LA CERTIFICATION DE SÉCURITÉ DE PRODUITS

PAR L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ANSSI)

VISA DE SÉCURITÉ

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI

VISA DE SÉCURITÉ

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION · ANSSI ·

LES VISAS DE SÉCURITÉ ANSSI RÉPONDENT À TROIS OBJECTIFS

1

DES OBJECTIFS RÉGLEMENTAIRES :

pour répondre aux règlements nationaux ou européens qui imposent l'utilisation de solutions garantissant un niveau de robustesse éprouvé ;

2

DES OBJECTIFS CONTRACTUELS :

pour répondre aux donneurs d'ordres publics ou privés qui exigent que les solutions utilisées aient préalablement obtenu un Visa de sécurité ANSSI ;

3

DES OBJECTIFS COMMERCIAUX :

pour permettre à un fournisseur de produits ou à un prestataire de services, ainsi qu'aux utilisateurs finaux de ces solutions, de se démarquer de la concurrence par la garantie d'un certain niveau de robustesse.

« Les Visas de sécurité sont un atout de compétitivité pour les fournisseurs de solutions de sécurité et un gage de sécurité pour les utilisateurs. »

Dans une société où le numérique devient omniprésent, nous apprécions quotidiennement les formidables opportunités qu'il offre. Mais cette transformation est également porteuse de menaces qui n'ont de cesse de s'accroître en nombre, en efficacité et en sophistication.

Alors que le risque touche sans distinction administrations, entreprises et citoyens, il est impératif de prendre conscience de l'importance vitale que revêt la mise en place de solutions adaptées pour sécuriser au juste niveau ses systèmes d'information. **MAIS SI LES SOLUTIONS DE CYBERSÉCURITÉ DISPONIBLES SUR LE MARCHÉ SONT NOMBREUSES ET VARIÉES, TOUTES N'OFFRENT PAS LE MÊME NIVEAU D'EFFICACITÉ ET DE ROBUSTESSE.**

C'est la raison pour laquelle l'Agence nationale de la sécurité des systèmes d'information (ANSSI), en sa qualité d'autorité nationale et consciente du besoin d'éclairage vis-à-vis de cette offre, accompagne entreprises et administrations dans leurs choix, grâce aux **Visas de sécurité**. Ces derniers permettent d'identifier facilement les solutions jugées les plus fiables par l'ANSSI à l'issue d'un processus de qualification ou de certification. Ils sont un gage de sécurité pour les utilisateurs et un atout de compétitivité pour les fournisseurs de produits et de services de sécurité qui disposent ainsi d'un atout concurrentiel fort.

Vous trouverez dans les pages qui suivent une présentation de la démarche de certification de sécurité par l'ANSSI. En complément, la liste des produits certifiés peut être consultée sur le site de l'Agence. ■

www.ssi.gouv.fr

QU'EST-CE QUE LA CERTIFICATION ?

La certification est **l'attestation du niveau de robustesse** d'un produit, basée sur une analyse de conformité et des tests de pénétration réalisés par un évaluateur tiers sous l'autorité de l'ANSSI, selon un schéma et un référentiel adaptés aux besoins de sécurité des utilisateurs et tenant compte des évolutions technologiques. L'ensemble du processus est géré au sein de l'ANSSI par le Centre de Certification National.

À QUOI SERT LA CERTIFICATION ?

En tant qu'utilisateur : en choisissant un produit certifié, vous êtes assuré que les fonctionnalités certifiées offrent un niveau de sécurité éprouvé, c'est-à-dire qu'elles résistent aux attaques d'un niveau déterminé ;

En tant que développeur de solutions numériques : la certification d'un produit vous permet d'accéder à de nombreux marchés de cybersécurité en France et à l'international.

COMMENT SE PASSE L'ÉVALUATION DANS LE PROCESSUS DE CERTIFICATION ?

La robustesse d'un équipement est éprouvée par une évaluation, qui consiste à tester un produit au regard d'une **cible de sécurité** définie en fonction d'un besoin de sécurité exprimé. Cette cible de sécurité identifie notamment la *Target Of Evaluation* (TOE) (cf. encart ci-dessous)

L'ÉVALUATION COMPORTE PRINCIPALEMENT DEUX VOLETS :

Une analyse de la conformité : il s'agit de s'assurer de la conformité des fonctions de sécurité implémentées à celles attendues, décrites dans la cible de sécurité, ainsi que la conformité aux référentiels et critères d'évaluation (analyse de l'implémentation, de la gestion et de la maîtrise de la configuration par le développeur, de la sécurité de l'environnement de développement, tests fonctionnels, etc.).

