PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, le 2 mars 2021

N° **466/ANSSI/SDE/PSS/CCN**

Référence **: ANSSI-CSPN-NOTE-06 v1.0**

NOTE D'APPLICATION

METHODOLOGIE D'EVALUATION CSPN POUR LES LOGICIELS DEPLOYES SUR DES INFRASTRUCTURES DE *CLOUD COMPUTING*

Application **:** Dès son approbation.

Diffusion **:** Publique

Le sous-directeur « Expertise »
de l'Agence nationale de la sécurité
des systèmes d'information

Renaud LABELLE
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

SUIVI DES MODIFICATIONS

Version	Date	Modifications
1.0	02/03/2021	Version initiale

En application du décret n°2002-535 du 18 avril 2002 modifié, la présente note a été soumise, lors de sa création, au comité directeur de la certification, qui a donné un avis favorable.

Cette note est également soumise pour avis lors de chaque modification majeure conformément au manuel qualité du centre de certification. Les évaluations mineures ne sont pas soumises au comité directeur de la certification.

La présente note est disponible en ligne sur le site institutionnel de l'ANSSI (www.ssi.gouv.fr).

TABLE DES MATIERES

1 Contexte et périmètre

La présente note vise à étendre la méthodologie CSPN au contexte du *Cloud Computing*, ou informatique en nuage[1].

La méthode CSPN présuppose que le produit évalué est mis en œuvre sous le contrôle direct de ses utilisateurs et administrateurs (c'est-à-dire les bénéficiaires de la sécurité rendue par le produit). Or, si ce présupposé est valide pour un logiciel installé et administré directement par l'utilisateur, ce n'est plus vrai dans le cas de logiciels fournis *en tant que service (SaaS[2])*.

Cette note définit donc des activités additionnelles permettant d'adapter la méthode CSPN aux logiciels ayant vocation à être fournis *en tant que service*. Elle affine les exigences de la méthodologie générique [CRI-CSPN].

La présente note ne concerne pas la certification de services, ni plus généralement la certification d'activités de prestataires de services d'informatique en nuage[3].

1.1 Notions générales

Bénéficiaire : le bénéficiaire désigne la personne morale (organisation, entité, etc.) ou physique (particulier) qui utilise la TOE *en tant que service (SaaS)* et qui tire, en tant qu'utilisateur, un « bénéfice sécuritaire » de la certification de la TOE.

Commanditaire : le commanditaire désigne l'organisation qui demande la certification à l'ANSSI et qui finance la prestation d'évaluation[4].

Développeur : le développeur désigne l'organisation qui spécifie, élabore et maintient la TOE[5].

Infrastructure technique : l'infrastructure technique désigne l'ensemble des composants matériels et logiciels nécessaires à la mise à disposition de ressources affectées à la demande (virtualisées ou non). Sur cette infrastructure vont typiquement s'exécuter des systèmes d'exploitation, éventuellement des intergiciels ou logiciels de base, et enfin la TOE.

Intégrateur du produit certifié : l'intégrateur désigne l'organisation qui fournit le produit certifié, en tant que service, au bénéficiaire. Il est notamment chargé d'installer et paramétrer la TOE.

Fournisseur du socle : le fournisseur du socle désigne l'organisation qui fournit le socle technique utilisé par l'intégrateur, le cas échéant, *en tant que service*.

MCO/MCS : maintien en conditions opérationnelles et maintien en conditions de sécurité.

Prestataire : le prestataire[6] désigne une organisation différente du bénéficiaire qui joue un rôle dans la mise en œuvre de la TOE. Ses activités sont vendues au bénéficiaire sous forme de service.

TOE : logiciel soumis à l'évaluation (*Target of Evaluation*).

1.2 Rôles

De nombreux types d'utilisateurs, avec des rôles divers, sont susceptibles d'interagir avec la TOE ou son environnement. La figure suivante donne une vue d'ensemble de ces rôles utilisateur :

---

[1] Modèle permettant un accès aisé, généralement à la demande, et au travers d'un réseau, à un ensemble de ressources informatiques partagées et configurables.

[2] *Software as a Service* : service mis en œuvre par un prestataire consistant en la fourniture d'un logiciel utilisable à distance, le plus souvent via un navigateur web.

[3] A titre d'information, Le référentiel [SecNumCloud] de l'ANSSI permet la qualification de prestataire de services de type *IaaS*, *PaaS* et *SaaS*.

[4] A ne pas confondre avec le commanditaire au sens de SecNumCloud : dans le référentiel d'exigences des prestataires de services d'informatique en nuage (SecNumCloud), le commanditaire est l'entité faisant appel à un prestataire de services d'informatique en nuage. Dans la présente note, ce rôle est désigné par le terme d'intégrateur.

[5] Les mécanismes de virtualisation et les systèmes d'exploitation ne sont pas visés par cette note.

