ETSI EN 303 645:
security of IoT consumer electronics

Kiwa Nederland
Wilmersdorf 50
7327 AC Apeldoorn
The Netherlands

www.kiwa.com

ETSI EN 303 645: security of IoT consumer electronics

Refrigerators, lighting, TV's, smoke detectors, toys, fitness trackers... An ever-increasing number of everyday electronic consumer products is connected to the internet. These 'smart' devices make our lives more pleasant and often easier, but they also entail security risks. The standard ETSI EN 303 645 contains guidelines for the protection of consumer electronics that are part of the Internet of Things (IoT).

Nowadays, smart devices can now be found in almost every household. These devices usually collect, store and transmit data from the user in one way or another. Too often, these devices are by default not or insufficiently protected against hacks, data leaks, etc. The European Telecommunications and Standardization Institute (ETSI) has therefore developed the standard ETSI EN 303 645. Based on this standard Kiwa tests and assesses whether IoT and consumer electronic products are sufficiently secure for end users.

Essential security requirements

By developing the standard ETSI EN 303 645, ETSI participants (manufacturers, network service providers, governments, telecom regulators and end users) have established effective, essential security requirements and best practices regarding cyber security and privacy protection of consumer electronics whitch partake in data traffic.

Cyber security IoT consumer products

ETSI EN 303 645 contains cybersecurity requirements and procedures for IoT consumer products. This not only concerns smart devices themselves, but also sensors and operating parts of these devices. Connected devices can often also be operated with a smartphone app. The safety thereof is not covered by ETSI EN 303 645, but as an optional service Kiwa can assess its safety using the RARS K21048 certification scheme.

Manufacturers of IoT consumer electronics

Certification by Kiwa according to ETSI EN 303 645 is of added value to developers and manufacturers of consumer electronics that can be connected to the web. Examples include baby monitors, smart doorbells, cameras, TV's and speakers, wearable health trackers and connected home appliances such as washing machines and refrigerators. Basically, any consumer electronic device utilizing data can be put to test according to ETSI EN 303645. Product development according to ETSI EN 303 645 contributes to better safety, updateability, transparency, structure, etc.

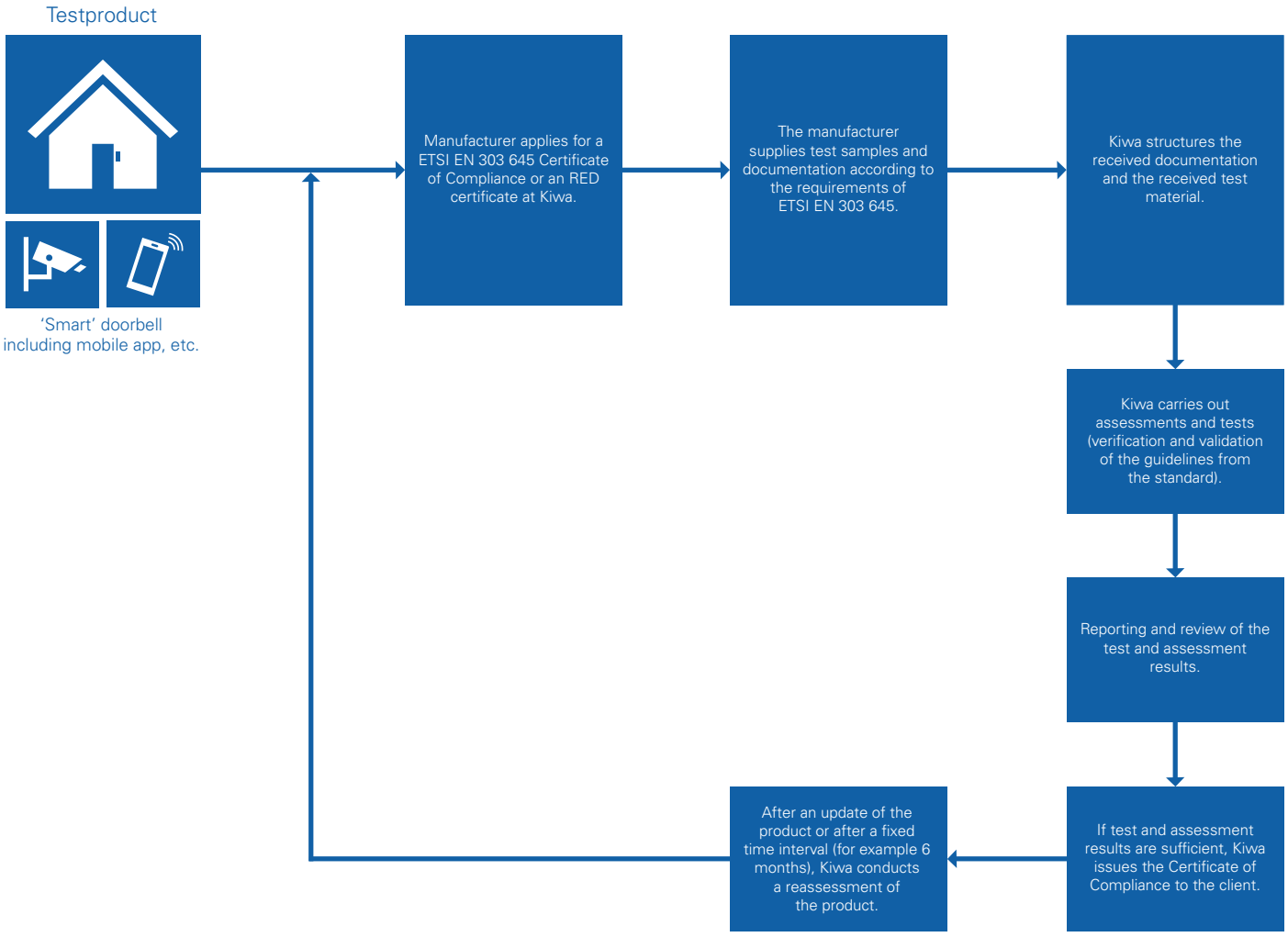
Radio Equipment Directive (RED) Compliance

