SECURITY CERTIFICATION OF PRODUCTS

BY THE FRENCH NATIONAL CYBERSECURITY AGENCY (ANSSI)

SECURITY VISA

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI

SECURITY VISA

THE ANSSI SECURITY VISAS MEET THREE OBJECTIVES

1

REGULATORY OBJECTIVES:

to meet the French or European regulations that enforce the use of solutions guaranteeing a tried and tested level of robustness.

2

CONTRACTUAL OBJECTIVES:

to provide a solution for public or private contractors who demand that the solutions they use have obtained an ANSSI security Visa.

3

COMMERCIAL OBJECTIVES:

to enable a **product supplier** or **service provider**, **as well as the final users of these solutions** to stand out from the competition by guaranteeing a certain level of robustness.

“Security Visas provide a competitive edge for the suppliers of security solutions and a guarantee of security for users.”

In a society where digital becomes ubiquitous, each day we recognise the extraordinary opportunities that it has to offer. However, this transformation does not come without new threats that are constantly increasing in number, effectiveness and sophistication.

At a time when these risks indiscriminately affects government authorities, businesses and individuals, it is crucial to be aware of the vital importance of putting in place appropriate solutions for securing information systems at the right level. **WHILE THERE ARE MANY AND VARIOUS CYBERSECURITY SOLUTIONS AVAILABLE ON THE MARKET, THEY ARE NOT ALL EQUALLY EFFECTIVE AND ROBUST.**

This is why the French National Cybersecurity Agency (Agence nationale de la sécurité des systèmes d’information – ANSSI), in its capacity as a national authority, and aware of the need for clarification about this market, is helping companies and government authorities to make a choice thanks to its **Security Visas**. They provide an easy way to identify solutions that ANSSI considers the most reliable following a qualification or certification process. They are a guarantee of security for users and provide a significant competitive edge for product suppliers and the providers of security services.

You will find in the following pages a description of the ANSSI’s qualification process. Additionally, the list of qualified products and services may be found on the Agency’s website. ■

www.ssi.gouv.fr

WHAT IS CERTIFICATION?

Certification demonstrates the robustness of products, based on a conformity analysis and penetration tests performed by a third-party evaluator under the authority of ANSSI, according to a process and framework in order to provide the best level of security given the market and technological requirements. The entire process is managed within ANSSI by the National Certification Centre.

WHAT IS THE PURPOSE OF CERTIFICATION?

For users: by choosing a certified product, you are assured that the certified functions provide a proven level of security, i.e. they withstand a specific level of attack.

For digital solutions developers: product certification enables the access to many cybersecurity markets in France and worlwide.

HOW DOES EVALUATION FIT INSIDE THE CERTIFICATION PROCESS?

Product robustness is tested by **an evaluation,** which consists in testing the product against a specific **security target,** defined for a specific security need. This security target identifies in particular the Target Of Evaluation (TOE).

GLOSSARY

THE TARGET OF EVALUATION (TOE) indicates the product or part of the product to be evaluated, and the associated documentation and development process.

THE SECURITY TARGET describes the TOE and how it works, and explains the security problem for which it must provide protection: information to be protected, threats to this information, security functions and product usage conditions stipulated to counter these threats.

A PROTECTION PROFILE is a generic security target for a predefined type of product and security need. Certification can, optionally, attest the compliance of the certified product with one or several protection profiles.

THE EVALUATION HAS TWO MAIN ASPECTS:

Product conformity assessment: the aim here is to ensure that the security functions implemented meet expectation, described in the security target, as well as compliance with the standards and evaluation criteria (analysis of the implementation, of the developer's configuration management and control, of the security of the development environment, functional tests, etc.).

Vulnerability analysis: based on the conformity assessment, the aim here is to make sure it is not possible to bypass or deactivate the TOE's security functions, for a preestablished level of competency and resources of the attacker (attacker's potential). It is based on an analysis of potential vulnerabilities and pentesting, vulnerabilities may be linked to the product architecture, implementation or operational use.

WHAT ARE THE VARIOUS TYPES OF CERTIFICATION?

The French scheme provides two types of certification:

COMMON CRITERIA (CC) CERTIFICATION

This is an internationally recognised standard based on multilateral recognition agreements. CC certifications are used to reach various levels of assurance for a product's security considering on one hand the associated development environment and process, and on the other hand, its resistance to a given attack potential.

If a higher level of assurance is targeted, more effort and more detailed evidence will be required. The certification process lasts between six and eighteen months on average (depending on the type of product, the targeted level, etc.).

FIRST LEVEL SECURITY CERTIFICATION (CSPN – CERTIFICATION DE SÉCURITÉ DE PREMIER NIVEAU)

The CSPN was introduced by ANSSI to provide an alternative to the CC evaluations in order to estimate the resistance of a product to a moderate level of attack.

