



WHITEPAPER

How to meet the IoT security requirements of today and tomorrow

Steve Hanna, Distinguished Engineer

Date: 07/2023

www.infineon.com



Table of contents

Abstract	3
1 Attacks on the IoT	4
2 Governments step In	5
2.1 Guidelines	5
2.2 Regulations	6
3 IoT defenses	8
4 How to meet the toughest regulations	9
5 Certifying compliance with global requirements	11
6 Security for today and the future	11
References	12

Abstract

Governments around the world are creating Internet of Things (IoT) security legislation and regulations designed to keep users safe in an increasingly connected world. Connectivity is good and, in fact, great but bad things can happen to people with unprotected or poorly protected IoT devices. Failing to meet government regulations or guidelines may lead to the inability to sell products in a region and thus to lost revenue. However, the regulations are constantly in a state of flux. This white paper provides updated background on what governments are suggesting or requiring as well as specific details on how to implement security defenses and obtain security certifications that can satisfy current and even future government requirements.

1 Attacks on the IoT

IoT security is necessary for all the things that connect to the internet to share data. This includes smart cars, smart cities and energy, smart industry, and the smart home and its numerous consumer devices. As shown in Figure 1, the IoT architecture consists of three layers:

- Devices that send and receive data and commands
- A network that conveys data and commands
- Servers, or the cloud, that gather data, analyze and send commands

IoT devices can be subject to attacks in each of these layers. On an unprotected network, an eavesdropper listening in on transmitted data or commands can reveal confidential or private information. A bad or fake server sending commands to IoT devices in the field can be used to trigger unplanned events, compromise devices, remotely load unauthorized software, cause malfunctions or even trigger a denial of service attacks, and more. A bad device injecting fake measurements can disrupt processes and cause the system to react inappropriately or dangerously. For example, security cameras are frequently attacked to spy on people or to send back normal images when a theft is actually in progress.

