Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Affaire suivie par : Philippe Blot

Paris, le 18 mars 2008

N°549/SGDN/DCSSI/SDR

Processus de qualification d'un produit de sécurité - niveau standard - version 1.1

(Remplace la version 1.0, n° 1591/SGDN/DCSSI/SDR du 23 juillet 2003)

Version	**Modifications**
version 1.1	Principales modifications apportées, suite au retour d'expérience de la mise en œuvre de la version 1.0 : - indication des usages de la qualification au niveau standard, - prise en compte de nouveaux référentiels (référentiels DCSSI, Critères Communs v3.1) et passage au niveau EAL3 augmenté, - nouvelle présentation des jalons par identification des fournitures attendues et du mode de franchissement des jalons, - transformation de certaines tâches d'évaluation en tâches d'expertise.
version 1.0 du 23 juillet 2003	Première version applicable

Sommaire

1. Introduction

1.1. Objectif de la qualification au niveau standard

La sécurisation des systèmes d'information repose en partie sur la mise en œuvre de fonctions techniques, logicielles et matérielles, fournies dans de nombreux cas par des produits de sécurité.

Pour apprécier la robustesse de ces produits, en particulier dès lors qu'ils sont susceptibles de protéger les informations sensibles de l'administration, mais aussi dans le cadre plus général de la sécurisation de l'administration électronique (conformément à l'article 9 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives), la DCSSI procède à leur qualification[1], selon trois niveaux : standard, renforcé et élevé.

Le niveau de robustesse standard, objet du présent processus, est atteint si le produit permet de résister à un attaquant doté d'un potentiel d'attaque élémentaire au sens des Critères Communs. De tels produits peuvent être notamment utiles pour la protection d'informations sensibles[2], ou pour être conformes à un niveau de sécurité donné pour des fonctions de sécurité traitées par le référentiel général de sécurité, conformément à l'ordonnance précitée (en particulier pour satisfaire les exigences du niveau ** des services de confiance de la politique de référencement intersectorielle de sécurité).

Le processus et les exigences définies dans ce processus s'appliquent également, le cas échéant, à des sous-systèmes ou briques techniques de sécurité, qui ne sont pas à proprement parler des produits, mais dont les enjeux de sécurité sont identiques, et pour lesquels le niveau de robustesse doit être attesté par le présent processus de qualification.

1.2. Objectif du document

Ce document définit le processus conduisant à la qualification au niveau standard d'un produit. Il est principalement destiné aux acteurs participant à la procédure de qualification (commanditaires de la qualification, développeurs, évaluateurs, …).

Il présente également les exigences générales applicables à la conception et à l'évaluation des produits visant une qualification au niveau standard. En parallèle, la DCSSI établit des référentiels d'exigences techniques applicables à ces produits, qui sont mis à disposition des acteurs sur internet : http://www.ssi.gouv.fr.

Il concerne de même les maîtrises d'ouvrage et maîtrises d'œuvre de systèmes ayant recours à des produits qualifiés au niveau standard, ainsi que les acheteurs de tels produits.

[1] Les conditions détaillées de l'usage de la qualification sont précisées dans [RÈGLES].

[2] Exemples : informations marquées « Diffusion Restreinte », le cas échéant « Spécial France », informations « Diffusion Restreinte OTAN » ou « Restreint UE », …

2. Documentation applicable

[RÈGLES] : Règles relatives à la qualification des produits de sécurité par la DCSSI, version 1.1, n° 451/SGDN/DCSSI/SDR du 26 février 2004.

[ORDONNANCE] : Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

[DÉCRET] : Décret n° 2002-535 du 18 avril 2002, relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.

[PRIS_RGS] : Politique de référencement intersectorielle de sécurité dans le cadre du référentiel général de sécurité, version 2.1 du 6 novembre 2006

[CC] : Critères Communs version 2.3 d'août 2005, et version 3.1 release 2 de septembre 2007.

[SURVEILLANCE] : Procédure de surveillance des produits certifiés, SUR/P/01.2, n° 3172/SGDN/DCSSI/SDR du 16 novembre 2005.