The CSPN is generally less exhaustive than CC certification and places greater emphasis on product analysis. It involves tests carried out under time and workload constraints (typically two months and 25 to 35 man-days).

The choice to go with one or the other of these certifications depends on the sponsor's situation, needs and expectations.

AN ADAPTABLE SCALE

The common criteria propose seven default levels of evaluation assurance. Each level corresponds to evaluation tasks that can be schematically divided into two conformity and vulnerability analysis phases:

- **EAL1:** functionally tested/resistant to a low attacker ("script-kiddie").
- **EAL2:** structurally tested/resistant to a basic attacker.
- **EAL3:** methodically tested and checked/resistant to a basic attacker.
- **EAL4:** methodically designed, tested and checked/resistant to an enhanced basic attacker.
- **EAL5:** semi-formally designed and tested/resistant to a moderate attacker.
- **EAL6:** Semi-formally verified design and tested/resistant to a high-level attacker.
- **EAL7:** formally verified design and tested/resistant to a high-level attacker.

The assurance level may be adjusted by selecting the most relevant evaluation tasks given the users' security needs (expressed in the form of type EAL4+ "augmentation").

Within the CSPN framework, the attacker considered corresponds to an enhanced basic level of CCs, with a less thorough compliance analysis.

WHAT IS THE REACH OF THE ANSSI CERTIFICATION?

ANSSI is the French authority for security certification of products. The Common Criteria certification benefits from European and worldwide recognition through the SOG-IS[1] and CCRA[2] agreements. European recognition for the First Level Security Certification (CSPN) represents a short to medium-term target.

WHAT IS THE CERTIFICATION SCOPE?

Certification may concern cybersecurity solutions and, more broadly, all digital solutions providing security functions, for example: Network products such as VPNs or firewalls, smartcards, HSM, TEE (Trusted Execution Environment), products for industrial systems (industrial PLCs, SCADA software), etc.

WHO IS IN CHARGE OF EVALUATING A PRODUCT IN THE CERTIFICATION PROCESS?

The evaluation is performed by a private IT Security Evaluation Facility (ITSEF), which has been:

- For the CC evaluation: accredited by COFRAC in accordance with the ISO/IEC 17025 standard, and licensed by ANSSI.
- For the CSPN evaluation: licensed by ANSSI.

Certification is the validation by ANSSI of a laboratory's expertise in the technical analysis of security.

The cost incurred for having a product or service evaluated by a CESTI is exclusively the responsibility of the product supplier. ANSSI provides continuous supervision for evaluations.

WHO TO CONTACT TO HAVE A PRODUCT CERTIFIED?

Certification applications should be presented to the French National Cybersecurity Agency - ANSSI (certification@ssi.gouv.fr).

Before submitting an application, it is recommended that you:

- consult ANSSI's website so that you are aware of the available protection profiles,
- consult an ITSEF for assistance in writing your security target,
- contact ANSSI's industrial policy and assistance bureau (industries@ssi.gouv.fr), if your project is part of a qualification project.

(1) The SOG-IS (Senior Officials Group – Information Security) agreement currently has 14 EU Members States and provides recognition of CC certificates up to level EAL4 by default and to level EAL7 for certain types of products. https://www.sogis.org/ for more information.
(2) The CCRA (Common Criteria Recognition Arrangement) agreement currently has 28 State members and enables recognition of CC certificates up to level EAL2 by default and to level EAL4 in certain cases. https://www.commoncriteriaportal.org/ccra/ for more information.

IS A CERTIFICATION DEFINITIVE?