[6] A ne pas confondre avec le prestataire au sens de SecNumCloud : dans le référentiel d'exigences de prestataires de services d'informatique en nuage (SecNumCloud), le prestataire est l'organisme proposant un service d'informatique en nuage. Dans la présente note, ce rôle peut être désigné par le terme de fournisseur du socle.

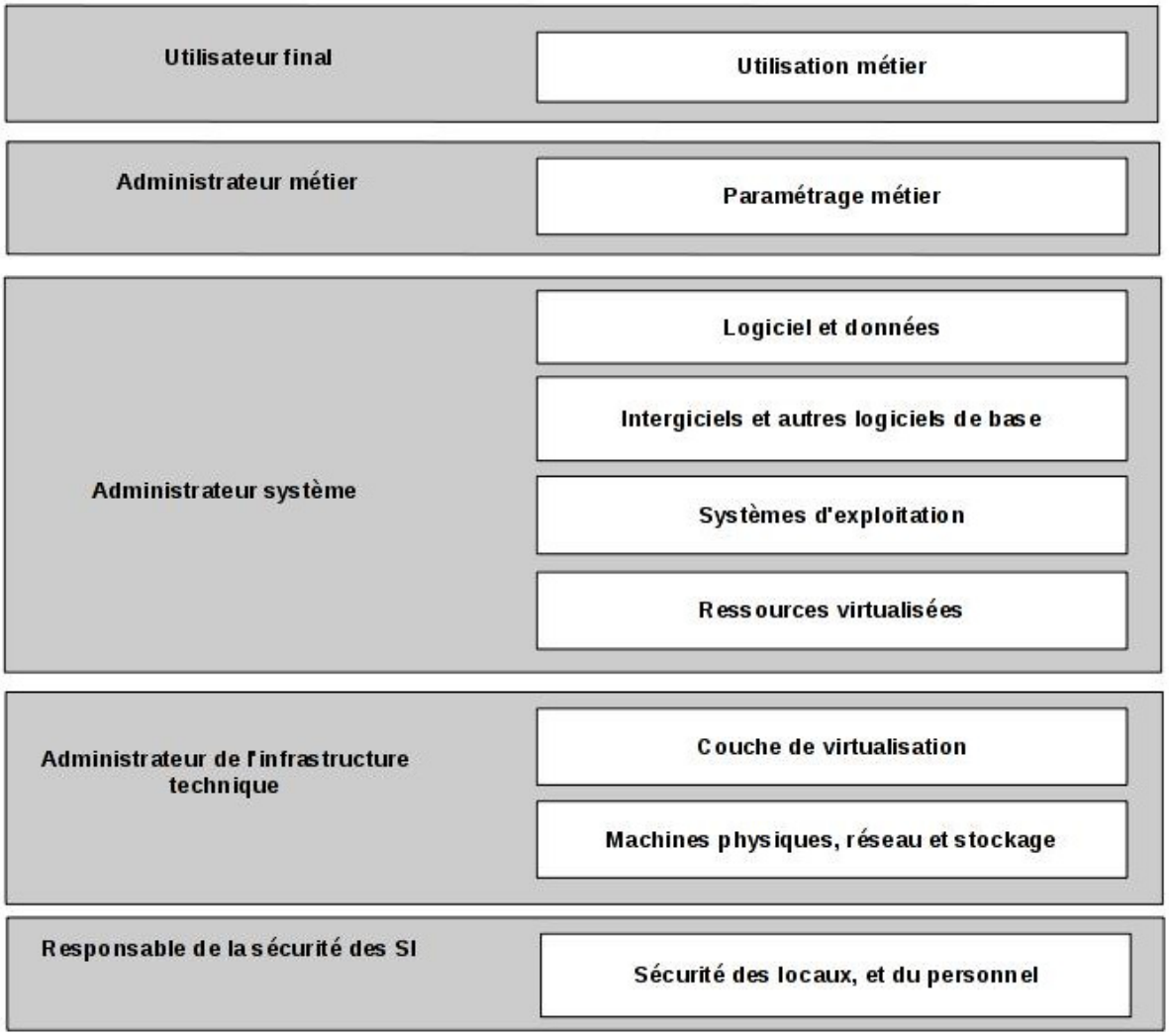

Figure 1 : Rôles utilisateurs vis-à-vis de la TOE

Utilisateur final : on inclut dans ce rôle l'ensemble des utilisateurs qui utilisent la TOE de façon non privilégiée.