[CONTINUITÉ] : Procédure de continuité d'assurance, MAI/P/01, n° 417/SGDN/DCSSI/SDR du 4 février 2005.

[RÉFÉRENTIELS] :

- Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard (version mise à jour régulièrement).
- Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques de niveau de robustesse standard (version mise à jour régulièrement).
- Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard (version mise à jour régulièrement).

[FOURNITURES CRYPTO] : Fournitures nécessaires à l'analyse de mécanismes cryptographiques, version 1.2 du 6 novembre 2006, n° 2336/SGDN/DCSSI/SDS.

Ces documents sont accessibles sur http://www.ssi.gouv.fr.

3. Organisation et jalons

3.1. Organisation du projet de qualification

La conduite du processus de qualification au niveau standard s'appuie sur une organisation de projet, dont la conduite est confiée à la DCSSI.

Le groupe projet de la qualification comprend :

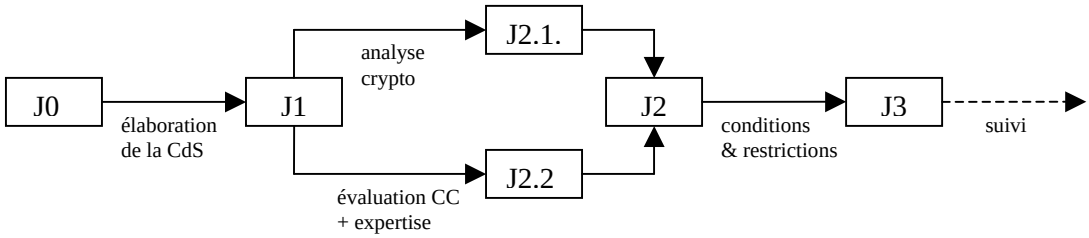
- le chef de projet DCSSI,
- le commanditaire de la qualification, qui peut s'entourer de représentants des utilisateurs du produit,
- le développeur (en fonction de la nature de l'ordre du jour),
- l'évaluateur et le certificateur (dès lors que l'évaluation est engagée).

3.2. Jalons du processus

Dans le cadre du processus de qualification au niveau standard, quatre jalons conduisant à la qualification sont définis :

- J0 : acceptation du projet de qualification,
- J1 : acceptation de la cible de sécurité du produit,
- J2 : acceptation des travaux d'évaluation,
    - J2.1 : analyse des mécanismes cryptographiques,
    - J2.2 : évaluation de l'implémentation matérielle et logicielle : évaluation selon les Critères Communs et expertise,
- J3 : notification de la qualification.

Puis la qualification fait l'objet d'un suivi.



3.3. Interruption du processus de qualification

A tout moment, la DCSSI ou le commanditaire peuvent décider de suspendre ou de mettre fin au processus de qualification. C'est notamment le cas lorsqu'un jalon ne peut être franchi, ou lorsque les coûts et délais nécessaires pour atteindre les objectifs de la cible de sécurité sont jugés excessifs.

3.4. J0 : acceptation du projet de qualification

Fournitures attendues :

Le commanditaire sollicite la DCSSI pour le lancement du processus de qualification, en lui fournissant les informations suivantes :

- le niveau de qualification visé pour le produit, au regard des usages prévus (protection d'informations sensibles, prise en charge à un niveau de sécurité donné de fonctions de sécurité traitées dans le référentiel général de sécurité conformément à [ORDONNANCE], …),
- le calendrier prévisionnel du projet de qualification,

- une première analyse de la problématique de sécurité, en terme de services à rendre par le produit, d'hypothèses d'emploi et de menaces prises en compte par le produit pour protéger ses biens sensibles.

Franchissement du jalon J0 :

Lors de son analyse de la demande, la DCSSI examine notamment la cohérence entre le niveau visé pour le produit et les besoins de l'administration.

La décision d'acceptation ou non du projet est prononcée par la DCSSI.

En cas d'acceptation, l'organisation du projet de qualification est définie en concertation avec les acteurs du projet (cf. §3.1).