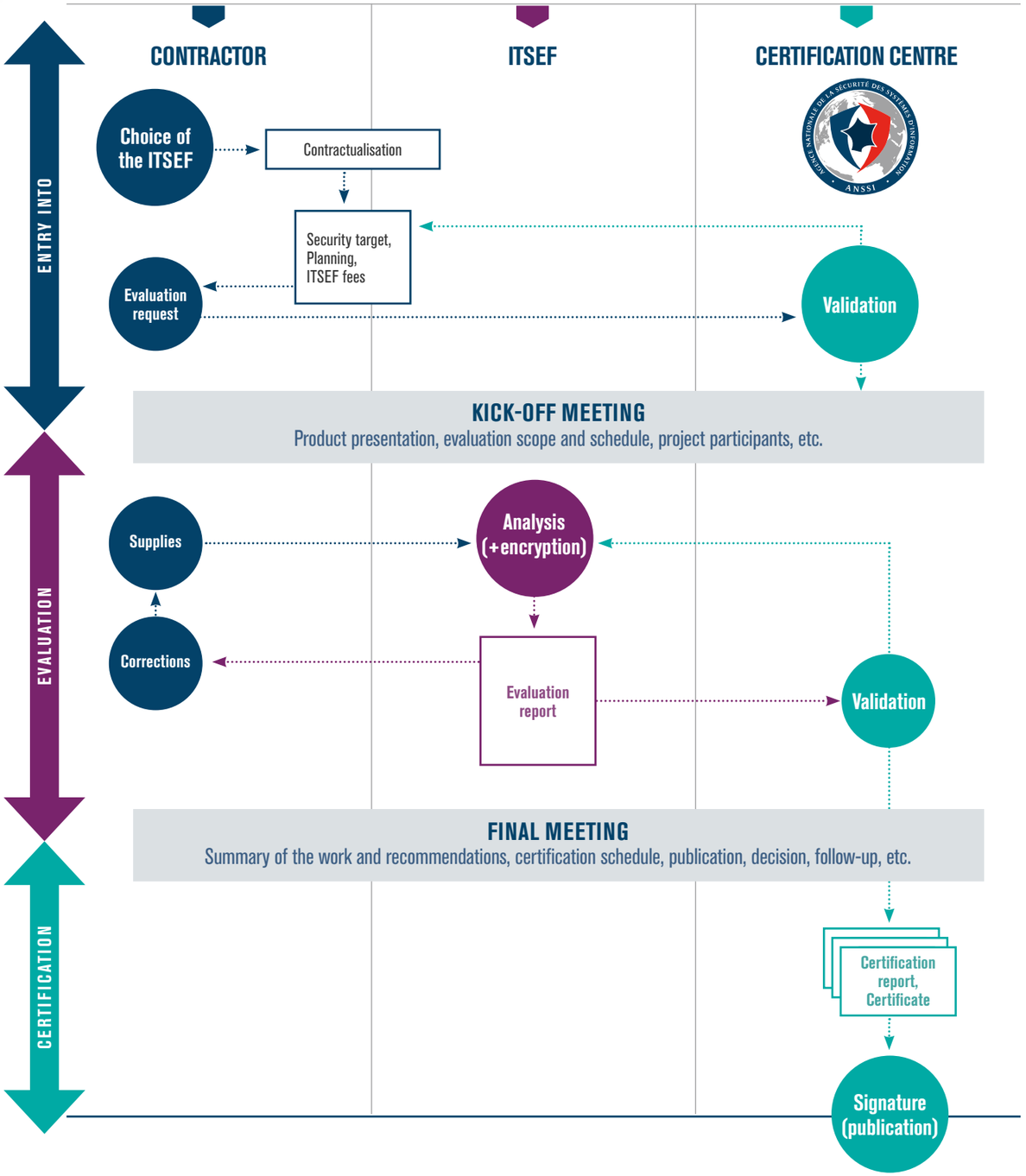
A CERTIFICATION IS ONLY VALID FOR A SPECIFIC VERSION OF A PRODUCT.
IF THE CONTRACTOR REQUESTS IT, IT IS POSSIBLE TO EXTEND THE CERTIFICATION'S PERIOD OF VALIDITY OR TO EXTEND IT TO OTHER PRODUCTS, IN ACCORDANCE WITH DIFFERENT OPTIONS:

- **Surveillance** involves testing, at regular intervals (decided by the sponsor, usually one year), the resistance of a previously certified product by taking into account the evolution of the nature of attacks. If applicable, it provides renewal of the assurance level on the previously certified product.
- **Maintenance** provides assurance continuity for a certified product for each minor change or update, that is, which has no impact on the security of the previously certified product.
- **Re-evaluation** applies to products that have undergone major changes (or those whose certification was unsuccessful), on the basis of a previous evaluation.