Administrateur : on inclut dans ce rôle l'ensemble des utilisateurs disposant de droits privilégiés sur un système d'information, chargés des actions d'administration[7] ou de maintenance sur celui-ci, responsable d'un ou plusieurs domaines techniques. On distinguera :

- **l'administrateur métier** qui est en charge de l'administration au sens fonctionnel du terme. C'est un utilisateur disposant de droits étendus sur la TOE, lui permettant de paramétrer l'utilisation qui peut en être faite par les utilisateurs finaux, ou de gérer les comptes d'utilisateurs finaux ;
- **l'administrateur système** qui est en charge de la gestion des ressources logiques supportées par l'infrastructure technique du service. L'administration système peut concerner des ressources abstraites (machines virtuelles, réseaux virtuels, etc.), des systèmes d'exploitation, des intergiciels (ou *middlewares*), etc. ;
- **l'administrateur de l'infrastructure technique** qui est en charge de la gestion et du MCO/MCS de l'infrastructure technique du service.

Officier de sécurité : on inclut dans ce rôle l'ensemble des utilisateurs disposant des responsabilités ayant trait à l'environnement des infrastructures techniques de la TOE. Cela inclut typiquement le personnel ou la sécurité physique des locaux.

[7] Installation, suppression, modification ou consultation d'une configuration d'un composant du système d'information, susceptible de modifier le fonctionnement ou la sécurité de celui-ci.

1.3 Acteurs

Les rôles définis précédemment sont associés à l'un ou l'autre des trois acteurs suivants :

- **le bénéficiaire** qui comprend, au minimum, le rôle d'utilisateur final de la TOE et tout ou partie le rôle d'administrateur métier ;
- **l'intégrateur** du produit certifié qui comprend le rôle d'administrateur système quand il gère le socle technique lui-même ou une partie du rôle d'administrateur système quand il s'appuie sur un socle technique fourni en tant que service (*IaaS*[8], *CaaS*[9] ou *PaaS*[10]) ;
- **le fournisseur du socle** qui comprend le rôle d'administrateur de l'infrastructure technique et le rôle d'officier de sécurité. Dans les cas où le socle technique est fourni en tant que service à l'intégrateur, il comprend aussi une partie du rôle d'administrateur système.

1.4 Hébergement

La note distingue deux types d'hébergements illustrés par la figure 2 :

- *On Premise* : On parle d'hébergement *On Premise* quand une même organisation assure l'ensemble des rôles. Dans ce type d'hébergement, l'organisation du bénéficiaire a un contrôle direct sur l'intégralité de l'environnement11 : elle peut et doit s'assurer que les hypothèses portant sur l'environnement de la TOE, définies dans sa cible de sécurité, sont satisfaites ;
- *Cloud* : on parle d'hébergement *Cloud* dans tous les autres cas de figure. Dans ces cas, tout ou partie du socle technique est fourni au bénéficiaire, en tant que service, par un intégrateur ou un fournisseur de socle[12]. Il faut, dans ce cas, que ce dernier les implique dans la vérification des hypothèses, ce que la méthode CSPN ne prévoit pas par défaut. La note distinguera par la suite :
    - le *Cloud* privé où l'infrastructure technique est dédiée au bénéficiaire ;
    - le *Cloud* non privé où l'infrastructure technique est partagée avec des entités ayant des intérêts en commun avec le bénéficiaire (*Cloud* dit « communautaire »), ou n'ayant potentiellement aucun rapport avec le bénéficiaire (*Cloud* dit « public »)[13].

[8] ***Infrastructure as a Service (IaaS) :*** le fournisseur de socle met à disposition de différents intégrateurs un ensemble de ressources matérielles sous forme abstraite (machines virtuelles) ou sous forme réelle (serveurs dits « *Bare Metal* »).

[9] ***Containers as a Service (CaaS) :*** le fournisseur de socle met à disposition des différents intégrateurs des conteneurs. Les conteneurs sont des environnements d'exécution distincts reposant sur des mécanismes d'abstraction gérés au niveau d'un système d'exploitation.

[10] ***Platform as a Service (PaaS) :*** le fournisseur de socle met à disposition des différents intégrateurs des « environnements-types » prêts à l'usage, permettant le développement et le déploiement direct d'applications.

[11] Un hébergement *On Premise* permet tout de même le recours à des sous-traitants ou des prestations d'infogérance, de même qu'il permet le déploiement sur des ressources mutualisées (hyperviseurs, baies de stockage partagées, etc.). Plus généralement, le mode *On Premise* désignera aussi les déploiements dans des *cloud privés*, s'ils sont sous le contrôle direct du bénéficiaire.

[12] L'intégrateur comme le fournisseur de socle sont alors des prestataires du bénéficiaire.

[13] De ce point de vue, un cloud dit « privé virtuel » sera considéré comme public ou communautaire selon les liens d'intérêt entre bénéficiaires, et non comme un cloud privé.

