WHITE PAPER

How PSA Certified Helps the Electronics Industry Become Cybersecurity Regulation Ready

psacertified™

As hacks have increased in recent years, governments have introduced new security laws to protect our online lives. In this white paper, we're exploring how the state of cybersecurity legal requirements evolved in 2023, particularly in Europe, and how PSA Certified can help you to become regulation-ready.

How PSA Certified Helps the Electronics Industry Become Cybersecurity Regulation Ready

As the Internet of Things (IoT) has evolved, so too has our approach to security. A decade ago, product developers were focused on seizing the opportunities that connectivity offered instead of slowing down progress by building in complex security features at the start of a project.

As a result, basic security principles were often ignored during the design phase or implemented as an afterthought, leaving customers' devices and data vulnerable to hackers. In the years since then, some of these weaknesses in security have been exploited. Connected cameras, smart locks, and even connected fish tanks and children's toys have all been hacked, sometimes with severe and far-reaching consequences. The incidents have been reported in mainstream media, which has brought cybersecurity to people's attention. This ripple effect worried governments, who all realize the potential of the technology to deliver significant economic and social benefits but are concerned about having billions of easily hackable devices that may adversely affect their citizens' lives, including implications to privacy and safety.

Contents

The State of IoT Security Regulations for Consumer Connected Devices in Europe and the USA

Where Are We Now?

Many security laws and baseline requirements are being introduced as governments move to protect the consumer. This section looks at the different regulations and their status. The regulations vary between regions and countries and differ in their approach. Some ask companies designing electronic products to state they follow best practices, while others insist on third-party evaluation.

Examples of Regulations Affecting Consumer OEMs in Europe

The EU Cyber Resilience Act

- The EU Cyber Resilience Act has a broad scope as it applies to "products with digital elements". That means it applies to chips, software, IP components and devices; the draft requirements will cover almost the entire electronics industry. It considers the lifecycle of products as well as baseline security requirements, for example, asking for five years of updates.
- Products are split into three categories with varying conformance approaches: self-assessment for non-critical, 3rd party assessment or application of a standard for Critical Class I products, and 3rd party under a national body for Critical Class II products.
- The draft requirements are functional in style, with 13 product requirements, eight regarding vulnerability handling and nine on information and user instructions.
- The EU Cyber Resilience Act isn't yet law, but the draft requirements were published in September 2022 and an updated version was made available with Council edits in the summer of 2023. Although it is likely to be several years before it becomes "in force", now is the time for the industry to consider what proactive steps they might want to take in preparation.

You can read our thoughts on the proposed Cyber Resilience Act here.

Developers can use PSA Certified Level 1 v3.0 to get a third-party lab assessment of their responses to the latest EU CRA requirements.

UK Product Security and Telecommunications Infrastructure Act (PSTI)

- The draft requirements are functional in style, with 13 product requirements, eight regarding vulnerability handling and nine on information and user instructions.
- Following the act, security requirements were set out in separate regulations presented to UK Parliament in May 2023. Key requirements include:
  - Manufacturers must publish information on how long products will receive security updates. This will include making customers aware of a product's security update support period before allowing product purchases on the manufacturer's website.
  - Manufacturers must publish contact information to allow vulnerabilities relating to their devices to be reported.
  - Manufacturers must declare they are compliant through a 'Statement of Compliance'. The regulations state that adherence to industry standards ETSI EN 303 645 and/or ISO/IEC 29147 can be used as evidence of compliance.
  - Manufacturers, importers, and distributors of the consumer connected devices will not be able to sell products in the UK if they are not accompanied by a Statement of Compliance.
  - Firms that fail to meet these new regulations could face fines of up to £10 million or four per cent of their global turnover, as well as up to £20,000 a day in the case of an ongoing contravention.

Developers can use PSA Certified Level 1 v3.0 to get a third-party lab assessment of their responses to UK PSTI requirements.

The Radio Equipment Directive (RED)

- The RED directive applies to wirelessly connected devices (also referred to as "Radio Equipment" and shortened to "Equipment") sold in the EU.
- The detailed security requirements are being developed into a "harmonized standard" but are not yet public. They are being written by CEN-CENELEC's JTC 13 Working Group 8 experts and are expected to be based on ETSI EN 303645. Device makers are waiting for the next version of CENELEC's draft to be published so that they can design to meet the detailed requirements and tests. The harmonized requirements are expected to be in force in 2025.
- The EU provided guidance on the technical requirements to CEN/CENELEC and it is this document that PSA Certified uses to help guide developers in getting ready for the future harmonized requirements.
- Manufacturers can self-assess if the product fufils a harmonized standard or use third-party assessment.

Developers can use PSA Certified Level 1 v3.0 to get a third-party lab assessment of their responses to RED requirements (using the standardisation request from EU to CEN/CENELEC as a starting point for a future harmonized standard).

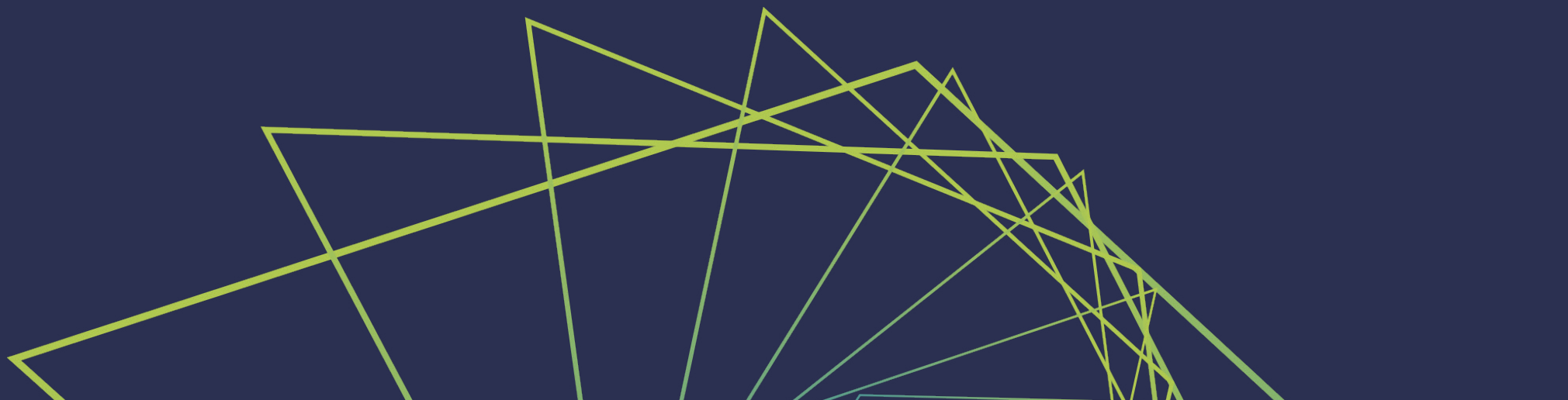
What About The USA?

Whilst Europe is on a journey to create enforceable security requirements by drafting laws, the USA has opted for a voluntary IoT labelling scheme. The U.S. Cyber Trust Mark was announced in a White House briefing, and the Federal Communications Commission (FCC) is currently developing the requirements. The introduction of a voluntary, consumer-facing security label is likely a significant and positive step for consumers. It will likely provide an external mark to show the device has been designed with security in mind and a means to access live, online information on those security features. While the program will be voluntary, many of the largest OEMs, technology companies, and retailers either participated in the White House launch event or have offered support for the program.

While the program will be voluntary, many of the largest OEMs, technology companies, and retailers either participated in the White House launch event or have offered support for the program; this level of support could indicate the "voluntary" program requirements may become quasi-mandatory in the US.The requirements are expected to be based on existing National Institute of Standards and Technology (NIST) cybersecurity baseline standards. NIST is an organization in the US that publishes recommendations on core features, functions, and activities that device manufacturers should take to protect customers. While publications like NISTIRs 8259 A/B and 8425 are not mandatory in the commercial marketplace, they are required for most IoT sales to the US government following the IoT Cybersecurity Improvement Act of 2020. Many OEMs may seek to meet these criteria so devices can be sold to the US government, which is a significant purchaser of technology.

PSA Certified Level 1 is already aligned to NISTIR 8259A, and developers can use the lab-based assessment to check if they are fulfilling these foundational requirements.

You can read our thoughts on the US Cyber Trust Mark here



Getting Ready for Legally Enforceable Security Requirements

The electronics industry can now prepare for EU CRA, EU RED and UK PSTI cybersecurity requirements.

The questions highlight the challenges we face as we look for ways to build a more secure future.

Questions to Ask Yourself

- Which legally enforceable cybersecurity requirements have been published (either at draft or final) that I must follow to sell my product?
- How can I demonstrate to my customers that I've followed best practices and ready to meet the legislation?
- Do I want a third-party assessment?
- Is third-party assessment (like PSA Certified) helpful for checking that we are ready for the new laws?