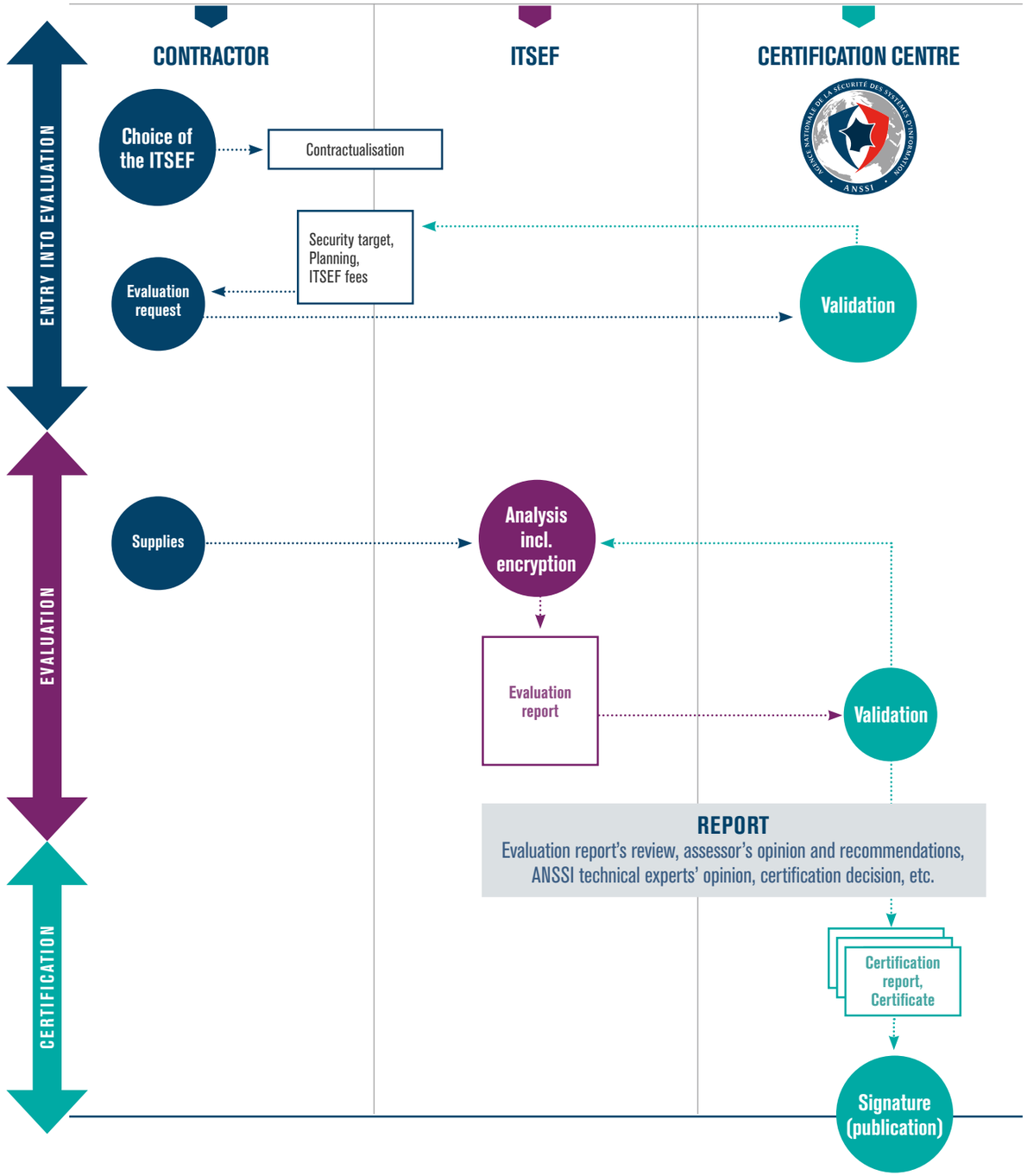
"Certification requests shall be sent to the French National Cybersecurity Agency - ANSSI (certification@ssi.gouv.fr)"

BY STEPS

CC EVALUATION



CSPN EVALUATION



KEY FIGURES

1,173

CERTIFICATIONS

(CC AND CSPN) HAVE BEEN ISSUED BY ANSSI, INCLUDING 115 IN 2016

20 YEARS

OF EXPERIENCE IN SECURITY CERTIFICATION

ANSSI IS...

THE FRENCH NATIONAL CYBERSECURITY AGENCY REPORTING TO THE SECRETARY GENERAL FOR DEFENCE AND NATIONAL SECURITY (SGDSN) WHICH IS PART OF THE FRENCH PRIME MINISTER SERVICES. ANSSI (AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION) ENSURES THE SECURITY AND DEFENCE OF THE GOVERNMENTAL INFORMATION SYSTEMS AND THE ONES OF THE OPERATORS OF VITAL IMPORTANCE BY ENABLING A TRUSTED ENVIRONMENT.

AS A PROMOTER OF TRUSTED SOLUTIONS AND KNOW-HOW, ANSSI CONTRIBUTES TO THE PROTECTION AND DEFENCE OF THE NATION'S ECONOMIC POTENTIAL AND PROVIDES MONITORING, DETECTION, ALERT AND RESPONSE SERVICES AGAINST CYBERATTACKS.

FOR ANY QUESTION ABOUT SECURITY CERTIFICATION OF PRODUCTS, CONTACT THE ANSSI:

certification@ssi.gouv.fr

LICENCE OUVERTE/OPEN LICENCE (ETALAB – V1)

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