

20 JUNE 2019

digital.security introduces the first European security label for connected solutions

This label can be used by IoT designers to check the security of systems that use connected objects. It serves as a reliable and independent indicator for future adopters or users, whether they are professionals or private individuals.

Paris, 20 June 2019 – digital.security, the leading European certifier for connected object security, has just announced the launch of the IoT Qualified as Secured (IQS) programme – the first certification programme for Internet of Things (IoT) designers who want to have the security of their IoT solutions checked by an independent third party.

With more than fourteen billion IoT devices currently in circulation and more than 25 billion scheduled to enter operation in 2021*, connected objects have become a favourite target for cyber criminals. They can either access the object physically and launch attacks on its components and the personal or sensitive data that they contain, or they can take control of them remotely using software radio.

Who is the programme aimed at?

Using the IoT Qualified as Secured – or IQS – programme, IoT manufacturers can check the security of their systems that use connected objects. And verified devices feature the IQS pictogram – proof of security for future adopters or users, whether they are companies or private individuals.

Characteristics

The IQS label can be awarded to companies in all economic sectors and is based on a reference framework made up of national and international security standards, good “security hygiene” practices and requirements derived from digital.security’s experience.

The core of IQS is EvalUbik – a platform for assessing the security of connected objects. This is a fully fledged test facility for creating the conditions under which a connected object is to be used, which can then be configured and managed.

Two levels of certification issued: standard and advanced.

Certification is issued for IoT solutions (objects and associated services) for a period of two years, adhering to a set of public security requirements (between 25 and 30, depending on the certification level).

digital.security’s aim is to cover most security requirements in EU countries in an objective and measurable way. The time-honoured approach underpinning the certification enables it to evolve as new European standards and regulations are introduced. This way, all IoT stakeholders can adopt a long-term security policy.

Certification process

The Certification Committee, made up of digital.security's independent cybersecurity experts, compares the anonymised assessment report with the framework selected for awarding the certification.

A reference framework of security requirements specifically for the IoT

The IQS certificate's security requirement reference framework has been derived from commonly accepted standards and good practices for protecting IT systems, and is supplemented by feedback from IoT audits conducted by digital.security. It covers the following:

- Protection of data exchanges (PDE)
- Protection of technical platforms (PTP)
- Protection of data access (PDA)
- Traceability (TRA)

All of the components making up a candidate IoT solution are assessed against the reference framework: the connected objects, the communications protocols, the servers that can be accessed over the Internet and the applications made available to users.

"You cannot innovate successfully without managing risks," says Jean-Claude Tapia, CEO of digital.security. "In a global market where the emphasis is more on time-to-market than carefully controlled development, we believed that it was essential to create the first label certifying the security of connected objects, revolutionising the way in which economic and social stakeholders interact with one another. Our aim in launching the IQS label – the first certification system for the IoT – is to come to the aid of all stakeholders and provide this digital revolution with long-term support," he adds.

Further information:

- [White Paper on IoT security](#)
- Website for the label iqs-label.com
- [IoT security watch](#) to get all the news about connected object security
- [CERT-DS TF-CSIRT](#) accreditation

(*) [Gartner](#) IoT Trends, November 2018

ABOUT DIGITAL.SECURITY

Digital.security, the first European certification company that is partly dedicated to connected objects, employs 250 consultants and specialists with numerous certifications. Its services cover auditing, consultancy and training, as well as integrating and operating (service centres) security solutions. digital.security has tried and tested knowledge and rare expertise (radio frequencies, electronics, SOC, IAM, DLP, PKI, etc.), as well as an IoT laboratory for assessing connected solutions and issuing certifications. It monitors the market and undertakes R&D, producing numerous publications and contributions to national and international research.

FOR MORE INFORMATION

<https://digital.security/>

Follow us on [Twitter](#) @iotcert

Press relations contact:

Audrey.desousa@elaneldelman.com -

Seifallah.Boussaada@elaneldelman.com

Tel.: +33 (0)6 35 38 28 22