A Holistic Approach: Establishing a Baseline

The PSA Certified 2023 Security Report found that 64% of those surveyed said that device security regulation was due to be more significant than GDPR. While each industry and region will have its own security requirements a program like PSA Certified that brings together the most important regulation and standards is vital; it is an obvious place to start. While each industry and country will have its own security requirements, having a program like PSA Certified, which encourages broad adherence is vital.

What is a Root of Trust?

A Root of Trust, commonly shortened to RoT, is the foundational security component of a connected device. While precise definitions can vary considerably, a RoT can be described as a set of implicitly trusted functions that the rest of the system or device can use to ensure security; it is the foundation on which a device maker can build their “tower of trust”.

The PSA Root of Trust (PSA-RoT) was developed specifically for connected devices and designed to assist developers looking to implement IoT security, even on low-cost microcontrollers. It provides an easy-to-use security component implemented by most of the world’s leading chip vendors.

Learn More

Aligning Security Requirements

PSA Certified adopts an approach that all connected devices need a 'minimum' set of security requirements, which are underpinned by a Root of Trust. Since the launch of PSA Certified in 2019, our founding members have been analyzing the key requirements of leading emerging regulations to establish a set of baseline security criteria.

Our advice is that a sensible approach as a device manufacturer is to adhere to cybersecurity best practices such as the PSA Certified Security Model, the baseline requirements of EN 303 645 and NISTIR 8259A. PSA Certified Level 1 brings these requirements together and has the added advantage of helping developers get ready for forthcoming cybersecurity law.

What is the PSA Certified Security Model?

The PSA Certified Security Model provides the security principles that underpin the PSA Certified scheme. The document outlines ten critical goals for designing devices based on essential security properties.

Learn more about the PSA Certified 10 Security Goals

The PSA Certified founders aligned with EN 303 645 and its predecessors from 2019, and today, PSA Certified Level 1 security evaluation continues to map to the ETSI specification's mandatory device requirements. PSA Certified includes the NIST Cybersecurity baseline requirements from NIST 8259A and the PSA Certified Security Model Goals.

You can also use PSA Certified Level 1 to demonstrate that you meet multiple cybersecurity regulatory requirements. The latest version has added a new section to cover published draft legal security requirements; the UK PSTI and EU CRA requirements are provided verbatim in the PSA Certified Level 1 v3.0 and RED follows EU to CEN/CENELEC guidance.

You can find the latest PSA Certified Level 1 documentation here.

