



EUROPEAN UNION AGENCY  
FOR CYBERSECURITY



# CYBERSECURITY ASSESSMENTS

Evaluations & Certifications - State of Play 2018-2022

JANUARY 2024

<https://t.me/learningnets>

# 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](http://www.enisa.europa.eu).

## CONTACT

For contacting the authors, please use [certification@enisa.europa.eu](mailto:certification@enisa.europa.eu).

For media enquiries about this paper, please use [press@enisa.europa.eu](mailto: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

This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to the Regulation (EU) No 2019/881.

ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source.

Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication.

Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

ENISA maintains its intellectual property rights in relation to this publication.

## COPYRIGHT NOTICE

© European Union Agency for Cybersecurity (ENISA), 2024

This publication is licenced under CC-BY 4.0 "Unless otherwise noted, the reuse of this document is authorised under the [Creative Commons Attribution 4.0 International \(CC BY 4.0\) licence](https://creativecommons.org/licenses/by/4.0/). This means that reuse is allowed, provided that appropriate credit is given and any changes are indicated".

For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

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



# TABLE OF CONTENTS

<b>1. INTRODUCTION</b>	<b>8</b>
<b>2. ICT PRODUCTS</b>	<b>9</b>
<b>2.1 COMMON CRITERIA</b>	<b>9</b>
2.1.1 Description	9
2.1.2 Statistics covering the last 5 years – Certified products according to Common Criteria	10
2.1.3 Focus on the European Union	10
<b>2.2 FIXED-TIME METHODOLOGIES</b>	<b>11</b>
2.2.1 CSPN – France	11
2.2.2 BSPA – The Netherlands	12
2.2.3 LINCE – Spain	13
2.2.4 BSZ - Germany	14
2.2.5 FITCEM	15
<b>2.3 CRYPTOGRAPHIC PRODUCTS</b>	<b>16</b>
2.3.1 FIPS 140-2 & FIPS 140-3	16
<b>2.4 IDENTITY &amp; DIGITAL SIGNATURE</b>	<b>17</b>
2.4.1 eIDAS	17
<b>2.5 ACCESS CONTROL</b>	<b>18</b>
2.5.1 Fido	18
2.5.2 IEC 62443	18
<b>2.6 MOBILE COMMUNICATIONS</b>	<b>19</b>
2.6.1 APP Defense Alliance	19
2.6.2 GSMA eUICC eSA	20
2.6.3 NESAS	21
2.6.4 NESAS CCS-GI	22
<b>2.7 PAYMENT</b>	<b>23</b>
2.7.1 EMVco	23
2.7.2 Common.SECC	23
2.7.3 PCI CPoC	24
2.7.4 PCI HSM	25
2.7.5 PCI MPoC	26
2.7.6 PCI PTS (Payment Terminals)	27
2.7.7 PCI SPoC	27
<b>2.8 TRANSPORT</b>	<b>28</b>
2.8.1 Calypso	28
2.8.2 FeliCa	29



2.8.3 MiFare	30
<b>2.9 IOT LABELS</b>	<b>31</b>
2.9.1 IoT Label – Germany	31
2.9.2 IoT Label – Finland	32
2.9.3 IoT Label – Singapore	33
2.9.4 PSA Certified	34
2.9.5 ioXt	35
2.9.6 Matter	36
2.9.7 Global Platform TEE	37
2.9.8 Global Platform SESIP	38
<b>3. CLOUD SERVICES</b>	<b>40</b>
<b>3.1 ISO/IEC 27001</b>	<b>40</b>
3.1.1 Description	40
3.1.2 Statistics covering the last 5 years – Certified ISMS, including cloud computing services according to ISO/IEC 27001	40
3.1.3 Data Collection	41
<b>3.2 EU CLOUD CODE OF CONDUCT</b>	<b>41</b>
3.2.1 Description	41
3.2.2 Statistics covering the last 5 years – Adhered cloud computing services according to EU Cloud Code of Conduct	41
3.2.3 Data Collection	42
<b>3.3 C5 – GERMANY</b>	<b>42</b>
3.3.1 Description	42
3.3.2 Statistics covering the last 5 years – Cloud Services Providers with a C5 attestation	42
3.3.3 Data Collection	43
<b>3.4 SECNUMCLOUD – FRANCE</b>	<b>43</b>
3.4.1 Description	43
3.4.2 Statistics covering the last 5 years – Qualified cloud services according to SecNumCloud	43
3.4.3 Data Collection	44
<b>3.5 ZEKER-ONLINE – THE NETHERLANDS</b>	<b>44</b>
3.5.1 Description	44
3.5.2 Statistics covering the last 5 years – Services marked according to Zeker-OnLine	44
3.5.3 Data Collection	45
<b>3.6 ENS – SPAIN</b>	<b>45</b>
3.6.1 Description	45
3.6.2 Statistics covering the last 5 years – Certified Companies, including CSPs, according to ENS	45
3.6.3 Data Collection	45
<b>3.7 FEDRAMP – UNITED STATES</b>	<b>46</b>
3.7.1 Description	46
3.7.2 Statistics covering the last 5 years – Authorised services according to FedRAMP	46
3.7.3 Data Collection	46



<b>3.8 CSA STAR</b>	<b>46</b>
3.8.1 Description	46
3.8.2 Statistics covering the last 5 years – Solutions listed according to CSA STAR	47
3.8.3 Data Collection	47
<b>3.9 HITRUST CSF</b>	<b>47</b>
3.9.1 Description	47
3.9.2 Data Collection	48
<b>3.10 PCI DSS</b>	<b>48</b>
3.10.1 Description	48
3.10.2 Data Collection	48
<b>4. ASSESSMENT BODIES</b>	<b>49</b>
<b>4.1 ACCREDITED LABORATORIES</b>	<b>49</b>
4.1.1 Description	49
4.1.2 Laboratories based in EU countries	50
4.1.3 Data Collection	50
<b>4.2 LICENSED CONFORMITY ASSESSMENT BODIES</b>	<b>50</b>
4.2.1 Description	50
4.2.2 Data Collection	51
<b>A ANNEX 1: FIGURES INDEX</b>	<b>52</b>
<b>B ANNEX 2: ACRONYMS TABLE REFERENCE</b>	<b>53</b>



# 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](#)<sup>1</sup>.

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.

---

<sup>1</sup> 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.



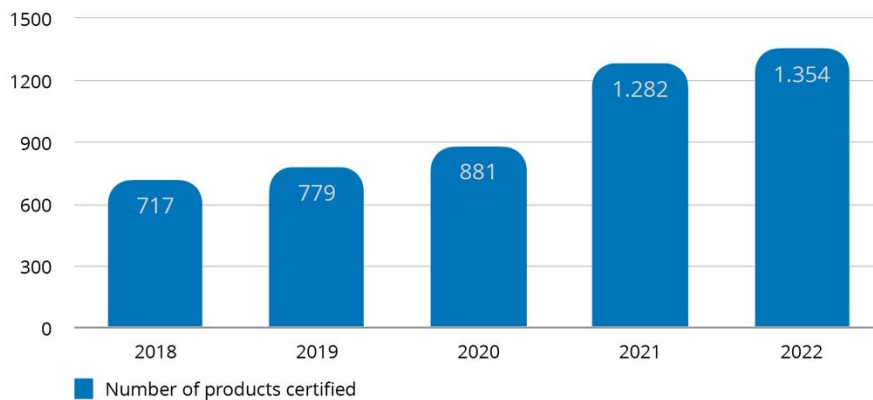
# EXECUTIVE SUMMARY

Taking into account the main third-party cybersecurity assessments methodologies for ICT products and cloud services as well as the number of assessment bodies, the report presents the current state of play of cybersecurity assessments based on the past 5 years data. This study aims at analysing and understanding the evolution of the cybersecurity assessment market and possibly measuring the future impacts of the future EU schemes; in particular where private schemes have been established or methodologies have been simplified to compensate some issues such as time-to-market certificates with existing national schemes that will be replaced by EU ones.

Looking at ICT products, it may be observed that the number of schemes and assessment methodologies is growing over the years. The cybersecurity assessment market for ICT products is not only based on Common Criteria. In the past years new schemes were born to answer either sectoral needs such as payment, telco or transport but also or technological with, for instance the rise of connected devices. Besides, some schemes and a new European adopted standard aiming at *a priori* limited, typically shorter timeframes, are emerging with the apparition of new fixed-time evaluation methodologies.

ICT products represent a significant part of the total market of cybersecurity assessment all schemes combined. As seen in Figure 1, the growth is significant in the past 3 years, specially between 2020 and 2021. However, the growth between 2021 and 2022 is not as remarkable. This should be further analysed in the following years to assess if it is a trend settling in or if external factors such as COVID have affected the numbers.

**Figure 1: Worldwide 5-year evolution of the total number of approved or certified ICT products, all cybersecurity assessments from the report combined**



It may be also highlighted that the increase of new standards and schemes in the last three years has been significant. Standards and schemes such as those reflected in the IoT labels or mobile communications sections, for example, are very recent.

Regarding ICT Cloud Services, there are less assessment frameworks due to the fact that the technology is more recent. However, ISO/IEC 27001 seems to stand out in terms of number of certified Information Security Management Systems. While new schemes appear and demonstrate the need to address cloud security, their adoption remains slow.

Cornerstone of third-party evaluations, the report aims at showcasing the number of licensed laboratories or conformity assessment bodies for the different assessment frameworks. The numbers show that the cybersecurity Certification market is growing worldwide and the European Union has significant capabilities. Regarding the



[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.



# 1. INTRODUCTION

The Cybersecurity Act (Regulation (EU) 2019/881) mandates the European Union Agency for Cybersecurity, ENISA, to build an EU Cybersecurity Certification framework and promote its implementation. While building the requirements needed for such schemes and in order to support the second goal, ENISA conducted in 2023 for the first time a statistical analysis of existing cybersecurity conformity assessment methodologies and related schemes.

