Secure IoT

Secure IoT refers to the practice that keeps IoT ecosystem safe. Several tools are used to protect the IoT system from threats and breaches, identify and monitor risks to reduce vulnerabilities, and ensure Confidentiality, Integrity, and Availability of the IoT solution. Objects or machines, known as things in IoT, can be connected each other over internet, or cellular networks to cloud applications and backends, which can send data, where there is security risk at every steps along the IoT journey. Secure IoT network is important to protect from attackers who could take advantage of the IoT system's vulnerability.

Technical Committees working on Secure IoT

– International level –

ISO/IEC JTC 1/SC 27 - **Information security, cybersecurity, and privacy protection**

- **Scope:**
  The development of standards for the protection of information and ICT including IoT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as:
  - Security requirements capture methodology;
  - Management of information and ICT security; in particular information security management systems, security processes, and security controls and services;
  - Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity, and confidentiality of information;
  - Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
  - Security aspects of identity management, biometrics, and privacy;
  - Conformance assessment, accreditation, and auditing requirements in the area of information security management systems;
  - Security evaluation criteria and methodology.

- 230 published standards
- 67 ongoing projects
- 5 Working Groups and 2 Joint Working Groups
- 27 national delegates

ISO/IEC JTC 1 SC 41 - **IoT and Digital Twin**

- **Scope:**
  Standardization in the area of Internet of Things and Digital Twin, including their related technologies to:
  - serve as the focus and proponent for JTC 1's standardization programme on the Internet of Things and Digital Twin, including their related technologies;
  - provide guidance to JTC 1, IEC, ISO and other entities developing Internet of Things and Digital Twin related applications.

- 44 published standards and 27 ongoing projects ongoing projects
- 5 Working Groups and 3 Joint Working Groups
- 13 national delegates

– European level –

ETSI TC Cyber - Cybersecurity

- **Scope:**
  The activities of ETSI TC Cyber include the following broad areas:
  - Cyber Security;
  - Security of infrastructures, devices, services and protocols;
  - Security advice, guidance and operational security requirements to users, manufacturers and network and infrastructure operators;
  - Security tools and techniques;
  - Provision of security mechanisms to protect privacy;
  - Creation of security specifications and alignment with work done in other TCs.

- 92 published standards
- 41 ongoing projects
- 1 Working Group (Quantum-Safe Cryptography)

Secure IoT standards

The following table lists the published and ongoing secure IoT related standards at the international and European levels.

Published standards and projects developed by ISO/IEC JTC 1/SC 27

ISO/IEC 27400:2022
Cybersecurity – IoT security and privacy – Guidelines

Scope:
The standard provides guidelines on risks, principles and controls for security and privacy of Internet of Things (IoT) solutions.

Overview:
IoT systems present particular challenges for information security and privacy in that they are highly distributed and involve a large number of diverse entities. This implies that there are a very large attack surface and a significant challenge for the information security management system (ISMS) to apply and maintain appropriate security controls across the whole system. This standard provides guidelines how to secure IoT ecoysystem and identifies security and privacy controls for stakeholders in an IoT system environment throughout the IoT system life cycle.

ISO/IEC FDIS 27402
Cybersecurity – IoT security and privacy – Device baseline requirements

Scope:
The standard is expected to specify a baseline or platform for IoT devices supporting information security and privacy controls.

Overview:
This project is intended to provide basic, commonplace security features expected of all networkable IoT devices, thereby enabling, providing or supporting the IoT security controls considered in ISO/IEC 27400.

ISO/IEC DIS 27403
Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics

Scope:
This standard is aimed squarely at the designers, manufacturers and security/privacy assessors of IoT domotics, rather than the users, for example consumers or retail customers.

Overview:
The standard is aimed to cover the information security and privacy aspects of device to device interactions as well as human to device plus device to sensors/actuators that physically interact with the home, and networking both within the home and beyond via Internet gateways.

Published standards and projects developed by ISO/IEC JTC 1/SC 41

ISO/IEC 30147:2021
Internet of things (IoT) – Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 system engineering processes

Scope:
This document provides system life cycle processes to implement and maintain trustworthiness in an IoT system or service by applying and supplementing ISO/IEC/IEEE 15288:2015. The system life cycle processes are applicable to IoT systems and services common to a wide range of application areas.

