for English version please refer to page 24 to 30:***

Description of the processes involved in the production / manufacturing of the evaluated product.

* Description of the work program for:
  + A product evaluation at the level EAL3 + ALC\_FLR.3 (with the composition and the expertise of the cryptographic implementation according to the Common Criteria version 3.1 revision 5.
  + A protection profile (PP) evaluation according to the Common Criteria version 3.1 revision 5.
  + A site evaluation at level AST + ALC\_CMC.3 + ALC\_CMS.3 + ALC\_DEL.1 + ALC\_FLR.3 + ALC\_LCD.1.

### Programme de travail de l’évaluation

Exemple pour une évaluation de produit au niveau EAL3 + ALC\_FLR.3 suivant les Critères Communs version 3.1 révision 4 :

**Description du processus intervenant dans la fabrication du produit évalué**

Les données sensibles qui doivent être protégées par l’environnement de développement évalué doivent être identifiées, de façon non ambiguë, au chapitre « mesures d’assurance » de la cible de sécurité (au titre des composants ALC).

Les activités de développement qui traitent ces données sensibles sont ici appelées « processus relatifs à la sécurité ».

Pour chacun de ces « processus relatifs à la sécurité », les informations suivantes sont attendues :

* localisation de ce processus (physiquement) ;
* entrées et sorties (celles-ci devant correspondre à des données sensibles).

Exemple pour un fabricant de microcircuits :

|  |  |  |  |
| --- | --- | --- | --- |
| **Processus** | **Localisation** | **Entrées** | **Sorties** |
| **Gestion code source client** | Londres | Code source client | - |
| **Conception et synthèse** | Paris et Rome | Spécifications du micro-circuit et de son logiciel dédié, avec ou sans code source client | Code source Verilog synthétisé  Netlist |
| **Placement routage** | Marseille | Netlist | GDSII |
| **Préparation du masque** |  | GDSII | Fichiers du masque |
| **Fabrication du masque** | Paris (sous-traitant) | Fichiers du masque | Masque physique |
| **Fabrication du microcircuit** | XXX | Masque physique | Wafers |
| **Tests avec sondes & configuration de sécurité** | XXX | Wafers | Wafers |
| **Sciage** | XXX | Wafers | Wafers sciés (puces nues ou masquées) |
| **FabLab** | XXX | Wafers / Wafers sciés (puces) | Résidus non fonctionnels (Scraps) |
| **Packaging** | XXX | Puces | Puces encapsulées (micromodules, DILs, …) |
| **Service informatique** |  |  |  |
| **Ressources humaines** |  | - | - |

Exemple pour un fabricant de cartes à puce :

|  |  |  |  |
| --- | --- | --- | --- |
| **Processus** | **Localisation** | **Entrées** | **Sorties** |
| **Conception JAVA** | XXX | Spécification, Code source crypto | Code source Java compilé |
| **Conception Crypto** | XXX | Spécification crypto | Code source crypto |
| **Conception de l’applet** | XXX | Spécification | Fichier CAP |
| **Fabrication du microcircuit** | XXX | Code source compilé | Microcircuits masqués |
| **Validation** | XXX | Microcircuits masqués | Microcircuits masqués validés,  Rapport de validation |
| **Pre-personnalisation / chargement de patch** | XXX | Fichier CAP, Patch | Produits avec applet chargée, Produits patchés |
| **Gestion des clés de personnalisation** | XXX |  |  |