Une analyse de vulnérabilité : sur la base de l'analyse de conformité, il s'agit de s'assurer qu'il n'est pas possible de contourner ou mettre en défaut les fonctions de sécurité de la TOE, pour un niveau de compétence et de moyens préétabli de l'attaquant (potentiel d'attaquant). Elle repose sur une analyse des vulnérabilités potentielles liées à l'implémentation, l'architecture ou la mise en œuvre du produit, et sur des tests de pénétration ciblés.

LEXIQUE

LA TARGET OF EVALUATION (TOE) désigne le produit ou partie du produit à évaluer, la documentation et le processus de développement associés.

LA CIBLE DE SÉCURITÉ décrit la TOE, son fonctionnement et expose le problème de sécurité auquel elle doit répondre : informations à protéger, menaces pesant sur ces informations, fonctions de sécurité et conditions d'utilisation du produit prévues pour contrer ces menaces.

UN PROFIL DE PROTECTION est une cible de sécurité générique pour un type de produits et un besoin de sécurité prédéfinis. La certification permet, de manière optionnelle, d'attester de la conformité du produit certifié à un ou plusieurs profils de protection.

QUELS SONT LES DIFFÉRENTS TYPES DE CERTIFICATION ?

Le schéma français offre deux types de certification.

LA CERTIFICATION CRITÈRES COMMUNS (CC)

Il s'agit d'un d'un standard internationalement reconnu s'inscrivant dans des accords de reconnaissance multilatéraux. Les CC permettent d'atteindre des niveaux d'assurance différents dans la sécurité du produit en considérant d'une part, ses caractéristiques de conception et son processus de développement et, d'autre part, sa résistance face à un niveau d'attaque donné.

Plus le niveau d'assurance visé est élevé, plus les éléments de preuve attendus sont précis et l'effort d'évaluation important. La durée du processus de certification varie entre 6 et 18 mois en moyenne (selon le type de produit, le niveau visé, etc.).

LA CERTIFICATION DE SÉCURITÉ DE PREMIER NIVEAU (CSPN)

Elle a été mise en place par l'ANSSI afin de proposer une alternative aux évaluations CC pour estimer la résistance d'un produit à des attaques de niveau modéré.

La CSPN est généralement moins exhaustive que la certification CC et met l'accent sur l'analyse du produit. Elle prend la forme de tests effectués en temps et charge contraints (par défaut 2 mois, 25 à 35 jours/homme).

Le choix de l'une ou l'autre de ces certifications s'effectue au regard de la situation du demandeur, de ses besoins et de ses attentes.

UNE ÉCHELLE ADAPTABLE

Les critères communs proposent par défaut 7 niveaux d'assurance d'évaluation. A chaque niveau correspondent des tâches d'évaluation que l'on peut schématiquement répartir en deux phases d'analyse de conformité et vulnérabilité :

- **EAL1 :** testé fonctionnellement/résistant à un attaquant de niveau élémentaire (« script-kiddie »).
- **EAL2 :** testé structurellement/résistant à un attaquant de niveau faible.
- **EAL3 :** testé et vérifié méthodiquement/résistant à un attaquant de niveau faible.
- **EAL4 :** conçu, testé et vérifié méthodiquement/résistant à un attaquant de niveau modéré.
- **EAL5 :** conçu de façon semi-formelle et testé/résistant à un attaquant de niveau moyen.
- **EAL6 :** conception vérifiée de façon semi-formelle et système testé/résistant à un attaquant de niveau élevé.
- **EAL7 :** conception vérifiée de façon formelle et système testé/résistant à un attaquant de niveau élevé.

Le niveau d'assurance peut être adapté en sélectionnant les tâches d'évaluation les plus pertinentes au regard des besoins de sécurité des utilisateurs (exprimé sous la forme « d'augmentation » type EAL4+).

Dans le cadre de la CSPN, l'attaquant considéré correspond au niveau modéré des CC, avec une analyse de conformité moins poussée.

QUELLE EST LA PORTÉE DE LA CERTIFICATION PAR L'ANSSI ?

L'ANSSI est l'autorité nationale pour la certification de sécurité de produits. La certification Critères Communs bénéficie d'une reconnaissance européenne et mondiale via les accords du SOG-IS[1] et du CCRA[2]. La reconnaissance de la CSPN à l'échelle européenne constitue un objectif à court ou moyen terme.