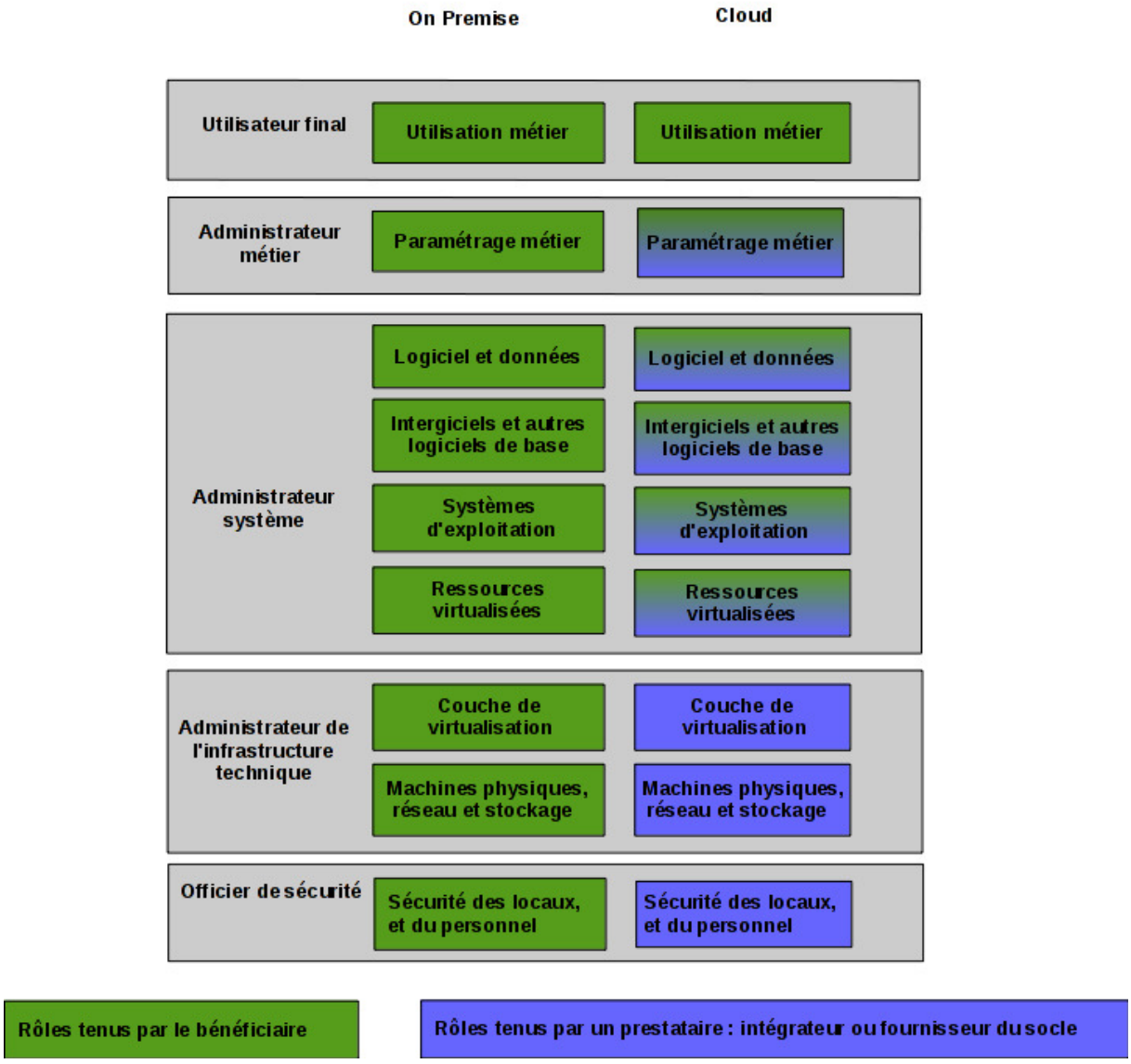

Figure 2 : Modes d'hébergement de la TOE

Dans le cas d'un hébergement *Cloud*, qu'il soit privé ou non, l'intégrateur s'appuie sur un socle lui-même fourni en tant que service (*IaaS*, *CaaS* ou *PaaS*) dont le choix influe sur la répartition des rôles entre les acteurs, comme le montre la figure 3.