Exemple pour un fabricant de firewall matériel :

|  |  |  |  |
| --- | --- | --- | --- |
| **Processus** | **Localisation** | **Entrées** | **Sorties** |
| **Développent du logiciel** | XXX | Spécification | Code source |
| **Intégration du logiciel au matériel** | XXX | Code source, plateforme matérielle | Appliance |

|  |  |  |  |
| --- | --- | --- | --- |
| **Evaluation de la cible de sécurité (classe ASE)** | | | |
| Le commanditaire doit fournir une cible de sécurité (ASE) | | Date de disponibilité : |  |
| Charge prévisionnelle d’évaluation : |  | | |
| Description des travaux à mener : | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Evaluation de la conception (classe ADV)** | | | |
| Le développeur doit concevoir et implémenter la TOE de telle sorte que les caractéristiques de la TSF[[12]](#footnote-13) ne puissent pas être contournées (ADV\_ARC.1.1D) | | Date de disponibilité : |  |
| Le développeur doit concevoir et implémenter la TSF de telle sorte qu’elle soit capable de se protéger elle-même de la falsification par des entités actives qui ne sont pas de confiances (ADV\_ARC.1.2D) | | Date de disponibilité : |  |
| Le développeur doit fournir une description de l’architecture de sécurité de la TSF (ADV\_ARC.1.3D) | | Date de disponibilité : |  |
| Le développeur doit fournir des spécifications fonctionnelles (ADV\_FSP.3.1D) | | Date de disponibilité : |  |
| Le développeur doit fournir une traçabilité entre les spécifications fonctionnelles et les SFR (ADV\_FSP.3.2D) | | Date de disponibilité : |  |
| Le développeur doit fournir la conception de la TOE (ADV\_TDS.2.1D) | | Date de disponibilité : |  |
| Le développeur doit fournir la correspondance entre les TSFI[[13]](#footnote-14) des spécifications fonctionnelles jusqu’au plus bas niveau disponible de décomposition de la conception de la TOE (ADV\_TDS.2.2D) | | Date de disponibilité : |  |
| Charge prévisionnelle d’évaluation : |  | | |
| Description des travaux à mener : | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Evaluation des guides (classe AGD)** | | | |
| Le développeur doit fournir un guide opérationnel de l’utilisateur (ou un guide du produit en opération) (AGD\_OPE.1.1D) | | Date de disponibilité : |  |
| Le développeur doit fournir la TOE et ses procédures de préparation (AGD\_PRE.1.1D) | | Date de disponibilité : |  |
| Charge prévisionnelle d’évaluation : |  | | |
| Description des travaux à mener : | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Evaluation du cycle de vie (classe ALC)** | | | |
| Le développeur doit fournir la TOE et une référence pour la TOE (ALC\_CMC.3.1D) | | Date de disponibilité : |  |
| Le développeur doit fournir la documentation de gestion de configuration (ALC\_CMC.3.2D) | | Date de disponibilité : |  |
| Le développeur doit utiliser un système de gestion de configuration (ALC\_CMC.3.3D) | | Date de disponibilité : |  |
| Le développeur doit fournir une liste de configuration pour la TOE (ALC\_CMS.3.1D) | | Date de disponibilité : |  |
| Le développeur doit documenter et fournir les procédures de livraison de la TOE ou de parties de celle-ci à l’utilisateur final (ALC\_DEL.1.1D) | | Date de disponibilité : |  |
| Le développeur doit utiliser les procédures de livraison (ALC\_DEL.1.2D) | | Date de disponibilité : |  |
| Le développeur doit produire et fournir la documentation relative à la sécurité du développement (ALC\_DVS.1.1D) | | Date de disponibilité : |  |
| Le développeur doit documenter et fournir les procédures de correction des failles de sécurité appliquées par les développeurs de la TOE (ALC\_FLR.3.1D) | | Date de disponibilité : |  |
| Le développeur doit établir une procédure pour accepter et traiter tous les rapports sur les failles de sécurité ainsi que pour requérir la correction de telles failles (ALC\_FLR.3.2D) | | Date de disponibilité : |  |
| Le développeur doit fournir un guide de correction des failles de sécurité adressé aux utilisateurs de la TOE. Le développeur doit fournir, aux utilisateurs de la TOE, la démarche pour remonter des failles de sécurité (ALC\_FLR.3.3D) | | Date de disponibilité : |  |
| Le développeur doit établir un modèle du cycle de vie utilisé pour le développement et la maintenance de la TOE (ALC\_LCD.1.1D) | | Date de disponibilité : |  |
| Le développeur doit fournir une documentation relative à la définition du cycle de vie (ALC\_LCD.1.2D) | | Date de disponibilité : |  |
| Charge prévisionnelle d’évaluation : |  | | |
| Description des travaux à mener : | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Evaluation des tests (classe ATE)** | | | |
| Le développeur doit fournir une analyse de la couverture des tests (ATE\_COV.2.1D) | | Date de disponibilité : |  |
| Le développeur doit fournir l’analyse de profondeur des tests (ATE\_DPT.1.1D) | | Date de disponibilité : |  |
| Le développeur doit tester la TSF et documenter les résultats (ATE\_FUN.1.1D) | | Date de disponibilité : |  |
| Le développeur doit fournir la documentation de test (ATE\_FUN.1.2D) | | Date de disponibilité : |  |
| Le développeur doit fournir la TOE afin d’exécuter les tests (ATE\_IND.2.1D) | | Date de disponibilité : |  |
| Charge prévisionnelle d’évaluation : |  | | |
| Description des travaux à mener : | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Estimation des vulnérabilités (classe AVA)** | | | |
| Le développeur doit fournir la TOE afin d’exécuter les tests (AVA\_VAN.2.1D) | | Date de disponibilité : |  |
| Charge prévisionnelle d’évaluation : |  | | |
| Description des travaux à mener : | | | |
|  | | | |