La DCSSI peut ne pas accepter le projet lorsque :
- le niveau et les objectifs de sécurité identifiés ne sont pas cohérents avec le besoin de sécurité de l'administration ;
- les responsables techniques du développeur, les matériels, les logiciels et la documentation nécessaires pour réaliser l'évaluation ne sont pas disponibles, et en particulier lorsque les conditions de développement du produit ne garantissent pas l'accès à ces ressources.

Dans le cas où le produit à qualifier fait l'objet d'un marché de développement et de qualification, le jalon J0 doit être de préférence franchi préalablement à la notification du marché.

3.5. J1 : acceptation de la cible de sécurité du produit

Fournitures attendues :

Le commanditaire soumet la documentation suivante à la DCSSI :
- en ce qui concerne le produit, la cible de sécurité établie conformément aux exigences des Critères Communs [CC], et :
  - s'appuyant sur les référentiels techniques de la DCSSI,
  - incluant les concepts d'emploi sur la base de scénarii d'utilisation, plus ou moins détaillés selon que le produit est autonome ou a des interfaces avec d'autres constituants de sécurité,
  - incluant des éléments d'architecture générale matérielle et logicielle du produit,
  - présentant la ou les plate(s)-forme(s) de test pour l'évaluation,
- le cas échéant, si le produit a de fortes adhérences avec le système qui le met en œuvre :
  - une analyse des risques au niveau système,
  - l'architecture générale de sécurité du système.

Franchissement du jalon J1 :

Lors de l'analyse de la documentation fournie, la DCSSI s'assure que le choix des menaces, des hypothèses, des objectifs de sécurité, du périmètre des fonctions évaluées (incluant les fonctions liées aux interfaces externes du produit, notamment en matière d'administration du produit), de la profondeur de l'évaluation, des mécanismes cryptographiques, est en adéquation avec le niveau d'exigences attendu par la DCSSI vis-à-vis du niveau de qualification visé, et respecte les référentiels applicables.

La DCSSI s'assure également que la ou les plate(s)-forme(s) de test pour l'évaluation corresponde(nt) aux architectures de déploiement du produit au sein de l'administration.

L'acceptation de la cible est prononcée formellement par la DCSSI.

3.6. J2 : acceptation des rapports d'évaluation

Deux activités d'évaluations sont conduites pour attester de la satisfaction des objectifs techniques définis dans la cible de sécurité :

- l'analyse des mécanismes cryptographiques, réalisée par la DCSSI,
- l'évaluation de l'implémentation matérielle et logicielle, réalisée par un centre d'évaluation agréé par la DCSSI, et décomposée en deux volets :
    - évaluation du produit selon les Critères Communs,
    - expertise de l'implémentation de la cryptographie.

Chacune d'elles suit des procédures qui leur sont propres, et chaque acceptation fait l'objet d'un jalon particulier.

3.6.1. Analyse des mécanismes cryptographiques

Tout algorithme, mode opératoire ou protocole cryptographique rendant un service de sécurité (par exemple : confidentialité, intégrité, authentification, preuve d'origine, …) décrit dans la cible de sécurité doit faire l'objet d'une analyse réalisée par la DCSSI, en vue d'attester de son respect du référentiel technique cryptographique, conformément à l'exigence du §4.1. Il en est de même pour la génération d'aléa et la gestion des clés utilisées dans des mécanismes cryptographiques.

Il est essentiel que cette analyse se déroule le plus tôt possible dans les phases de définition ou de réalisation du produit.

Afin de répondre aux différentes questions de la DCSSI, le développeur désigne un interlocuteur pour tous les aspects relevant de la cryptographie.

Fournitures attendues :

Le développeur fournit les éléments requis pour l'analyse des mécanismes cryptographiques, conformément à [FOURNITURES CRYPTO].

Franchissement du jalon J2.1 :

L'analyse donne lieu à un rapport établi par la DCSSI, qui met en évidence le niveau de respect des référentiels, et ainsi le niveau de protection atteignable par les services cryptographiques avec, le cas échéant, les conditions associées.

3.6.2. Évaluation selon les Critères Communs et expertise

L'évaluation de l'implémentation matérielle et logicielle est conduite par un centre d'évaluation agréé par la DCSSI, dans le cadre de [DÉCRET].