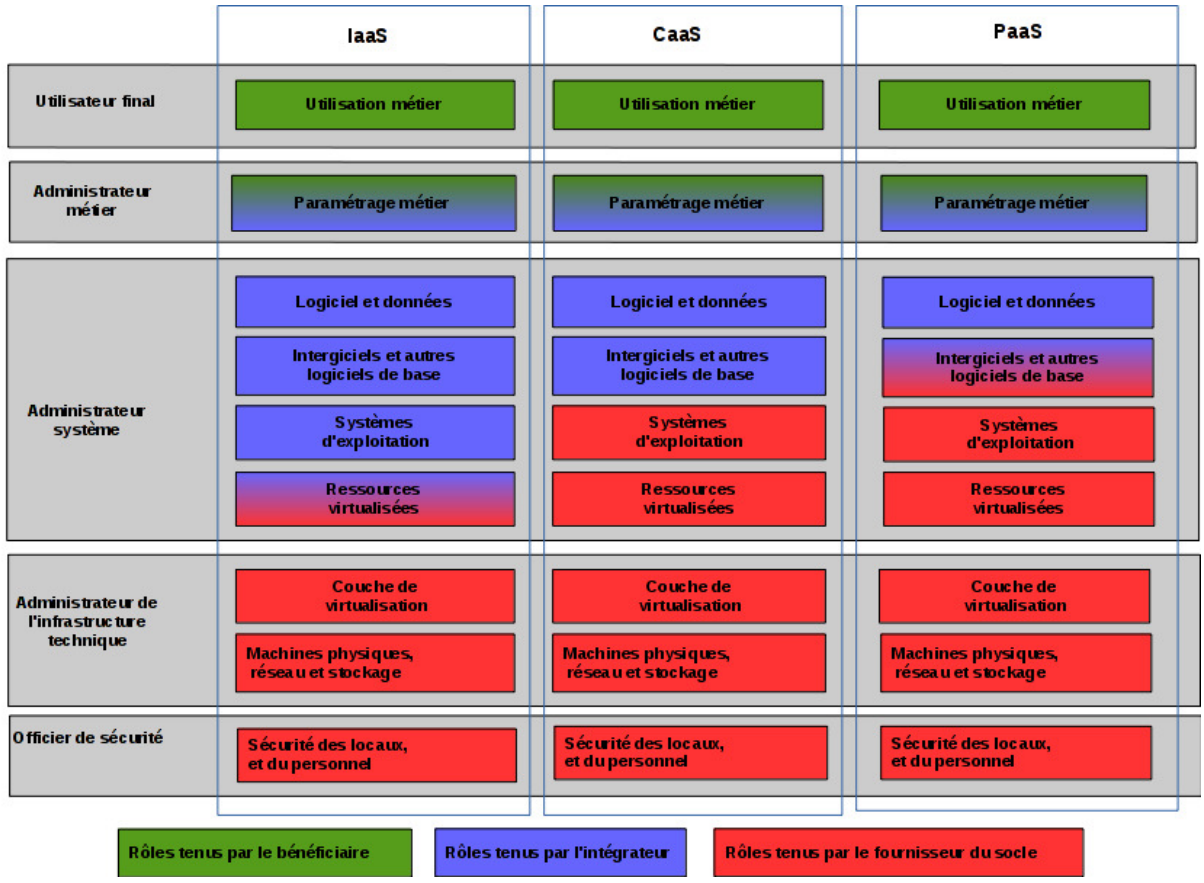

Figure 3 : Répartition des rôles entre acteurs en hébergement *Cloud*

1.5 Principes d'architecture (Single ou Multi-tenant)

La note distingue deux principes d'architecture parmi les TOE soumises à évaluation.

Au sens premier, le *tenant* désigne le locataire d'une infrastructure partagée ; ce terme désigne par extension l'ensemble des ressources qui lui sont allouées. En dérivent les termes :

- *Single-tenant* : principe d'architecture de la TOE où chaque bénéficiaire dispose de son propre *tenant* ; en d'autres termes, il existe une instance de la TOE par bénéficiaire. Le cloisonnement entre bénéficiaires est typiquement assuré par le socle, et non par le produit lui-même (conteneurs, virtualisation, serveurs différents, etc.) ;
- *Multi-tenant* : principe d'architecture de la TOE où une seule instance de celle-ci est utilisée par plusieurs bénéficiaires. Entre autres conséquences, cela impose au produit lui-même d'assurer le cloisonnement entre les différents bénéficiaires du service.

2 Exigences pour l'évaluation de la TOE

Les sections ci-après ajoutent à la méthode [CSPN] certaines exigences. Ces exigences sont classées selon la phase concernée.

2.1 Phase 1 – Analyse de la cible de sécurité

2.1.1 Identification non ambiguë du produit

Le nom du produit soumis à évaluation doit être désigné comme

Logiciel *[sélectionner parmi :* ***single–*** *et/ou* ***multi–]tenant*** *[nom du logiciel]* **en tant que service (SaaS) version** *[…]*

En hébergement *[sélectionner parmi :*

- ***On Premise ;*** *ou*
- ***Cloud*** *[sélectionner parmi :* **privé** *ou* **non privé***]*, **sur socle** *[sélectionner parmi :* **IaaS** *et/ou* **CaaS** *et/ou* **PaaS***]*

].

Exemple : **Logiciel *multi–tenant XXX* en tant que service (SaaS) version Y.Z, en hébergement *Cloud* privé sur socle PaaS.**

Un produit peut viser plusieurs types de déploiement (par exemple en hébergement *On Premise* ou en *Cloud* privé). Dans ce cas, l'évaluateur devra appliquer la méthodologie relative aux gammes de produits, décrite dans la [NOTE-21].