Compliance to the ETSI EN 303 645 activates article 3.3d, e, f and i of the RED. This means that on your RED certificate compliance to the ETSI EN 303 645 will be stated as well. Communicating to your stakeholder that your RED compliancy also includes cybersecurity for consumer electronic products will allow your product to standout in a world where cyber threats are rampant!

ETSI EN 303 645: security of IoT consumer electronics

Certification process

What requirements must consumer electronics using internet functionality meet to obtain the ETSI EN 303 645 compliance? As an example we take a 'smart' doorbell. This doorbell with camera records who rings the doorbell and then sends a push message to the resident who can then communicate with the visitor via an app. A nice piece of technology, with interesting security aspects. Below is a schematic overview of the certification process for this product.



What aspects of IoT products do we assess?

Kiwa's IoT security experts perform tests based on the standard ETSI EN 303 645 and evaluate whether an IoT or 'smart' application meets the requirements that ensure that the product can be used safely by everyone involved. The product is hereby subject to the requirements of ETSI EN 303 645. Aspects that are checked and assessed include:

- Application of the standard: Not all requirements of the standard must be met, but if that is the case this must be reported and motivated accordingly;
- Quality of passwords: Standard Passwords such as 1234, admin, 0000 etc. do not meet the security requirements; Having a way or manner to ensure more secure passwords is therefore recommended
- Vulnerability reporting: Manufacturers should ensure that security researchers, among others, are able to report vulnerabilities transparently and then based on the feedback resolve the illuminated problems.
- Update policy: Developing and implementing security updates in a timely manner is one of

ETSI EN 303 645: security of IoT consumer electronics

of the most important actions a company can take to protect customers and the wider technical ecosystem;
- Storage sensitive security info: Security parameters (e.g. passwords, access levels, fail safe mechanisms and IP addresses) are important for ensuring the general security of a product. These parameters must be stored properly and securely;
- Avoid exposed attack surfaces: A combination of technology, processes and interactions can create 'openings' (consciously or unconsciously) in software that can be misused by malicious parties. This is also known as attack surface. By reducing attack surfaces, which means reducing vulnerabilities in various dimensions, breaches etc. can be prevented.;
- Integrity of software: Demonstrate that the software used for the product is of good quality and safe and is actually intended for the product in question; This ensures that software ran by devices (and its surrounding ecosystem) is not corrupted.
- Protection of personal data: The manufacturer is expected to ensure that personal data is processed in accordance with relevant laws and regulations such as the GDPR;
- Robustness of the system: Can the system absorb failures and disruptions in such a way that functionality is not hindered?
- Investigate telemetry data: Telemetry data from consumer IoT devices and services can be investigated to detect security anomalies;
- Ability to delete private information: For privacy reasons, it should be possible for the end user of a product to delete personal information;
- Installation and maintenance instructions: Errors during installation and maintenance can cause vulnerabilities (consciously or unconsciously). Procedures for this must therefore be clear and simple for the end user;
- Validate input data: Make sure that main and sub-processes exchange input with each other that is honest, true and correct.

ETSI EN 303 645 Compliance

The certification process results in a test report. If the product meets the requirements of the standard, the manufacturer will receive a certificate of compliance. If the manufacturer applied for a RED certificate their compliance to the ETSI EN 303 645 will be mentioned on the RED Certificate. This allows the manufacturer to demonstrate that the product meets the basic requirements in the field of IoT and Cyber security which is becoming increasingly important. In this way, a manufacturer not only creates trust among the (potential) users of his product, but can also distinguish himself from other manufacturers.

Relevant Services

We can help you with the following services as well:
- K21048 RARS: For cybersecurity of systems that utilize remote access with for example mobile applications
- FCC/ ISAD Market Access: Testing and certifying your products for market access to north-America
- IEC 62443: Cyber Security for Industrial Systems