En cas de composition :

|  |  |  |  |
| --- | --- | --- | --- |
| **Travaux de composition : éléments du composant sous-jacent** | | | |
| Cible de sécurité publique | | Date de disponibilité : |  |
| *ETR-Lite for composition*  (Si le centre d’évaluation en charge de la présente évaluation est différent du centre d’évaluation qui a évalué le composant sous-jacent)*)* | | Date de disponibilité : |  |
| Guides | | Date de disponibilité : |  |
| Echantillons en mode ‘ouvert’  (pour une évaluation *hardware* uniquement) | | Date de disponibilité : |  |
| Travaux de cartographie du micro-circuit  (pour l’évaluation d’une carte à puce uniquement) | | Date de disponibilité : |  |
| Charge prévisionnelle d’évaluation : |  | | |
| Description des travaux à mener : | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Analyse de la cryptographie (cotation théorique et expertise de l’implémentation de la cryptographie)** | | | |
| Spécifications cryptographiques | | Date de disponibilité : |  |
| Code source | | Date de disponibilité : |  |
| Moyens de compilation | | Date de disponibilité : |  |
| Documentation des interfaces et de leurs tests | | Date de disponibilité : |  |
| Documentation sur la protection en confidentialité et intégrité des éléments sensibles | | Date de disponibilité : |  |
| Si applicable, documentation sur la gestion des nombres aléatoires | | Date de disponibilité : |  |
| Charge prévisionnelle d’évaluation : |  | | |
| Description des travaux à mener : | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Analyse de la génération de nombres aléatoires** | | | |
| Si AIS20/31 PTRNG : document conforme à “*Developer evidence for the evaluation of a physical true random number generator, version 0.8*” | | Date de disponibilité : |  |
| Si AIS20/31 DRNG : document conforme à “*Developer evidence for the evaluation of a deterministic random number generator, version 0.9*” | | Date de disponibilité : |  |
| Si AIS20/31 PTRNG + DRNG : document conforme aux deux documents nommés ci-dessus | | Date de disponibilité : |  |
| Charge prévisionnelle d’évaluation : |  | | |
| Description des travaux à mener : | | | |
|  | | | |

Exemple pour une évaluation de profil de protection (PP) suivant les Critères Communs version 3.1 révision 4 :

|  |  |  |  |
| --- | --- | --- | --- |
| **Evaluation du profil de protection (classe APE)** | | | |
| Le commanditaire doit fournir le profil de protection (APE) | | Date de disponibilité : |  |
| Charge prévisionnelle d’évaluation : |  | | |
| Description des travaux à mener : | | | |
|  | | | |