Overview:
The standard is to provide guidance to realize IoT trustworthiness. This is because existing documents are targeted to each application area and do not necessarily cover all the challenges faced by the IoT system and service according to the above conditions and characteristics specific to IoT systems and services. This document provides system life cycle processes to realize IoT trustworthiness by applying and supplementing ISO/IEC/IEEE 15288:2015.

ISO/IEC CD 30149
Internet of Things (IoT) – Trustworthiness Principles

Scope:
This document is expected to provide principles for IoT trustworthiness based on ISO/IEC 30141 – IoT Reference Architecture.

Overview:
Considering today’s inherent risks on products and solutions in IoT ecosystem, it might be difficult to trust without the correct context or technical understanding of the solution. Trust is a concept that needs to ensure all relevant stakeholders understand the specific trust elements of a solution and any potential risks to their given use case. This standard is expected to leverage the system architecture-based approach to ensure alignment to products and services used in ISO/IEC 30141 - Internet of Things - Reference Architecture which will allow all stakeholders to implement trustworthiness for products and solutions.

ISO/IEC DTS 30168
Internet of Things (IoT) – Generic Trust Anchor Application Programming Interface for Industrial IoT Devices

Scope:
This document is intended to specifiy a generic application programming interface (API) for the integration of secure elements within Industrial Internet of Things (IIoT) devices.

Overview:
This document is expected to provide a flexible Application Programming Interface (API) for security to allow a generic integration of secure elements into IIoT devices, which will be technology and vendor independent to allow easy redesign for different secure elements and to support software-hardware co-design for security.

Standards developed by ETSI TC Cyber

ETSI TS 103 645 V2.1.2 (2020-06)
Cyber Security for Consumer Internet of Things: Baseline Requirements

Scope:
The document specifies high-level security and data protection provisions for consumer IoT devices that are connected to network infrastructure (such as the Internet or home network) and their interactions with associated services.

Overview:
The document provides basic guidance through examples and explanatory text for organizations involved in the development and manufacturing of consumer IoT on how to implement those provisions. It has primarily considered the following list of examples as consumer IoT devices:

- connected children's toys and baby monitors;
- connected smoke detectors, door locks and window sensors;
- IoT gateways, base stations and hubs to which multiple devices connect;
- smart cameras, TVs and speakers;
- wearable health trackers;
- connected home automation and alarm systems, especially their gateways and hubs;
- connected appliances, such as washing machines and fridges; and
- smart home assistants.

ETSI EN 303 645 V2.1.1 (2020-06)
Cyber Security for Consumer Internet of Things: Baseline Requirements

Scope:
The present document specifies high-level security and data protection provisions for consumer IoT devices that are connected to network infrastructure (such as the Internet or home network) and their interactions with associated services.

Overview:
The document was developed primarily to help protect consumers, however, other users of consumer IoT equally benefit from the implementation of the provisions set out in this document.

ETSI TR 103 621 V1.2.1 (2022-09)
Guide to Cyber Security for Consumer Internet of Things

Scope:
The document serves as guidance to help manufacturers and other stakeholders to meet the cyber security provisions defined for Consumer IoT devices in ETSI EN 303 645 and ETSI TS 103 645.

Overview:
The document is complementary to ETSI EN 303 645 and ETSI TS 103 701 to explain the relationship between these specifications and how they can be used together. It also provides a non-exhaustive set of example implementations that can be used to meet the provisions of ETSI EN 303 645 and ETSI TS 103 645.

ETSI TS 103 701 V1.1.1 (2021-08)
Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements

Scope:
The document specifies a conformance assessment methodology for consumer IoT devices, their relation to associated services and corresponding relevant processes against ETSI TS 103 645 /ETSI EN 303 645, addressing the mandatory and recommended provisions as well as conditions and complements of ETSI TS 103 645 /ETSI EN 303 645 by defining test cases and assessment criteria for each provision.

Overview:
The document intends to contribute to the protection of consumer IoT products against the most common cybersecurity threats. The Test Scenarios (TSOs) are targeting basic effort regarding test depth and test circumference in accordance to ETSI TS 103 645 /ETSI EN 303 645 which addresses a baseline security level.