La référence pour l'évaluation est la version de la cible de sécurité approuvée lors du jalon J1 : si des modifications de la cible de sécurité sont proposées au cours de l'évaluation, elles sont soumises à nouvelle acceptation par la DCSSI.

Fournitures attendues :

Le commanditaire transmet à l'évaluateur :

- les fournitures requises pour les tâches d'évaluation selon les Critères Communs correspondant au paquet d'assurance retenu pour la qualification au niveau standard, précisé au §4.2.1,
- les fournitures requises pour les tâches d'expertise de l'implémentation de la cryptographie, conformément au §4.2.2.

Des rapports intermédiaires (rapports de fin de tâche d'évaluation pour chacune des classes d'assurance et rapport d'expertise de l'implémentation de la cryptographie) sont établis par

l'évaluateur, ainsi qu'un rapport technique d'évaluation en fin d'évaluation. Ce dernier fait apparaître la conformité du produit à sa cible de sécurité, les résultats des tests réalisés, ainsi que les vulnérabilités résiduelles identifiées à partir des résultats de l'évaluation selon les Critères Communs et des résultats de l'expertise de l'implémentation de la cryptographie. Ces rapports sont transmis à la DCSSI.

Franchissement du jalon J2.2 :

Suite à la réception des documents et conformément à l'article 7 du [DÉCRET], la DCSSI délivre un certificat ou refuse la certification. Le rapport de certification précise les restrictions d'usage du produit.

3.7. J3 : notification de la qualification

Fournitures attendues :

La qualification est instruite sur la base des rapports d'évaluation. Elle repose sur l'engagement du commanditaire à conduire les opérations de maintenance, tels que décrits au §3.8.

Franchissement du jalon J3 :

A partir des rapports d'évaluation, la DCSSI juge de la compatibilité des conditions et restrictions résultant de chacune des évaluations, et décide ou non de prononcer la qualification au niveau standard du produit dans sa configuration évaluée. Elle en informe le commanditaire.

La qualification fait état des conditions et restrictions issues du franchissement du jalon J1, ainsi que de celles issues des évaluations. Elle fait également apparaître, le cas échéant, les usages liés à cette qualification :

- protection d'informations sensibles : le domaine des informations pouvant être protégées peut le cas échéant être précisé (informations marquées « Diffusion Restreinte », …),
- prise en charge à un niveau de sécurité donné de fonctions de sécurité traitées dans le référentiel général de sécurité conformément à [ORDONNANCE].

La DCSSI assure la publication de certains éléments relatifs à cette qualification, conformément au §5.

3.8. Suivi de la qualification

La DCSSI a mis en place le processus de qualification afin de disposer de produits de confiance, dans la durée.

Elle impose que le commanditaire établisse avec le centre d'évaluation un contrat de surveillance du certificat telle que prévue dans [SURVEILLANCE], pour s'assurer que le produit, non modifié, conserve ses qualités vis-à-vis de l'évolution de l'état de l'art de la menace.

En cas d'évolution du produit, il est impératif que le développeur mette en œuvre le processus de continuité d'assurance du certificat tel que prévu dans [CONTINUITÉ] pour s'assurer que les modifications apportées ne remettent pas en cause ses qualités.

La DCSSI peut décider à tout moment de retirer une qualification.

4. Référentiels applicables

La DCSSI tient à jour un référentiel des exigences techniques applicables par niveau de qualification : les exigences de [RÉFÉRENTIELS] sont applicables au produit, pour le niveau standard.

En complément, la DCSSI dispose, par type de produits (pare-feu, chiffreur IP, …), de référentiels d'exigences techniques sous forme de Profils de Protection établis au profit de la qualification au niveau standard, et disponibles sur http://www.ssi.gouv.fr. La DCSSI demande aux développeurs de présenter à la DCSSI le positionnement des cibles de sécurité de leurs produits par rapport à ces Profils de Protection.

Dans tous les cas, les exigences ci-après s'appliquent.

