How to evaluate your product according to ETSI EN 303 645 cybersecurity standard

DEKRA

On the safe side.

Cybersecurity importance in Consumer IoT devices

Data and privacy of consumers using IoT devices are **daily exposed**.

There are **boundless ways** to **compromise** the security of an **IoT device**.

IoT devices experience an average of **5200 attacks per month***.

Cyber threats increase as more connected devices are used.

ETSI EN 303 645, the Cybersecurity Standard

ETSI has **created** a **cybersecurity standard** with a baseline of security and privacy provisions applicable to **all consumer IoT devices.**

Apply ETSI EN 303 645 to your product and prove you **meet the best cybersecurity practices.**

At **DEKRA**, we **evaluate your products** according to the **ETSI EN 303 645.**

Protect user of IoT devices in a connected world.

(*) source Symantec

ETSI EN 303 645: The Cybersecurity Standard for Consumer IoT Devices

What is the ETSI EN 303 645?

- The **first globally applicable cybersecurity standard for consumer IoT** (Internet-of-Things) devices.
- Designed to **protect against** the most common **cybersecurity threats** and to **prevent** large-scale **attacks** against connected devices.
- Establishes a common baseline that **covers security and privacy best practices** and provides a **basis for** future **IoT certification schemes** (The EU Cybersecurity Act (CSA)).
- **Contains** a set of **13 security categories** and some provisions specifically focused on **Data Protection.** In total, the ETSI EN 303 645 includes 33 mandatory provisions and 35 recommendations that consumer IoT devices shall meet.

What devices does ETSI EN 303 645 cover?

This standard covers **consumer IoT devices** that are **connected to network** infrastructure and their **interactions with associated services.** For example:


Smart TV's


Smart speakers


Smart cameras


Smart home assistants


Connected children's toys and baby monitors.


Wearable health trackers


Connected appliances (e.g., washing machines, refrigerator, etc).


Connected smoke detectors, door locks and windows sensors.


Connected home automation and alarm systems (gateways and hubs).


IoT gateways, base stations and hubs to which multiple devices connect.

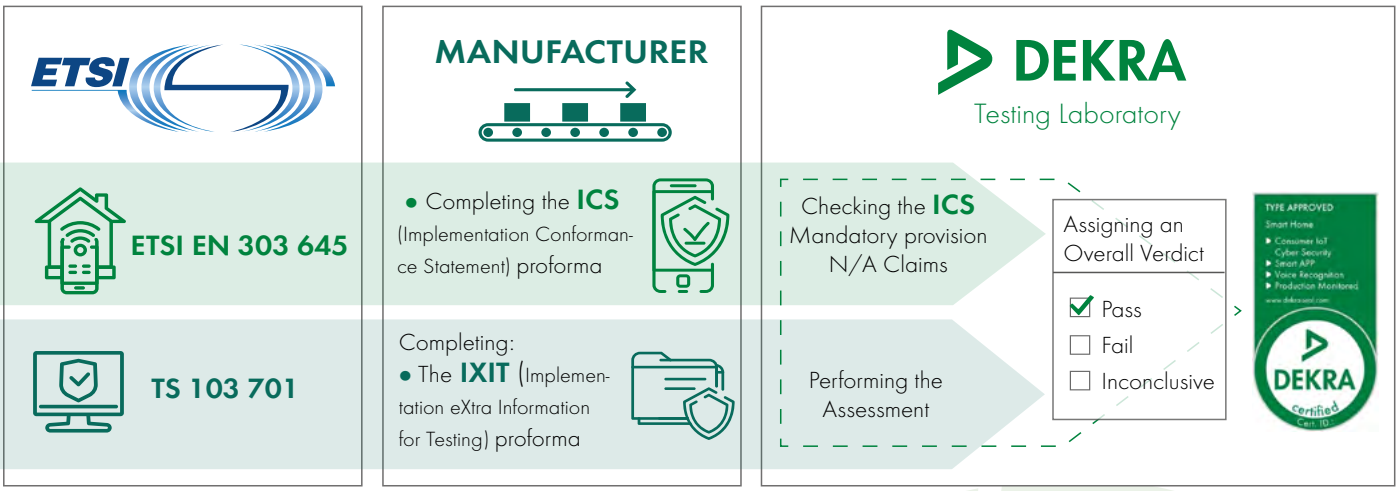
Why should you implement ETSI EN 303 645 requirements in your product?

- To **improve** the **security** of the device and **minimize** cyber **threats.**
- This standard is considered as the **foundation** for a basic level **IoT consumer assurance,** providing the baseline for future **IoT certification schemes.**
- It intends to **help manufacturers** of consumer IoT devices to provide a number of features to **protect personal data** from a strictly technical perspective considering laws and regulations related to personal data (e.g. GDPR).

