EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CYBERSECURITY ASSESSMENTS

Evaluations & Certifications - State of Play 2018-2022

JANUARY 2024

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors, please use certification@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS & CONTRIBUTORS

Chloé Blondeau, ENISA
José Ruiz, JTSEC Beyond IT Security SLU

ACKNOWLEDGEMENTS

We thank EU Cybersecurity Certification Ad-Hoc Working Groups members for their contribution as well as all organisations owning an assessment framework or scheme that accepted to provide detailed information.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-660-6, DOI 10.2824/70639

FOREWORD

This Report aims at presenting the current state of play of cybersecurity assessments of ICT products and cloud services.

In order to study the dynamic of the related market, the report focuses on the evolution of the number of assessed ICT solutions and assessment bodies in the past 5 years. It takes into account the various ways to assess cybersecurity of ICT solutions such as standards, national, and private, certification schemes and methodologies. The assessment frameworks and methodologies presented in the report were selected after consultation with stakeholders involved in the EU Cybersecurity Certification Ad-Hoc Working Groups. These groups are supporting ENISA in the development of the candidate schemes on EUCC, EUCS and EU5G[1].

The 5 years' data comes from several sources such as: websites, surveys, tools or direct contact with the schemes' owner. However, it was not always possible to retrieve the data. In some cases, such information is not made public or the history of the last five years is missing. In that case the data is indicated as "not available".

In case the authors of the report have missed or misinterpreted some data, we invite the owners of the mentioned schemes to reach out to ENISA in order to improve the next edition.

[1] EUCC: Common Criteria based European candidate cybersecurity certification scheme, EUCS: European Union Cybersecurity Certification Scheme on Cloud Services, EU5G: European Union Cybersecurity Certification Scheme on 5G.

Common Criteria scheme for ICT products, 44% of the total assessment bodies are in Europe. This number can be explained by the SOG-IS (“Senior Officials Group Information Systems Security“) Mutual Recognition agreement existing in the Union and signed by 17 member states, which makes possible to recognize evaluations up to the highest assurance level of the Common Criteria, and that applies a lot to sensitive ICT products such as smart cards and other hardware security modules broadly developed by EU industry.

2. ICT PRODUCTS

ICT products such as component, chips, hardware and software are at the heart of any information system. Ensuring that they provide a satisfying level of security could be a fastidious task without the ability to rely on recognized third-party cybersecurity assessment methodologies.

The selected ICT products assessment methodologies are organized by type: horizontal or technology as well as by method such a fixed time evaluation.

2.1 COMMON CRITERIA

2.1.1 Description

Common Criteria (CC) is an international family of standard (ISO/IEC 15408 and ISO/IEC 18045) and the most recognised certification used for assessing security in ICT products. The standard was developed by the governments of the U.S., Canada, Germany, France, the UK and the Netherlands.

Common Criteria is the result of combining the CTCPEC (Canada), the TCSEC (U.S.), and the ITSEC (European) standards. Common Criteria standards support verifying that a product meets a specification of security requirements with a guarantee aligned with the level of assessment established. Depending on the Evaluation Assurance Level (EAL) the requirements of the standard increase (up to EAL 7), in accordance with the possible potential of attackers trying to tamper with the target of evaluation (TOE).

Common Criteria is a horizontal scheme, therefore different types of products are certified using Common Criteria such as telecommunication, ePassports, digital signature, etc…

Date of Creation	1994
Scope	International (more than 30 countries)
Validity of Certificate	5 years
Mutual recognition	There is an international agreement that established a framework for mutual recognition known as the Common Criteria Recognition Arrangement (CCRA). It gathers countries and organisations that have agreed to recognise and accept the results of security evaluations conducted under Common Criteria.

It's important to note that the SOG-IS agreement includes both European Union (EU) member countries and countries from the European Free Trade Association (EFTA), totalling 17 countries on the list. These countries work together to improve the security of information and communication systems, facilitate cooperation, and ensure mutual recognition of information technology security evaluations and certifications within the European region:

2.1.3.1 Data collection

Modality	Data collected from CCScraper which is a tool developed by JTSEC that collects automatically the information from the Common Criteria and Certification Bodies portals using OCR capabilities and other features.

2.2 FIXED-TIME METHODOLOGIES

This type of methodology was created in Europe; in fact, four EU Member States (France, Germany, the Netherlands and Spain) have developed their fixed-time methodology at national level. All of these methodologies have some common points in common such as:

- Effort and duration are known beforehand
- Focus on vulnerability analysis and penetration testing, more emphasis on product testing than on documentation
- In terms of assurance: not targeting assurance level similar to the highest assurance levels of the Common Criteria (AVA_VAN.4 and 5)
- Certification processes that SMEs can afford
- National scope with so far only limited mutual recognition arrangement (ANSSI/CSPN – BSI/BSZ)

2.2.1 CSPN – France

2.2.1.1 Description

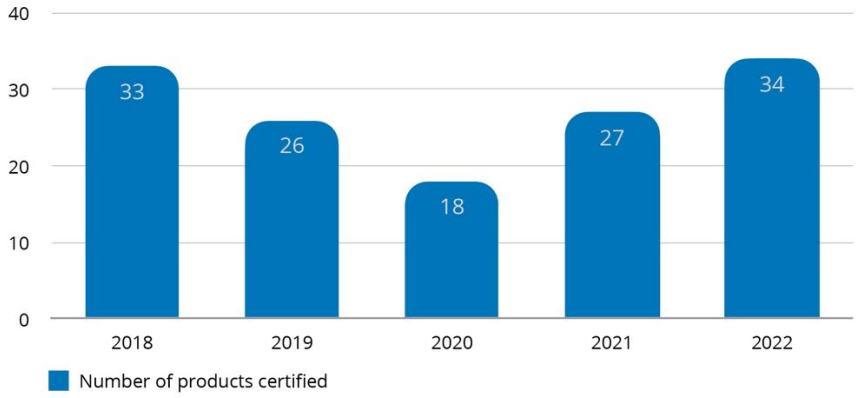
According to the ANSSI (Agence nationale de la sécurité des systèmes d'information – National Agency for the safety of information systems) website: "The First Level Security Certification (CSPN Certification de Sécurité de Premier Niveau or The First Level Security Certification), aims to certify the robustness of a technological product, based on a conformity analysis and intrusion tests carried out by a CESTI (Centre d'Evaluation de Sécurité des Technologies de l'Information), an ITSEF licensed by ANSSI".

This certification is delivered for a specific product version. All subsequent versions of the product must therefore be re-certified. CSPN certification applies to several types of cybersecurity products such as "secure storage", "identification, authentication and access control", or "secure communication". Holding a CSPN allows to receive a Security Visa from ANSSI and to be included in the Security Visa Catalogue of certified solutions published by the French cybersecurity agency.

Date of Creation	2008
Scope	France
Validity of Certificate	3 years
Mutual recognition	with Germany through BSZ

2.2.1.2 Statistics covering the last 5 years - Certified products according to CSPN

Figure 4: Certified products according to CSPN in the last 5 years



The number of certified products under this methodology had a decreasing trend starting in 2019 and ending in 2020, a year with only 18 certificates, maybe due to external factors such as Covid-19. The number of certifications began to recover in 2021 and after the number even surpassed the 2018 figure, with a total of 34 certifications.

2.2.1.3 Data collection

Modality	The Agence Nationale de la Sécurité des Systèmes d'information (ANSSI), the certification body for CSPN, provided the information.
Date of data Collection	12/04/2023

2.2.2 BSPA – The Netherlands

2.2.2.1 Description

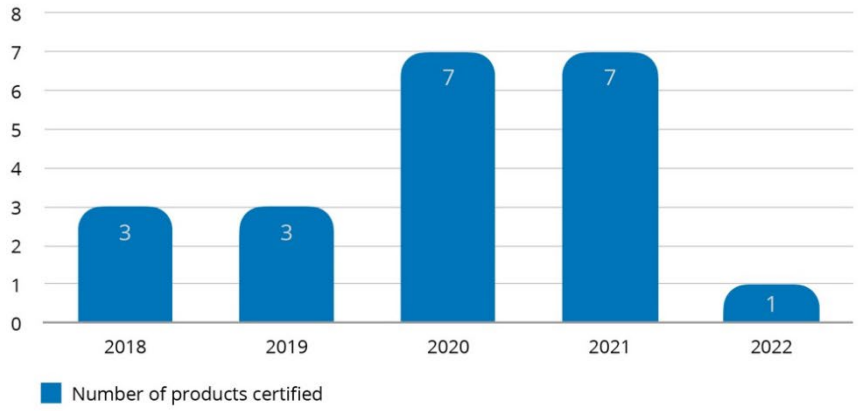
The BSPA is an ICT product assessment scheme developed and maintained by NLNCSA (Nationaal Bureau voor Verbindingsbeveiliging, NBV – Netherlands National Communications Security Agency) –.

This scheme provides a framework in which products (both hardware and software components) can be tested in a limited timeframe (and cost) against a baseline of security requirements (Government security baseline). Compliance to the BSPA is required for manufacturers willing to work with Dutch government agencies.

Date of Creation	2015
Scope	The Netherlands
Validity of Certificate	3 years
Mutual recognition	None

2.2.2.2 Statistics covering the last 5 years – Certified products according to BSPA

Figure 5: Certified products according to BSPA in the last 5 years



During the years of 2018 and 2019, 3 products were certified in both years, the certification trend then increased to 7 certified products in the following two years, but dropped in the 2022 with only one certified product.

2.2.2.3 Data collection

Modality	The Nationaal Bureau voor Verbindingsbeveiliging (NBV) provided the information. Therefore, the data is extracted from information provided by the Certification Body.
Date of data Collection	03/05/2023

2.2.3 LINCE – Spain

2.2.3.1 Description

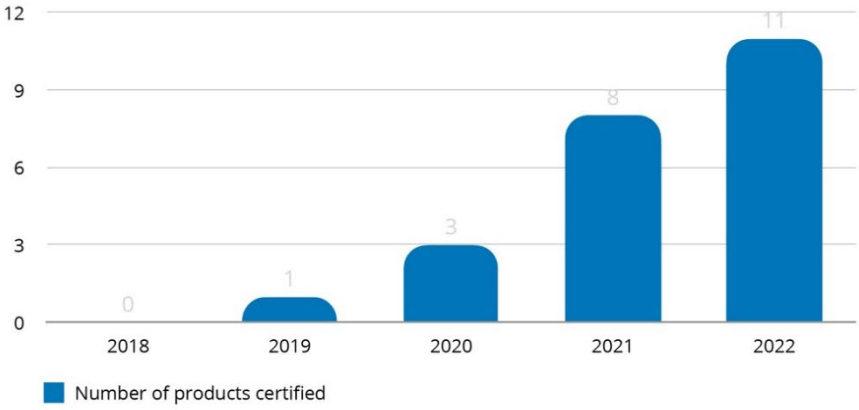
LINCE (Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad) is an evaluation and certification methodology for ICT security products developed by the Spanish CCN (Centro Criptológico Nacional – National Cryptologic Center). This scope-limited and time limited methodology is designed for ICT products requiring certification with medium or low security criticality.

The objective of a LINCE assessment is to enable an evaluation laboratory to verify whether a product conforms to its specification by determining the effectiveness of the security functionality implemented. Holding a LINCE certification allows to be included in the CPSTIC Catalogue, which is the CCN-STIC-105 reference catalogue for cybersecure ICT products in the Spanish Public Administration.

Date of Creation	2018
Scope	Spain
Validity of Certificate	5 years
Mutual recognition	None

2.2.3.2 Statistics covering the last 5 years – LINCE product according to CCN

Figure 6 LINCE certified products in the last 5 years



The number of certified products under this methodology has been growing every year. The LINCE methodology has been widely accepted in the Spanish market, due to its agility, flexibility and lower cost both financially and in terms of effort on the part of manufacturers compared to other methodologies.

2.2.4 BSZ - Germany

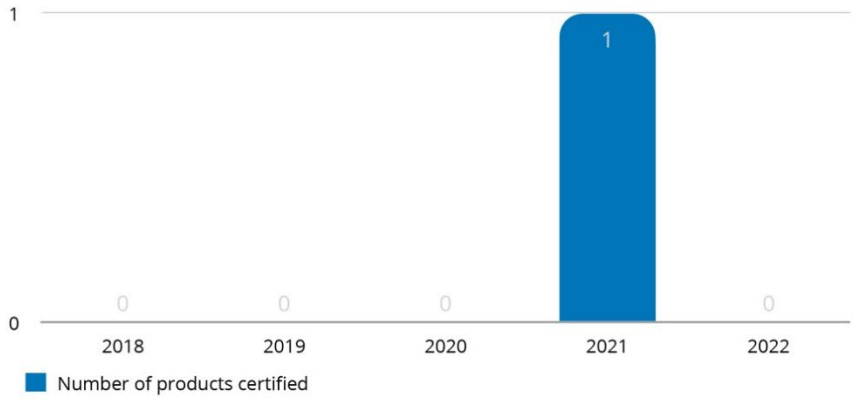
2.2.4.1 Description

According to BSI (Bundesamt für die Sicherheit in der Informationstechnik – Federal Office for Security in Information Technology) website, "the Beschleunigte Sicherheitszertifizierung (BSZ – Accelerated security certification) enables manufacturers to have their security statements regarding a product confirmed by an independent certificate. The associated certification scheme is based on predictable evaluation times and ensures a reasonable level of expenditure for product manufacturers, particularly when it comes to documentation. The evaluation follows a risk-driven approach that establishes a high level of trust in the security statements."

Date of Creation	2021
Scope	Germany
Validity of Certificate	2 years
Mutual recognition	with France through CSPN

2.2.4.2 Statistics covering the last 5 years – Certified products according to BSZ in the last 5 years

Figure 7: Certified products according to BSZ in the last 5 years



Only one product has been certified since that date to the end of 2022.

2.2.4.3 Data collection

Modality	BSI,the chief architect of secure digitalization in Germany, provided information. Therefore, the data is extracted from information provided by the Certification Body
Date of data Collection	12/04/2023

2.2.5 FiTCEM

2.2.5.1 Description

Developed by CEN/CENELEC, EN 17640 “Fixed-time Cybersecurity Evaluation Methodology for ICT Products” (FiTCEM) is inspired from the existing national methodologies from France, Spain, The Netherlands and Germany; as mentioned on the standardisation organisation website, it “is the first standard that implements by design the requirements of the European Cybersecurity Act (CSA), which establishes the rules for future cybersecurity certification schemes in Europe. For this reason, it provides future CSA schemes with the necessary building blocks to conduct evaluations at the three assurance levels "basic", "substantial" and "high", together with further legal requirements. At the same time, the standard can be adapted to the requirements of specific markets requiring cybersecurity certification or in general security evaluation.”

Date of Creation	2022 (not implemented)
Scope	European Union and members of the European standardisation system (EU members+ Iceland, Norway, Switzerland, North Macedonia, Serbia, Turkey, and the United Kingdom
Validity of Certificate	Not applicable
Mutual recognition	Not applicable

2.3 CRYPTOGRAPHIC PRODUCTS

2.3.1 FIPS 140-2 & FIPS 140-3

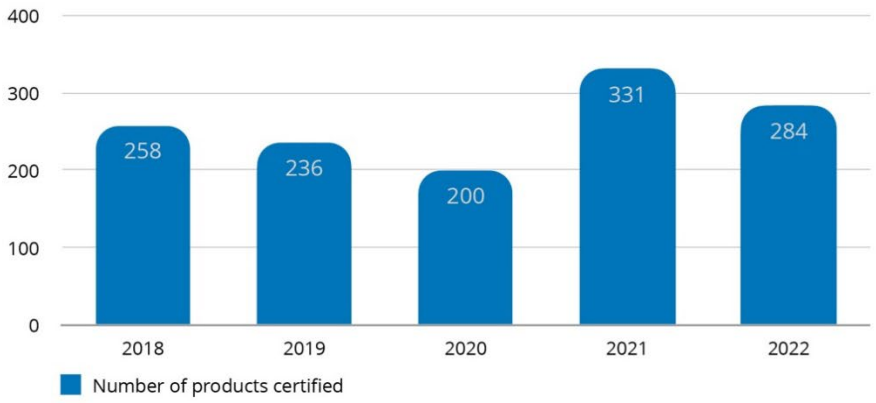
2.3.1.1 Description

FIPS is a standard developed by the National Institute of Standards and Technology (NIST) and Communications Security Establishment Canada (CSEC) to define the requirements to be satisfied by a cryptographic module in order to protect sensitive information.

Date of Creation	2001
Scope	International
Validity of Certificate	5 years
Mutual recognition	None

2.3.1.2 Statistics covering the last 5 years – Certified products according to FIPS

Figure 8: Certified products according to FIPS in the last 5 years



A large number of certificates are issued every year following this scheme. In the last 5 years, the number of certifications has never fallen below 200. 2020 was the year with the least number of certifications and 2021 the highest with 331. There was a slight decrease in 2022 compared to 2021, but it was still the second-best year with 284 certifications.

2.3.1.3 Data collection

Modality	Data collected manually from the official website of FIPS. In calculating the data, the three types of validation status that FIPS gives to certificates have been taken into account (active, historical and revoked).
Date of data Collection	02/03/2023

2.4 IDENTITY & DIGITAL SIGNATURE

2.4.1 eIDAS

2.4.1.1 Description

The eIDAS acronym stands for “electronic Identification, Authentication and trust Services” and designates Regulation (EU) No. 910/2014 of the European Parliament and Council of July 23, 2014.

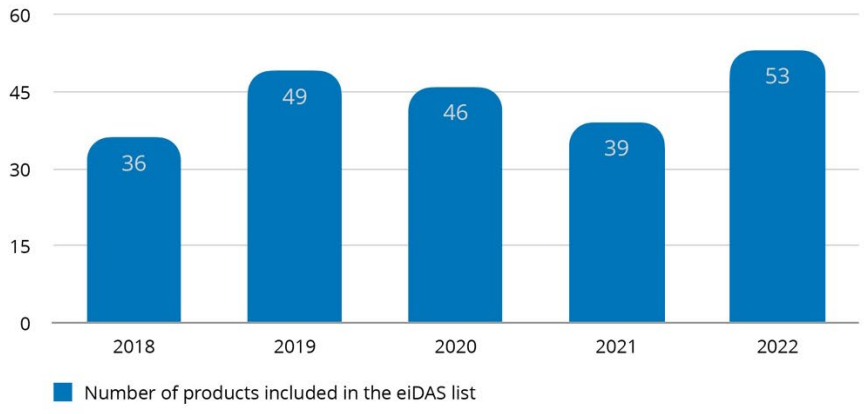
The eIDAS certification sets the standards and criteria for simple electronic signature, advanced electronic signature, qualified electronic signature, qualified certificates and online trust services. Furthermore, it rules electronic transactions and their management.

The eIDAS framework manages the certificate issuance of a qualified electronic signature, being possible to keep confidence in the identity of a person from another recognised certificate.

Date of Creation	2014
Scope	European Union
Validity of Certificate	5 years
Mutual recognition	Mutual recognition of eIDAS certificates is implicit across the European Union. In addition, there are development with MRA to 3rd countries outside the European Union.

2.4.1.2 Statistics covering the last 5 years – Number of qualified signature/seal creation devices and secure signature creation devices included in the eIDAS list

Figure 9: Number of eIDAS qualified signature/seal creation devices and secure signature creation devices in the last 5 years



During the last 5 years, there have been ups and downs in the number of certified products. Although we can observe a significant growth between 2018 and 2022.

2.4.1.3 Data collection

Modality	Data collected manually from the official website of eIDAS. Collection is based on the effective starting date description. The products with no effective starting date are not counted in this report because it is complicated to find the date on which they were listed.
Date of Data Collection	12/05/2023

2.5 ACCESS CONTROL

2.5.1 Fido

2.5.1.1 Description

The FIDO Alliance was founded by major tech players, and work on a passwordless authentication protocol began. The idea was to work on an industry standard designed around public key crypto, enabling a passwordless log-in backed purely by local authentication.

The FIDO protocols use standard public key crypto techniques to provide stronger authentication and are designed from the ground up to protect user privacy. The protocols do not provide information that can be used by different online services to collaborate and track a user across the services. Biometric information, if used, never leaves the user's device.

Date of Creation	2013
Scope	International
Validity of Certificate	No Expiration
Mutual Recognition	None

2.5.1.2 Data collection

Modality	No public data available

2.5.2 IEC 62443

2.5.2.1 Description

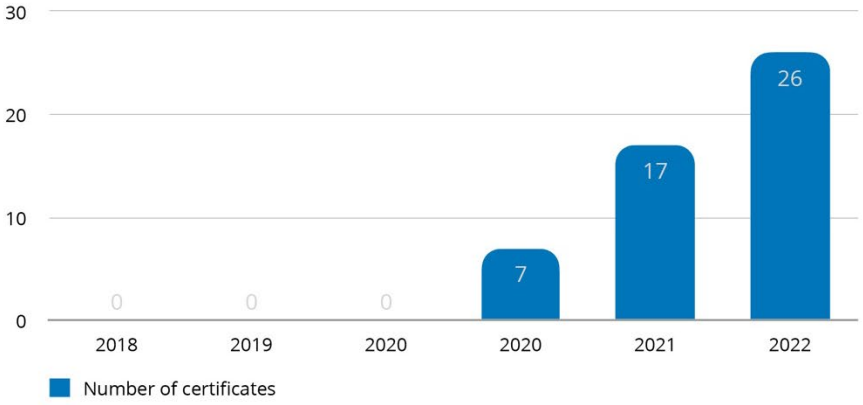
IEC 62443 is a framework developed to secure industrial automation and control systems (IACS) throughout their lifecycle. It currently includes nine standards, technical reports (TR) and technical specifications (TS). The standard family addresses not only the technology that comprises a control system, but also the work processes, countermeasures, and employees . Component certification is made against the requirements of IEC 62443-4-2.

Certificates are emitted by IECEE but private conformity assessment bodies can issue labels & certifications for these standards. ISA Secure which we also took into account in this report, is the only global IEC 62443 certification programme that requires its certification bodies to be accredited to ISO/IEC 17065.

Date of Creation	2019
Scope	International
Validity of Certificate	The duration of these certificates varies depending on the certifying body, as well as the specific programme the organisation adheres to.
Mutual Recognition	None

2.5.2.2 Statistics covering the last 5 years – Number of certified products according to IEC 62443-4-2

Figure 10: Certified products according to IEC 62443-4-2 in the last 5 years



Launched in 2020, IEC 62443-4-2 shows a rather steady increase in the past three years.

2.5.2.3 Data collection

Modality	Data collected manually from the official website of IECEE Certificates and ISA/IEC 62443-4-2 Certified Components Besides EICEE and ISA certificates, private conformity assessment bodies can issue labels & certifications for these standards. They have not been taken into account in the report.
Date of Data Collection	20/04/2023

2.6 MOBILE COMMUNICATIONS

2.6.1 APP Defense Alliance

2.6.1.1 Description

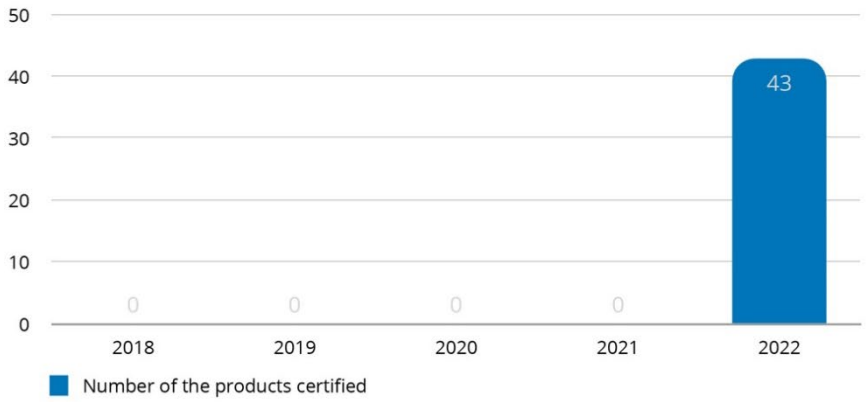
The App Defense Alliance is focused on improving applications quality. It relies on recognized industry standards, such as OWASP MASVS. Through App Defense Alliance, developers can have their apps validated against a common standard.

As of November 2023 Google, Microsoft, and Meta announced they are formally partnering as the founding steering committee to improve app security through a newly restructured App Defense Alliance, under the Joint Development Foundation, part of the Linux Foundation family.

Date of Creation	2022
Scope	International
Validity of Certificate	None
Mutual Recognition	None

2.6.1.2 Statistics covering the last 5 years – Certified products according to APP Defense Alliance

Figure 11: Certified products according to APP Defense Alliance in the last 5 years



Being the first year in which this certification was in operation, in 2022 a total of 43 certifications were done. The evolution of the App Defense Alliance announced while joining the Linux Foundation can only attract more developers to test their apps against the scheme.

2.6.1.3 Data collection

Modality	Data collected manually from the official website of APP Defense Alliance.
Date of Data Collection	01/11/2023

2.6.2 GSMA eUICC eSA

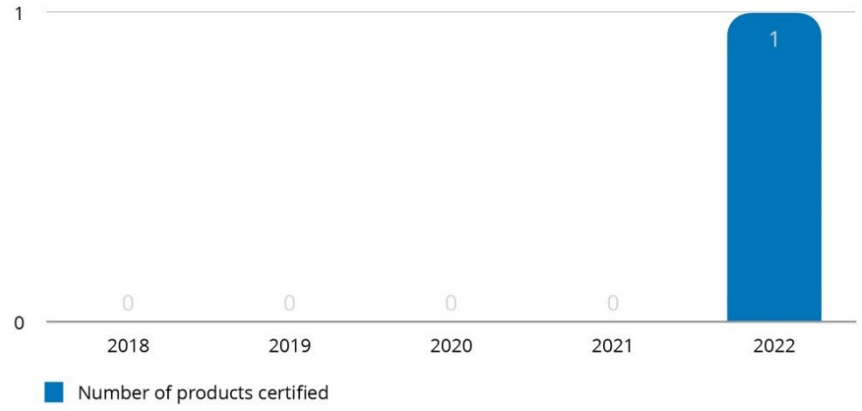
2.6.2.1 Description

GSMA eSA (eUICC Security Assurance) is based on the Common Criteria approach and the GSMA Protection Profiles (i.e., SGP.05 (for M2M devices) and SGP.25 (for Consumer devices)) but defines a more dynamic set of procedures for the security evaluation of Embedded Universal Integrated Circuit Cards (eUICCs).

Date of Creation	2021
Scope	International
Validity of Certificate	None
Mutual Recognition	None

2.6.2.2 Statistics covering the last 5 years – Certified products according to eUICC Security Assurance (eSA)

Figure 12: Certified products according to GSMA eUICC (eSA) in the last 5 years



Version 1.0 of this scheme was launched in 2021, so no products were evaluated before 2021.

2.6.2.3 Data collection

Modality	Data collected manually from GSMA Network. website
Date of Data Collection	01/11/2023

2.6.3 NESAS

2.6.3.1 Description

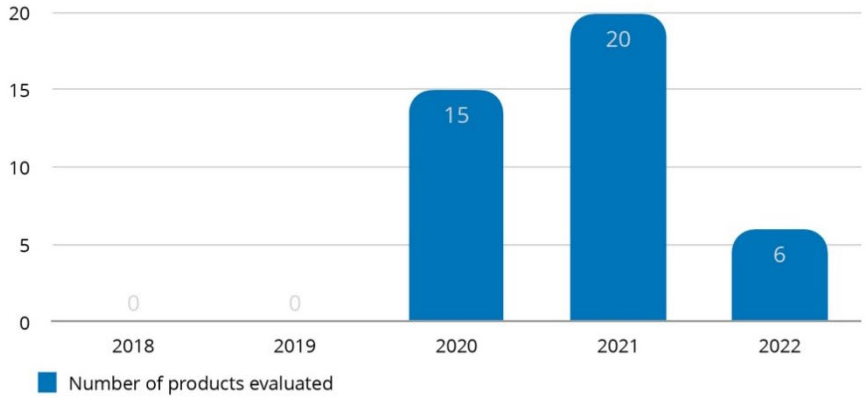
The GSMA Network Equipment Security Assurance Scheme (NESAS) facilitates improvements in network equipment security levels, across the mobile industry. Providing one universal and global security assurance framework. Ultimately, raising confidence and trust in mobile network equipment.

The purpose of the program is to audit and test network equipment vendors, and their products, against a security baseline. So, they can demonstrate to network operators that they are conforming to the desired standard. The program has been defined by industry experts through GSMA and 3GPP. Therefore, it reflects the security needs of the entire ecosystem, including governments, mobile network operators and regulators. Currently, audits and evaluations do not lead to GSMA certification but to reports.

Date of Creation	2019
Scope	International
Validity of Certificate	None
Mutual Recognition	None

2.6.3.2 Statistics covering the last 5 years – Assessed products according to NESAS

Figure 13: Assessed products according to NESAS in the last 5 years.



Version 1.0 of this scheme was launched in October 2019, so no products were evaluated before 2020. 15 products were evaluated in 2020 and 20 in 2021. However, the figures have dropped significantly in 2022.

2.6.3.3 Data collection

Modality	Data collected manually from the official website of GSMA Network. This program includes two modalities: products evaluated and process audits. Just products evaluated are included in this report
Date of Data Collection	12/04/2023

2.6.4 NESAS CCS-GI

2.6.4.1 Description

NESAS CCS-GI is a certification scheme operated by BSI, based on the same principles as GSMA NESAS accompanied with specific rules and guidelines. This national certification scheme for 5G mobile network equipment allows equipment vendors to demonstrate compliance with required security features through an IT security certificate.

Date of Creation	2022
Scope	Germany
Validity of Certificate	2.5 years
Mutual Recognition	NESAS

2.6.4.2 Statistics covering the last 5 years – Certified according to NESAS-GI

As the scheme was launched in 2022, there are no statistics from 2018-2022.

2.6.4.3 Data collection

Modality	Data collected manually from the official website of BSI - Certified Products
Date of Data Collection	13/04/2023

2.7 PAYMENT

There are several cybersecurity certifications that focus on payment security and are relevant for professionals working in the payment industry. Cybersecurity certifications play a crucial role in the payment industry due to the sensitive nature of payment transactions and the potential risks associated with handling financial data.

In the case of the traditional smart cards market, evaluations of integrated circuits and operation systems for the payment sector have reused the evaluation efforts of the Common Criteria standard being a common practice to do both certifications within the same evaluation effort.

Specific Assessment methodologies have been developed to address different specificities of the industry, either from the stakeholders individually but also through the PCI SSC standing for Payment Card Industry Security Standards Council and gathering the major actors from the industry: American Express, Discover, JCB international, MasterCard and Visa Inc.

2.7.1 EMVco

2.7.1.1 Description

EMVCo is a technical body that develops and maintain the specifications overseen by the major banking card industry players: American Express, Discover, JCB, MasterCard, UnionPay and Visa. As mentioned on their website, “EMV Specifications incorporate advanced encryption and authentication technologies to enhance card payment security as part of an industry-wide approach to battling fraud.

2.7.1.2 Data collection

Modality	As the official EMVCo website does not display products by certification date, but by expiry date, no data can be collected.

2.7.2 Common.SECC

2.7.2.1 Description

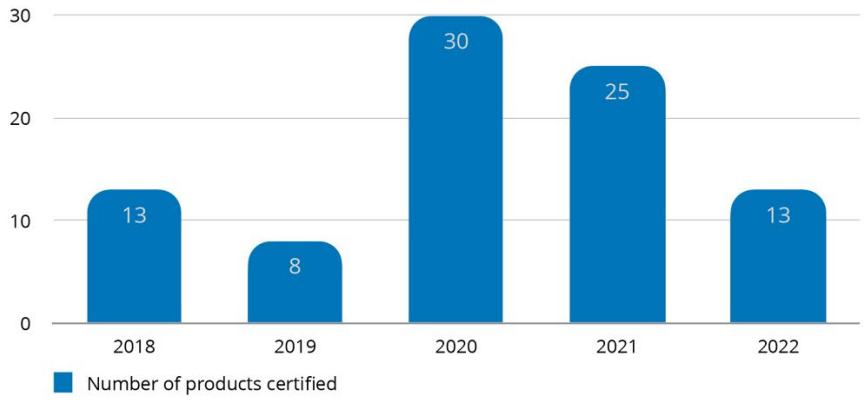
Common.SECC is an international security certification scheme for card payment. Common.SECC covers the Point of Interactions (POIs) deployed at merchants in Germany and the UK, but that scope may be extended. Common.SECC requires that terminals are evaluated for security using Common Criteria.

As mentioned on their website: “Common.SECC ensures recognition by the regulators (EU, ECB and ECSG) as providing an adequate degree of security, operational reliability and business continuity according to the ECB’s Oversight Framework for Card Payment Schemes Standards, covering all related SEPA standards of the ECSG’s Volume Book of Requirements. Regulation is aimed at banks.”

Date of Creation	2005
Scope	International
Validity of Certificate	6 years
Mutual Recognition	None

2.7.2.2 Statistics covering the last 5 years – Certified products according to Common. SECC

Figure 14: Certified products according to Common.SECC in the last 5 years



The figure shows ups and downs, with the first and last year being the same in terms of number of certificates, 13. The year with most certificates was 2020 reaching 30 certified products and the year with lowest number of certificates was 2019 with only 8 items.

2.7.2.3 Data collection

Modality	Data collected manually from the official website of Common.SECC
Date of Data Collection	13/04/2023

2.7.3 PCI CPoC

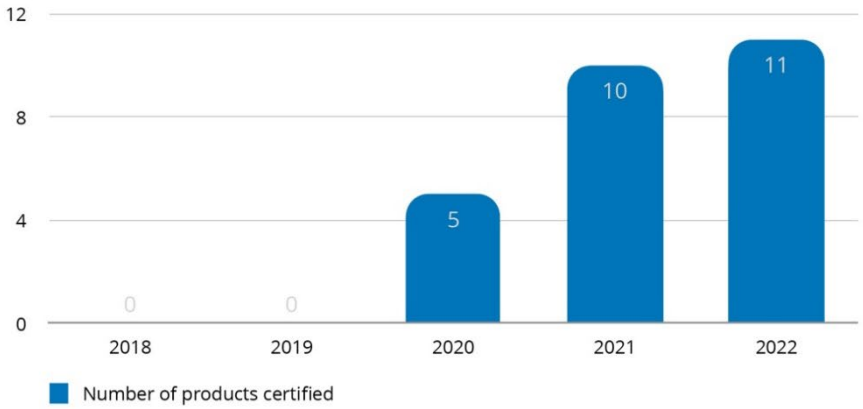
2.7.3.1 Description

The PCI CPoC Standard is the second standard released by the PCI Council to address mobile contactless acceptance. The purpose of Contactless Payments on COTS (CPoC™) Security and Test Requirements, is to provide a set of principles and requirements for a mobile payment-contactless acceptance solution on Merchant Mobile Devices Using NFC (Near-Field Communication).

Date of Creation	2019
Scope	International
Validity of Certificate	3 years
Mutual Recognition	None

2.7.3.2 Statistics covering the last 5 years – Certified products according to PCI CPoC

Figure 15: Certified products according to PCI CPoC in the last 5 years



Due to its release date, the first certified products date from 2020 with 5 items. The following year, the number of certified products doubled to 10. The statistics remained positive in 2022, but with a much slower growth rate.

2.7.3.3 Data collection

Modality	Data collected manually from the official website of PCI Security Standards.
Date of Data Collection	13/04/2023

2.7.4 PCI HSM

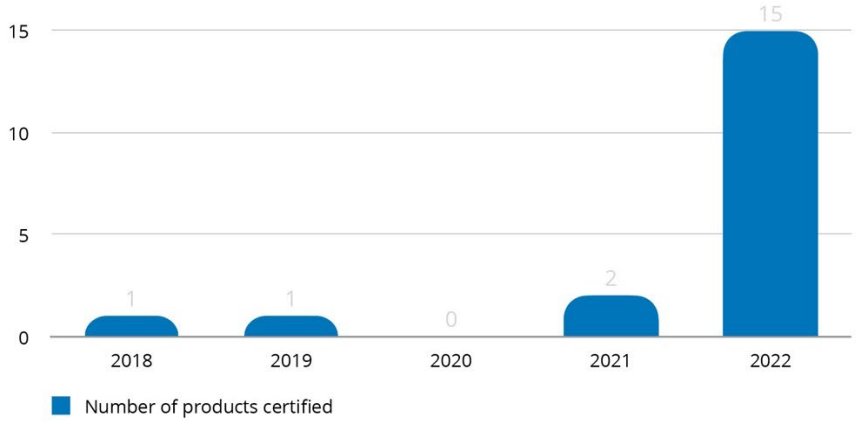
2.7.4.1 Description

The PCI HSM (Hardware security modules) standard defines a set of logical and physical security compliance standards for HSMs specifically for the payments industry.

Date of Creation	2009
Scope	International
Validity of Certificate	6 years
Mutual Recognition	None

2.7.4.2 Statistics covering the last 5 years – Certified products according to PCI HSM

Figure 16: Certified products according to PCI HSM in the last 5 years



A significant increase can be observed in 2022 with 15 products certified, compared to the previous years, where there were barely any certified products.

2.7.4.3 Data collection

Modality	Data collected manually from the official website of PCI Security Standards.
Date of Data Collection	26/10/2023

2.7.5 PCI MPoC

2.7.5.1 Description

PCI Security Standards Council (PCI SSC) published a standard designed to support the evolution of mobile payment acceptance solutions. As described on their blog, the " PCI Mobile Payments on COTS (MPoC) builds on the existing PCI Software-based PIN Entry on COTS (SPoC) and PCI Contactless Payments on COTS (CPoC) Standards which individually address security requirements for solutions that enable merchants to accept cardholder PINs or contactless payments, using a smartphone or other commercial off-the-shelf (COTS) mobile device. The PCI MPoC Standard aims to provide increased flexibility not only in how payments are accepted, but in how COTS-based payment acceptance solutions can be developed, deployed, and maintained.

Date of Creation	2022
Scope	International
Validity of Certificate	3 years
Mutual Recognition	None

2.7.5.2 Statistics covering the last 5 years – Certified products according to PCI MPoC

Due to its recent creation, there are no certified products under this standard yet.

2.7.5.3 Data collection

Modality	Data collected manually from the official website of PCI Security Standards.
Date of Data Collection	14/04/2023

2.7.6 PCI PTS (Payment Terminals)

2.7.6.1 Description

Payment Terminals are evaluated using the PCI-PTS standard, which is defined by the Payment Card Industry Security Standards Council (PCI SSC) and addresses the logical and physical protection of the cardholder and other sensitive data in payment security devices. Th standard evaluates the products against a common module of requirements that refer to safe construction and design of the devices and another set of optional requirements depending on the features implemented by the module such as communication with wireless standard or the ability to encrypt account data.

Date of Creation	2010
Scope	International
Validity of Certificate	Depending on the version of the norm and the approval class of the product
Mutual Recognition	None

2.7.6.2 Data collection

Modality	As the official PCI website does not display products by certification date, but by expiry date, no data can be collected

2.7.7 PCI SPoC

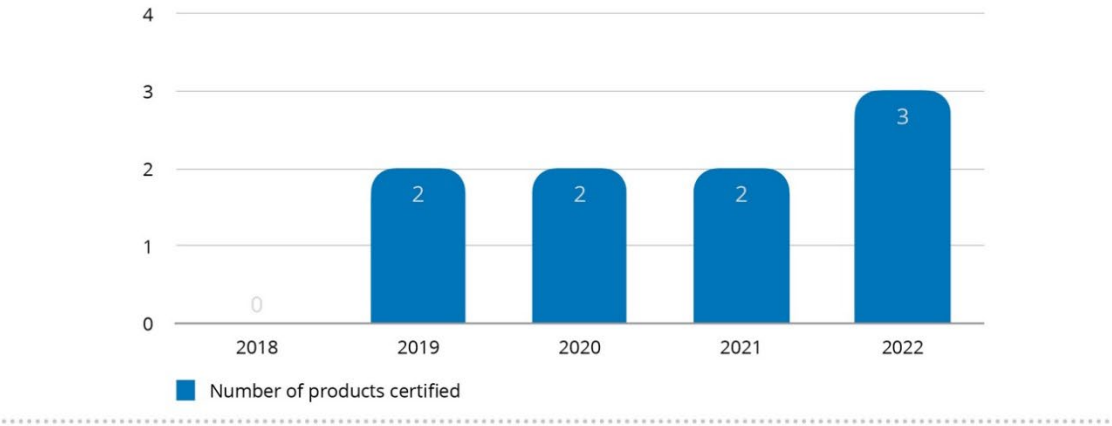
2.7.7.1 Description

PCI SPoC is a security standard announced by the Payment Card Industry Security Standards Council (PCI SSC) to regulate the security of electronic mobile transactions on commercial off-the-shelf devices (COTS).

Date of Creation	2018
Scope	International
Validity of Certificate	3 years
Mutual Recognition	None

2.7.7.2 Statistics covering the last 5 years - Certified products according to PCI SPoC

Figure 17: Certified products according to PCI SPoC in the last 5 years



Due to its inception date, April 2018, no certified products exist in that year. In the period from 2019 to 2021, only two products per year are certified. The trend rises in 2022 with 3 certified products.

2.7.7.3 Data collection

Modality	Data collected manually from the official website of PCI Security Standards.
Date of Data Collection	14/04/2023

2.8 TRANSPORT

Transport sector started to develop its own standards and assessment methodologies in order to support ticketing systems. Existing schemes focus on the interoperability of ticketing systems and the security of the different smart mobility solutions.

2.8.1 Calypso

2.8.1.1 Description

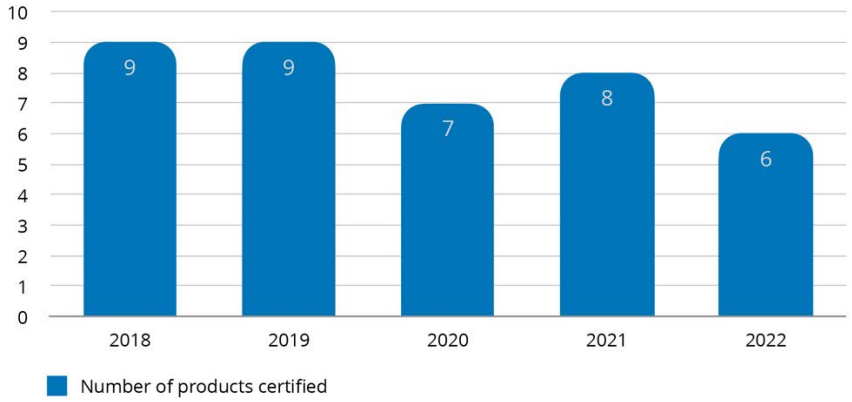
Calypso is an "open, secure ticketing standard that promotes innovation" and is used in more than 25 countries globally. It has been designed by transport operators gathered within the Calypso Networks Association:

The scheme's website indicates that "Calypso details how to securely transmit a ticket's data between a traveller's card, a phone or watch for example, and a transport/mobility authorities' ticketing reader – such as an access control barrier, vending machine, handheld reader. The specifications cover card personalisation, purchase, reload, validation and control of tickets and transport contracts."

Date of Creation	1993
Scope	International (25 countries), including 12 EU Members States: Austria, Belgium, France, Germany, Italy, Latvia, Malta, The Netherlands, Poland, Portugal, Romania and Spain.
Validity of Certificate	7 years
Mutual Recognition	None

2.8.1.2 Statistics covering the last 5 years – Certified products according to Calypso

Figure 18: Certified products according to Calypso in the last 5 years



A slight downward progression in 2022 is noted, with only 6 certified products, compared to 2018 and 2019 with 9 items. A fairly stable number of certified products is showed.

2.8.1.3 Data collection

Modality	Data collected manually from the official website of Calypso. All types of certified cards are included:
Date of Data Collection	12/04/2023

2.8.2 FeliCa

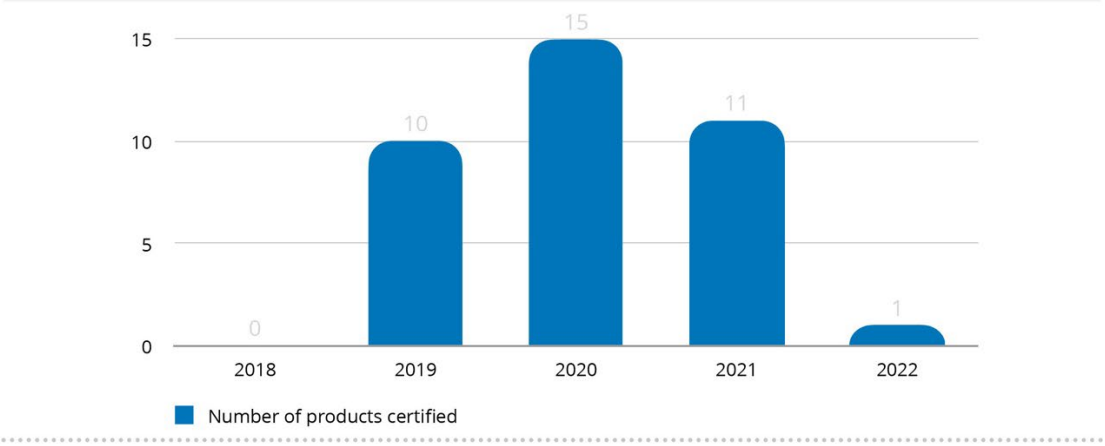
2.8.2.1 Description

FeliCa is an IC Card technology developed by Sony, which has a wide variety of uses, such as in ticketing systems for public transportations, e-money, and residence door keys. FeliCa supports the entire life cycle of IC cards including application development, card issuance, personalisation, and daily operation.

Date of Creation	1997
Scope	Hong Kong, Indonesia, Japan, Macau, the Philippines, Singapore and the United States.
Validity of Certificate	10 years
Mutual Recognition	None

2.8.2.2 Statistics covering the last 5 years – Certified products according to FeliCa

Figure 19: Certified products according to FeliCa in the last 5 years



Regarding the figures a certain instability in the different years is remarkable. The year that stands out above all others is 2020 with 15 certifications. However, 2018 shows no certification and 2022 just one.

2.8.2.3 Data collection

Modality	Data collected manually from the official website of FeliCa Networks.
Date of Data Collection	12/04/2023

2.8.3 MiFare

2.8.3.1 Description

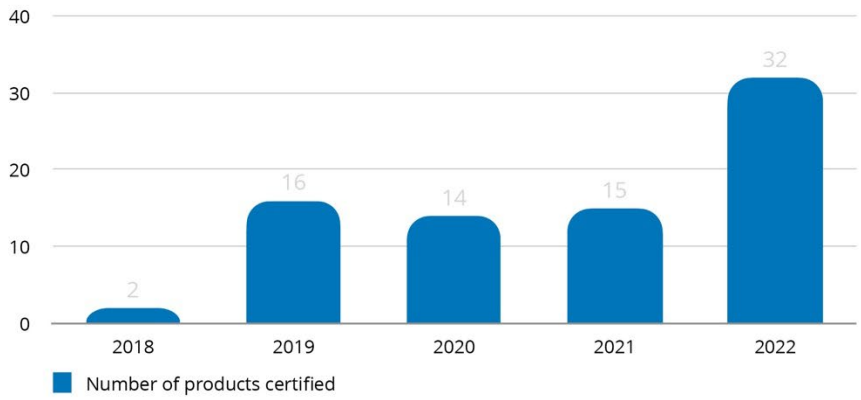
MIFARE® is NXP's brand providing a wide range of contactless IC products, integrated circuit (IC) chips used in contactless smart cards and proximity cards. One of the business areas at MIFARE provides smart mobility solutions: ferry cards, car rentals, fleet management, road tolling, mobile ticketing, taxi cards, parking, transport ticketing or bike rentals.

The cybersecurity part of MIFARE is based on various levels of the ISO/IEC 14443 Type A 13.56 MHz contactless smart card standard. It uses AES and DES/Triple-DES encryption standards, as well as an older proprietary encryption algorithm, Crypto-1.

Date of Creation	2007
Scope	International.
Validity of Certificate	5 years
Mutual Recognition	None

2.8.3.2 Statistics covering the last 5 years – Certified products according to MiFare

Figure 20: Certified products according to MiFare in the last 5 years



The progression in terms of the number of certified products is quite remarkable in the past five years with one certificate delivered in 2018 to 32 delivered in 2022. The trend is being quite stable during the years 2019, 2020 and 2021, with around 15 products per year.

2.8.3.3 Data Collection

Modality	Data collected manually from the official website of MiFare Certificates.
Date of Data Collection	12/04/2023

2.9 IOT LABELS

IoT (Internet of Things) labels are the new family of assessment methodologies born in the last years. While remaining voluntary these schemes aim at bringing some clarity in the diverse ecosystem of IoT devices.

IoT products time-to-market and cost sensitivities are key drivers for these labels.

2.9.1 IoT Label – Germany

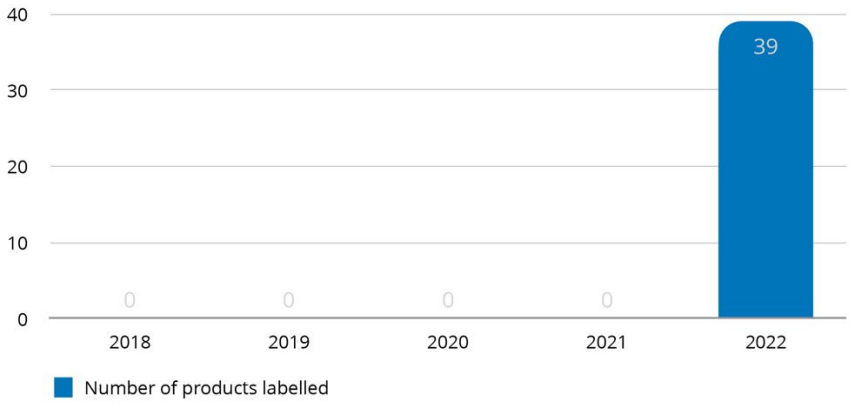
2.9.1.1 Description

According to the IT-Security Act 2.0 published in 2021, the BSI was tasked with introducing a voluntary IT Security Label. The IT Security Label creates transparency for consumers, revealing basic security features of IT products. While more and more everyday objects are linked to the Internet and with other smart things, it is becoming increasingly difficult for consumers to assess which devices and services possess specific security requirements.

Date of Creation	2021
Scope	Germany
Validity of Certificate	2 years
Mutual Recognition	Agreement with Singapore cybersecurity IoT label thanks to a Memorandum of Understanding (MoU) signed in 2022 mutually recognising the cybersecurity labels issued by CSA and the Federal Office for Information Security of Germany (BSI)

2.9.1.2 Statistics covering the last 5 years – Products labelled according to IoT Label – Germany

Figure 21: Products labelled according to IoT Label – Germany in the last 5 years



Evaluation started in 2022 with a total of 37 products tagged with this label. This represents an impressive number for a newly published voluntary scheme.

2.9.1.3 Data collection

Modality	Data collected manually from the official BSI website.
Date of Data Collection	14/04/2023

2.9.2 IoT Label – Finland

2.9.2.1 Description

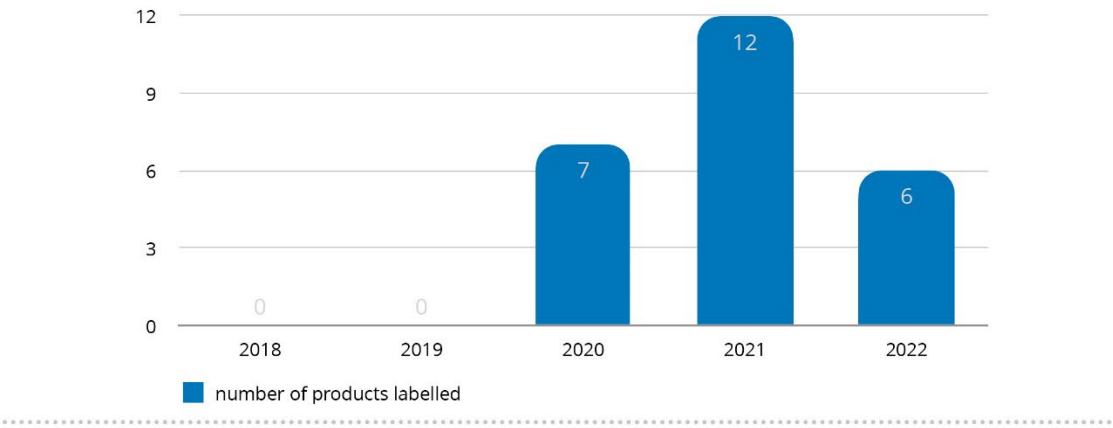
The National Cyber Security Centre Finland (NCSC-FI – Kyberturvallisuuskeskus) acting as the National Communications Security Authority is part of Traficom, the Finnish National Transport and Communications Agency, the authority responsible for permit, license, registration, approval, safety and security matters in Finland.

The agency created the Cybersecurity Label to help the consumer make more secure choices when purchasing IoT devices or services. The voluntary Label shows that the product is secure by design, and that certain security features are updated for the duration of the Label. The requirements of the Label are based on ETSI EN 303 645 and have been prioritised using the OWASP IoT TOP 10 Threat List (2018).

Date of Creation	2020
Scope	Finland
Validity of Certificate	N/A
Mutual Recognition	Agreement with Singapore cybersecurity IoT label thanks to a Memorandum of Understanding (MoU) signed in 2021 mutually recognising the Cybersecurity Labels issued by CSA and the Transport and Communications Agency of Finland (Traficom)

2.9.2.2 Statistics covering the last 5 years – Products labelled according to IoT Label – Finland

Figure 22: Products labelled according to IoT Label – Finland in the last 5 years



The first year of the label showcase 7 labelled product. In 2021, a growth in the number of products is shown, being 12 products included. However, in 2022, the number of products dropped by half even lower than in the first year of the scheme's launch.

2.9.2.3 Data collection

Modality	Data collected manually from the official website of The National Cyber Security Centre Finland (NCSC-FI)
Date of Data Collection	14/04/2023

2.9.3 IoT Label – Singapore

2.9.3.1 Description

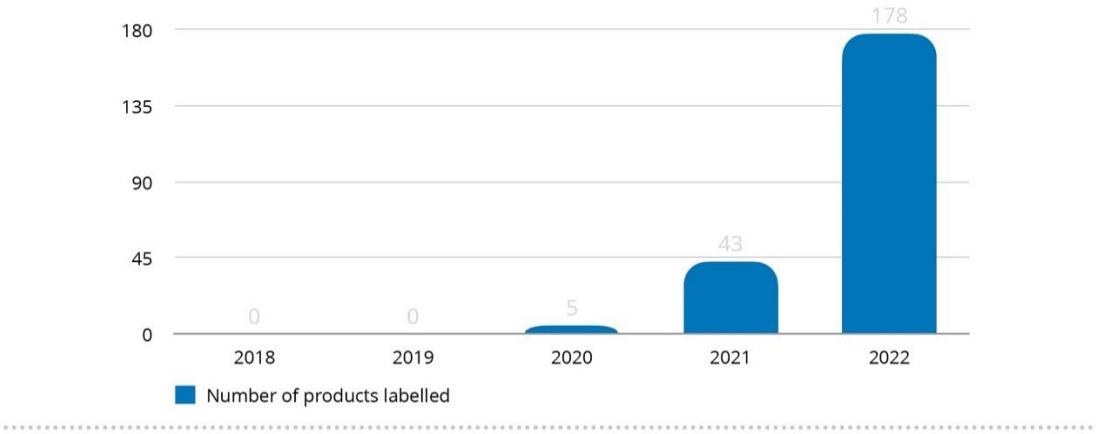
According the official web of The Cyber Security Agency of Singapore (CSA): “CSA has launched the Cybersecurity Labelling Scheme (CLS) for consumer smart devices, as part of efforts to improve Internet of Things (IoT) security, raise overall cyber hygiene levels and better secure Singapore's cyberspace.” . Under the scheme, smart devices are rated according to their levels of cybersecurity provisions. This enables consumers to identify products with better cybersecurity provisions and make informed decisions.

The CLS was first introduced to cover Wi-Fi routers and smart home hubs. These products were prioritised because of their wider usage, as well as the impact that a compromise of the products could have on users. It has since been extended to include all categories of consumer IoT devices, such as IP cameras, smart door locks, smart lights and smart printers.

Date of Creation	2020
Scope	Singapore
Validity of Certificate	3 years
Mutual Recognition	**Finland:** Consumer IoT products that have met the requirements of Finland's Cybersecurity Label are recognised as having met the requirements of Level 3 of Singapore's Cybersecurity Labelling Scheme, and products with CLS Level 3 and above are recognised by Finland to have met their requirements. **Germany:** Smart consumer products issued with Germany's IT Security Label will be recognised by CSA to have fulfilled Level 2 of Singapore's Cybersecurity Labelling Scheme, and products with CLS Level 2 and above are recognised by Germany to have met their requirements

2.9.3.2 Statistics covering the last 5 years – Products labelled according to IoT Label – Singapore

Figure 23: Products labelled according to IoT Label – Singapore in the last 5 years



As all IoT label, CLS is a relatively recent scheme, therefore, the first certified products dates back to 2020. The growth in the number of Certified labelled under this scheme is exponential, in just three years the number of labelled products jumped from 5 to 178.

2.9.3.3 Data collection

Modality	The Certification Body Singapore (CSA Singapore) provided the information. Therefore, the data is extracted from information provided by the Certification Body.
Date of Data Collection	12/04/2023

2.9.4 PSA Certified

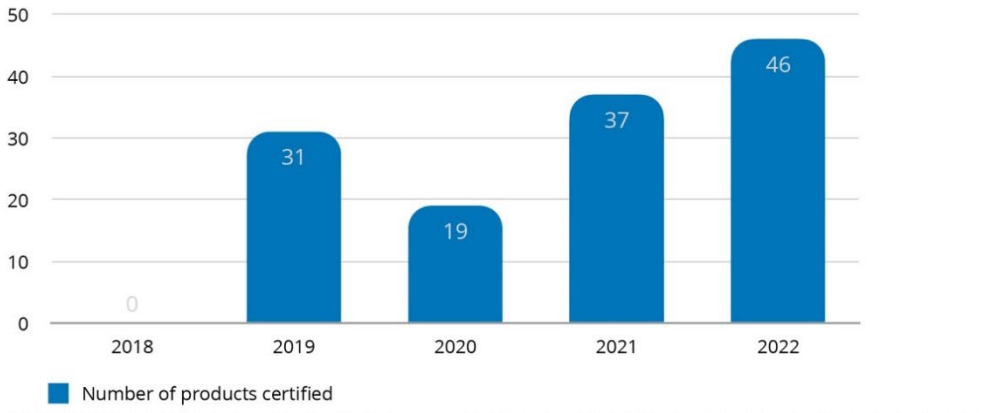
2.9.4.1 Description

PSA Certified (PSA for Platform Security Architecture) is a security certification dedicated to IoT hardware such as chips, software and devices. The scheme provides standardised resources to limit the growing fragmentation of IoT requirements and ensure security of the solution from development phase. The different levels of certification address different stakeholders;

Date of Creation	2019
Scope	International
Validity of Certificate	None
Mutual Recognition	None

2.9.4.2 Statistics covering the last 5 years

Figure 24: Certified products according to PSA in the last 5 years



PSA certifications started in 2019, where a total of 31 are reached. There is a small decline the following year, with 19 certifications in 2020. From here the trend is upward, totalling 37 certifications in 2021 and 46 in 2022.

2.9.4.3 Data collection

Modality	Data collected manually from the official website of PSA Certified.
Date of Data Collection	10/04/2023

2.9.5 ioXt

2.9.5.1 Description

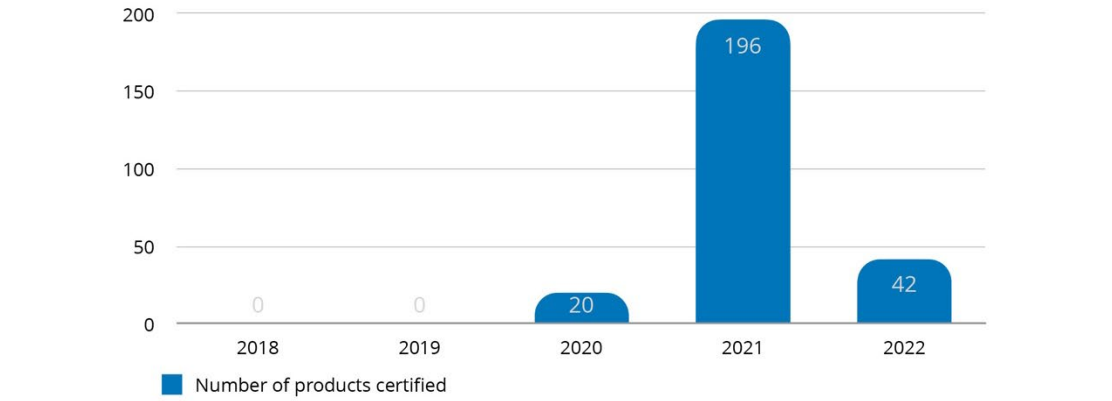
The ioXt security certification has been developed by the ioXt Alliance founded by leading technology companies willing to build confidence in IoT products.

According to the ioXt website: “The program measures a product against each of the eight ioXt principles with clear guidelines to quantify the appropriate level of security required for a specific product.” The scheme is addressing products involved with: smart home, lighting controls, smart building, IoT Bluetooth, smart retail, portable medical, smart home, mobile apps, pet trackers, routers and automotive technology.

Date of Creation	2020
Scope	International
Validity of Certificate	None
Mutual Recognition	None

2.9.5.2 Statistics covering the last 5 years – Certified products according to ioXt

Figure 25: Certified products according to ioXt in the last 5 years



The certifications began in 2020, with a total of 20 certifications. The following year there was a more than significant upturn in certifications, reaching a total of 196. Subsequently, in 2022, certifications dropped significantly again with a total of only 42.

2.9.5.3 Data collection

Modality	Data collected manually from the official website of ioXt.
Date of Data Collection	14/04/2023

2.9.6 Matter

2.9.6.1 Description

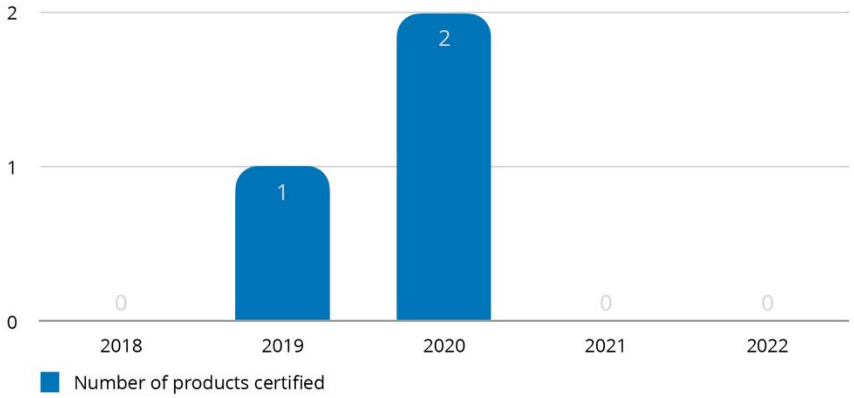
Created in 2002, the Connectivity Standards Alliance (CSA), gathers more than 600 entities offering IoT technologies and solutions. Amongst other standards, the organisation developed and maintains Matter. Now published in version 1.2, the standard aims at improving and securing interoperability between IoT devices and technologies. Matter proposes a unifying protocol enabling devices to connect to different cloud services and reinforces, and secure, interoperability by addressing the application layer.

Date of Creation	

Date of Creation	2015
Scope	International
Validity of Certificate	The user of the certified product should consider the results of the certification within an appropriate risk management process and define the period of time after which the re-assessment of the product is required.
Mutual Recognition	None

2.9.7.2 Statistics covering the last 5 years – Certified products according to Global Platform TEE

Figure 27: Certified products according to Global Platform TEE in the last 5 years



Just three certifications have been issued, 1 in 2019 and 2 in 2020. In the following years certifications drop to 0.

2.9.7.3 Data collection

Modality	Data collected manually from the official website of Global Platform Certified Products. The certified products have been filtered by the security category, as these are the ones that include a cybersecurity module in the product.
Date of Data Collection	10/04/2023

2.9.8 Global Platform SESIP

2.9.8.1 Description

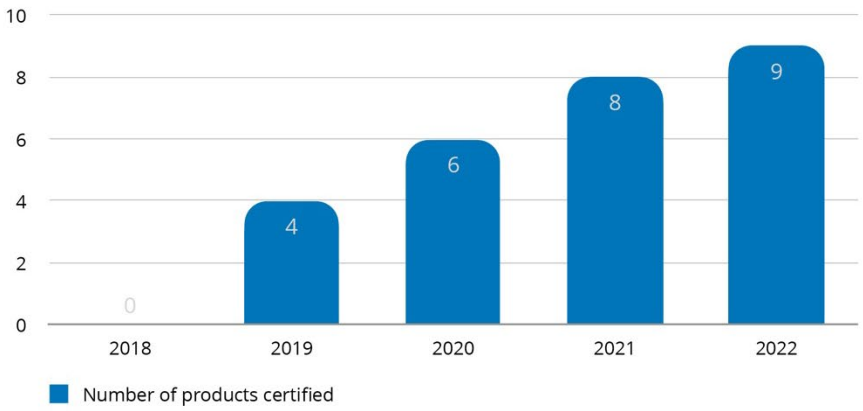
Inspired by the experience of the Common Criteria, the SESIP methodology (Security Evaluation Standard for IoT Platforms) provides a common and optimised approach for evaluating the security of IoT components and platforms.

As per November 2023, the SESIP methodology has been adopted as a European Standard by CEN/CENELEC, as EN 17927.

Date of Creation	2018
Scope	International
Validity of Certificate	2 Years.
Mutual Recognition	None

2.9.8.2 Statistics covering the last 5 years – Certified products according to SESIP

Figure 28: Certified products according to SESIP in the last 5 years



Certifications began in 2019, starting with a total of 4. The trend from this year onwards is steadily increasing, to reach a total of 9 certifications in 2022.

2.9.8.3 Data collection

Modality	Data collected manually from the official website of SESIP Certificates.
Date of Data Collection	17/04/2023

3. CLOUD SERVICES

Cloud services bring by nature a new layer of risks that requires a different approach in terms of security evaluation. While most assessment methodologies are rather young and know a timid adoption, ISO/IEC 27001 stands as the inevitable standards to address information security management systems.

However, the question of data managed raised through the use of cloud services lead several countries to build their own assessment scheme.

3.1 ISO/IEC 27001

3.1.1 Description

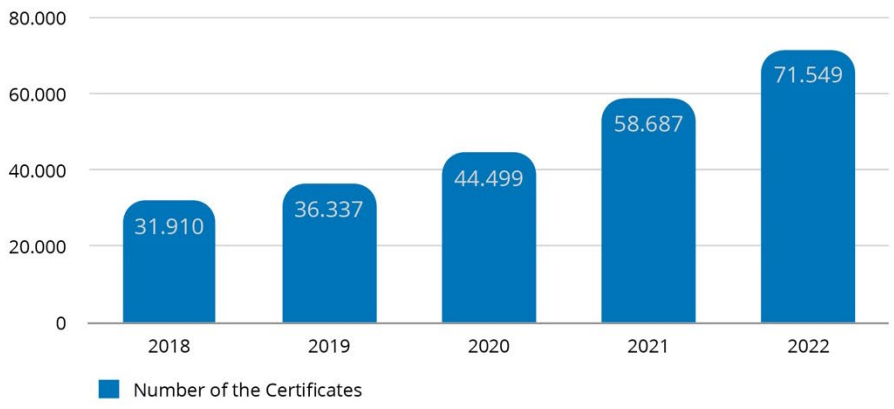
While ISO/IEC 27001, the world's best-known standard for information security management systems (ISMS**), is not specifically designed for cloud computing services, it provides relevant best practices that are used as references for many cloud certification schemes.**

ISO Standard website indicates that: "the ISO/IEC 27001 standard provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system. (…) Conformity with ISO/IEC 27001 means that an organisation or business has put in place a system to manage risks related to the security of data owned or handled by the company, and that this system respects all the best practices and principles enshrined in this International Standard."

Date of Creation	2005
Scope	International
Validity of Certificate	3 years
Mutual Recognition	None

3.1.2 Statistics covering the last 5 years – Certified ISMS, including cloud computing services according to ISO/IEC 27001

Figure 29: Certified ISMS, including cloud computing services, according to ISO/IEC 27001 in the last 5 years



While the trend is comparable, the past 5 years figure shows a number of certificates at another order of magnitude with other schemes. The adoption of ISO/IEC 27001 is well above any other security assessment methodologies presented in the report. Number of certificates keeps increasing every year: 2021 indicates an increase of 32% maybe due to external factors like Covid that affected the previous year. 2020 and 2022 both indicate an increase of 22% of certificate compared to the previous year.

3.1.3 Data Collection

Modality	Data comes from the survey that ISO leads every year
Date of Data Collection	30/11/2023

3.2 EU CLOUD CODE OF CONDUCT

3.2.1 Description

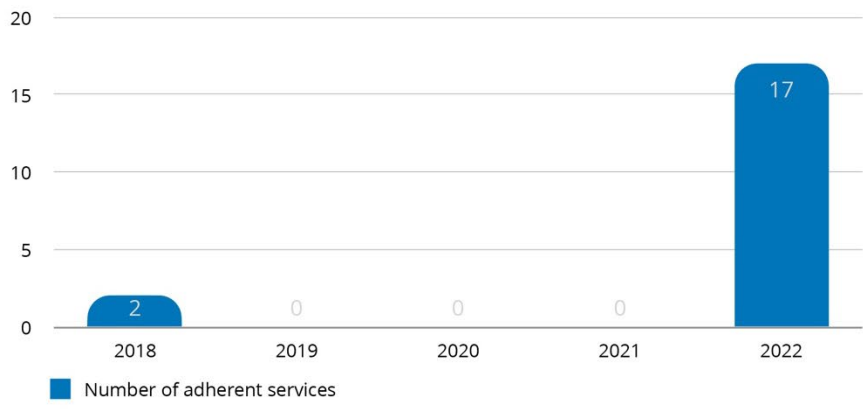
The EU Cloud Code of Conduct (EU Cloud CoC) was drafted together with the industry and authorities of the European Union. The first version of the Code was published in April 2017 and the first product certified was in 2018.

As mentioned on the website: "The EU Cloud Code of Conduct consists of requirements for CSPs that wish to adhere to the Code, plus a governance section that is designed to support the effective and transparent implementation, management, and evolution of the Code.(…) The primary objective of the EU Cloud CoC is to harmonize the implementation of GDPR requirements."

Date of Creation	2017
Scope	European Union
Validity of Certificate	1 year
Mutual Recognition	None

3.2.2 Statistics covering the last 5 years – Adhered cloud computing services according to EU Cloud Code of Conduct

Figure 30: Services adhered according to EU Cloud Code of Conduct in the last 5 years



The data shown is certainly odd with 2 adherent services in 2018 and 17 in 2022, being an empty period in 2019, 2020 and 2021 with no new services adhering.

3.2.3 Data Collection

Modality	Data collected manually from the official website of EU Cloud CoC.
Date of Data Collection	29/05/2023

3.3 C5 – GERMANY

3.3.1 Description

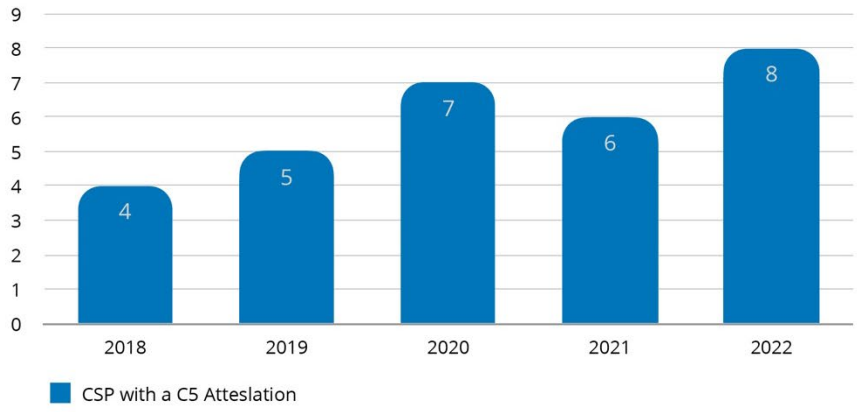
The C5 (Cloud Computing Compliance Criteria Catalogue) published by the German Federal Office for Information (BSI) Security specifies minimum requirements for secure cloud computing. It is primarily intended for professional cloud providers, their auditors and customers.

European and global cloud providers, as well as a wide range of cloud services. Medium-sized and small providers now use the catalogue too. C5 gives cloud customers an important guide to selecting a provider. It is the foundation for putting a customer-specific system of risk management in place. C5 was completely revised in 2019 to consider the latest developments in detail and increase quality still further.

Date of Creation	2016
Scope	Germany
Validity of Certificate	1 year
Mutual Recognition	None (a reciprocal agreement called “ESCloud” was signed with the French SecNumCloud but not applied)

3.3.2 Statistics covering the last 5 years – Cloud Services Providers with a C5 attestation

Figure 31: CSP with a C5 attestation in the last 5 years



3.3.3 Data Collection

Modality	Personal website listing all attestations: Home (c5-attestations.com)
Date of Data Collection	05/12/2023

3.4 SECNUMCLOUD – FRANCE

3.4.1 Description

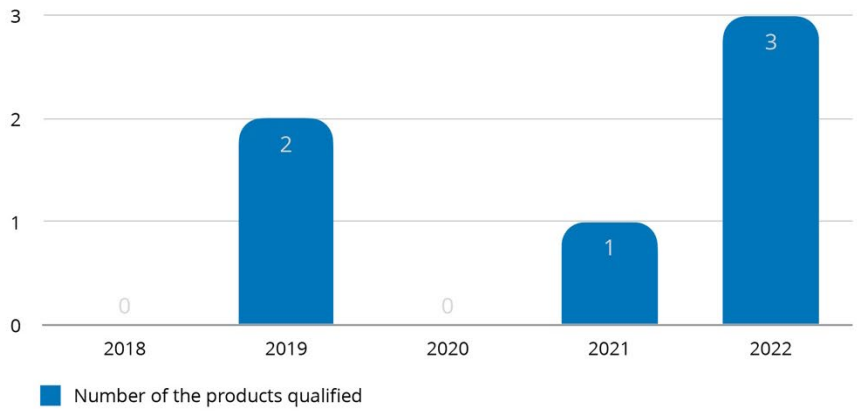
SecNumCloud is the qualification proposed by ANSSI to distinguish cloud operators who respect good security practices. It offers services in PaaS (Platform as a Service), IaaS (Infrastructure as a Service) or SaaS (Software as a service).

The objectives of SecNumcloud are to promote, enrich and improve the offer of cloud providers for public and private entities wishing to outsource the hosting of their data, applications or information systems to trusted providers. SecNumCloud certification is built upon international standards like ISO/IEC 27001, ISO/IEC 27017, and ISO/IEC 27018 which outline security requirements.

Date of Creation	2016
Scope	France
Validity of Certificate	3 years
Mutual Recognition	None (a reciprocal agreement called “ESCloud” was signed with the German C5 but not applied)

3.4.2 Statistics covering the last 5 years – Qualified cloud services according to SecNumCloud

Figure 32: Cloud Computing services qualified according to SecNumCloud in the last 5 years



In 2019, two Cloud computing services were qualified, while none were qualified in 2020. Although the numbers remain low, the years after show an increase in terms of qualification.

3.4.3 Data Collection

Modality	Data collected directly from ANSSI.
Date of Data Collection	14/04/2023

3.5 ZEKER-ONLINE – THE NETHERLANDS

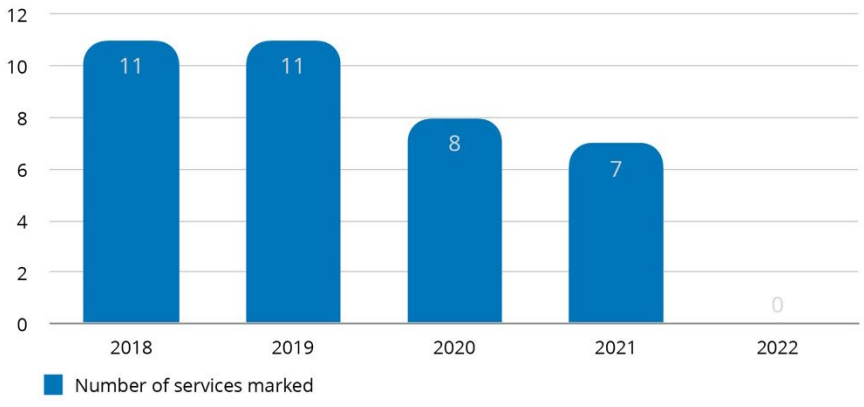
3.5.1 Description

The Zeker-OnLine Quality Mark is granted by the Foundation Zeker-OnLine, owner of the Quality Mark. This Foundation grants the Quality Mark to the providers of cloud solutions on the basis auditor's report confirming that the provider's solution complies with the quality requirements.

Date of Creation	2013
Scope	The Netherlands
Validity of Certificate	The duration or years of validity of a Zeker-OnLine certificate may vary depending on the terms and conditions set by the certifying body and the specific requirements of the program. Generally, security certificates have limited validity and require periodic renewals to ensure that companies continue to meet evolving security requirements
Mutual Recognition	None

3.5.2 Statistics covering the last 5 years – Services marked according to Zeker-OnLine

Figure 33: Services marked according to Zeker-OnLine in the last 5 years



The number of services has been decreasing in recent years. From 11 in 2018 to 0 in 2022. According to the Foundation Zeker-OnLine, the evaluations have been temporarily stopped due to some reasons among which we can find that there was little interest in this scheme among both the consumers and users and the seal of approval has been losing added value in the market. Therefore, there was no longer any commitment from the Tax Authority to promote the seal of approval.

3.5.3 Data Collection

Modality	Foundation Zeker-OnLine provided the information. Therefore, the data is extracted from information provided by the Foundation.
Date of Data Collection	09/06/2023

3.6 ENS – SPAIN

3.6.1 Description

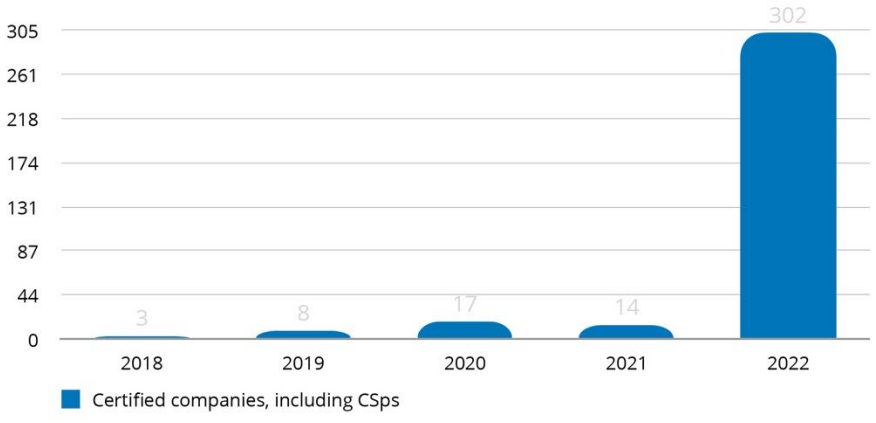
The National Security Framework, is applicable to the entire Public Sector (ENS by its acronym in Spanish), as well as its suppliers. It offers a common framework of basic principles, requirements and security measures for the adequate protection of the information processed and the services provided. The framework does not only apply to cloud services providers (CSPs) but to any company and entity providing ICT services to the public sector.

The last update of the scheme is from 2022 with Royal Decree 311/2022.

Date of Creation	2010
Scope	Spain
Validity of Certificate	2 years
Mutual Recognition	None

3.6.2 Statistics covering the last 5 years – Certified Companies, including CSPs, according to ENS

Figure 34: Certified Companies, including CSPs, according to ENS in the last 5 years



3.6.3 Data Collection

Modality	Data collected manually on the website. Does not only include CSPs but all certified private companies providing ICT services.
Date of Data Collection	05/12/2023

3.7 FEDRAMP – UNITED STATES

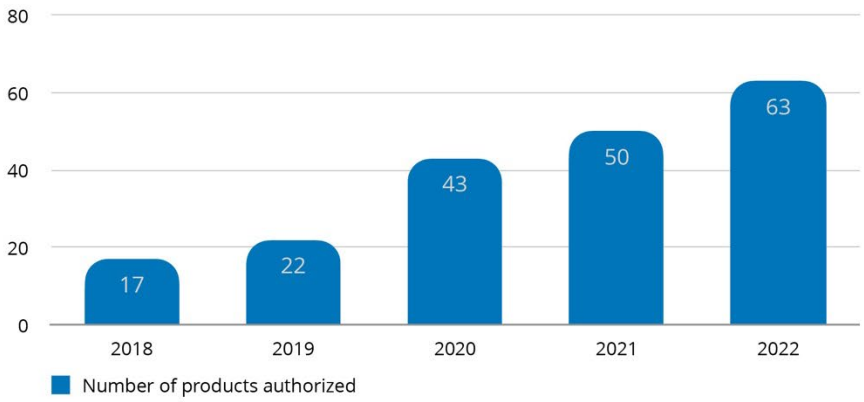
3.7.1 Description

As mentioned on their website: "The Federal Risk and Authorisation Management Program (FedRAMP®) was established in 2011 to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the United States' federal government. FedRAMP empowers agencies to use modern cloud technologies, with an emphasis on security and protection of federal information. (…) It promotes the adoption of secure cloud services by providing a standardised approach to security and risk assessment for cloud technologies and federal agencies."

Date of Creation	2011
Scope	United States
Validity of Certificate	1 year
Mutual Recognition	None

3.7.2 Statistics covering the last 5 years – Authorised services according to FedRAMP

Figure 35: Services authorised according to FedRAMP in the last 5 years



Looking at the data shown in the Figure, a gradual increase in the number of authorised services is being noted, from 17 in 2018 to 63 achieved in 2022. The trend is upward in the coming years.

3.7.3 Data Collection

Modality	Data collected manually from the official website of FedRAMP
Date of Data Collection	25/05/2023

3.8 CSA STAR

3.8.1 Description

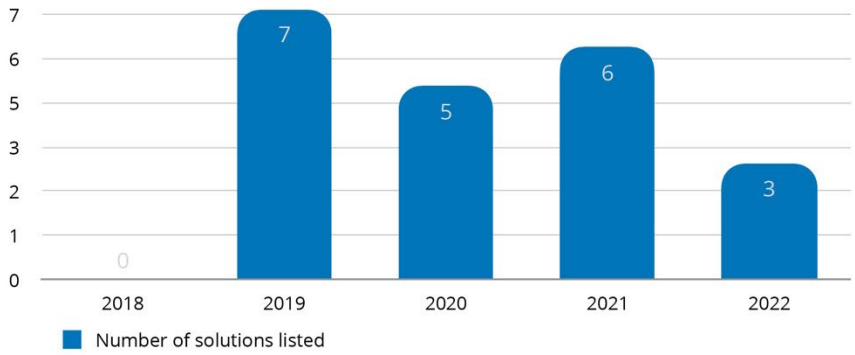
CSA STAR stands for Cloud Security Alliance, Security Trust and Assurance Registry. It is a certification led by the Cloud Security Alliance Association gathering members from enterprises and Cloud Services Providers (CSPs) worldwide. It includes two levels of assurance, the first one being a self-assessment. CSA STAR covers both

operational security and privacy legal compliance. The certification is designed to work as a complement to the ISO/IEC 27001 framework and aims at demonstrating a higher level of security.

Date of Creation	2013
Scope	International
Validity of Certificate	3 years – ISO/IEC 27001 is a prerequisite to maintain the certification valid
Mutual Recognition	None

3.8.2 Statistics covering the last 5 years – Solutions listed according to CSA STAR

Figure 36: Solutions listed according to CSA STAR in the last 5 years



The data included in this report are only for level 2 listed solutions, those validated by a third party. The number of listed solutions in the last 5 years is not very high, with 2019 being the year with the most solutions included, with 7 listed solutions.

3.8.3 Data Collection

Modality	Data collected manually from the official website of CSA.
Date of Data Collection	29/05/2023

3.9 HITRUST CSF

3.9.1 Description

HITRUST was founded in 2007 in collaboration with privacy, information security and risk management leaders from the public and private sectors -mostly health sector. The organisation developed and maintains the HITRUST CSF (Common Security Framework) which integrates and harmonizes existing information protection requirements such as ISO, NIST, PCI, the European GDPR and HIPAA. It allows tailoring of the requirements by an organization based on specific organizational, system, and compliance risk factors.

Date of Creation	2007
Scope	International
Validity of Certificate	2 years
Mutual Recognition	None

3.9.2 Data Collection

Modality	No public data available

3.10 PCI DSS

3.10.1 Description

PCI DSS v4.0 (Payment Card Industry Data Security Standards) is a set of network security and business guidelines proposed by the PCI Security Standards Council (PCI SSC). It imposes a “minimum security standard” to protect stored, processed and transmitted customers' payment card information. Entities dealing with customers’ bank card information are required to follow the standard or prove compliance.

Date of Creation	2008
Scope	International
Validity of Certificate	Depending on the version of the standard and the approval class of the solution
Mutual Recognition	None

3.10.2 Data Collection

Modality	No public data available

Figure 37: Number of laboratories per ICT products assessment methodology

4.1.2 Laboratories based in EU countries

EU countries have a large number of laboratories evaluating different methodologies and schemes. Among all the laboratories counted in the previous point, 88 of them belong to EU countries. Common Criteria scheme is particularly represented with 44 of the 87 laboratories being located in the EU.

4.1.3 Data Collection

Modality	Data collected manually from the official website of the different schemes. For standards that do not have a unique scheme website, like ISO/IEC 27001, data have not been collected.
Date of Data Collection	20/06/2023

4.2 LICENSED CONFORMITY ASSESSMENT BODIES

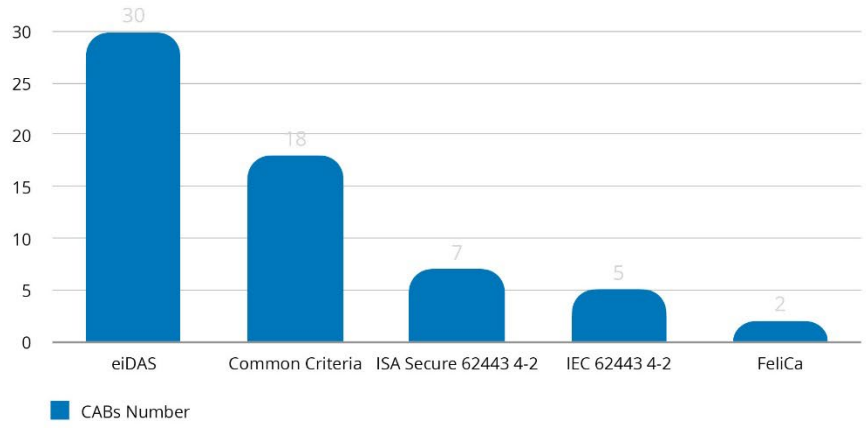
4.2.1 Description

Conformity Assessment Bodies (CAB) can be called differently depending on the terminology of the scheme under consideration, for instance: Certification Bodies (CBs), validators, monitoring bodies…

The CAB is the body in charge of validating the tests and work done by the laboratories or by the manufacturer itself. CABs have received formal accreditation from Accreditation bodies to do this validation phase. CABs are usually accredited using ISO/IEC 17065.

The graph below only mentions schemes that count more than one accredited CAB.

Figure 38: Number of CABs per assessment methodology



4.2.2 Data Collection

Modality	Data collected manually from the official website of the different schemes.
Date of Data Collection	20/06/2023

ANNEX 2: ACRONYMS TABLE REFERENCE

Listed in order of appearance

Acronym	Meaning
3GPP	3rd Generation Partnership Project
AMEX	American Express
ANSSI	Agence Nationale de la Sécurité des Systèmes d'information
AVA_VAN	Vulnerability Assessment
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSPA	Baseline Security Product Assessment
BSZ	Beschleunigte Sicherheitszertifizierung
C5	Cloud Computing Compliance Criteria Catalogue
CAB	Conformity Assessment Body
CB	Certification Body
CC	Common Criteria
CCN	Centro Criptológico Nacional
CCRA	Common Criteria Recognition Arrangement
CESTI	Centres d'Évaluation de la Sécurité des Technologies de l'Information
CLS	Finnish Transport and Communications Agency
COTS	commercial off-the-shelf
CPoC	Contact Payment on COTS
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación
CRA	Cyber Resilience Act
CSA	Connectivity Standard Alliance

CSA	Cybersecurity Agency of Singapore
CSA STAR	Cloud Security Alliance Security Trust Assurance and Risk
CSP	Cloud Services Provider
CSPN	Certification de Sécurité de Premier Niveau
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
DISC	Discover Information Security & Compliance
EAL	Evaluation Assurance Level
ECB	European Central Bank
ECSG	European Cards Stakeholders Group
EFTA	European Free Trade Association
eIDAS	Electronic IDentification, Authentication and trust Services
EMV	Europlay Mastercard Visa
ENISA	European Union Agency for Cybersecurity
eSA	eUICC Security Accreditation
ETSI	European Telecommunications Standards Institute
EU	European Union
EU5G	European Union Cybersecurity Certification Scheme on 5G
EUCC	Common Criteria based European candidate cybersecurity certification scheme
EUCS	European Union Cybersecurity Certification Scheme on Cloud Services
FedRAMP	Cloud Computing Compliance Criteria Catalogue
FeliCa	Felicity Card
FIDO	Fast Identity Online
FIPS	Federal Information Processing Standards
GCA	Global Cyber Alliance
GSM	Global System for Mobile Communication
HSM	Hardware security module

IC	Integrated Chip
ICT	Information and communications technology
IEC	International Electrotechnical Commission
IECEE	IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components being a body of the International Electrotechnical Commission
IOT	Internet of Thing
ioXt	Internet Of Secure Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISA	International Society of Automation
ISAE	International Standard on Assurance Engagements
ISO	International Organization for Standardization
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
JCB	Japan Credit Bureau
LINCE	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad
MiFare	MIkron FARE Collection System
MPoC	Mobile Payments on COTS
MRA	Mutual Recognition Agreement
NBV	Nationaal Bureau voor Verbindingsbeveiliging
NCSC-FI	National Cyber Security Centre Finland
NESAS	Network Equipment Security Assurance Scheme
OCR	Optical Character Recognition
OS	Operating System
OWASP	Open Source Foundation for Application Security
PCI DSS	Payment Card Industry Data Security Standards

PCI PTS	PCI Payment Terminal System
PCI SSC	PCI Security Standards Council
POI	Point of Interaction
PSA	Platform Security Architecture
PSWG	Product Security Working Group
SCADA	Supervisory Control And Data Acquisition
SESIP	Security Evaluation Standard for IoT Platforms
SME	Small and Medium Enterprises
SOG-IS	Senior Officials Group Information Systems Security
SPoC	Software-based PIN entry on Commercial off-the-shelf devices (SPoC)
SSAE	Statement on Standards for Attestation Engagements
STIC	Servicios de Seguridad de las Tecnologías de la Información y la Comunicación
TCSEC	Trusted Computer System Evaluation Criteria
TEE	Trusted Execution Environments
TOE	Target of Evaluation
Traficom	Finnish Transport and Communications Agency
TTP	Tactics, Techniques and Procedures
UK	United Kingdom
US	United States of America

TP-06-23-029-EN-N

ABOUT ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

ISBN 978-92-9204-660-6
DOI 10.2824/70639