4.1. En matière de cryptographie

Les mécanismes cryptographiques et la gestion des clés utilisées par ces mécanismes doivent atteindre le niveau de robustesse standard : les exigences relatives pour ce niveau sont définies dans le référentiel technique cryptographique géré par la DCSSI ([RÉFÉRENTIELS]).

Les fournitures requises pour l'analyse des mécanismes cryptographiques doivent être conformes à [FOURNITURES CRYPTO].

Elles sont exigibles dans tous les cas, y compris lorsque le développeur s'appuie sur une bibliothèque cryptographique ou reprend du code existant.

4.2. En matière d'implémentation matérielle et logicielle

4.2.1. Évaluation du produit selon les Critères Communs

Les fournitures requises sont celles d'une évaluation selon les principes décrits dans [DÉCRET], pour un niveau Critères Communs EAL3 augmenté, conformément aux paquets d'assurance définis ci-après :

- en CC v2.3 : il s'agit du niveau EAL3 augmenté des composants ALC_FLR.3 et AVA_VLA.2, le niveau de résistance des fonctions de sécurité (SOF) requis étant le niveau élevé,
- en CC v3.1 : il s'agit du niveau EAL3 augmenté des composants ALC_FLR.3 et AVA_VAN.3.

Au titre de l'évaluation, l'évaluateur doit s'assurer qu'il n'existe pas de vulnérabilité connue qui remettrait en cause les hypothèses prises sur l'environnement technique du produit, et vérifier que ces hypothèses sont bien déclinées dans la documentation (guides) du produit.

Si la sécurité du produit repose sur une configuration particulière de son environnement d'exploitation, notamment dans le cas où le développeur a adapté le système d'exploitation (choix de packages particuliers, paramétrages, …), l'évaluateur doit compléter les tâches d'évaluation définies par les Critères Communs par une expertise de cette configuration et de ces adaptations. Le besoin de cette expertise est validé lors du franchissement du jalon J1. Ses résultats sont réinjectés dans les tâches d'analyse de vulnérabilité du produit.

La tâche d'analyse des vulnérabilités AVA_VLA.2 ou AVA_VAN.3 prend en compte l'expertise de l'implémentation de la cryptographie décrite ci-après : il est ainsi admis que cette expertise se substitue aux tâches nominalement requises au titre des dépendances prévues par les Critères Communs pour mener l'analyse de vulnérabilité.

4.2.2. Expertise de l'implémentation de la cryptographie

L'implémentation des services cryptographiques concerne à la fois :

1. les fonctions cryptographiques de haut niveau spécifiques au produit (ouverture d'un tunnel, signature d'un message,…), parfois intégrées au sein de services fonctionnels métiers,
2. les briques intermédiaires (S/MIME, IPsec, SSL/TLS, SNMPv3, protocole propriétaire, …),

3. les primitives cryptographiques (AES, SHA, 3DES, RSA, SHA, HMAC, ECDSA, …).

Les fournitures requises sont d'une part les fournitures établies pour l'analyse des mécanismes cryptographiques par la DCSSI (cf. §3.6.1) et d'autre part :

- le code source complet du produit,
- les moyens de compilation (outils, options, …),
- une documentation des interfaces entre les fonctions cryptographiques de haut niveau et les briques intermédiaires, ainsi que les tests et résultats de tests industriels de la conformité de mise en œuvre de ces interfaces et de la bonne gestion des codes retour, notamment des erreurs,
- une documentation des tests unitaires et de leurs résultats déroulés sur les primitives cryptographiques,
- une documentation sur les moyens mis en œuvre pour protéger la confidentialité des clés et autres éléments sensibles en clair, ainsi que l'intégrité de l'ensemble des éléments sensibles : protection du stockage, gestion de la réutilisation des objets, mécanismes d'effacement, …,
- le cas échéant, une documentation relative à la gestion des nombres aléatoires précisant les mécanismes utilisés avant retraitement et pour le retraitement, ainsi que les fonctions du produit qui les utilisent,
- l'accès au développeur pour des discussions techniques.