Exemple pour une certification de site réalisée selon la démarche décrite par le document CCDB-2007-11-001 au niveau AST + ALC\_CMC.3 + ALC\_CMS.3 + ALC\_DEL.1 + ALC\_FLR.3 + ALC\_LCD.1 :

|  |  |  |  |
| --- | --- | --- | --- |
| **Evaluation de la cible de sécurité (classe AST)** | | | |
| Le commanditaire doit fournir une cible de sécurité de site (ASE) | | Date de disponibilité : |  |
| Charge prévisionnelle d’évaluation : |  | | |
| Description des travaux à mener : | | | |
|  | | | |

Dans le cas d’évaluation de composants ALC génériques, compléter le tableau ci-dessous pour chaque de site en précisant son nom, son adresse et les charges associées.

|  |  |  |  |
| --- | --- | --- | --- |
| **Evaluation du cycle de vie (classe ALC)** | | | |
| Le développeur doit fournir la TOE et une référence pour la TOE (ALC\_CMC.3.1D) | | Date de disponibilité : |  |
| Le développeur doit fournir la documentation de gestion de configuration (ALC\_CMC.3.2D) | | Date de disponibilité : |  |
| Le développeur doit utiliser un système de gestion de configuration (ALC\_CMC.3.3D) | | Date de disponibilité : |  |
| Le développeur doit fournir une liste de configuration pour la TOE (ALC\_CMS.3.1D) | | Date de disponibilité : |  |
| Le développeur doit documenter et fournir les procédures de livraison de la TOE ou de parties de celle-ci à l’utilisateur final (ALC\_DEL.1.1D) | | Date de disponibilité : |  |
| Le développeur doit utiliser les procédures de livraison (ALC\_DEL.1.2D) | | Date de disponibilité : |  |
| Le développeur doit produire et fournir la documentation relative à la sécurité du développement (ALC\_DVS.1.1D) | | Date de disponibilité : |  |
| Le développeur doit documenter et fournir les procédures de correction des failles de sécurité appliquées par les développeurs de la TOE (ALC\_FLR.3.1D) | | Date de disponibilité : |  |
| Le développeur doit établir une procédure pour accepter et traiter tous les rapports sur les failles de sécurité ainsi que pour requérir la correction de telles failles (ALC\_FLR.3.2D) | | Date de disponibilité : |  |
| Le développeur doit fournir un guide de correction des failles de sécurité adressé aux utilisateurs de la TOE. Le développeur doit fournir, aux utilisateurs de la TOE, la démarche pour remonter des failles de sécurité (ALC\_FLR.3.3D) | | Date de disponibilité : |  |
| Le développeur doit établir un modèle du cycle de vie utilisé pour le développement et la maintenance de la TOE (ALC\_LCD.1.1D) | | Date de disponibilité : |  |
| Le développeur doit fournir une documentation relative à la définition du cycle de vie (ALC\_LCD.1.2D) | | Date de disponibilité : |  |
| Charge prévisionnelle d’évaluation : |  | | |
| Description des travaux à mener : | | | |
|  | | | |

***Evaluation work program***

*Example for a product evaluation at level EAL3 + ALC\_FLR.3 according to the Common Criteria version 3.1 revision 4:*

***Description of the processes involved in the building of the evaluated product***

*The “sensitive” data that have to be protected by the evaluated development environment must be identified unambiguously in the “assurance measures” section of the security target (ALC component).*

*Development activities that handle those “sensitive” data are here called “security relevant processes”.*

*For each “security relevant process”, the following information is needed:*

* *Location of the process (physically).*
* *Inputs and outputs (that shall correspond to “sensitive” data).*