QUEL EST LE PÉRIMÈTRE DE LA CERTIFICATION ?

La certification peut concerner les solutions de cybersécurité et, plus largement, toutes les solutions numériques offrant des fonctionnalités de sécurité. Par exemple : les produits réseaux de type VPN ou pare-feu, les cartes à puces, les HSM, les TEE (*Trusted Execution Environment*), les produits pour systèmes industriels (automates programmables industriels, serveurs SCADA) etc.

QUI EST EN CHARGE DE L'ÉVALUATION D'UN PRODUIT DANS LE PROCESSUS DE CERTIFICATION ?

L'évaluation est menée par un laboratoire privé, dénommé Centre d'Evaluation de la Sécurité des Technologies de l'Information (CESTI), qui a été :

- pour l'évaluation CC : accrédité suivant la norme ISO/IEC 17025 par le COFRAC et agréé par l'ANSSI ;
- pour l'évaluation CSPN : agréé par l'ANSSI.

L'agrément est la validation des compétences d'un laboratoire en matière d'analyse technique de la sécurité. Les frais d'évaluations d'un produit par un CESTI sont à la charge exclusive du commanditaire de l'évaluation. L'ANSSI assure un contrôle continu des évaluations.

QUI CONTACTER POUR CERTIFIER UN PRODUIT ?

Les dossiers de demande de certification sont à déposer auprès du Centre de certification national de l'ANSSI (certification@ssi.gouv.fr)

En amont d'une demande, il vous est recommandé :

- de consulter le site de l'ANSSI pour connaître les profils de protection disponibles ;
- de consulter un CESTI pour une assistance à la rédaction de votre cible de sécurité ;
- si votre projet s'inscrit dans le cadre d'un projet de qualification, de contacter le bureau politique industrielle et assistance de l'ANSSI (industries@ssi.gouv.fr).

(1) L'accord du SOG-IS (Senior Officials Group – Information Security) regroupe actuellement 14 pays européens et permet une reconnaissance des certificats CC jusqu'au niveau EAL4 par défaut et EAL7 pour certains types de produits. https://www.sogis.org/ pour plus de détails.
(2) L'accord du CCRA (Common Criteria Recognition Arrangement) regroupe actuellement 28 pays et permet la reconnaissance des certificats CC jusqu'au niveau EAL2 par défaut et EAL4 dans certains cas. https://www.commoncriteriaportal.org/ccra/ pour plus d'informations.

UNE CERTIFICATION EST-ELLE DÉFINITIVE ?