Les tâches demandées à l'évaluateur au titre de l'expertise sont :

- la compilation du code source afin de s'assurer de sa cohérence avec le produit évalué et également, dans le cas de la réutilisation de bibliothèques cryptographiques ou de code existant, de vérifier que le développeur a bien exploité des codes sources et n'a pas uniquement procédé à la récupération directe de codes précompilés,
- l'analyse de conformité des mécanismes cryptographiques et de gestion des clés effectivement implémentés avec [FOURNITURES CRYPTO] et, dans le cas de recours à une bibliothèque cryptographique ou de code existant, la vérification de leur bonne utilisation (cela recouvre à la fois la mise en œuvre des mécanismes cryptographique et de gestion des clés conformément à ce qui a été déclaré dans [FOURNITURES CRYPTO], mais aussi le respect des recommandations d'usage dans le cas d'une bibliothèque ou de code publics et des conditions de validité énoncées dans son rapport de certification pour une bibliothèque ou du code existant ayant fait l'objet d'une évaluation),
- la validation de la conformité des primitives et des modes cryptographiques (recalage cryptographique),
- l'analyse du code source pour détecter des anomalies évidentes de codage d'une part, et d'autre part vérifier le respect des exigences de gestion des clés (stockage, effacement, …),
- si cela est applicable, la vérification de l'implémentation de la génération d'aléa, des tests statistiques sur l'aléa produit avant retraitement cryptographique, la vérification des fonctions de retraitement, et la vérification de l'exhaustivité de la liste fournie des fonctions appelant les fonctions de génération d'aléa.

Les résultats de l'expertise sont consignés dans un rapport d'expertise de l'implémentation de la cryptographie.

4.3. Documentation

La documentation nécessaire à la conduite de la qualification d'un produit de sécurité, et en particulier des différentes évaluations, est fournie en langue française.

Les rapports d'évaluation sont établis en français.

5. Protection, publication et exploitation des résultats

5.1. Protection des développements et des résultats des évaluations

La documentation de développement du produit n'est pas rendue publique.

La documentation d'évaluation n'est pas rendue publique (dans le respect de l'art. 6 du [DÉCRET]).

Les vulnérabilités identifiées pendant l'évaluation ou en maintenance sont :

- soit corrigées, ceci pouvant conduire l'évaluateur à demander, en coordination avec la DCSSI, une reprise d'évaluation,
- soit prises en compte au niveau des restrictions d'usage du produit,
- soit ignorées car hors cible ou hors objectifs de sécurité (risques résiduels acceptés).

La DCSSI juge de l'opportunité d'informer de ces vulnérabilités les utilisateurs du produit qualifié.

5.2. Publication des qualifications

Sauf avis contraire du développeur ou du commanditaire, le certificat obtenu au titre de [DÉCRET] est publié par la DCSSI, avec le rapport de certification, la cible de sécurité, et éventuellement la documentation d'accompagnement requise (documentation d'installation du produit, …).

En complément, la DCSSI gère au profit des administrations un catalogue des produits de sécurité à usage gouvernemental, qui comprend l'ensemble des produits qualifiés ou en cours de qualification.

Dans ce catalogue figurent, outre les informations directement liées au processus de qualification (cible de sécurité du produit, rapport de certification, attestation de qualification), des informations relatives :

- aux performances des produits (débits, MTBF, dimension, poids, …),
- aux coûts des produits (ainsi que de leurs éventuels périphériques ou des équipements requis pour leur mise en œuvre, de leur maintenance, …),
- aux délais d'approvisionnement,
- aux contacts commerciaux du développeur.

La DCSSI demande aux développeurs de lui fournir les informations utiles pour la constitution de ce catalogue.

Les produits sont intégrés dans le catalogue dès lors que la réunion de lancement de l'évaluation selon les Critères Communs a été menée.

Le catalogue des produits qualifiés ou en cours de qualification au niveau standard, est mis à disposition du public par publication sur http://www.ssi.gouv.fr.

5.3. Exploitation des résultats

En vue de constituer ou d'améliorer les référentiels d'exigences techniques de sécurité, la DCSSI se réserve le droit de réutiliser les résultats des qualifications (cibles de sécurité, résultats de travaux d'évaluation, …).