2.1.2 Argumentaire d'un produit

Seul le logiciel peut être soumis à évaluation. Les couches sous-jacentes sont hors-périmètre.

2.1.3 Environnement technique de fonctionnement du produit

La cible de sécurité décrit l'environnement technique du produit, sans préjuger du fait qu'il soit ou non « de confiance »[14]. Ainsi, la cible devra par hypothèse décrire quel est l'environnement attendu en matière de système d'exploitation, mais aussi d'intergiciels de mécanismes de virtualisation, etc.

De plus, les hypothèses devront décrire quelle solution d'hébergement est recommandée, en cohérence avec l'identification[15]. Lorsque le produit a recours à un service *CaaS*, *PaaS* ou *IaaS*, l'hypothèse doit mentionner que ce service est considéré par principe comme étant « de confiance ».

Quel que soit le mode d'hébergement, le socle ou le mode retenu, le développeur peut être amené à émettre des guides ou recommandations à destination des différents rôles (utilisateur final, administrateur métier, administrateur système, administrateur de l'infrastructure technique, officier de sécurité). Tous les guides et recommandations disponibles doivent être soumis à l'évaluateur.

La cible devra clarifier la répartition des rôles entre acteurs, sur le modèle de la figure 3. Dans la mesure où la figure 3 laisse une certaine marge dans la répartition des rôles, la cible devra clarifier de façon non ambiguë où s'arrêtent les responsabilités respectives du bénéficiaire, de l'intégrateur et du fournisseur de socle.

2.1.4 Biens sensibles devant être protégés

Les biens sensibles doivent être identifiés comme :

[14] Par exemple, la cible ne dit pas que « le système d'exploitation est de confiance », mais peut par exemple faire l'hypothèse que le système d'exploitation est une version *Debian LTS* en cours de support, à jour de ses correctifs de sécurité.

[15] Par exemple, pour un produit identifié comme « en hébergement *Cloud* public sur socle *CaaS* », les hypothèses devront indiquer le ou les services *CaaS* recommandés. Le développeur est invité à vérifier attentivement si la définition de cloud « privé » de son fournisseur correspond bien à celle que retient cette note.

- un bien sensible de l'utilisateur final de la TOE[16] ; ou
- un bien sensible de l'administrateur métier de la TOE[17] ; ou
- un bien sensible de la TOE elle-même[18].

La TOE étant limitée au logiciel, elle n'a en particulier pas vocation à protéger les biens sensibles de l'administrateur système ou de l'administrateur d'infrastructure technique.

Si la TOE protège des biens du prestataire plutôt que des utilisateurs finaux et administrateurs, alors le produit n'est pas à considérer comme un produit *Cloud*. Une évaluation suivant la méthode générale CSPN est suffisante – le nom du produit évalué ne pourra en revanche pas mentionner les termes *Cloud, SaaS, PaaS, CaaS ou IaaS*.

2.1.5 Mesures d'environnement

L'évaluateur doit s'assurer que les hypothèses décrites dans la cible de sécurité sont identifiées comme :

- une déclaration signalant qu'un rôle donné est considéré « de confiance ». De telles hypothèses seront faites notamment pour les administrateurs, car la TOE étant limitée au logiciel, elle ne peut se prémunir contre les administrateurs (métier, système ou d'infrastructure) ;
- une tâche permettant de placer le produit dans une configuration sûre recommandée par le commanditaire. Ces tâches devront être décrites selon la typologie suivante :
    - Tâches de l'utilisateur final de la TOE[19],
    - Tâches de l'administrateur métier de la TOE[20],
    - Tâches de l'administrateur système :
        - Administration du logiciel et des données[21],
        - Administration des intergiciels[22],
        - Administration des systèmes d'exploitation[23],
        - Administration des ressources virtualisées[24] ;
    - Tâches de l'administrateur d'infrastructure technique :
        - Administration de la couche de virtualisation[25],

[16] Exemple : dans le cas d'une messagerie sécurisée en déploiement SaaS, les biens sensibles de l'utilisateur seraient les messages échangés.

[17] Exemple : dans le cas d'une messagerie sécurisée en déploiement SaaS, les biens sensibles de l'administrateur métier pourraient être son mot de passe ou sa clé de connexion SSH.

[18] Exemple : dans le cas d'une messagerie sécurisée en déploiement SaaS, les biens sensibles de la TOE pourraient inclure des clés de session pour des canaux sécurisés, ou encore les journaux de la TOE.

[19] Exemple : « l'utilisateur final suit les règles ANSSI pour construire un mot de passe robuste et s'assure que ce mot de passe n'est partagé avec d'autres utilisateurs ».

[20] Exemple : « L'administrateur métier accède à l'interface d'administration depuis un poste dédié à cet usage ».

