



ETSI EN 303 645 IoT Compliance

- **Who is this for?**
IoT Product/Service Developers and Manufacturers
- **What are the deliverables?**
Compliance report and gap analysis
- **What is the result?**
Demonstrated compliance against European Norm security baseline

What is ETSI EN 303 645?

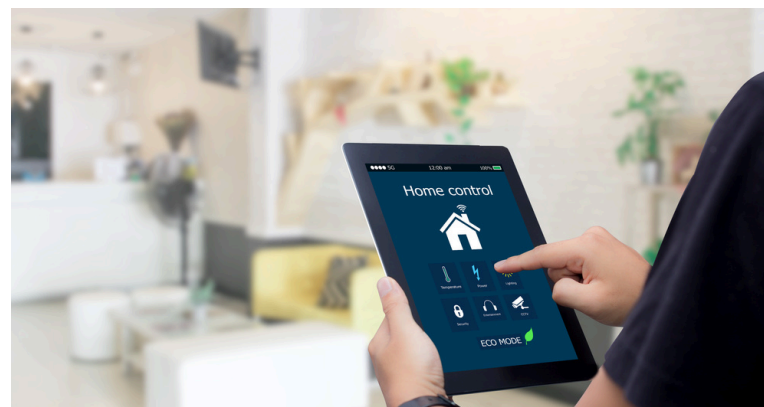
The ETSI EN 303 645 norm is currently one of the main standards for the assessment and validation of IoT products, with a special focus and relevance on the side of consumer IoT.

Originally inspired by the UK IoT Code of Practice for security, the ETSI EN 303 645 grew up to an EU recognized framework, therefore being a very good reference for upcoming EU level certification schemes for consumer IoT products. Aligning to the requirements of the norm would therefore be an important health check for your IoT product, as well as a good preparation for upcoming EU level certification.

Scope of Evaluation

The possible scope of products to be assessed based on the ETSI EN 303 645 norm includes:

- Consumer products such as wearables, smart applications, connectivity modules.
- Smart home products such as thermostats, smart cameras, lighting, smart appliances.



ETSI EN 303 645 Compliance for IoT Products

The ETSI EN 303 645 norm is designed to provide an efficient, baseline assessment methodology for the evaluation of IoT products and solutions. Aspects of this methodology include:

- Password security
- Secure software updates
- Security of interfaces and data communications
- Product's availability
- Completeness and correctness of user guidance
- Vulnerability disclosure procedures and patch management
- Product logging
- Protection of personal data
- Validation of data inputs

The ETSI EN 303 645 norm is getting increasingly more attention, as it is considered a future reference baseline for the definition of EU level IoT certification schemes. Bureau Veritas Cybersecurity has defined an efficient assessment methodology based on the requirements of this norm. The assessment will contain a combination of testing on the product in scope, as well as review of available documentation and processes.

Bureau Veritas Cybersecurity will intake the product to be assessed, as well as the rest of the associated documentation (security description and architecture, user guides, test reports, etc.). Afterwards, Bureau Veritas Cybersecurity assesses the product based on the applicable requirements, and finally issue a Compliance Report to the customer. The report will include the compliance state against all the considered requirements, as well as the identified security gaps.

Would you like to know more about ETSI EN 303 645 Compliance for your IoT product?

Contact us today to discuss our services in more detail and find out which service fits your product best.



Why choose Bureau Veritas Cybersecurity

Bureau Veritas Cybersecurity is your expert partner in cybersecurity. We help organizations identify risks, strengthen defenses and comply with cybersecurity standards and regulations. Our services cover people, processes and technology, ranging from awareness training and social engineering to security advice, compliance and penetration testing.

We operate across IT, OT and IoT environments, supporting both digital systems and connected products. With over 300 cybersecurity professionals worldwide, we combine deep technical expertise with a global presence. Bureau Veritas Cybersecurity is part of the Bureau Veritas Group, a global leader in testing, inspection and certification.



Interested?



cybersecurity@bureauveritas.com

Contact us today:



[cybersecurity.bureauveritas.com](https://www.bureauveritas.com/cybersecurity)