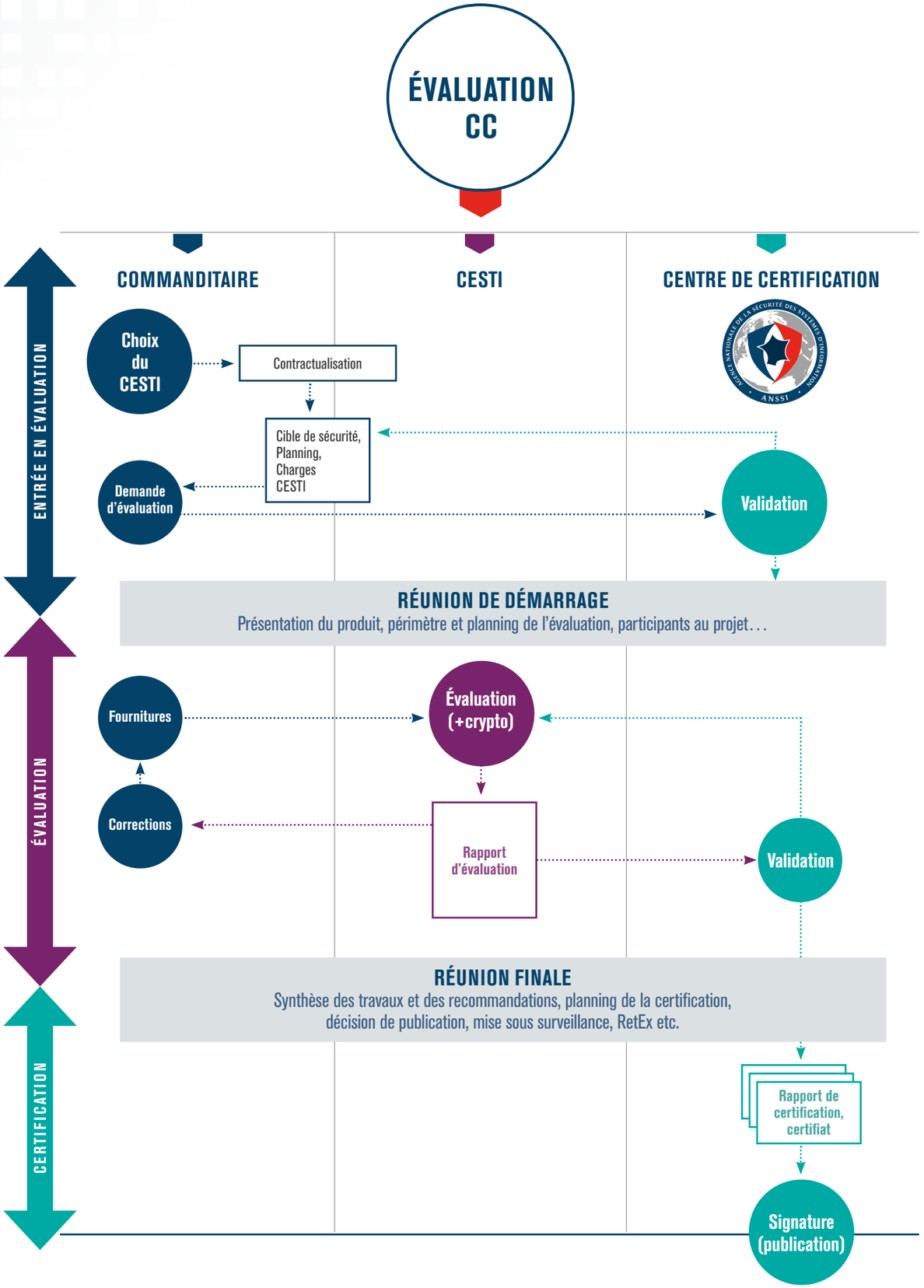
UNE CERTIFICATION N'EST VALABLE QUE POUR UNE VERSION DONNÉE D'UN PRODUIT. À LA DEMANDE DU COMMANDITAIRE, IL EST POSSIBLE DE PROLONGER UNE CERTIFICATION DANS LE TEMPS OU DE L'ÉTENDRE À D'AUTRES PRODUITS, SELON DIFFÉRENTES MODALITÉS.

- **La surveillance** consiste à tester, à intervalle de temps régulier (défini par le commanditaire, généralement 1 an), la résistance d'un produit initialement certifié en prenant en compte l'évolution de la nature des attaques. Elle permet le cas échéant de renouveler le niveau d'assurance dans le produit initialement certifié.
- **La maintenance** permet la continuité de l'assurance dans un produit certifié dans le cas où celui-ci connaîtrait des évolutions et mises à jour mineures, c'est-à-dire, qui n'impactent pas la sécurité du produit initialement certifié.
- **La réévaluation** s'applique aux produits ayant subi des évolutions majeures (ou ceux dont la certification n'a pas abouti) sur la base d'une précédente évaluation.