The ENISA Cybersecurity Certification Statistics report aims to understand the market size and evolution of cybersecurity certifications. It takes into consideration:

- ICT products
- ICT cloud services
- Assessment bodies

The report contains a quantitative analysis of the market. Each of the sections referring to the different conformity assessment methodologies and related schemes is composed with following elements:

- Description and introduction (including: the scope, validity of the certificate and mutual recognition between certificates).
- Statistics of the last 5 years (number of approved/certified/listed products or solutions per year).
- Data collection information (date and modality)

The report focuses on schemes based on third-party assessment and ruled by government bodies and private entities (such as associations or private companies) that have a European and worldwide impact. Schemes with only a local impact or in lack of use in the last 5 years have not been taking into account, as well as those that do not involve product-focused cyber security assessment. Schemes that do not have a European impact have not been taken into account. The list of schemes will be revised in future versions of the report.

For instance, the report does not take into account the following conformity assessment methodologies:

- Cybersecurity labels relying on the made-in criterium: such as France Cybersecurity Label or Made in Europe Label.
- Outdated methodologies like FIPS 140-1.
- Methodologies not focused on products like SCADA or Information Security Management System (ISMS).
- Schemes related to production or evaluation sites such as Site Certification in Common Criteria or SAS for UICC Production (SAS-UP).
- Managed Security Services.

When counting certificates, only new ones have been taken into account. i.e., maintained certificates have not been taken into account.

Different methods and sources were used for collecting information, depending mainly on whether or not the data was publicly available. In the case of private assessment schemes, such as those related to payment, it is often more complicated to obtain data.

The first check was of the website and online sources of the methodology/scheme itself. If the requested information was not found, contact was made with the association/organisation in charge of the creation and maintenance of the standard. In the case of Common Criteria, a tool developed by a private laboratory (JTSEC) has been used to obtain the data.



## 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).

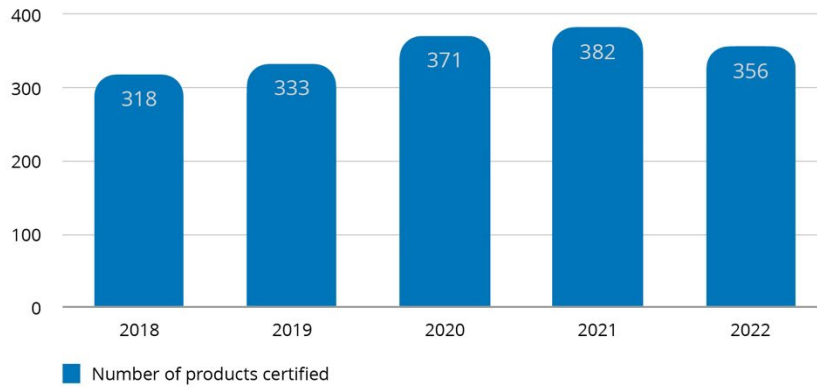
Common Criteria is a horizontal scheme, therefore different types of products are certified using Common Criteria such as telecommunication, ePassports, digital signature, etc...

<i>Date of Creation</i>	1994
<i>Scope</i>	International (more than 30 countries)
<i>Validity of Certificate</i>	5 years
<i>Mutual recognition</i>	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.



## 2.1.2 Statistics covering the last 5 years – Certified products according to Common Criteria

Figure 2: Common Criteria certified products in the last 5 years



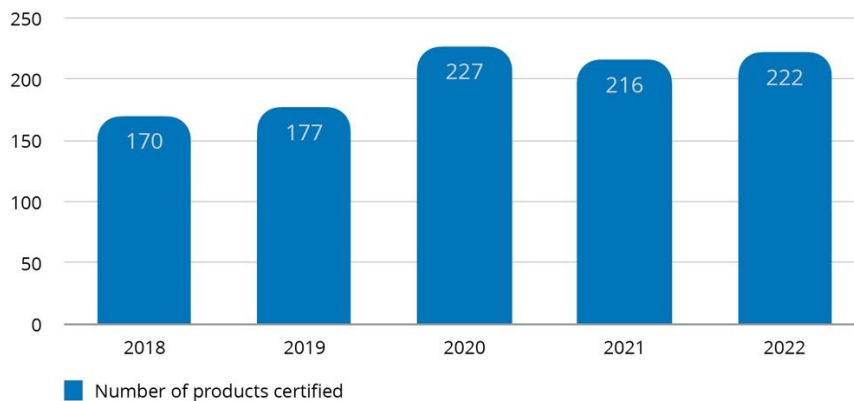
A continued growth in the number of Common Criteria certificates issued between 2018 and 2021 can be observed, however, in 2022 a slight decrease in the number of certified products is noted. It is worth remarking that 2021 was the record year in the history of the Common Criteria standard in terms of the number of certificates issued.

## 2.1.3 Focus on the European Union

There are 7 countries in the European Union that are able to certify against the Common Criteria: France, Germany, Italy, The Netherlands, Poland, Spain and Sweden.

It's important to note that the SOG-IS agreement allowing mutual recognition of CC evaluation made by third parties includes both European Union (EU) member countries and countries from the European Free Trade Association (EFTA), totalling 28 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.

Figure 3 Common Criteria certified products in the European Union in the last 5 years



Some remarkable figures can be found, with a significant growth in 2020, being number of certificates every year, with a relatively stable number since then.



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”.

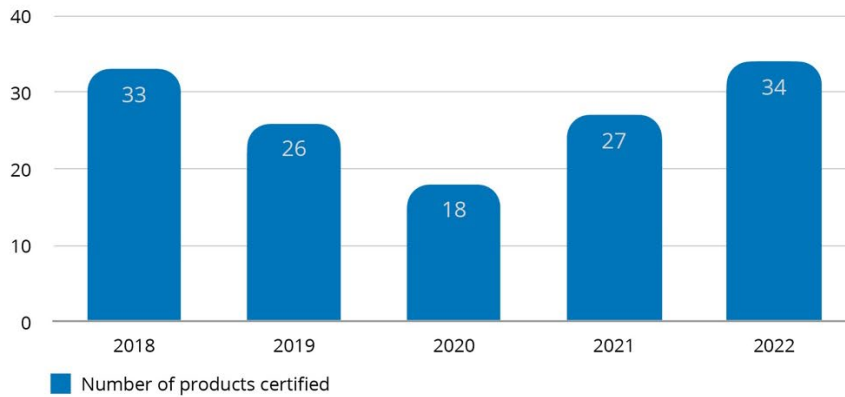
This certification is delivered for a specific product version. All subsequent versions of the product must therefore be re-certified. CSPN certification applies to several types of cybersecurity products such as “secure storage”, “identification, authentication and access control”, or “secure communication”. 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.

<i>Date of Creation</i>	2008
<i>Scope</i>	France
<i>Validity of Certificate</i>	3 years
<i>Mutual recognition</i>	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**

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

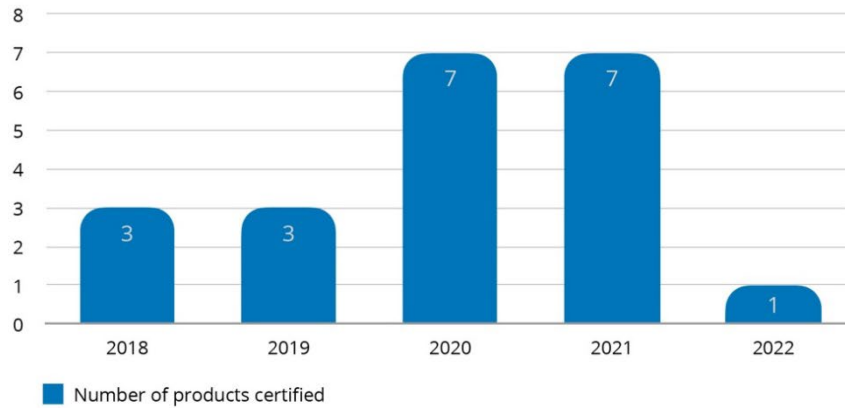
This scheme provides a framework in which products (both hardware and software components ) can be tested in a limited timeframe (and cost) against a baseline of security requirements (Government security baseline). Compliance to the BSPA is required for manufacturers willing to work with Dutch government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

<i>Date of Creation</i>	2015
<i>Scope</i>	The Netherlands
<i>Validity of Certificate</i>	3 years
<i>Mutual recognition</i>	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

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

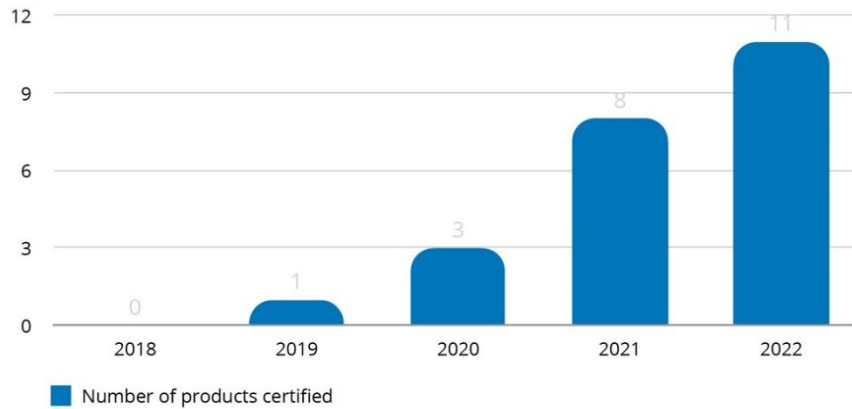
The objective of a LINCE assessment is to enable an evaluation laboratory to verify whether a product conforms to its specification by determining the effectiveness of the security functionality implemented. Holding a LINCE certification allows to be included in the CPSTIC Catalogue, which is the CCN-STIC-105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

<i>Date of Creation</i>	2018
<i>Scope</i>	Spain
<i>Validity of Certificate</i>	5 years
<i>Mutual recognition</i>	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

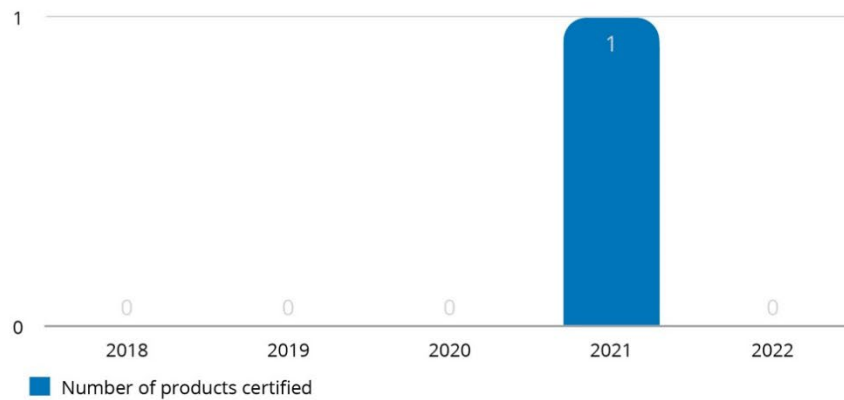
According to [BSI \(Bundesamt für die Sicherheit in der Informationstechnik – Federal Office for Security in Information Technology\) website](#), “the Beschleunigte Sicherheitszertifizierung (BSZ – Accelerated security certification) enables manufacturers to have their security statements regarding 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.”

<i>Date of Creation</i>	2021
<i>Scope</i>	Germany
<i>Validity of Certificate</i>	2 years
<i>Mutual recognition</i>	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

<i>Modality</i>	BSI, the chief architect of secure digitalization in Germany, provided information. Therefore, the data is extracted from information provided by the Certification Body
<i>Date of data Collection</i>	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.”

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



## 2.3 CRYPTOGRAPHIC PRODUCTS

### 2.3.1 FIPS 140-2 & FIPS 140-3

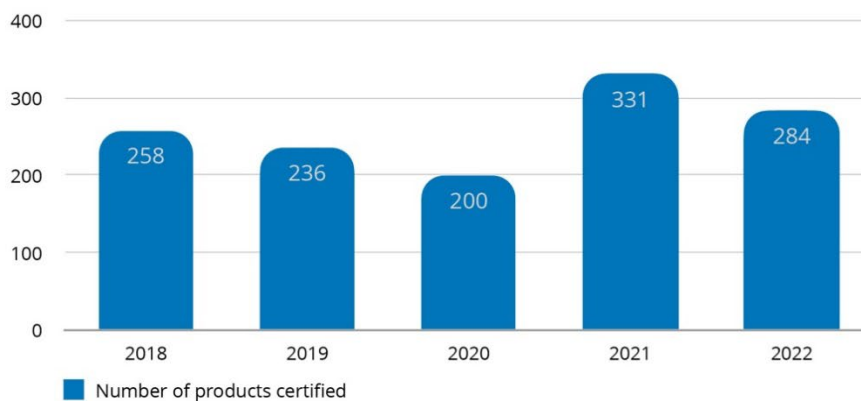
#### 2.3.1.1 Description

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.

<i>Date of Creation</i>	2001
<i>Scope</i>	International
<i>Validity of Certificate</i>	5 years
<i>Mutual recognition</i>	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

<i>Modality</i>	Data collected manually from the official website of <a href="#">FIPS</a> . In calculating the data, the three types of validation status that FIPS gives to certificates have been taken into account (active, historical and revoked).
<i>Date of data Collection</i>	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.

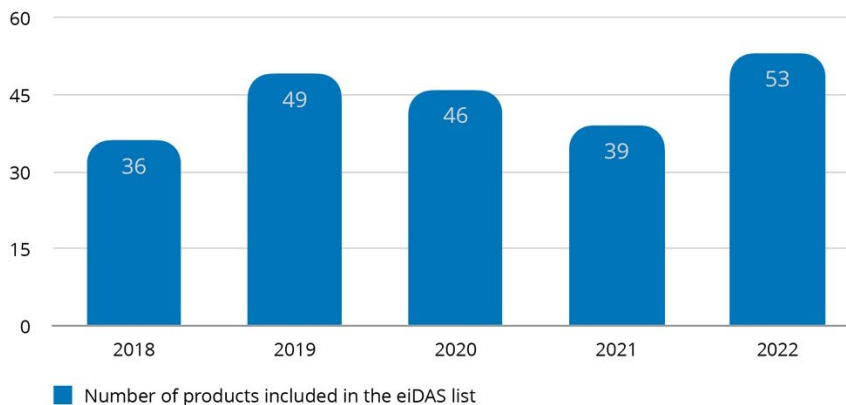
The eIDAS certification sets the standards and criteria for simple electronic signature, advanced electronic signature, qualified electronic signature, qualified certificates and online trust services. Furthermore, it rules electronic transactions and their management.

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.

<i>Date of Creation</i>	2014
<i>Scope</i>	European Union
<i>Validity of Certificate</i>	5 years
<i>Mutual recognition</i>	Mutual recognition of eIDAS certificates is implicit across the European Union. In addition, there are development with MRA to 3 <sup>rd</sup> 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**

<i>Modality</i>	Data collected manually from the official website of <a href="#">eIDAS</a> . 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.
<i>Date of Data Collection</i>	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.

<i>Date of Creation</i>	2013
<i>Scope</i>	International
<i>Validity of Certificate</i>	No Expiration
<i>Mutual Recognition</i>	None

**2.5.1.2 Data collection**

<i>Modality</i>	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.

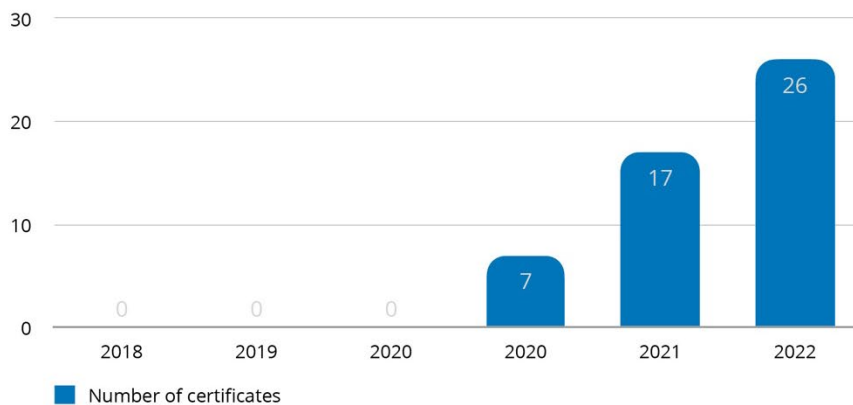
Certificates are emitted by IECEE but private conformity assessment bodies can issue labels & certifications for these standards. ISA Secure which we also took into account in this report, is the only global IEC 62443 certification programme that requires its certification bodies to be accredited to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



<i>Date of Creation</i>	2019
<i>Scope</i>	International
<i>Validity of Certificate</i>	The duration of these certificates varies depending on the certifying body, as well as the specific programme the organisation adheres to.
<i>Mutual Recognition</i>	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

<i>Modality</i>	Data collected manually from the official website of <a href="#">IECEE Certificates</a> and <a href="#">ISA/IEC 62443-4-2 Certified Components</a> . 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.
<i>Date of Data Collection</i>	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.

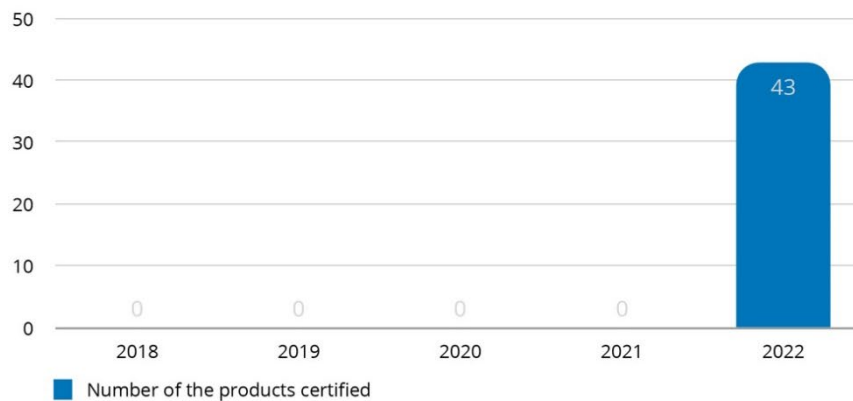
As of November 2023 Google, Microsoft, and Meta announced they are formally partnering as the founding steering committee to improve app security through a newly restructured App Defense Alliance, under the Joint Development Foundation, part of the [Linux Foundation family](#).



<i>Date of Creation</i>	2022
<i>Scope</i>	International
<i>Validity of Certificate</i>	None
<i>Mutual Recognition</i>	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

<i>Modality</i>	Data collected manually from the official website of <a href="#">APP Defense Alliance</a> .
<i>Date of Data Collection</i>	01/11/2023

## 2.6.2 GSMA eUICC eSA

### 2.6.2.1 Description

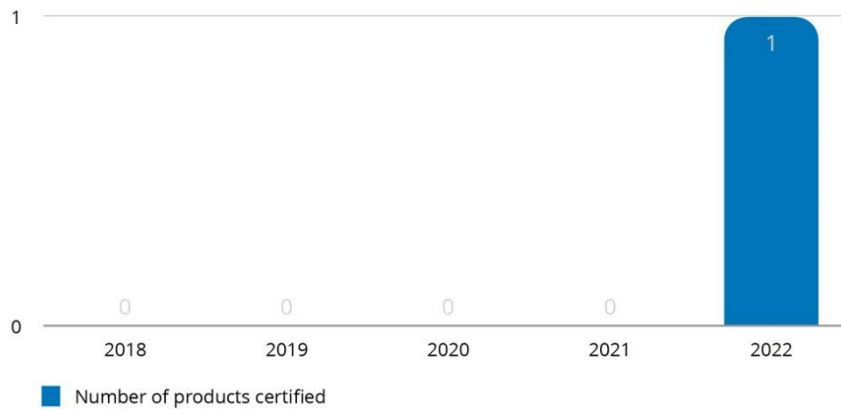
[GSMA eSA \(eUICC Security Assurance\)](#) is based on the Common Criteria approach and the GSMA Protection Profiles (i.e., SGP.05 (for M2M devices) and SGP.25 (for Consumer devices)) but defines a more dynamic set of procedures for the security evaluation of Embedded Universal Integrated Circuit Cards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

<i>Date of Creation</i>	2021
<i>Scope</i>	International
<i>Validity of Certificate</i>	None
<i>Mutual Recognition</i>	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

<i>Modality</i>	Data collected manually from <a href="#">GSMA Network</a> . website
<i>Date of Data Collection</i>	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.

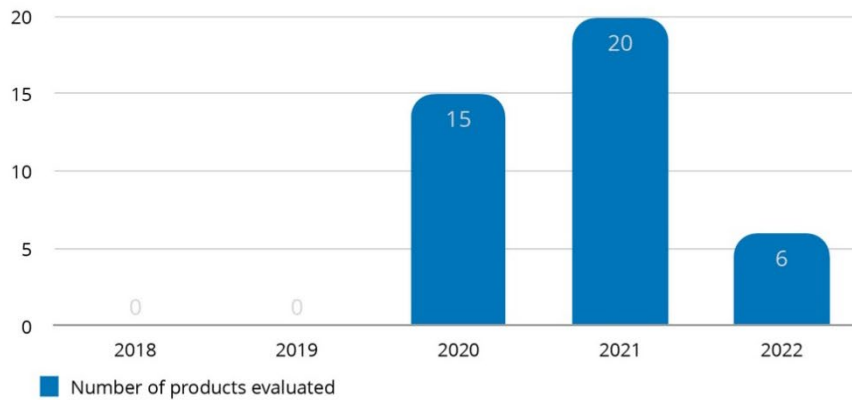
The purpose of the program is to audit and test network equipment vendors, and their products, against a security baseline. So, they can demonstrate to network operators that they are conforming to the desired standard. The program has been defined by industry experts through GSMA and 3GPP. Therefore, 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.

<i>Date of Creation</i>	2019
<i>Scope</i>	International
<i>Validity of Certificate</i>	None
<i>Mutual Recognition</i>	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

<i>Modality</i>	Data collected manually from the official website of <a href="#">GSMA Network</a> . This program includes two modalities: products evaluated and process audits. Just products evaluated are included in this report
<i>Date of Data Collection</i>	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.

<i>Date of Creation</i>	2022
<i>Scope</i>	Germany
<i>Validity of Certificate</i>	2.5 years
<i>Mutual Recognition</i>	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**

<i>Modality</i>	Data collected manually from the official website of <a href="#">BSI - Certified Products</a>
<i>Date of Data Collection</i>	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**

<i>Modality</i>	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.

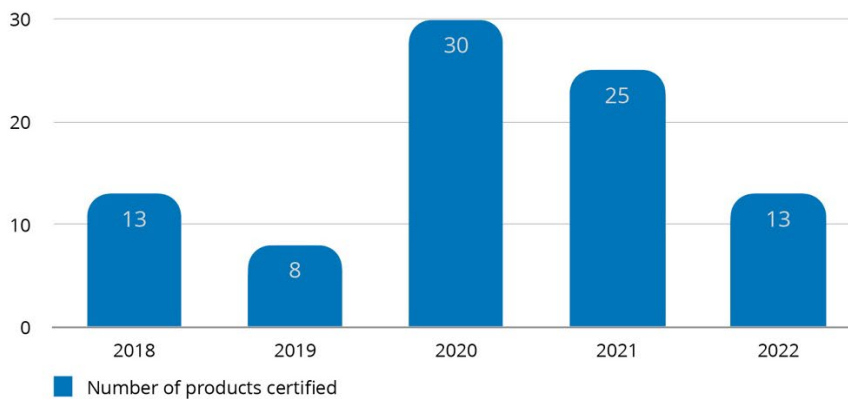
As mentioned on their website: “Common.SECC ensures recognition by the regulators (EU, ECB and ECSG) as providing an adequate degree of security, operational reliability and business continuity according to the ECB’s Oversight Framework for Card Payment Schemes Standards, covering all related SEPA standards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



<i>Date of Creation</i>	2005
<i>Scope</i>	International
<i>Validity of Certificate</i>	6 years
<i>Mutual Recognition</i>	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

<i>Modality</i>	Data collected manually from the official website of <a href="#">Common.SECC</a>
<i>Date of Data Collection</i>	13/04/2023

## 2.7.3 PCI CPoC

### 2.7.3.1 Description

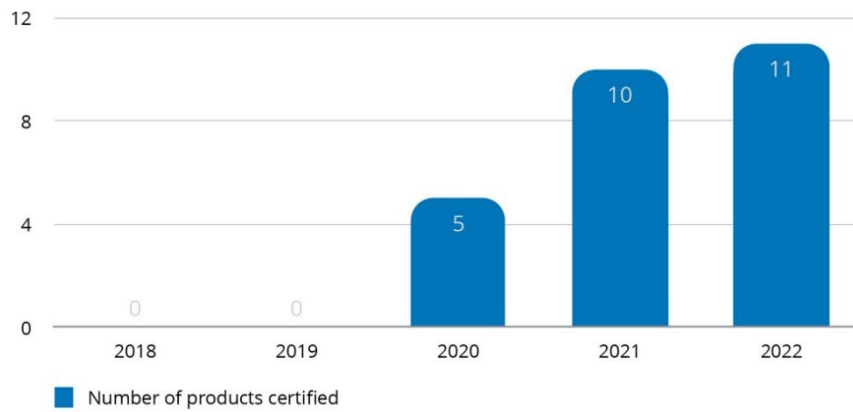
The PCI CPoC Standard is the second standard released by the PCI Council to address mobile contactless acceptance. The purpose of Contactless Payments on COTS (CPoC™) Security and Test Requirements, is to provide a set of principles and requirements for a mobile payment-contactless acceptance solution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



<i>Date of Creation</i>	2019
<i>Scope</i>	International
<i>Validity of Certificate</i>	3 years
<i>Mutual Recognition</i>	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

<i>Modality</i>	Data collected manually from the official website of <a href="#">PCI Security Standards</a> .
<i>Date of Data Collection</i>	13/04/2023

## 2.7.4 PCI HSM

### 2.7.4.1 Description

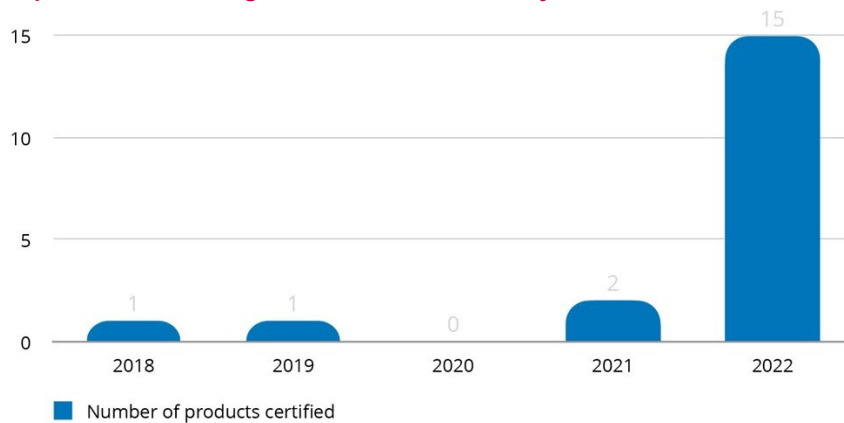
The PCI HSM (Hardware security modules) standard defines a set of logical and physical security compliance standards for HSMs specifically for the payments industry.



<i>Date of Creation</i>	2009
<i>Scope</i>	International
<i>Validity of Certificate</i>	6 years
<i>Mutual Recognition</i>	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

<i>Modality</i>	Data collected manually from the official website of <a href="#">PCI Security Standards</a> .
<i>Date of Data Collection</i>	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.



<i>Date of Creation</i>	2022
<i>Scope</i>	International
<i>Validity of Certificate</i>	3 years
<i>Mutual Recognition</i>	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**

<i>Modality</i>	Data collected manually from the official website of <a href="#">PCI Security Standards</a> .
<i>Date of Data Collection</i>	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.

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

**2.7.6.2 Data collection**

<i>Modality</i>	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**

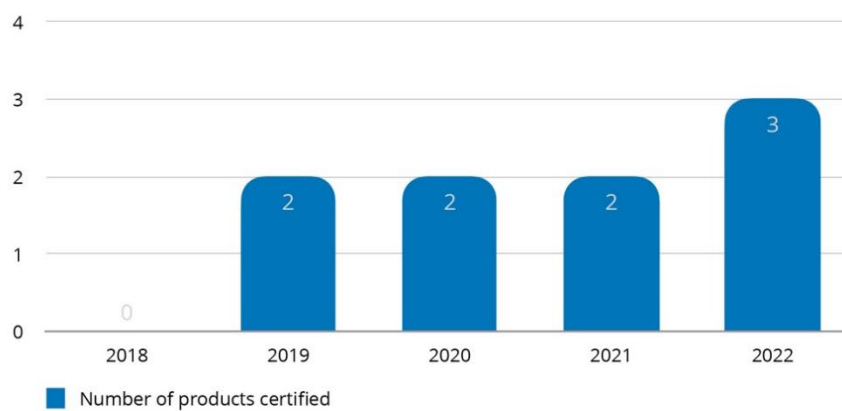
PCI SPoC is a security standard announced by the Payment Card Industry Security Standards Council (PCI SSC) to regulate the security of electronic mobile transactions on commercial off-the-shelf devices (COTS).



<i>Date of Creation</i>	2018
<i>Scope</i>	International
<i>Validity of Certificate</i>	3 years
<i>Mutual Recognition</i>	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

<i>Modality</i>	Data collected manually from the official website of <a href="#">PCI Security Standards</a> .
<i>Date of Data Collection</i>	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:

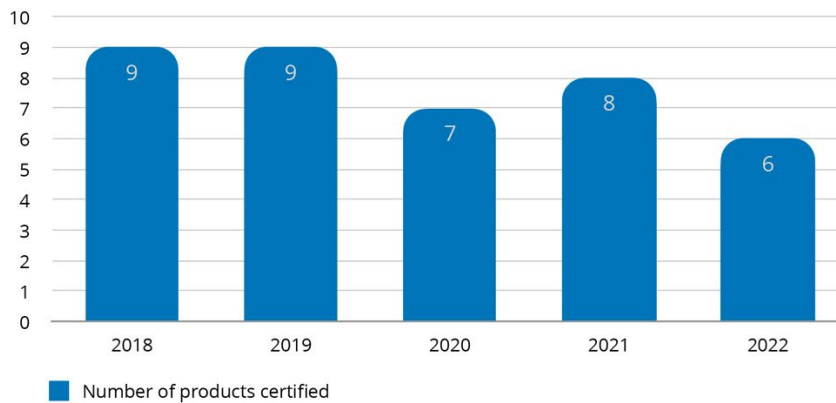
The scheme’s website indicates that “Calypso details how to securely transmit a ticket’s data between a traveller’s card, a phone or watch for example, and a transport/mobility authorities’ ticketing reader – such as an access control barrier, vending machine, handheld reader. The specifications cover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



<i>Date of Creation</i>	1993
<i>Scope</i>	International (25 countries), including 12 EU Members States: Austria, Belgium, France, Germany, Italy, Latvia, Malta, The Netherlands, Poland, Portugal, Romania and Spain.
<i>Validity of Certificate</i>	7 years
<i>Mutual Recognition</i>	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

<i>Modality</i>	Data collected manually from the official website of <a href="#">Calypso</a> . All types of certified cards are included:
<i>Date of Data Collection</i>	12/04/2023

## 2.8.2 FeliCa

### 2.8.2.1 Description

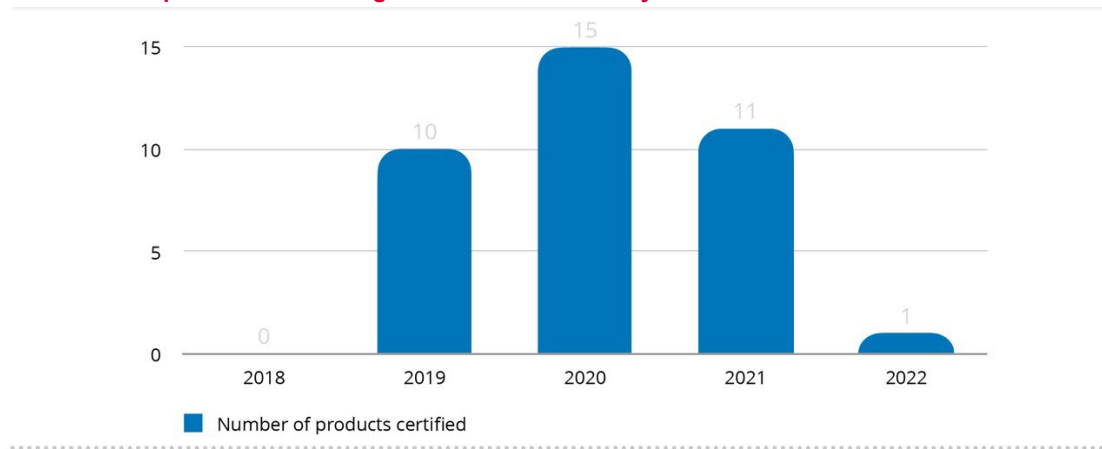
[FeliCa](#) is an IC Card technology developed by Sony, which has a wide variety of uses, such as in ticketing systems for public transportations, e-money, and residence door keys. FeliCa supports the entire life cycle of IC cards including application development, card issuance, personalisation, and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



<i>Date of Creation</i>	1997
<i>Scope</i>	Hong Kong, Indonesia, Japan, Macau, the Philippines, Singapore and the United States.
<i>Validity of Certificate</i>	10 years
<i>Mutual Recognition</i>	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

<i>Modality</i>	Data collected manually from the official website of <a href="#">FeliCa Networks</a> .
<i>Date of Data Collection</i>	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.

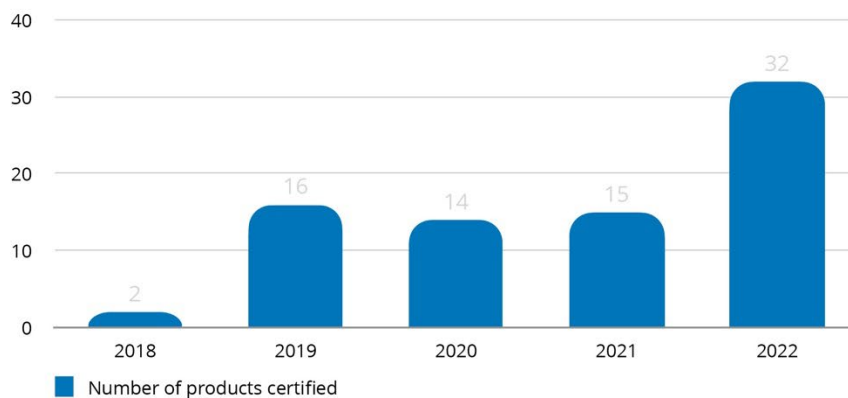
The cybersecurity part of MIFARE is based on various levels of the ISO/IEC 14443 Type A 13.56 MHz contactless smart card standard. It uses AES and DES/Triple-DES encryption standards, as well as an older proprietary encryption algorithm, Crypto-1.



<i>Date of Creation</i>	2007
<i>Scope</i>	International.
<i>Validity of Certificate</i>	5 years
<i>Mutual Recognition</i>	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

<i>Modality</i>	Data collected manually from the official website of <a href="#">MiFare Certificates</a> .
<i>Date of Data Collection</i>	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

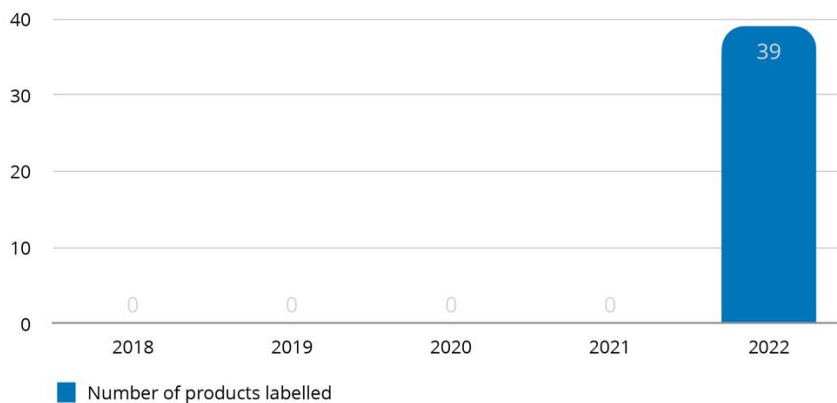
According to the IT-Security Act 2.0 published in 2021, the BSI was tasked with introducing a voluntary IT Security Label. The IT Security Label creates transparency for consumers, revealing basic security features of IT products. While more and more everyday objects are linked to the Internet and with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



<i>Date of Creation</i>	2021
<i>Scope</i>	Germany
<i>Validity of Certificate</i>	2 years
<i>Mutual Recognition</i>	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

<i>Modality</i>	Data collected manually from the <a href="#">official BSI website</a> .
<i>Date of Data Collection</i>	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.

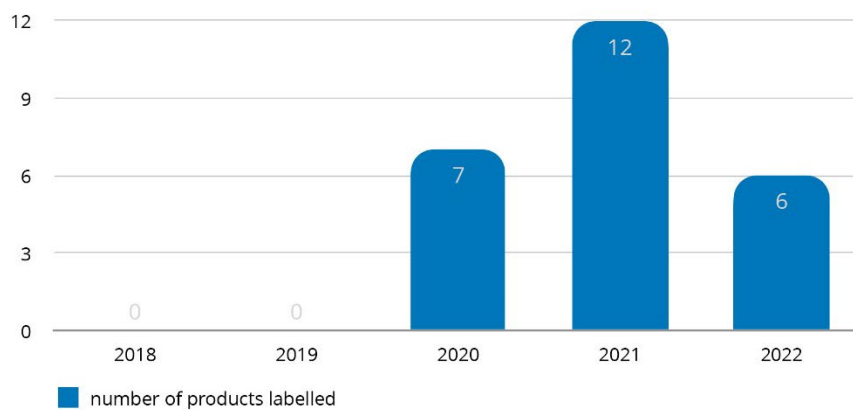
The agency created the [Cybersecurity Label](#) to help the consumer make more secure choices when purchasing IoT devices or services. The voluntary Label shows that the product is secure by design, and that certain security features are updated for the duration of the Label. The requirements of the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



<i>Date of Creation</i>	2020
<i>Scope</i>	Finland
<i>Validity of Certificate</i>	N/A
<i>Mutual Recognition</i>	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

<i>Modality</i>	Data collected manually from the official website of <a href="#">The National Cyber Security Centre Finland (NCSC-FI)</a>
<i>Date of Data Collection</i>	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.

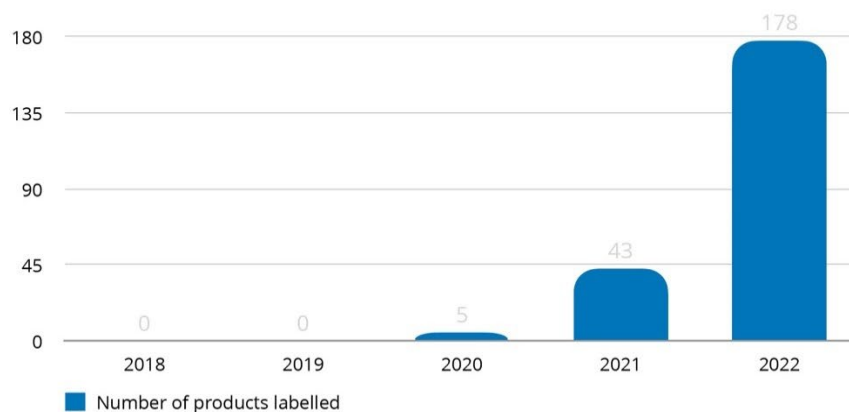
The CLS was first introduced to cover Wi-Fi routers and smart home hubs. These products were prioritised because of their wider usage, as well as the impact that a compromise of the products could have on users. It has since been extended to include all categories of consumer IoT devices, such as IP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



<i>Date of Creation</i>	2020
<i>Scope</i>	Singapore
<i>Validity of Certificate</i>	3 years
<i>Mutual Recognition</i>	<p><b>Finland:</b> 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.</p> <p><b>Germany:</b> 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</p>

### 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

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

## 2.9.4 PSA Certified

### 2.9.4.1 Description

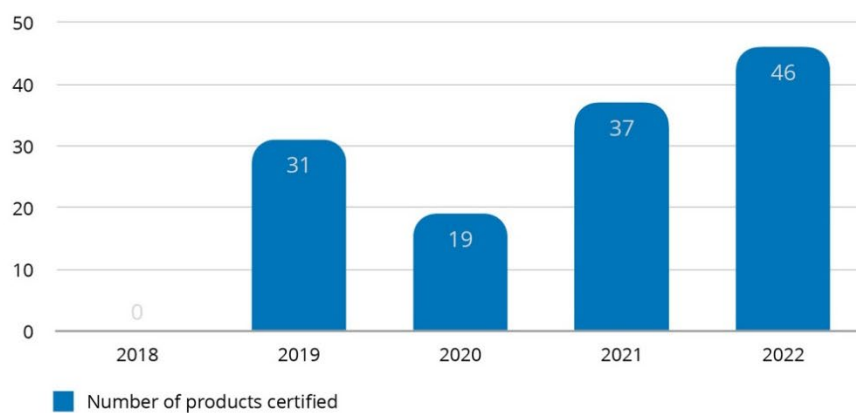
PSA Certified (PSA for Platform Security Architecture) is a security certification dedicated to IoT hardware such as chips, software and devices. The scheme provides standardised resources to limit the growing fragmentation of IoT requirements and ensure security of the solution from development phase.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



<i>Date of Creation</i>	2019
<i>Scope</i>	International
<i>Validity of Certificate</i>	None
<i>Mutual Recognition</i>	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

<i>Modality</i>	Data collected manually from the official website of <a href="#">PSA Certified</a> .
<i>Date of Data Collection</i>	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.

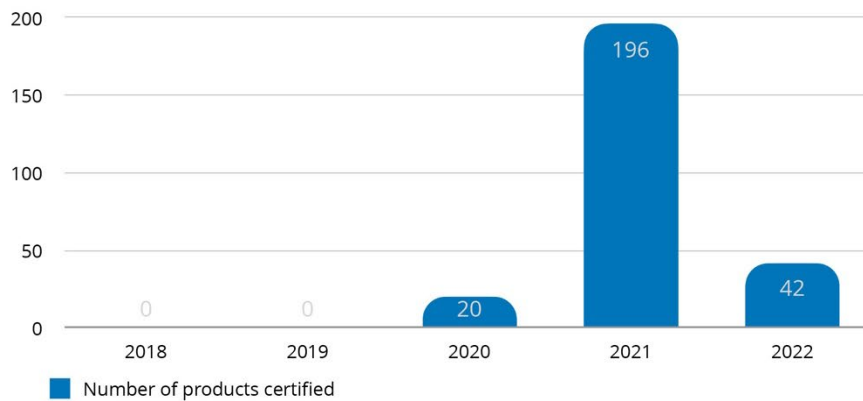
According to the ioXt [website](#): "The program measures a product against each of the eight ioXt principles with clear guidelines to quantify the appropriate level of security required for a specific product." The scheme is addressing products involved with: smart home, lighting controls, smart building,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



<i>Date of Creation</i>	2020
<i>Scope</i>	International
<i>Validity of Certificate</i>	None
<i>Mutual Recognition</i>	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

<i>Modality</i>	Data collected manually from the official website of <a href="#">ioXt</a> .
<i>Date of Data Collection</i>	14/04/2023

## 2.9.6 Matter

### 2.9.6.1 Description

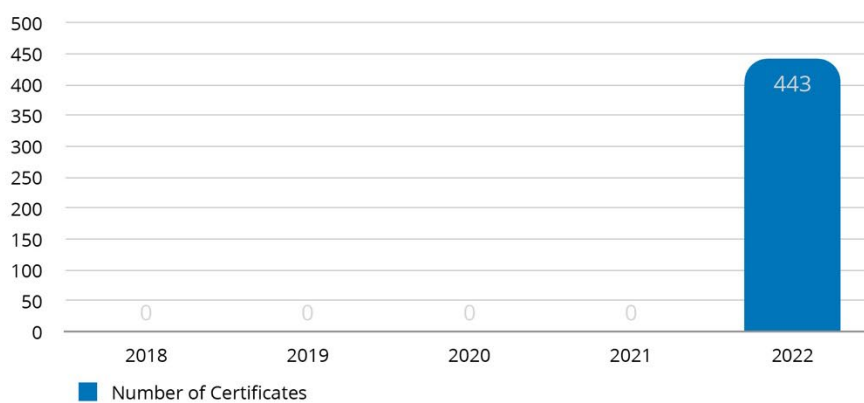
Created in 2002, [the Connectivity Standards Alliance](#) (CSA), gathers more than 600 entities offering IoT technologies and solutions. Amongst other standards, the organisation developed and maintains Matter. Now published in version 1.2, the standard aims at improving and securing interoperability 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.



<i>Date of Creation</i>	2022, version 1.2 published in October 2023
<i>Scope</i>	International
<i>Validity of Certificate</i>	according to the product lifetime
<i>Mutual Recognition</i>	None

### 2.9.6.2 Statistics covering the last 5 years – Certified products according to Matter

Figure 26: Certified products according to Matter in the last 5 years



Launched in late 2022, the first version of Matter encounters a fair success with 443 certified solutions in just few months.

### 2.9.6.3 Data collection

<i>Modality</i>	Data collected manually from the <a href="#">CSA IOT website</a>
<i>Date of Data Collection</i>	05/12/2023

## 2.9.7 Global Platform TEE

### 2.9.7.1 Description

The Global Platform TEE (Trusted Execution Environment) Certification Scheme defines an open security architecture for consumer and connected devices using a Trusted Execution Environment product to secure those devices and enable the development and deployment of secure services from multiple service providers.

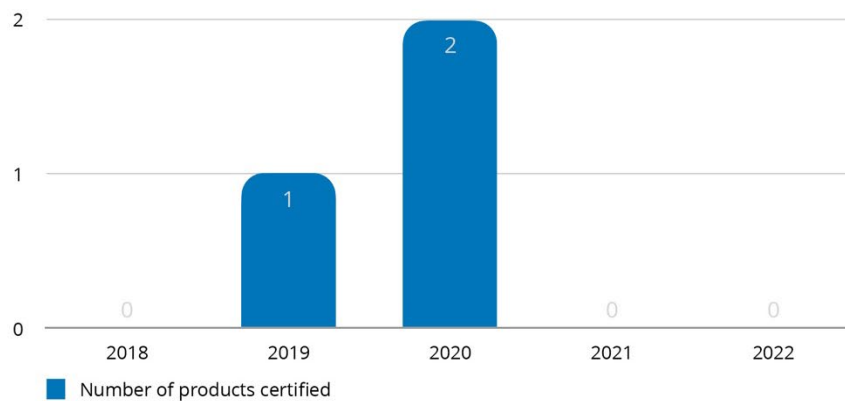
The certified products have been filtered by the security category, as these are the ones that include a cybersecurity module in the product.



<i>Date of Creation</i>	2015
<i>Scope</i>	International
<i>Validity of Certificate</i>	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.
<i>Mutual Recognition</i>	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

<i>Modality</i>	Data collected manually from the official website of <a href="#">Global Platform Certified Products</a> . The certified products have been filtered by the security category, as these are the ones that include a cybersecurity module in the product.
<i>Date of Data Collection</i>	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.

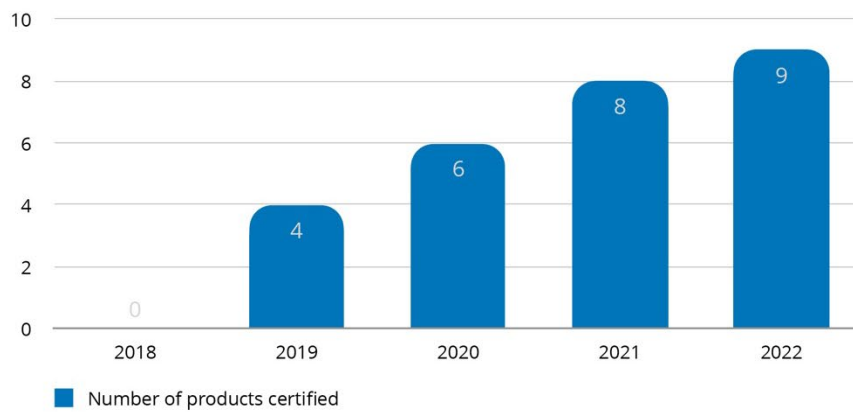
As per November 2023, the SESIP methodology has been adopted as a European Standard by CEN/CENELEC, as EN 17927.



<i>Date of Creation</i>	2018
<i>Scope</i>	International
<i>Validity of Certificate</i>	2 Years.
<i>Mutual Recognition</i>	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

<i>Modality</i>	Data collected manually from the official website of <a href="#">SESIP Certificates</a> .
<i>Date of Data Collection</i>	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

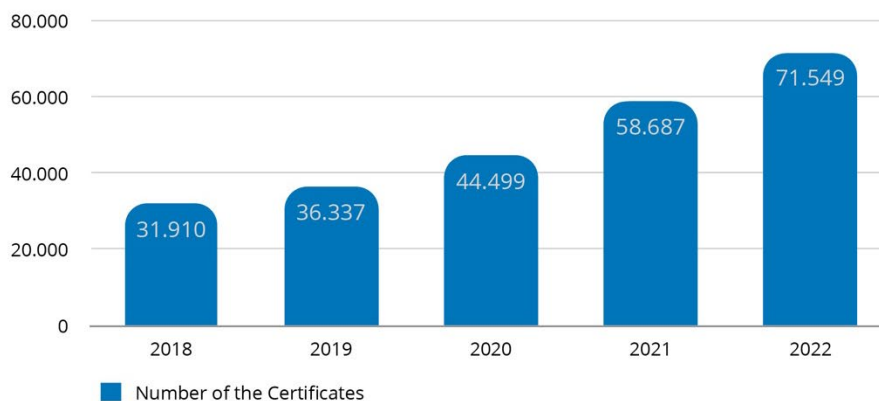
While ISO/IEC 27001, the world's best-known standard for information security management systems (ISMS), is not specifically designed for cloud computing services, it provides relevant best practices that are used as references for many cloud certification schemes.

[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."

