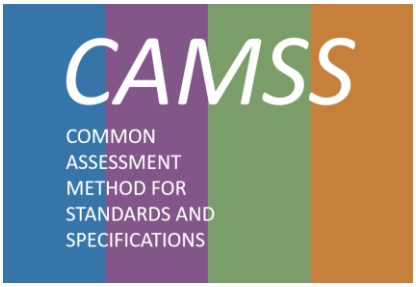

ASSESSMENT SUMMARY v1.0.0

Cyber Security for Consumer Internet of Things Baseline Requirements (EN 303 645)1

European Telecommunications Standards Institute (ETSI)2

[1] The EN 303 645 specification homepage: https://www.etsi.org/technologies/consumer-iot-security

[2] The development organisation homepage: https://www.etsi.org/

Change Control

Modification	Details
Version 1.0.0	
Initial version	

TABLE OF CONTENT

1. INTRODUCTION

The present document is a summary of the assessment of EN 303 645 carried out by CAMSS using the CAMSS Assessment EIF scenario[3]. The purpose of this scenario is assessing the compliance of a standard or specification with the European Interoperability Framework (EIF)[4].

2. ASSESSMENT SUMMARY

The **Cyber Security for Consumer Internet of Things: Baseline Requirements (EN 303 645)** is a comprehensive, single-purpose specification that manufacturers and IoT stakeholders need in order to meet basic security requirements. The scope of the specification is security in domestic devices.

EN 303 645 is a standard for cybersecurity on the Internet of Things and is considered as a security baseline for Internet-connected consumer products. Cybersecurity is a growing concern at European level and is a key area in the EU's Cybersecurity Strategy[5]; therefore, the specification might lay the foundation for IoT certification schemes in the EU.

The specification has been developed by the European Telecommunications Standards Institute (ETSI), which is an international community concerned with the development, ratification and testing of globally applicable standards for ICT-enabled systems, applications, and services. It is worth to note, that it has been developed in close collaboration with the European Commission, as it is stated in the EU Cybersecurity Act[6].

2.1. EIF Interoperability Principles

Interoperability principles are fundamental behavioural aspects that drive interoperability actions. They are relevant to the process of establishing interoperable European public services. They describe the context in which European public services are designed and implemented.

***The specification does not support the principles setting context for EU actions on interoperability*:**

- **Subsidiarity and proportionality**

[3] EUSurvey EIF Scenario: https://ec.europa.eu/eusurvey/runner/EIFScenario_v500

[4] The EIF specification homepage: https://ec.europa.eu/isa2/eif_en

[5] EU's Cybersecurity Strategy (Shaping Europe's digital future website): https://digital-strategy.ec.europa.eu/en/policies/cybersecurity#:~:text=The%20EU%E2%80%99s%20Cybersecurity%20Strategy%20aims%20to%20strengthen%20our,areas%20of%20action%3A%20resilience%2C%20technical%20sovereignty%20and%20leadership%3B

[6] EU Cybersecurity Act: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

There is no Member State that includes the EN 303 645 in their National Interoperability Framework (NIF)[7] in alignment with the three categories of the European Interoperability Framework (EIF).

The specification partially supports the principles setting context for EU actions on interoperability:

- **Openness**

  The EN 303 645 specification addresses the most significant and widespread security weaknesses. Then, the specification purpose relates to the security of data and its protection. The development process carried out by the Technical Committee (TC) CYBER (Cybersecurity)8, is publicly accessible, and is transparent in the sense that it accepts external contributions from different stakeholders. However, the topic selection of these reviews is independent of the external contributors. The TC CYBER is the developer community that maintains this specification.

  EN 303 645 is part of different cross-border cybersecurity initiatives, and since its recognition as a European Standard in 2019 the specification has been extended to meet the specific requirements that the European ICT environment postulates and to be recommended by some of the European Member States. In terms of availability, EN 303 645 is publicly available for free at ETSI's webpage[9]. It is licensed under the royalty-free basis for its implementation or study.

- **Transparency**

  The EN 303 645 specification ensures the protection of personal data according to the sixth clause of the specification documentation[10] about 'Data protection provisions for consumer IoT', in compliance with all the European Regulations and Policies[11]. However, the purpose of the EN 303 645 specification is not related to the visibility nor the comprehensibility of administrative procedures, rules data, and services, and does not ensure the availability of interfaces on its own.

- **Reusability**

  EN 303 645 is associated to the consumer IoT device and the data security domain. The specification is a comprehensive, single-purpose specification that manufacturers and IoT stakeholders need in order to meet basic security requirements, and therefore its use is out of

[7] National Interoperability Framework (NIF): https://joinup.ec.europa.eu/collection/national-interoperability-framework-observatory-nifo/nifo-factsheets

[8] ETSI TC CYBER reference: https://www.etsi.org/cyber-security/tc-cyber-roadmap

[9] EN 303 645 homepage reference: https://www.etsi.org/technologies/consumer-iot-security

[10] EN 303 645 specification documentation: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

[11] ETSI Role in Europe reference : https://www.etsi.org/about/etsi-in-europe?highlight=WyJldXJvcGVhbiIsIidldXJvcGVhbiIsImV1cm9wZWFuJ3MiLCJyZWd1bGF0aW9ucyIsImV1cm9wZWFuIHJlZ3VsYXRpb25zIl0=

the public domain. Nevertheless, European directives are currently making an effort to verticalise the consumer IoT industry and extend it to more sectors in the context of the digitisation[12].

- **Technological neutrality and data portability**
  EN 303 645 is a set of security best practices for Internet-connected consumer devices and is intended to support all parties involved in the development and manufacture of consumer IoT devices. In this sense, the specification is not intended to depend on any specification and is highly adaptable to a large consumer IoT landscape. Also, there is no risk of hampering interoperability nor scalability since the specification has no substantial implications for data portability and it is designed in a way that allows for partial implementation.

***The specification does not support the principles related to generic user needs and expectations*:**

- **User-centricity**
  EN 303 645 is a set of security best practices for Internet-connected consumer devices. However, it is not focused on reuse of relevant data nor the implementation of the OOP.

- **Inclusion and accessibility**
  The purpose of EN 303 645 is not related to e-accessibility. Therefore, this criterion is considered not applicable to this specification.

- **Security and privacy**
  EN 303 645, more specifically provision 5.8 and 5.4, explicitly addresses and enables the secure and trustworthy data exchange and processing.

- **Multilingualism**
  The purpose of EN 303 645 is not related to the delivery of multilingual European Public Services. Therefore, this criterion is considered not applicable to this specification.

The specification partially supports the foundation principles for cooperation among public administrations:

- **Administrative Simplification**
  Up to date, EN 303 645 does not enable digital service delivery channels, but contributes to simplify the delivery of public services. For example, the Eurosmart IoT Certification Scheme[13], which relies on the EN 303 645 specification, sets the first common certification scheme for IoT

[12] Europe Plans on IoT:

https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/internet-things

[13] Eurosmart IoT Certification Scheme: https://www.eurosmart.com/eurosmart-iot-certification-scheme/

devices in Europe and facilitates the delivery of European public services. New delivery channels could arise once the EU cybersecurity certification framework for ICT products[14] is consolidated.

- **Preservation of information**
  The purpose of EN 303 645 is not related to the long-term preservation of data/information/knowledge. Therefore, this criterion is considered not applicable to this specification.

- **Assessment of effectiveness and efficiency**
  There is no evidence of any study directly assessing the efficiency of the EN 303 645 specification. However, there are some organisations from the private sector, offering solutions based on the specification's performance with respect to the market, that indirectly assess the specification's effectiveness and efficiency. It is the case of TÜV SÜD[15], which offers testing against the EN 303 645 specification.

2.2. EIF Interoperability Layers

The interoperability model which is applicable to all digital public services includes:
- Four layers of interoperability: legal, organisational, semantic and technical;
- A cross-cutting component of the four layers, 'integrated public service governance';
- A background layer, 'interoperability governance'.

The Specification supports the implementation of digital public services complying with the EIF interoperability model:

- **Interoperability governance**
  This specification is not currently included in the EIRA Library of Specifications (ELIS) but will be included in the next release of the ELIS (Security Framewrok ABB of the Organisational View). However, EN 303 645 is mappable to the European Interoperability Reference Architecture (EIRA). Despite not having been included in any Member State's catalogue, the specification has been recommended by some European national agencies like the Federal Office for Information Security (BSI)[16] in Germany, or has been integrated in a public service like the Cybersecurity label in Finland to certify safe smart devices and assist consumers in buying safer products[17]. In terms

[14] EU cybersecurity framework: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework

[15] TÜV SÜD - EN 303 645:

https://www.tuvsud.com/en-us/industries/consumer-products-and-retail/iot-cybersecurity/

[16] German BSI:

https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2020/SmartHome_130720.html

[17] Finnish Transport and Communications Agency Traficom:

of implementation conformity, there is no available validation tool provided by ETSI but there exist some manual testing alternatives to assess the conformance of the specification's implementation.

- **Legal Interoperability**
  Although the EN 303 645 specification is a European Standard. After checking assessments carried out in order to verify the specification's compliance with European Standardisation regulation 1025/2012, the specification is fully aligned with the European Cybersecurity Act[18].

- **Organisational interoperability**
  The EN 303 645 specification facilitates business modelling, as the specification can be deployed into any architecture for consumer IoT in a home environment. The specification establishes a cybersecurity baseline for connected consumer products and could set the basis for future IoT certification systems in Europe[19].

- **Semantic Interoperability**
  EN 303 645 is available for its use and implementation on ETSI. ETSI, as an acknowledged European standardisation, offers different channels for the creation of communities and the sharing of data and results in European platforms.

https://www.kyberturvallisuuskeskus.fi/en/news/finland-becomes-first-european-country-certify-safe-smart-devices-new-cybersecurity-label

[18] Europe Plans on IoT: https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/internet-things

[19] Cybersecurity Act reference:

https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act#:~:text=The%20EU%20Cybersecurity%20Act%20introduces%20an%20EU-wide%20cybersecurity,see%20their%20certificates%20recognised%20across%20the%20European%20Union.

3. ASSESSMENT RESULTS

This section presents an overview of the results of the CAMSS assessments for **EN 303 645**. The CAMSS "Strength" indicator measures the reliability of the assessment by calculating the number of answered (applicable) criteria. On the other hand, the number of favourable answers and the number of unfavourable ones are used to calculate the "Automated Score" per category and an "Overall Score".

Category	Automated Score	Assessment Strength	Compliance Level
Principle setting the context for EU actions on interoperability	20/100	100%	Ad-hoc
Core interoperability principles	1660/2100	71%	Sustainable
Principles related to generic user needs and expectations	500/500	40%	Seamless
Foundation principles for cooperation among public administrations	220/500	80%	Essential
Interoperability layers*	800/1100	100%	Sustainable
Overall Score	3200/4300	77%	

**The technical interoperability layer is covered by the criteria corresponding to the core interoperability principle ''Openness''.*

With a 77% of assessment strength, this assessment can be considered representative of the specification compliance with the EIF principles and recommendations.

The Overall Automated Score of 74,42% (3120/4300) demonstrates that the specification does not support the European Interoperability Framework in the domains where it applies.