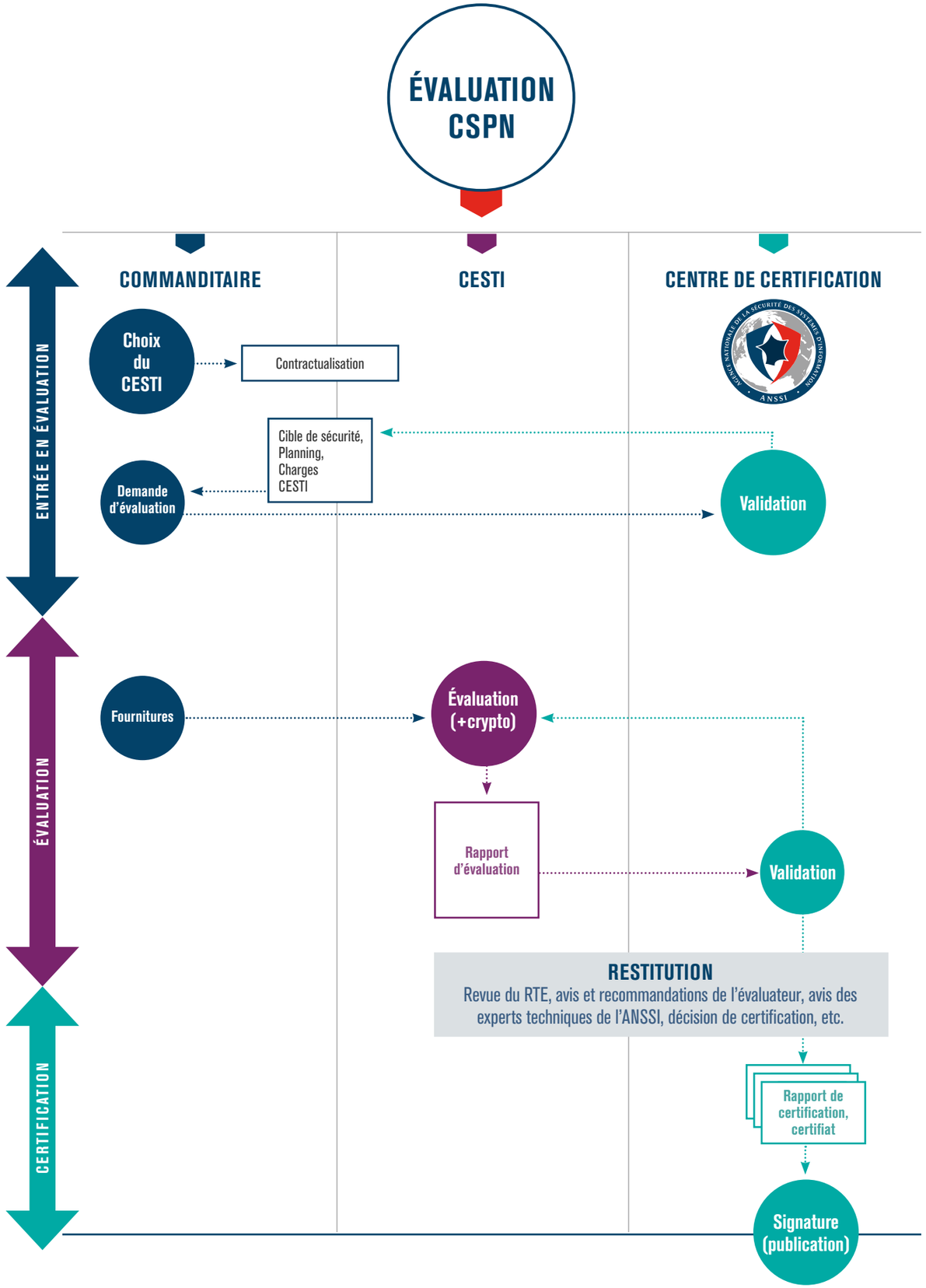
« Les dossiers de demande de certification sont à déposer auprès du Centre de certification national de l'ANSSI (certification@ssi.gouv.fr) »

PAR ÉTAPES

ÉVALUATION CC



ÉVALUATION CSPN



EN CHIFFRES

1 173

CERTIFICATIONS

(CC ET CSPN) ONT ÉTÉ DÉLIVRÉES PAR L'ANSSI AU TOTAL DONT 115 EN 2016

20 ANS

D'EXPÉRIENCE EN CERTIFICATION DE SÉCURITÉ

L'ANSSI C'EST

SERVICE DU PREMIER MINISTRE RATTACHÉ AU SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE (SGDSN), L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ANSSI) ASSURE LA SÉCURITÉ ET LA DÉFENSE DES SYSTÈMES D'INFORMATION DE L'ÉTAT ET DES OPÉRATEURS D'IMPORTANCE VITALE (OIV) EN CRÉANT LES CONDITIONS D'UN ENVIRONNEMENT DE CONFIANCE.

PROMOTRICE DE SOLUTIONS ET DE SAVOIR-FAIRE, ELLE PARTICIPE À LA PROTECTION ET À LA DÉFENSE DU POTENTIEL ÉCONOMIQUE DE LA NATION ET ASSURE UN SERVICE DE VEILLE, DE DÉTECTION, D'ALERTE ET DE RÉACTION AUX ATTAQUES INFORMATIQUES.

EN CAS DE QUESTION RELATIVE À LA CERTIFICATION, LES ÉQUIPES DE L'ANSSI SONT À VOTRE DISPOSITION

certification@ssi.gouv.fr

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI – 51, BOULEVARD DE LA TOUR-MAUBOURG – 75700 PARIS 07 SP

www.ssi.gouv.fr – visa.securite@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN