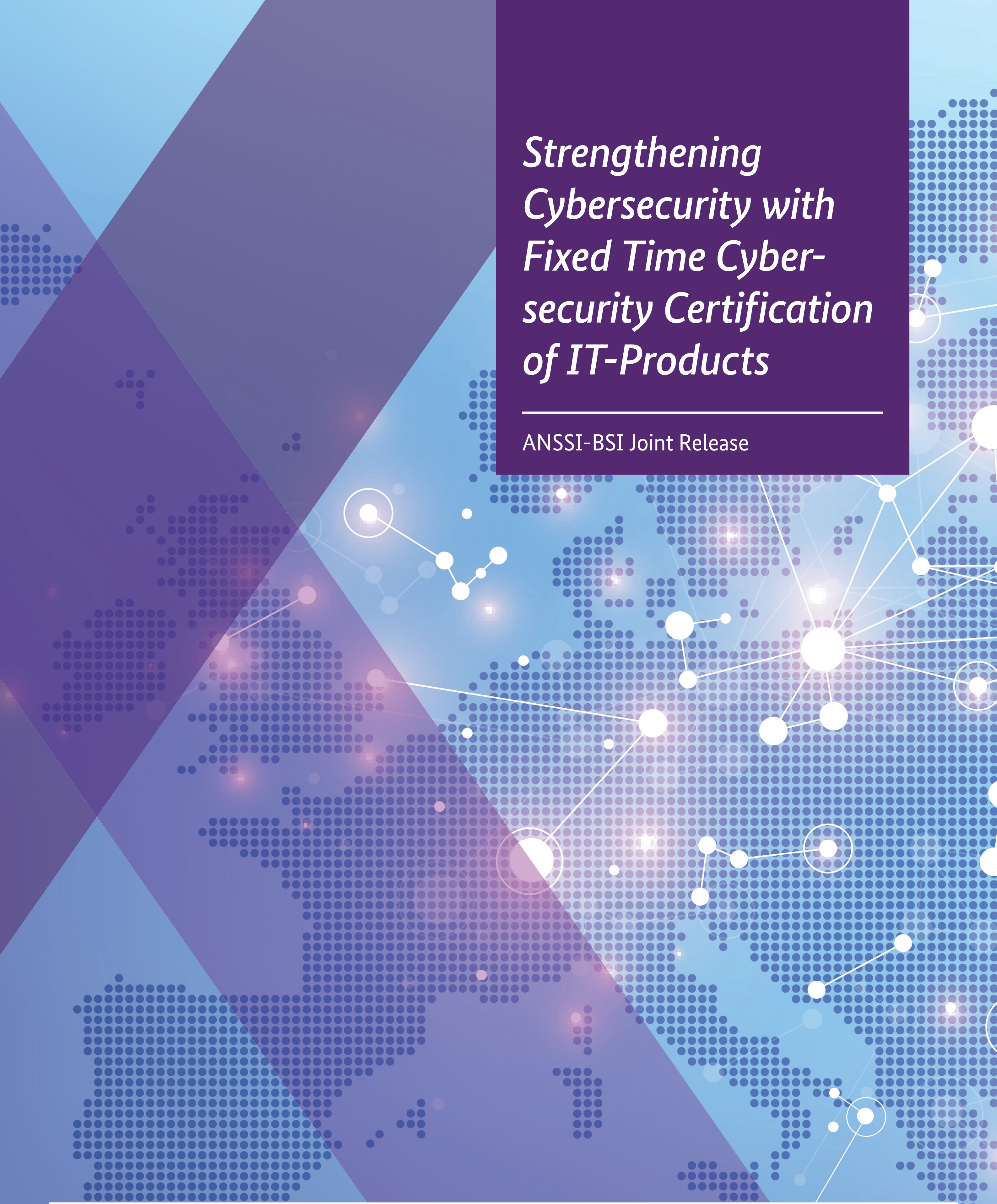


Strengthening Cybersecurity with Fixed Time Cybersecurity Certification of IT-Products

ANSSI-BSI Joint Release

Federal Office
for Information Security

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

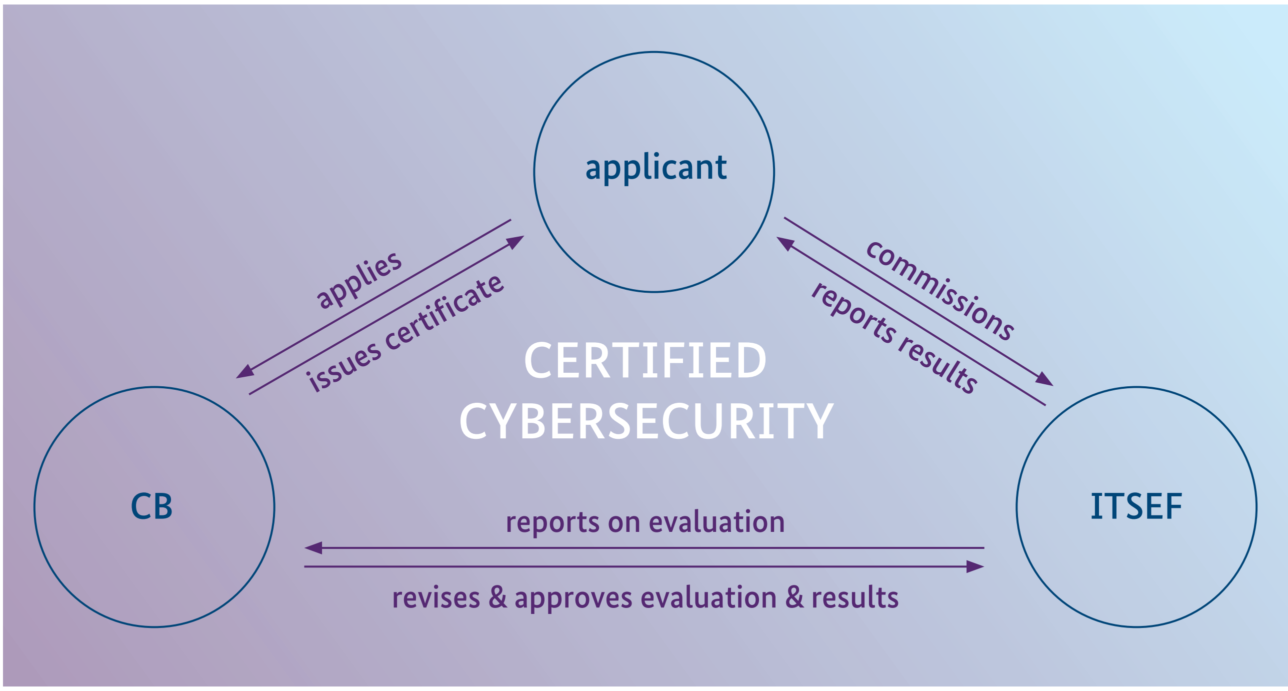
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

Fixed Time Cybersecurity Certification

In many areas of the fast growing IT-landscape, cybersecurity is an ever more important aspect. The digitalisation of significant parts of critical infrastructure, industry, civil services and many more sectors demands for security of the systems and products employed. This is where the cybersecurity certification of IT-products comes into play. It enables manufacturers and vendors of IT-products to have their security statements regarding a product confirmed by a cybersecurity certificate. Analogous to certificates in other areas, e.g., food safety and sustainability, it provides potential product users with an independent assurance on the properties of the product that are difficult to assess by the product users themselves. In particular, the independent attestation of the product's security functions demonstrates the fulfilment of specified security requirements and allows potential product users to assess the compliance of the product with their specific security demands and risk management.

Three Party model – Ensuring Quality

Trust in an IT-product certificate requires trust in the competence and impartiality of the issuing authority. This is guaranteed by three parties working closely together: the applicant, e.g. a manufacturer of the product to be certified, an IT Security Evaluation Facility (ITSEF) that evaluates the product‘s cybersecurity properties, and the Certification Body (CB) that oversees the procedure. The applicant is the party that initiates a certification procedure. Therefore, the applicant prepares the application letter including all required documents and evidences, commissions an ITSEF and applies to the certification body. The ITSEF and the certification body then assess whether the product is suitable for certification under the requested certification scheme.



If this is the case, the ITSEF prepares the evaluation plan to verify that the product meets the security statements of the applicant. This includes planning the tests and testing strategy. Then the evaluation of the IT-product begins. After completion of the evaluation, the ITSEF reports on the evaluation to the CB, describing the evaluation procedure, tests, and results as well as providing a recommendation on the certification. The CB reviews the evaluation, scrutinising the report of the ITSEF. The final decision on whether the product receives a certificate is made by the certification body.

Following this approach, cybersecurity agencies around the globe have been offering the IT security certification of products for more than three decades. They operate many certification schemes with different evaluation methodologies and scopes of application. The tests to verify the security statements differ depending on the methodology as well as the security perimeter and assurance level(s).

Each product evaluation consists of several tests, usually with a mixture of different test types, to ensure a high level of trust in the security statements made (i.e., the security functions of the respective product). The evaluation does not only verify conformity to the claimed security features and standards but does also include penetration tests that address the quality and robustness of their implementation.

Evaluating Cybersecurity:

Conformity of security features – do they:

- conform to the ones claimed by the applicant?
- conform to claimed standards?
- conform to required standards?

Effectiveness / Robustness: Penetration testing

- simulation of an attacker with predefined skills and resources
- evaluators try to break or circumvent security features
- each product needs an individually adapted strategy

Concept of Fixed Time Evaluation

One of these evaluation methodologies is called the fixed time evaluation methodology. It provides a high level of trust while enabling a predictable evaluation schedule and keeping the effort for the product manufacturer manageable.

To keep the product manufacturer's effort manageable, the required deliverables are mainly limited to documents describing the product with its respective security features. Here, the centrepiece is the Security Target (ST) document, a rather short document of approximately 10 pages mainly describing the operating environment and security features of the product.

To achieve a fixed time schedule, ITSEF and the certification body agree on a fixed time budget for the evaluation before it starts. The time budget is consistent with the strength of an expected potential attacker and ranges from 15 to 60 person days. It is determined for each particular procedure according to the complexity and scope of features of the product. The ITSEF conducts the evaluation without direct involvement of the other parties. In particular, communication between the parties is reduced during the evaluation, and it is not possible to change or update the version of the evaluated product. With these principles in place, the evaluation can be finished within a predefined timeframe.

Purpose of the Certification Body:

Management of the certification scheme:

- implement evaluation methodology
- monitor certificate use
- ensure qualification of evaluators employed by ITSEFs

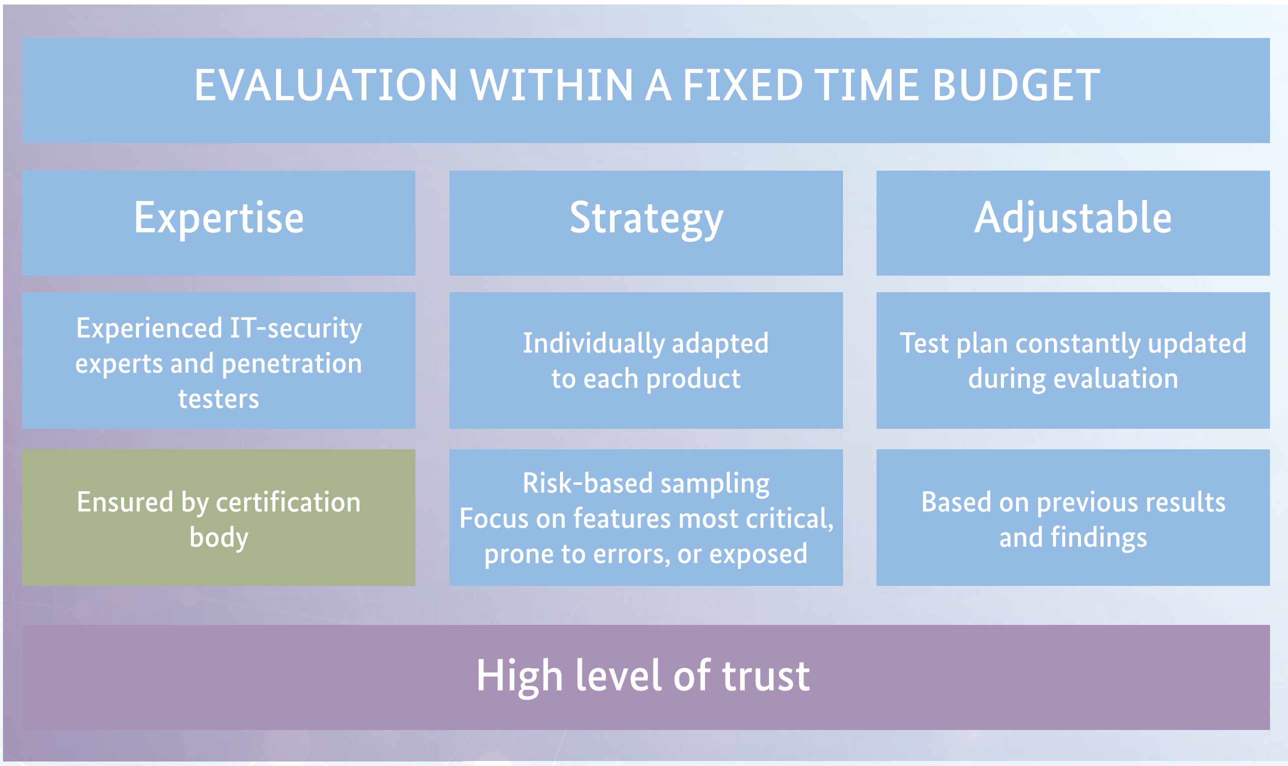
Supervision of the evaluation:

- oversee each evaluation
- ensure consistent approach and methodology across all evaluations
- enforce independence of certificate

Fixed Time Certification Schemes: CSPN and BSZ

The demand for security-certified IT-products rises with the advancing digitalisation in many important and critical areas. A little more than 10 years ago, in order to meet this demand, the French cybersecurity agency ANSSI introduced the first certification scheme employing a fixed time evaluation: the Certification de sécurité de premier niveau (CSPN) [CSPN]. The goal was to reduce the entrance threshold for manufacturers by minimizing the preparation effort and focussing the testing on the parts that contribute most to the security statements.

The German federal cybersecurity agency BSI followed with the introduction of the Beschleunigte Sicherheitszertifizierung (BSZ) [BSZ] in 2021. Thanks to the intensive and continuous bilateral cooperation between the two agencies, both schemes have a common methodology and comparable quality standards. For this reason, the authorities launched the mutual recognition of certificates under these schemes in 2022.



EVALUATION WITHIN A FIXED TIME BUDGET

Expertise	Strategy	Adjustable
Experienced IT-security experts and penetration testers	Individually adapted to each product	Test plan constantly updated during evaluation
Ensured by certification body	Risk-based sampling Focus on features most critical, prone to errors, or exposed	Based on previous results and findings

High level of trust

International Harmonisation and Recognition of Certificates

During the development and introduction of the certification schemes, it became apparent that the demand for certificates is best met when certificates are not only focused on the national market but are recognized in other markets. This renders the need for multiple certification procedures of the same product in different markets obsolete. Consequently, the effort and costs for product manufacturers are reduced, trade barriers are lowered, and the freed capacitates of ITSEFs and CBs can be used for the certification of more products.

Mutual Recognition Agreement – Extended Cooperation

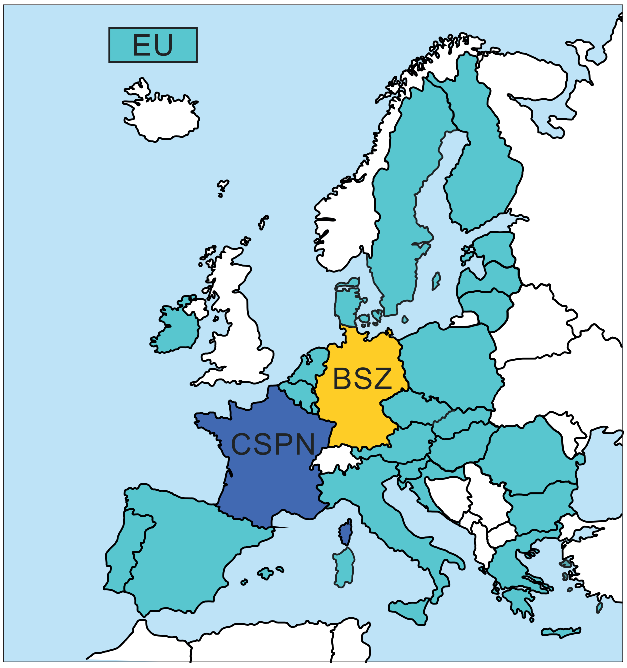
The BSZ scheme was developed with the aim to be compatible to the CSPN scheme. Thus, ANSSI and BSI were able to negotiate and sign a mutual recognition agreement for certificates under those schemes in June 2022 [MRA]. This agreement is initially limited to two years and states that in principle, BSI will recognise all CSPN certificates and in turn, ANSSI will recognise all BSZ certificates. Some certificates can be exempted e.g. when special national regulations apply or the certificates are based on specific notes and interpretations of the schemes.

The agreement also deepens the cooperation between ANSSI and BSI by formalising the regular technical exchange concerning CSPN and BSZ. One aim of this exchange is the further harmonisation of both schemes to reduce the amount of exemptions from recognition. Another goal is to conjointly develop new technical scopes and standardise requirements for the evaluation, e.g., common attack methods, in both schemes.

Towards Standardisation and European Harmonisation

In addition to BSI and ANSSI, other European national cybersecurity agencies have also implemented certification schemes based on a fixed time methodology. However, these national schemes differ in some of the key aspects and partly address different assurance levels. Thus, the certificates of the individual schemes are not readily comparable.

The new European standard EN 17640 "Fixed Time Cybersecurity Evaluation Methodology" (FiT CEM) [FiT CEM] aims to address the patchwork of different fixed time certification schemes. It does so by providing a common evaluation methodology which subsumes the national schemes and methodologies. Therefore, EN 17640 does not strive to copy existing concepts, but to expand them in a flexible way with specified evaluation tasks for different levels of assurance. With its holistic scope and great flexibility, FiT CEM opens the possibility to implement a harmonised European certification scheme under the European Cyber Security Act (CSA) [CSA]. These CSA certification schemes are developed on behalf of the European Commission and under supervision of the European Union Agency for Cybersecurity (ENISA). The respective certificates issued under those schemes are recognized in every EU member state, hence enlarging markets for certified ICT products, services and processes and further reducing the efforts and costs for manufacturers. Additionally, this large European market for certified ICT products, services and processes manifests a global influence on cybersecurity standards and product certification.



Bibliography

[MRA] Mutual Recognition Agreement of Cybersecurity Evaluation Certificates issued under a Fixed-time Certification Process 2022, ANSSI & BSI https://bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/BSZ/Abkommen_Anerkennung_ANSSI_BSI.html

[FiT CEM] EN 17640 ‚Fixed-time cybersecurity evaluation methodology for ICT products' (FiT CEM), October 2022, Cen/Cenelec

[CSA] REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

[CSPN]
www.ssi.gouv.fr/administration/produits-certifies/cspn/

[BSZ]
www.bsi.bund.de/bsz

Imprint

Published by
Bundesamt für Sicherheit in der Informationstechnik
53133 Bonn, Germany
Tel.: +49 22899 9582- 0

Source:
Federal Office for Information Security (BSI)
Section WG24 – Public Relations
Godesberger Allee 185 - 189
53175 Bonn, Germany
Phone: +49 (0) 228 99 9582-0
E-mail: bsi@bsi.bund.de

Agence nationale de la sécurité des systèmes d'information
Secrétariat général de la défense et de la sécurité nationale
51, boulevard de La Tour-Maubourg
75700 Paris 07 SP, France
Phone: +33 (0)1 71 76 85 85
E-Mail: communication@ssi.gouv.fr

Last updated: December 2022

Item number: BSI-LaB22/003

Image credits: Front page and page 4:
AdobeStock © BAIVECTOR

The publication is provided free of charge and is not intended for sale.