*Example for an IC manufacturer:*

|  |  |  |  |
| --- | --- | --- | --- |
| ***Processes*** | ***Location*** | ***Inputs*** | ***Outputs:*** |
| ***Management of client source code*** | *London* | *Client source code* | *-* |
| ***Design & Synthesis*** | *Paris & Rome* | *IC and dedicated software specification with or without client source code* | *Synthesised Verilog source code;*  *Netlist* |
| ***Place & route*** | *Marseille* | *Netlist* | *GDSII* |
| ***Mask preparation*** |  | *GDSII* | *Mask files* |
| ***Mask fabrication*** | *Paris (sub-contractor)* | *Mask files* | *Physical Masks* |
| ***IC fabrication*** | *XXX* | *Physical Masks* | *Wafers* |
| ***Probe testing & security configuration*** | *XXX* | *Wafers* | *Wafers* |
| ***Sawing*** | *XXX* | *Wafers* | *Sawn wafers (naked or masked chip)* |
| ***FabLab*** | *XXX* | *Wafers/ Sawn wafers (chips)* | *Scraps* |
| ***Packaging*** | *XXX* | *Chips* | *Packaged chip (micro modules, DILs, …)* |
| ***IT services*** |  |  |  |
| ***Human resources*** |  |  |  |

*Example for a Smart Card manufacturer:*

|  |  |  |  |
| --- | --- | --- | --- |
| ***Processes*** | ***Location*** | ***Inputs*** | ***Outputs*** |
| ***JAVA******Design*** | *XXX* | *Specification, Crypto source code* | *Compiled Java source code* |
| ***Crypto Design*** | *XXX* | *Specification* | *Crypto source code* |
| ***Applet Design*** | *XXX* | *Specification* | *CAP file* |
| ***IC manufacturing*** | *XXX* | *Compiled source code* | *Masked ICs* |
| ***Validation*** | *XXX* | *Masked ICs* | *Validated Masked ICs, validation report* |
| ***Pre personalization / patch loading*** | *XXX* | *CAP file, Patch, products* | *Product with applet loaded, Patched products.* |
| ***Personalization’s key management*** | *XXX* |  |  |

*Example for a hardware firewall:*

|  |  |  |  |
| --- | --- | --- | --- |
| ***Processes*** | ***Location*** | ***Inputs*** | ***Outputs*** |
| ***Design*** |  | *Specification* | *source code* |
| ***Integration to the appliance*** |  | *source code*  *hardware platform* | *appliance* |

