STORMSHIELD

QUALIFIED SECURITY SOLUTIONS

CHOOSING A TRUSTED SOLUTION

Julien Paffumi
Product Marketing Manager, Stormshield

How much do you trust the security solution that protects your information system? It's a key question, but one that isn't asked often enough. Whether you're a business or a government body, you need complete confidence in the solution that's there to protect you. What's the use of rolling out a security product if it's inefficient... or worse, if it has backdoors that make your information accessible to outsiders?

In the real world, where tensions and suspicions are rife, how do you choose with confidence from a plethora of international solutions? At the international level, several certifications for certifying product robustness currently exist. But what about this concept of trust? To fill this gap, a number of European countries have created another type of quality label: qualifications. But what's the difference between «qualification» and «certification»? And how do you make sense of it all?

Certification or qualification: what's the difference?

Let's consider the case of France and its National Cybersecurity Agency (ANSSI), which can boast many years of experience on the subject of qualification. There are several types of label: **Common Criteria Certification**, First Level Security Certification (CSPN), and Qualification, which itself can be either Basic, Standard or Enhanced. But how do you know what's what?

CERTIFICATION

Certification is a statement attesting to the **robustness** of the security product. Software publishers define a «security target» which describes the security functions under evaluation and the context of their use. An accredited independent laboratory, the *Centre d'Évaluation de la Sécurité des Technologies de l'Information* (CESTI) carries out an assessment of the product development process and its resistance to a given level of attack.

Common Criteria (CC) certification is recognised and issued in many countries.

It shows the level to which the product's robustness against attack has been evaluated. For example, a firewall may be certified to EAL3+, EAL4+, etc.

COMMON CRITERIA CERTIFIED EAL3+

COMMON CRITERIA

COMMON CRITERIA CERTIFIED EAL4+

COMMON CRITERIA

First Level Security Certification (CSPN) has been implemented by ANSSI as an alternative to CC Certification evaluations, whose cost and lengthy duration can be an obstacle. Tests are conducted using limited timescales and loads (typically 2 months, 25 to 35 working days). But be aware of a small nomenclature issue: unlike CC Certification, which is recognised internationally, CSPN is currently a purely French label. However, the aim is to obtain Europe-wide recognition in the future.

Note - Something you may not know about certification

- Unless the certification process subsequently leads to qualification, the issuing country's Agency is not involved in defining the security target. To some extent, therefore, publishers can customise the target as they see fit and potentially exclude some of the product's security functions from the evaluation. It is therefore essential to make a careful examination of the security target chosen by the publisher, compared to your need for security: this is your responsibility when choosing the security solution in question.
- The certification report can raise reservations or recommendations for use, which need to be examined carefully with reference to your own situation.
- Lastly, a certification applies to specific software or hardware versions, so make sure the resulting certification doesn't apply to a product or version from several years ago, which may no longer be sold or supported.

QUALIFICATION

More than just certification, qualification represents a **recommendation** by ANSSI, and is a statement of the French state's **confidence** in the security product and its publisher.

The first prerequisite is to obtain a certification of a sufficiently high level, but with a **security target validated by ANSSI**. In addition, over and above the certification process, ANSSI carries out additional analyses, including an **audit of the evaluated product's source code**. Beware of bold claims: you should be suspicious if a publisher claims that their qualification is pending, but isn't able to produce an official letter confirming the start of the qualification process.

This **product qualification** is recognised in France, and (in some cases) in Europe too. It is also a prerequisite for a product to be approved for the protection of «NATO Restricted» or «EU Restricted» classified information.

NATO RESTRICTED

The «NATO restricted» label

«NATO restricted» status applies to information whose unauthorised disclosure would be contrary to the interests of NATO or of some of its Member States.

To be included in the catalogue of solutions authorised to secure such information, certification alone is not sufficient: the product must have obtained Standard Qualification.

EU RESTRICTED

The «EU restricted» label

«EU restricted» status applies to information whose unauthorised disclosure would be contrary to the interests of the European Union or of some of its Member States.

To be included in the catalogue of solutions authorised by the EU for securing such information, a product must have been qualified by two EU Member State agencies (in France, the Standard Qualification). Here again, certification alone is not sufficient.

Why choose a product qualified by ANSSI outside France?

Although in France, their use is mandatory in some regulatory contexts, solutions qualified by the French national agency are definitely not reserved exclusively for French organisations! When you choose an ANSSI-qualified solution, you're choosing a product recommended by a well-reputed and trusted security agency of a Member State of the European Union.

- This guarantees you **a product whose robustness has been tried and tested** through the certification process.
- On **an evaluation and usage target validated** by ANSSI,
- Whose **source code has been audited**,
- And produced by **a company whose development, delivery and support processes are recognised as trusted** by a Member State of the European Union.

Recently, to support French organisations in making their choice, ANSSI has been offering a catalogue of qualified solutions bearing a new label: **the "Security Visa"**. This visa rewards solutions recognised by the French government as being robust and trustworthy, following rigorous testing and thorough analysis. With this visa and the support of the **German BSI (Bundesamt fur Sicherheit in der Informationstechnik) cybersecurity agency**, ANSSI is consolidating its position of promoting high-level security requirements in Europe.

So what about you? Do you have concrete evidence that you can trust your current security solution and the company that produces it? Do you trust the labels and certifications it has been issued with?

Stormshield is a wholly-owned subsidiary of Airbus CyberSecurity that provides innovative end-to-end security solutions for protecting networks (Stormshield Network Security), workstations (Stormshield Endpoint Security) and data (Stormshield Data Security).

www.stormshield.com