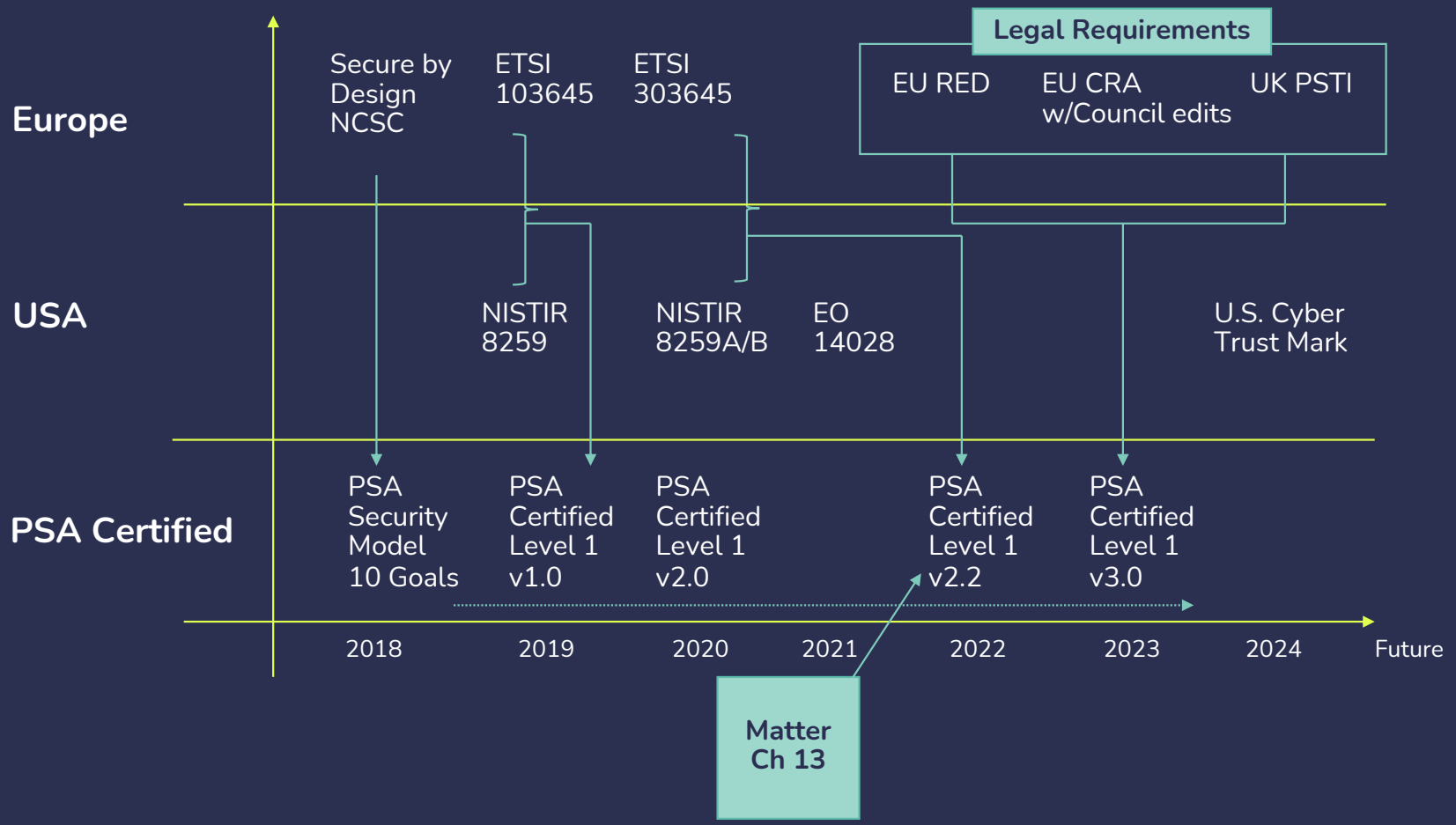
By achieving PSA Certified Level 1 and completing the section on legal cybersecurity requirements you can get your responses to the requirements independently assessed, and assure your customers or management team that your product is getting ready for the new laws that will be in force. The companies that develop PSA Certified will continue to monitor the landscape of legally enforceable requirements and help you reduce your time to market.

Chip vendors, software companies and device manufacturers can use PSA Certified to show they have met security by design principles and getting ready for future legal requirements. Together, we can prevent some of the most common vulnerabilities and many future potential IoT cyber incidents.

How PSA Certified Level 1 Maps to Standards and Regulation

Requirement	PSA Certified Level 1 version 3.0	EN 303 645	NIST 8259A	California SB-327	PSTI	EU-CRA	RED
Authentication/Password	X	X	X	X	X	X	X
Configuration	X	X	X			X	
Crypto	X	X	X			X	
Secure Communication	X	X	X			X	X
Hardening	X	X	X			X	X
Logging	X		X			X	X
Privacy	X	X	X			X	X
Secure Storage	X	X	X			X	X
Update	X	X	X		X	X	X

PSA Certified Alignment of Requirements



psacertified™

Summary

Governments are setting out legally enforceable security requirements to help ensure that as the number of connected devices grows, the risk to people's privacy and welfare does not increase. As a result, product developers risk losing access to large and important markets if they fail to consider security. As an industry, we have an essential role in building people's trust in the IoT, which is fundamental to accepting new technologies. We must use our combined expertise to lead new security initiatives and help shape emerging legislation and regulations.

Since 2019, PSA Certified has been operating as an independent certification scheme, measuring the robustness and assurance of products at different levels. Our entry-level scheme, PSA Certified Level 1, is applicable to devices, system software and chips and has been used in over 130 product evaluations. It is designed to be a business-to-business stamp demonstrating security best practice. Chip vendors can achieve higher PSA Certified levels for their PSA-RoT enabling OEMs to choose an appropriately robust SoC.

The PSA Certified members meet weekly to create the specifications, helping the technology ecosystem follow security best practice and get ready for future cybersecurity legislation. Our PSA Certified Level 1 document, now on its third version, includes EU and UK published cybersecurity regulations. PSA Certified is an efficient way to show you are meeting multiple sets of security requirements and getting ready for future cybersecurity law, use the link below to download it and get started.

Next Steps

Learn more about PSA Certified Level 1

Download PSA Certified documentation

Find PSA Certified products