|  |  |  |  |
| --- | --- | --- | --- |
| **Security Target evaluation (class ASE)** | | | |
| *The sponsor must provide a Security Target (ASE)* | | Availability: |  |
| Evaluation Workload: |  | | |
| Description of work: | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Evaluation of development (class ADV)** | | | |
| *The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed (ADV\_ARC.1.1D)* | | Availability: |  |
| *The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities (ADV\_ARC.1.2D)* | | Availability: |  |
| *The developer shall provide a security architecture description of the TSF (ADV\_ARC.1.3D)* | | Availability: |  |
| *The developer shall provide a functional specification (ADV\_FSP.3.1D)* | | Availability: |  |
| *The developer shall provide a tracing from the functional specification to the SFRs (ADV\_FSP.3.2D)* | | Availability: |  |
| *The developer shall provide the design of the TOE (ADV\_TDS.2.1D)* | | Availability: |  |
| *The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design (ADV\_TDS.2.2D)* | | Availability: |  |
| Evaluation Workload: |  | | |
| Description of work: | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Evaluation of guidance documents (class AGD)** | | | |
| *The developer shall provide operational user guidance (AGD\_OPE.1.1D)* | | Availability: |  |
| *The developer shall provide the TOE including its preparative procedures(AGD\_PRE.1.1D)* | | Availability: |  |
| Evaluation Workload: |  | | |
| Description of work: | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Evaluation of life-cycle support (class ALC)** | | | |
| *The developer shall provide the TOE and a reference for the TOE (ALC\_CMC.3.1D)* | | Availability: |  |
| *The developer shall provide the configuration management documentation (ALC\_CMC.3.2D)* | | Availability: |  |
| *The developer shall use a configuration management system (ALC\_CMC.3.3D)* | | Availability: |  |
| *The developer shall provide a configuration list for the TOE (ALC\_CMS.3.1D)* | | Availability: |  |
| *The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer (ALC\_DEL.1.1D)* | | Availability: |  |
| *The developer shall use the delivery procedures (ALC\_DEL.1.2D)* | | Availability: |  |
| *The developer shall produce and provide development security documentation (ALC\_DVS.1.1D)* | | Availability: |  |
| *The developer shall document and provide flaw remediation procedures addressed to TOE developers (ALC\_FLR.3.1D)* | | Availability: |  |
| *The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws (ALC\_FLR.3.2D)* | | Availability: |  |
| *The developer shall provide flaw remediation guidance addressed to TOE users (ALC\_FLR.3.3D)* | | Availability: |  |
| *The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE (ALC\_LCD.1.1D)* | | Availability: |  |
| *The developer shall provide life-cycle definition documentation (ALC\_LCD.1.2D)* | | Availability: |  |
| Evaluation Workload: |  | | |
| Description of work: | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Evaluation of tests (class ATE)** | | | |
| *The developer shall provide an analysis of the test coverage (ATE\_COV.2.1D)* | | Availability: |  |
| *The developer shall provide the analysis of the depth of testing (ATE\_DPT.1.1D)* | | Availability: |  |
| *The developer shall test the TSF and document the results (ATE\_FUN.1.1D)* | | Availability: |  |
| *The developer shall provide test documentation (ATE\_FUN.1.2D)* | | Availability: |  |
| *The developer shall provide the TOE for testing (ATE\_IND.2.1D)* | | Availability: |  |
| Evaluation Workload: |  | | |
| Description of work: | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Vulnerability assessment (class AVA)** | | | |
| *The developer shall provide the TOE for testing (AVA\_VAN.2.1D)* | | Availability: |  |
| Evaluation Workload: |  | | |
| Description of work: | | | |
|  | | | |

*In case of composition:*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Composition activities** | | | | |
| *Integrated circuit Security Target (ST)-Lite* | | Availability: |  | |
| *ETR-Lite for composition* | | Availability: |  | |
| *Security Guidance* | | Availability: |  | |
| *Chip samples in ‘open’ mode* | | Availability: |  | |
| *Integrated circuit cartography work* | |  | |  | |
| Evaluation Workload: |  | | | |
| Description of work: | | | | |
|  | | | | |

*In the case the product is under the qualification process:*

|  |  |  |  |
| --- | --- | --- | --- |
| **Cryptography implementation expertise** | | | |
| *Cryptographic specifications* | | Availability: |  |
| *Source code* | | Availability: |  |
| *Compilation means* | | Availability: |  |
| *Documentation about interfaces and their tests* | | Availability: |  |
| *Documentation about confidentiality and integrity protection of sensitive elements* | | Availability: |  |
| *If applicable, random number management documentation* | | Availability: |  |
| Evaluation Workload: |  | | |
| Description of work: | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Random generator analysis** | | | |
| *If AIS20/31 PTRNG : in conformance with “Developer evidence for the evaluation of a physical true random number generator, version 0.8”* | | Availability: |  |
| *If AIS20/31 DRNG : in conformance with “Developer evidence for the evaluation of a deterministic random number generator, version 0.9”* | | Availability: |  |
| *If AIS20/31 PTRNG + DRNG : in conformance with the two documents listed above* | | Availability: |  |
| Evaluation Workload: |  | | |
| Description of work: | | | |
|  | | | |

*Example for a protection profile evaluation (PP) according to the Common Criteria version 3.1 release 4:*

|  |  |  |  |
| --- | --- | --- | --- |
| **Evaluation of the protection profile (APE class)** | | | |
| *The sponsor must provide the protection profile (APE)* | | Availability: |  |
| Evaluation workload: |  | | |
| Description of work: | | | |
|  | | | |