How to test and certify your product according to ETSI EN 303 645?

Assessment Procedure

There are different steps to request a certification for a product according to ETSI EN 303 645 requirements**.**



1. Meet ETSI EN 303 645 requirements

Manufacturers need to **implement** the **requirements** defined by the ETSI EN 303 645 standard in their products, which includes 33 requirements and 35 recommendations grouped over 13 categories of **security** and one for **privacy**:

1. No universal default passwords.
2. Implement a means to manage reports of vulnerabilities.
3. Keep software updated.
4. Securely store sensitive security parameters.
5. Communicate securely.
6. Minimize exposed attack surfaces.
7. Ensure software integrity.
8. Ensure that personal data is protected.
9. Make systems resistant to outages.
10. Examine system telemetry data.
11. Make it easy for consumers to delete personal data.
12. Make installation and maintenance of devices easy.
13. Validate input data

\+ Additional provisions (5) for data protection

2. Prepare documentation

The **manufacturer** shall prepare the following documents to evaluate their devices:

- **Implementation Conformance Statement proforma (ICS):**

  In this document the supplier states which capabilities are implemented or supported in the product based on the provisions from ETSI EN 303 645.

- **Implementation eXtra Information for Testing proforma (IXIT):**

  This document contains additional necessary information to evaluate the product. It especially provides design details for the testing laboratory and it is the basis for grey-box testing methodology which is used for the assessment.

3. Test your product

- **DEKRA evaluates products against the provisions defined in ETSI EN 303 645,** following the Technical Specification determined in ETSI TS 103 701.
- **DEKRA** issues an **evaluation report** of the product.

4. Certify your product

DEKRA issues a DEKRA Seal if the product complies with the ETSI EN 303 645 standard.

DEKRA cybersecurity services for ETSI EN 303 645

- **Training:** We offer guidance for the prepation of the ICS and IXIT documents, as well as further information manufacturers shall provide to perform the evaluation.
- **GAP Analysis:** We assesses the product to determine the differences between the current security implementation of the product and the provisions defined in ETSI EN 303 645.
- **Product Evaluation:** We evaluate the product based on the applicable provisions of the ETSI EN 303 645 and will issue a conformance evaluation report as well as the identified security gaps.
- **Statement of Conformity:** DEKRA issues a Statement of Conformity when the evaluated product meets the requirements defined in ETSI EN 303 645.

Additional DEKRA's cybersecurity services for IoT products

We offer Testing & Certification services for Consumer IoT devices according to:

- **ioXt Security Certification:** We are an Authorized Lab by the ioXt Alliance to provide services for Android devices, smart speakers, consumer cameras, smart TV's, lighting systems, HVAC appliances and automotive infotainment.
- **CTIA Cyber Security Certification Test Plan:** We are a CTIA Authorized Testing Laboratory (CATL) for CTIA Cyber Security Certification Test Plan for IoT Devices.
- **Amazon AVS Security Verification:** We are an Authorized Security Lab for Alexa and offer device evaluation programs.
- **NISTIR 8259:** We assess devices according to NISTIR 8259A, the Foundational Cybersecurity Activities for IoT Device Manufacturers standard that is part of the NIST Cybersecurity for IoT program.

Other cybersecurity services

- **Common Criteria and ISO 15408.**
- **FIPS 140-3 and ISO 19790.**
- **eIDAS.**
- **UNECE WP29 Cybersecurity Regulation.**
- **Product Penetration Testing.**
- **IEC 62443.**
- **LINCE.**
- **NESAS (3GPP).**
- **GSMA.**

About DEKRA

DEKRA has been active in the field of safety for more than 90 years. Founded in 1925 in Berlin as Deutscher Kraftfahrzeug-Überwachungs-Verein e.V., it is today one of the world's leading expert organizations. DEKRA SE is a subsidiary of DEKRA e.V. and manages the Group's operating business. In 2020, DEKRA generated preliminary sales totaling 3.2 billion euros. The company currently employs more than 43,000 people in approximately 60 countries on all six continents. With qualified and independent expert services, they work for safety on the road, at work and at home. These services range from vehicle inspection and expert appraisals to claims services, industrial and building inspections, safety consultancy, testing and certification of products and systems, as well as training courses and temporary work. The vision for the company's 100th birthday in 2025 is that DEKRA will be the global partner for a safe world.

https://www.dekra-product-safety.com/en/etsi-en-303-645-cybersecurity-standard