<i>Date of Creation</i>	2005
<i>Scope</i>	International
<i>Validity of Certificate</i>	3 years
<i>Mutual Recognition</i>	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

<i>Modality</i>	Data comes from the <a href="#">survey</a> that ISO leads every year
<i>Date of Data Collection</i>	30/11/2023

## 3.2 EU CLOUD CODE OF CONDUCT

### 3.2.1 Description

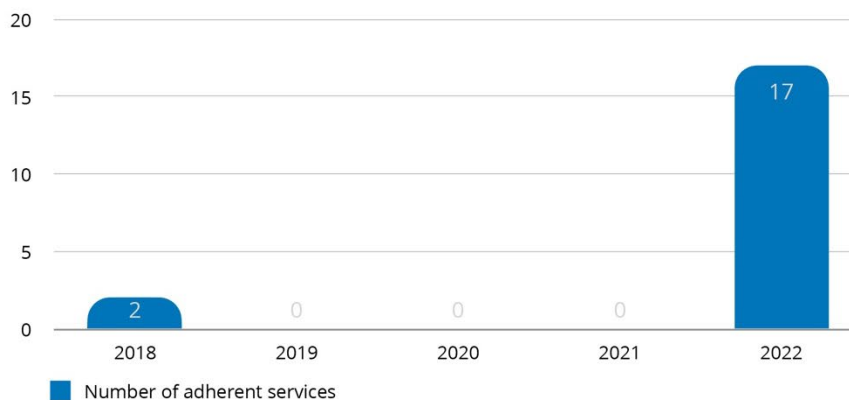
The EU Cloud Code of Conduct (EU Cloud CoC) was drafted together with the industry and authorities of the European Union. The first version of the Code was published in April 2017 and the first product certified was in 2018.

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.”

<i>Date of Creation</i>	2017
<i>Scope</i>	European Union
<i>Validity of Certificate</i>	1 year
<i>Mutual Recognition</i>	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

<i>Modality</i>	Data collected manually from the official website of <a href="#">EU Cloud CoC</a> .
<i>Date of Data Collection</i>	29/05/2023

## 3.3 C5 – GERMANY

### 3.3.1 Description

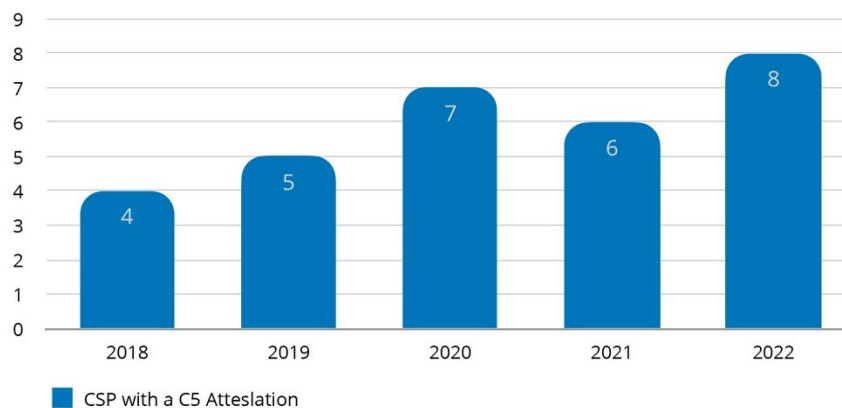
The [C5 \(Cloud Computing Compliance Criteria Catalogue\)](#) published by the German Federal Office for Information (BSI) Security specifies minimum requirements for secure cloud computing. It is primarily intended for professional cloud providers, their auditors and customers.

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.

<i>Date of Creation</i>	2016
<i>Scope</i>	Germany
<i>Validity of Certificate</i>	1 year
<i>Mutual Recognition</i>	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

<i>Modality</i>	Personal website listing all attestations: <a href="https://c5-attestations.com">Home (c5-attestations.com)</a>
<i>Date of Data Collection</i>	05/12/2023

## 3.4 SECNUMCLOUD – FRANCE

### 3.4.1 Description

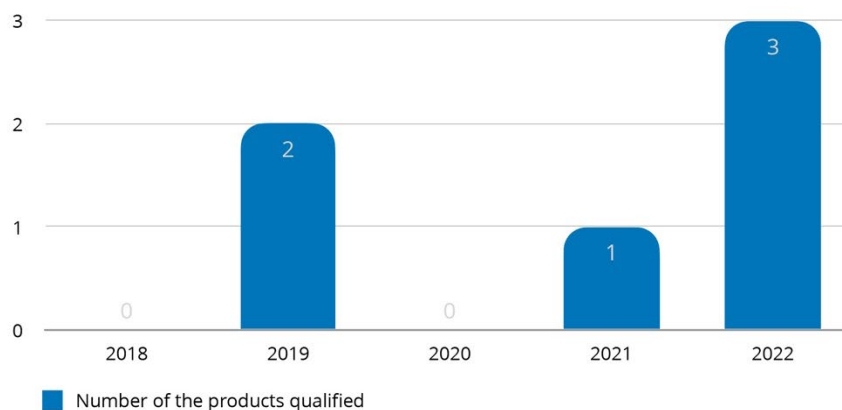
SecNumCloud is the qualification proposed by [ANSSI](https://www.anssi.fr) to distinguish cloud operators who respect good security practices. It offers services in PaaS (Platform as a Service), IaaS (Infrastructure as a Service) or SaaS (Software as a service).

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.

<i>Date of Creation</i>	2016
<i>Scope</i>	France
<i>Validity of Certificate</i>	3 years
<i>Mutual Recognition</i>	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

<i>Modality</i>	Data collected directly from <a href="#">ANSSI</a> .
<i>Date of Data Collection</i>	14/04/2023

## 3.5 ZEKER-ONLINE – THE NETHERLANDS

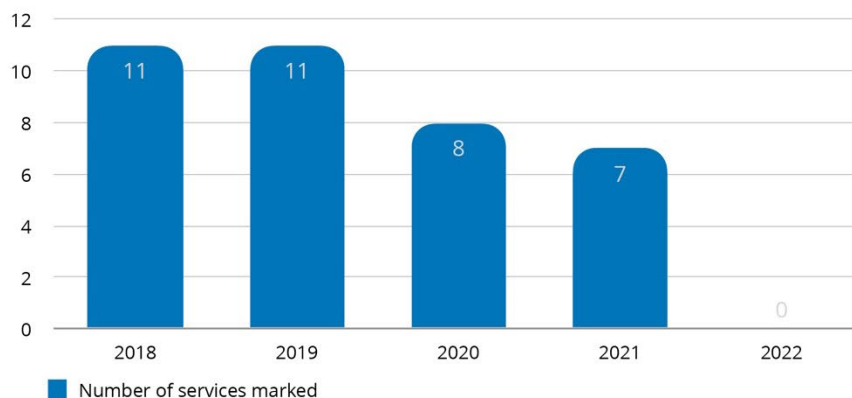
### 3.5.1 Description

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.

<i>Date of Creation</i>	2013
<i>Scope</i>	The Netherlands
<i>Validity of Certificate</i>	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
<i>Mutual Recognition</i>	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

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

## 3.6 ENS – SPAIN

### 3.6.1 Description

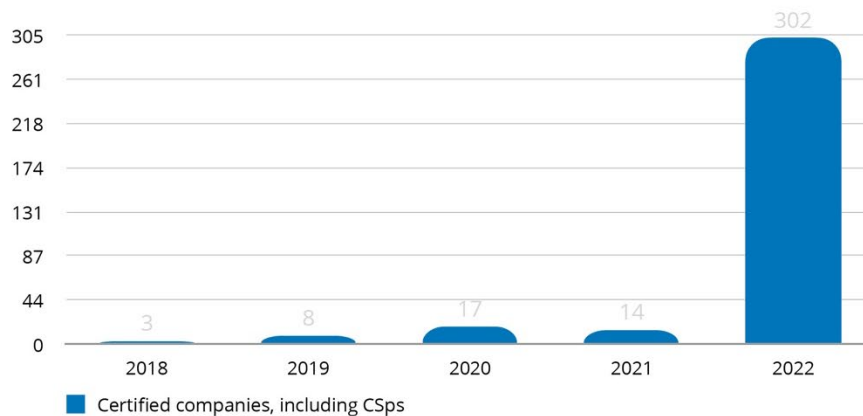
The [National Security Framework](#), is applicable to the entire Public Sector (ENS by its acronym in Spanish), as well as its suppliers. It offers a common framework of basic principles, requirements and security measures for the adequate protection of the information processed and the services provided. 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](#).

<i>Date of Creation</i>	2010
<i>Scope</i>	Spain
<i>Validity of Certificate</i>	2 years
<i>Mutual Recognition</i>	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

<i>Modality</i>	Data collected manually on <a href="#">the website</a> . Does not only include CSPs but all certified private companies providing ICT services.
<i>Date of Data Collection</i>	05/12/2023



### 3.7 FEDRAMP – UNITED STATES

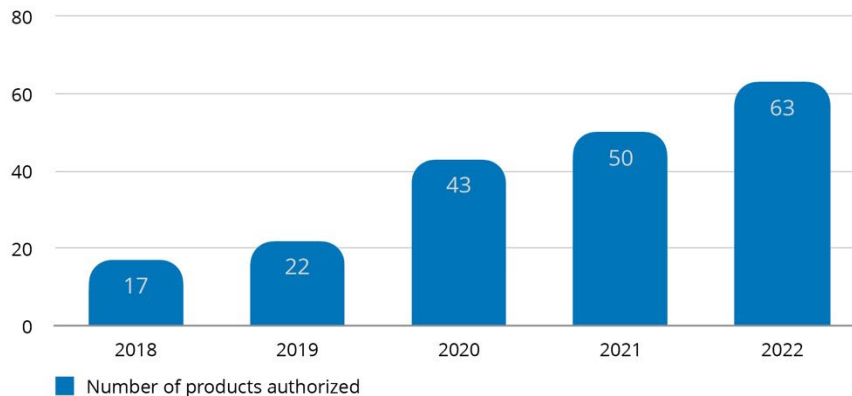
#### 3.7.1 Description

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.”

<i>Date of Creation</i>	2011
<i>Scope</i>	United States
<i>Validity of Certificate</i>	1 year
<i>Mutual Recognition</i>	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

<i>Modality</i>	Data collected manually from the official website of <a href="#">FedRAMP</a>
<i>Date of Data Collection</i>	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

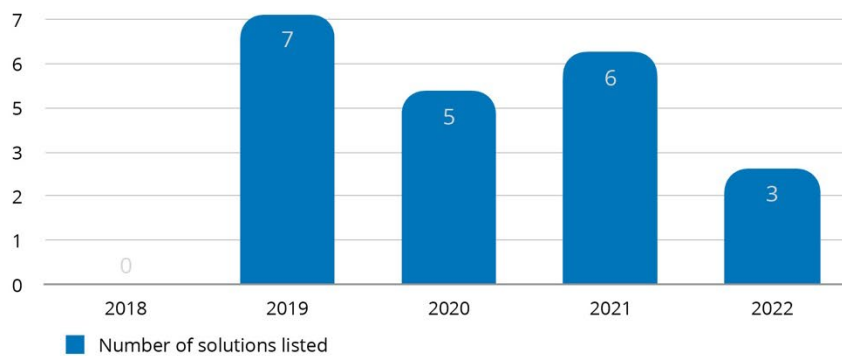


operational security and privacy legal compliance. The certification is designed to work as a complement to the ISO/IEC 27001 framework and aims at demonstrating a higher level of security.

<i>Date of Creation</i>	2013
<i>Scope</i>	International
<i>Validity of Certificate</i>	3 years – ISO/IEC 27001 is a prerequisite to maintain the certification valid
<i>Mutual Recognition</i>	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

<i>Modality</i>	Data collected manually from the official website of <a href="#">CSA</a> .
<i>Date of Data Collection</i>	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.



<i>Date of Creation</i>	2007
<i>Scope</i>	International
<i>Validity of Certificate</i>	2 years
<i>Mutual Recognition</i>	None

### 3.9.2 Data Collection

<i>Modality</i>	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.

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

### 3.10.2 Data Collection

<i>Modality</i>	No public data available
-----------------	--------------------------



# 4. ASSESSMENT BODIES

Third-party Security assessment activities would not work without relying on accredited assessment bodies processing with the evaluation of security controls and when applicable, formally approving the satisfactory results.

The chapter only includes the assessment bodies related to the different ICT products cybersecurity assessment methodologies studied in the report. The data on cloud services auditors (or evaluators) could not be gathered for this version of the report due to the variety of the standards.

## 4.1 ACCREDITED LABORATORIES

### 4.1.1 Description

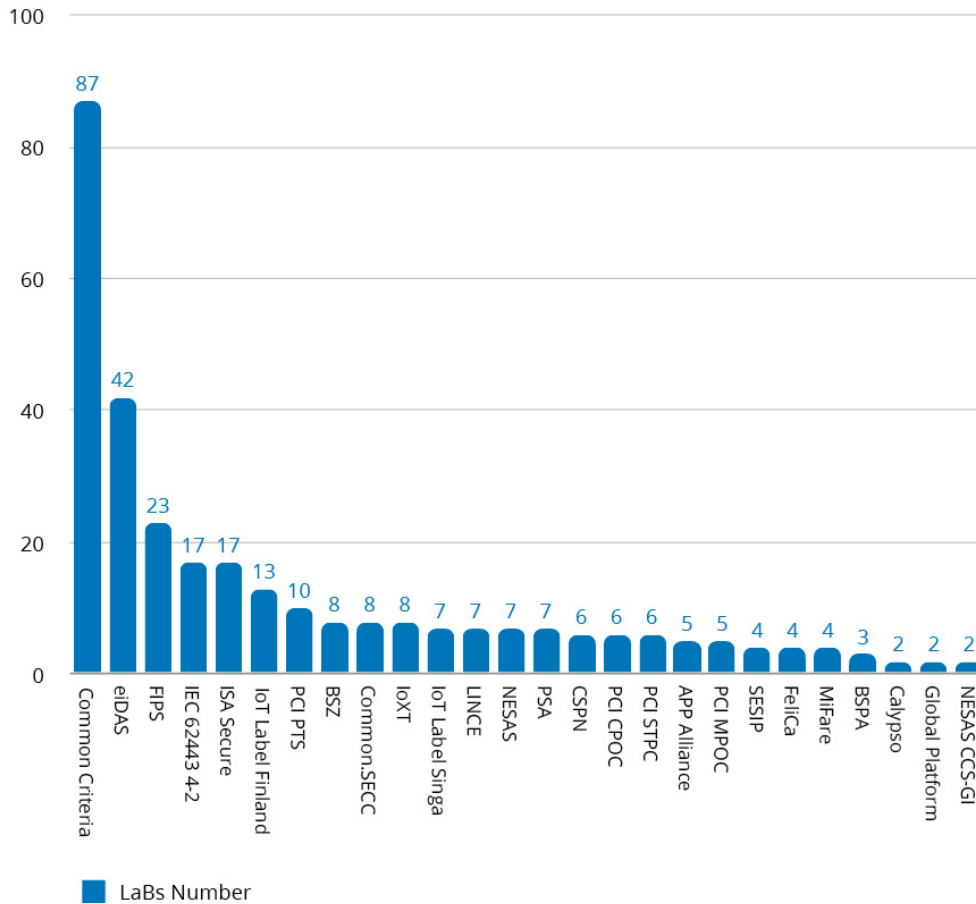
In this section we include all accredited laboratories assessing against ICT products schemes. The word laboratory encompasses many terminologies depending on the assessment methodology. They can be referred to as laboratory, assessor, evaluator, ITSEF and more.

Being formally accredited by accreditation bodies, laboratories represent the cornerstone of third-party cybersecurity assessments. They are the ones in charge of performing the competent tests. Laboratories are usually accredited using ISO/IEC 17025.

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



**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

<i>Modality</i>	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.
<i>Date of Data Collection</i>	20/06/2023

### 4.2 LICENSED CONFORMITY ASSESSMENT BODIES

#### 4.2.1 Description

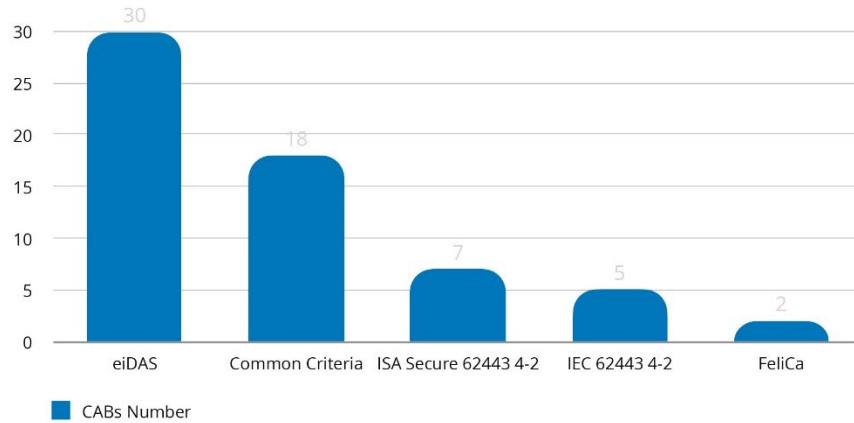
Conformity Assessment Bodies (CAB) can be called differently depending on the terminology of the scheme under consideration, for instance: Certification Bodies (CBs), validators, monitoring bodies...



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

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



# ANNEX 1: FIGURES INDEX

Figure 1: Worldwide 5-year evolution of the total number of approved or certified ICT products, all cybersecurity assessments from the report combined.....	6
Figure 2: Common Criteria certified products in the last 5 years.....	10
Figure 3 Common Criteria certified products in the European Union in the last 5 years.....	10
Figure 4: Certified products according to CSPN in the last 5 years.....	12
Figure 5: Certified products according to BSPA in the last 5 years.....	13
Figure 6 LINCE certified products in the last 5 years.....	14
Figure 7: Certified products according to BSZ in the last 5 years.....	15
Figure 8: Certified products according to FIPS in the last 5 years.....	16
Figure 9: Number of eIDAS qualified signature/seal creation devices and secure signature creation devices in the last 5 years.....	17
Figure 10: Certified products according to IEC 62443-4-2 in the last 5 years.....	19
Figure 11: Certified products according to APP Defense Alliance in the last 5 years.....	20
Figure 12: Certified products according to GSMA eUICC (eSA) in the last 5 years.....	21
Figure 13: Assessed products according to NESAS in the last 5 years.....	22
Figure 14: Certified products according to Common.SECC in the last 5 years.....	24
Figure 15: Certified products according to PCI CPoC in the last 5 years.....	25
Figure 16: Certified products according to PCI HSM in the last 5 years.....	26
Figure 17: Certified products according to PCI SPoC in the last 5 years.....	28
Figure 18: Certified products according to Calypso in the last 5 years.....	29
Figure 19: Certified products according to FeliCa in the last 5 years.....	30
Figure 20: Certified products according to MiFare in the last 5 years.....	31
Figure 21: Products labelled according to IoT Label – Germany in the last 5 years.....	32
Figure 22: Products labelled according to IoT Label – Finland in the last 5 years.....	33
Figure 23: Products labelled according to IoT Label – Singapore in the last 5 years.....	34
Figure 24: Certified products according to PSA in the last 5 years.....	35
Figure 25: Certified products according to ioXt in the last 5 years.....	36
Figure 26: Certified products according to Matter in the last 5 years.....	37
Figure 27: Certified products according to Global Platform TEE in the last 5 years.....	38
Figure 28: Certified products according to SESIP in the last 5 years.....	39
Figure 29: Certified ISMS, including cloud computing services, according to ISO/IEC 27001 in the last 5 years.....	40
Figure 30: Services adhered according to EU Cloud Code of Conduct in the last 5 years.....	41
Figure 31: CSP with a C5 attestation in the last 5 years.....	42
Figure 32: Cloud Computing services qualified according to SecNumCloud in the last 5 years.....	43
Figure 33: Services marked according to Zeker-OnLine in the last 5 years.....	44
Figure 34: Certified Companies, including CSPs, according to ENS in the last 5 years.....	45
Figure 35: Services authorised according to FedRAMP in the last 5 years.....	46
Figure 36: Solutions listed according to CSA STAR in the last 5 years.....	47
Figure 37: Number of laboratories per ICT products assessment methodology.....	50
Figure 38: Number of CABs per assessment methodology.....	51



# ANNEX 2: ACRONYMS TABLE REFERENCE

Listed in order of appearance

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



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



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



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





## 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](http://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](http://enisa.europa.eu)



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