*Example for a site certification site performed based on CCDB-2007-11-001 method at level AST + ALC\_CMC.3 + ALC\_CMS.3 + ALC\_DEL.1 + ALC\_FLR.3 + ALC\_LCD.1:*

|  |  |  |  |
| --- | --- | --- | --- |
| **Site Security Target Evaluation (class AST)** | | | |
| *The sponsor shall provide a site security target (ASE)* | | Availability: |  |
| Evaluation workload: |  | | |
| Description of work: | | | |
|  | | | |

*In case of ALC generic components evaluation, fill in the below table for each site and provide its name, its location and the associated workload.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Evaluation of life-cycle support (class ALC)** | | | |
| *The developer shall provide the TOE and a reference for the TOE (ALC\_CMC.3.1D)* | | Availability: |  |
| *The developer shall provide the configuration management documentation (ALC\_CMC.3.2D)* | | Availability: |  |
| *The developer shall use a configuration management system (ALC\_CMC.3.3D)* | | Availability: |  |
| *The developer shall provide a configuration list for the TOE (ALC\_CMS.3.1D)* | | Availability: |  |
| *The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer (ALC\_DEL.1.1D)* | | Availability: |  |
| *The developer shall use the delivery procedures (ALC\_DEL.1.2D)* | | Availability: |  |
| *The developer shall produce and provide development security documentation (ALC\_DVS.1.1D)* | | Availability: |  |
| *The developer shall document and provide flaw remediation procedures addressed to TOE developers (ALC\_FLR.3.1D)* | | Availability: |  |
| *The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws (ALC\_FLR.3.2D)* | | Availability: |  |
| *The developer shall provide flaw remediation guidance addressed to TOE users (ALC\_FLR.3.3D)* | | Availability: |  |
| *The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE (ALC\_LCD.1.1D)* | | Availability: |  |
| *The developer shall provide life-cycle definition documentation (ALC\_LCD.1.2D)* | | Availability: |  |
| Evaluation Workload: |  | | |
| Description of work: | | | |
|  | | | |

1. Désigné ci-après par « objet à certifier » ou « objet à évaluer ». [↑](#footnote-ref-2)
2. *Designated hereafter as “object”, “object to certify” or “object to evaluate”* [↑](#footnote-ref-3)
3. *Class ALC : life cycle support* des Critères communs [↑](#footnote-ref-4)
4. *Computer Emergency Response Team,* Centre gouvernemental de veille, d’alerte et de réponse aux attaques informatique. [↑](#footnote-ref-5)
5. Si « oui », la liste des sites impliqués doit être identifiée dans le présent document (voir le tableau « Evaluation du cycle de vie (classe ALC) » de la section « Programme de travail prévisionnel pour l’évaluation »). [↑](#footnote-ref-6)
6. *If “yes”, the list of all involved sites has to be identified in the document (see the table “****Evaluation of life-cycle support (class ALC)****” in the “Provisional Evaluation Work Program” section).* [↑](#footnote-ref-7)
7. *Target Of Evaluation* [↑](#footnote-ref-8)
8. *Collaborative protection profile* défini dans l’annexe K de l’accord du CCRA [↑](#footnote-ref-9)
9. 7 *Collaborative protection profile* defined in the appendix K of the CCRA [↑](#footnote-ref-10)
10. Une modification de l'évaluation (périmètre, cycle de vie du produit évalué, existence de sites non déclarés, etc.) aura des conséquences contractuelles sur l'évaluation (délais, coûts, etc.) si elle n'a pas été initialement prévue. [↑](#footnote-ref-11)
11. *A change of the evaluation (scope, life cycle of the evaluated product, undeclared site, etc.) will have contractual consequences on the evaluation (deadlines, cost, etc.) if it was not initially planned.* [↑](#footnote-ref-12)
12. *TOE Security Functionality* [↑](#footnote-ref-13)
13. *TSF Interface*. [↑](#footnote-ref-14)