[21] Exemple : « l'administrateur système vérifie que la signature de la TOE est correcte avant de l'installer ».

[22] Exemple : « l'administrateur système vérifie que la base de données est paramétrée de façon à activer le chiffrement des données » ou encore « L'administrateur système s'assure que le serveur web s'exécute avec des droits utilisateur restreints ».

[23] Exemple : « l'administrateur système vérifie que l'OS est à jour des patches de sécurité ».

[24] Exemple : « l'administrateur système doit configurer les groupes de sécurité réseau de façon à ne permettre que les flux identifiés dans le §X du guide YYY ».

[25] Exemple : « l'administrateur d'infrastructure technique doit s'assurer que l'hyperviseur est à jour des patches de sécurité ».

- Administration de l'environnement physique[26] ;

- Tâches de l'officier de sécurité[27].

Aucun autre type d'hypothèse ne doit être présent dans la cible.

2.1.6 Description des menaces

La cible doit considérer trois grandes catégories de menaces :

- la cible doit inclure les menaces hors-bénéficiaires (attaques provenant d'un individu non bénéficiaire cherchant à compromettre un bien sensible de la TOE ou du bénéficiaire) ;
- si le bénéficiaire est une organisation multi-utilisateurs, la cible doit inclure les menaces intra-bénéficiaires (attaques provenant d'utilisateurs appartenant au bénéficiaire, dans l'objectif de compromettre des biens sensibles de la TOE, ou d'un autre utilisateur du même bénéficiaire) ;
- si la TOE vise un hébergement en *Cloud non privé,* ou si elle implémente une *architecture multi-tenant*, la cible doit inclure les menaces inter-bénéficiaires (attaques provenant d'un bénéficiaire, dans l'objectif de compromettre un autre bénéficiaire).

2.1.7 Description des fonctions de sécurité

Afin de couvrir de la façon la plus claire le problème de sécurité du produit, la description des fonctions de sécurité doit clairement faire apparaître les mécanismes de cloisonnement de la TOE. Ainsi, les fonctions suivantes devront impérativement faire partie de la cible de sécurité :

Couverture des menaces	Obligatoire ou optionnel	Fonctions requises
Hors-bénéficiaires	Obligatoire	**Identification et authentification du bénéficiaire** (ou de chaque utilisateur[28] appartenant au bénéficiaire, s'il s'agit d'une organisation)
Intra-bénéficiaires	si le bénéficiaire est une organisation multi-utilisateurs	**Contrôle d'accès et gestion des droits/privilèges entre utilisateurs[29] appartenant au bénéficiaire**

Tableau 1 : Synthèse des fonctions de sécurité obligatoires pour la TOE

2.2 Phase 2 – Installation du produit

L'évaluateur doit installer le produit sur la base des guides, afin d'estimer la sécurité de ce processus, et notamment le risque de dégradation accidentelle de la sécurité lors de l'installation. Le développeur doit assister à cette phase, afin de signaler les erreurs éventuelles que commettrait l'évaluateur[30]. Le cas échéant, ces erreurs sont documentées dans le RTE au titre de l'analyse de la « Mise en œuvre du produit » (voir §3.1.2 de [RTE]) et le développeur mettra à jour ses guides en conséquence.

L'installation effectuée par l'évaluateur sera impérativement une installation locale au CESTI (typiquement un déploiement dans une machine virtuelle, sur un serveur maîtrisé par le CESTI), même si la cible de sécurité vise un déploiement sur un service *Cloud* commercial.

[26] Exemple : « l'administrateur d'infrastructure technique doit vérifier que les interfaces d'administration des équipements sont accessibles uniquement aux personnels habilité ».

[27] Exemple : « l'officier de sécurité s'assure que les personnels habilités à effectuer des opérations d'administration sont de confiance » ou encore « l'officier de sécurité s'assure que les locaux sont protégés contre les intrusions ».

[28] Ces utilisateurs pouvant être des utilisateurs finaux ou des administrateurs métiers.

[29] Idem.

[30] Dans certains cas, comme celui des produits *On Premise*, l'installation peut devenir très complexe car elle implique la mise en œuvre de l'intégralité de l'infrastructure technique. Il est envisageable d'accepter au cas par cas que le développeur participe directement à l'installation. Cependant, l'installation devra bien être effectuée spécialement pour l'évaluation (l'évaluateur ne travaille pas sur un système déjà installé).

A l'issue de l'installation, l'évaluateur doit décrire précisément les configurations de test dans le RTE, incluant au minimum :

- un diagramme de réseau logique (correspondant aux informations de la couche 3 : adressage, masques, identifiants de réseaux virtuels, etc.) ;
- les références et versions des machines physiques et virtuelles utilisées ;
- les composants déployés sur chaque machine (identifiants et versions de systèmes d'exploitation).

L'évaluateur doit s'assurer que l'affichage de la version du logiciel est accessible à tous les rôles, depuis l'administrateur de l'infrastructure technique jusqu'à l'utilisateur du logiciel. Toutes les procédures d'identification sont décrites dans le RTE.

2.3 Phase 7 – Analyse de vulnérabilité

L'évaluateur devra porter la plus grande attention aux déploiements prévus par la cible, afin de détecter s'ils :

- permettent des configurations non sûres par construction ;
- incluent des hypothèses cachées qu'il convient d'expliciter ;
- s'appuient sur des hypothèses abusives non réalisables en pratique ;
- etc.

Cette vérification pourra nécessiter pour l'évaluateur de stresser l'environnement IT du produit, afin de s'assurer de la pertinence du déploiement, ou encore effectuer une recherche de vulnérabilités publiques sur certains éléments de l'environnement IT, en particulier s'ils sont nécessaires au bon fonctionnement de la TOE et s'ils ont un impact fort sur la sécurité[31].

En revanche, le recours à des services *CaaS*, *PaaS* ou *IaaS* constituent une limite « dure » de l'évaluation : la cible fera l'hypothèse que ce service est de confiance, et cette hypothèse ne sera pas questionnée par l'évaluateur. Le rapport de certification pourra rappeler aux utilisateurs que le certificat obtenu n'a de sens que s'ils ont confiance en ce service, qui n'a pas été évalué lors de la CSPN.

[31] En pratique, cela signifie que si la cible impose une technologie précise pour ses couches sous-jacentes, l'évaluateur devra s'assurer que ces technologies disposent d'un suivi de sécurité. De la même manière, si la cible impose une version précise de ces technologies, l'évaluateur devra vérifier si des vulnérabilités existent sur ces versions. Toutes ces vérifications sont imposées, bien que les couches sous-jacentes en question soient au sens strict hors-périmètre. En effet, il ne serait pas acceptable qu'un produit, même sûr, impose à l'utilisateur d'être déployé sur une couche sous-jacente entraînant des failles de sécurité.

3 Règles d'usage du certificat

3.1 Responsabilité du commanditaire et du développeur

Le développeur et le commanditaire s'engagent à travers la signature du dossier d'évaluation, à communiquer clairement sur le fait que seul le déploiement évalué est visé par la version certifiée du produit. Ils s'engagent également à ce que toute modification ultérieure du produit soit matérialisée par un changement de la version affichée aux différents rôles.

3.2 Responsabilité des acteurs

3.2.1 Maîtrise des prestataires

Les restrictions d'usage et recommandations listées dans le rapport de certification doivent être mises en œuvre par les rôles auxquels elles s'adressent. Ces restrictions d'usage et recommandations incluent en particulier le respect de la cible de sécurité, qui impose, à travers ses mesures d'environnement (voir 2.1.5), des exigences applicables à :

- l'utilisateur final du logiciel ;
- l'administrateur métier ;
- l'administrateur système ;
- l'administrateur d'infrastructure technique ;
- l'officier de sécurité.

Il est de la responsabilité du bénéficiaire de faire respecter ces exigences par tous les acteurs assumant ces rôles, même s'il s'agit de prestataires. Pour ce faire, il pourra être amené à imposer :

- des exigences contractuelles spécifiques pour le prestataire ;
- si nécessaire, une démarche d'évaluation ou d'audit des activités du prestataire.

3.2.2 Analyse de la cible et installation du produit

En début d'évaluation, l'analyse de la cible et l'installation du produit sont menées en parallèle.

L'évaluateur a l'obligation d'analyser la phase d'installation du produit, sur la base des guides destinés à l'intégrateur ou au fournisseur du socle, afin d'estimer la sécurité de ce processus, et notamment le risque de dégradation accidentelle de la sécurité lors de l'installation.

Le développeur assiste à cette phase, sans procéder à l'installation lui-même. Le développeur doit signaler les erreurs éventuelles que commettrait l'évaluateur. Le cas échéant, ces erreurs seront documentées dans le RTE au titre de l'analyse de la *Mise en œuvre du produit* (voir §3.1.2 de [RTE]) ou conduise à une mise à jour des guides.

ANNEXE A. Références

Référence	Document
[CRI_CSPN]	Procédure – Critères pour l'évaluation en vue d'une Certification de sécurité de premier niveau, ANSSI-CSPN-CER-P-02, version en vigueur.
[SecNumCloud]	Prestataires de services d'informatique en nuage (SecNumCloud) – référentiel d'exigences, version 3.1 du 11 juin 2018.
[NOTE-21]	Note d'application – Méthodologie pour l'évaluation d'une gamme de produits, ANSSI-CC-NOTE-21, version en vigueur.

La plupart de ces documents peuvent être consultés et téléchargés depuis le site de l'ANSSI (www.ssi.gouv.fr).