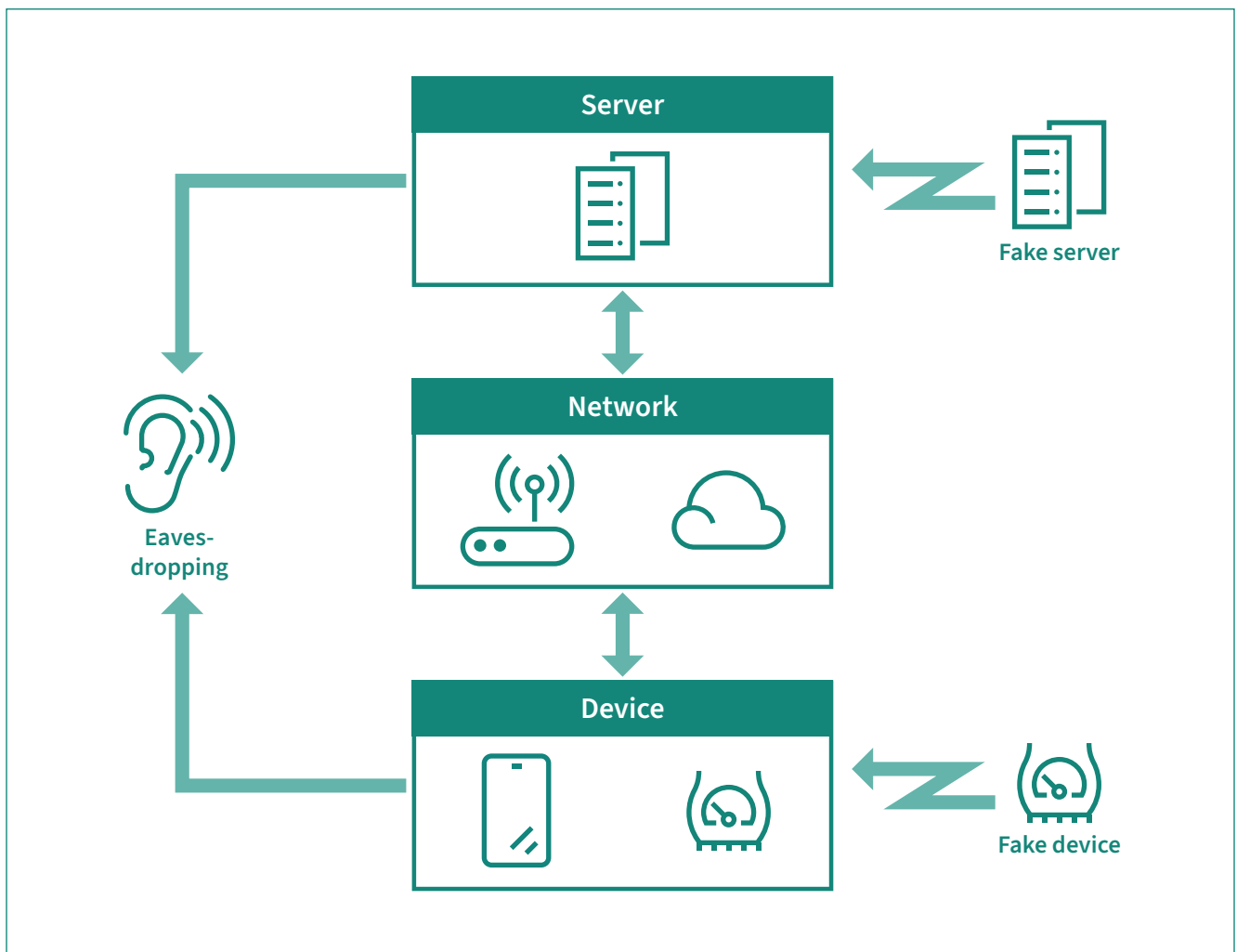


Figure 1 Every IoT layer is a potential target for a cybersecurity attack.

2 Governments step in

To prevent these cyberattacks, countries and regions around the world are creating IoT security guidelines and regulations. Although these rules were initially voluntary, they are gradually becoming mandatory. As attacks and problems mount, more countries are creating new guidelines or adopting existing ones and making them mandatory. Mandatory regulations usually include penalties and can even prevent the sale of products within the regulating region.

To understand the nature and impact of these guidelines and regulations, a brief review is needed. First, we will cover the leading technical guidelines. Then we will cover some of the laws and regulations that drive enforcement of these guidelines.

2.1 Guidelines

In May 2020, the U.S. National Institute of Standards and Technology (NIST) released Internal Report (IR) NISTIR 8259A [1], IoT Device Cybersecurity Capability Core Baseline. This document provides baseline cybersecurity best practices and guidance for IoT device manufacturers. Table 1 shows the six capabilities recommended by this document.

Table 1 Device cybersecurity recommended product capabilities identified in NISTIR 8259A and NISTIR 8425.

Item	Description
1	Unique identity
2	Only authorized entities can change device configuration
3	Protect stored and transmitted data from unauthorized access and mods
4	Restrict access to local and network interfaces, protocols and services
5	Permit software and firmware updates using secure, configurable mechanist
6	Report device cybersecurity state to authorized parties

The broad guidelines of NISTIR 8259A have since been elaborated in two profiles for specific applications. NIST IR 8425 expresses the requirements for consumer IoT applications. NIST SP 800-213 describes how to determine requirements for government IoT applications. More profiles are being developed by NIST for other IoT applications.

The European Telecommunications Standards Institute (ETSI) ETSI EN 303 645 was initially created in June 2020 in order to define requirements for IoT security in Europe. Since that time, ETSI EN 303 645 has been adopted by countries around the world [2]. The primary requirements in ETSI EN 303 645 are shown in Table 2.

Table 2 ETSI EN 303 645 primary requirements [2]

Item	Description
1	No universal default passwords
2	Implement a means to manage reports of vulnerabilities
3	Keep software updated
4	Securely store sensitive security parameters
5	Communicate securely
6	Minimize exposed attack surfaces
7	Ensure software integrity
8	Ensure that personal data is secure
9	Make systems resilient to outages
10	Examine system telemetry data
11	Make it easy for consumers to delete personal data
12	Make installation and maintenance of devices easy
13	Validate input data

Although organizations beyond NIST and ETSI have defined their own guidelines and new revisions are being made, the guidelines described above (NISTIR 8425 and ETSI EN 303 645) are the main ones that governments are referring to in their recent laws, rules, and regulations for consumer IoT.

2.2 Regulations

The United States (US) has adopted several mandatory and voluntary programs to boost IoT cybersecurity, all based on the NIST guidelines described above.

In December 2020, the IoT Cybersecurity Improvement Act of 2020 [3], previously approved by both Houses of Congress by unanimous consent, was signed into law by the President. This unprecedented unity to address a national security problem in these contentious times confirms its importance and the confidence in the solution.

The provisions contained in this bill direct NIST to develop guidelines for security of IoT devices purchased by the U.S. government. It also directs the Office of Management and Budget to develop rules for agencies to follow when they purchase IoT devices in the future. NIST SP 800-213 was developed as a result of this law so it is becoming a requirement for US government purchases of IoT.

In this same timeframe, two other US IoT security requirements were implemented by the executive branch in response to major attacks. The Executive Order on Improving the Nation's Cybersecurity [4], May 12, 2021, mandated several changes to improve cybersecurity. Most relevant to this white paper is a requirement for NIST to initiate a pilot program for IoT security device labeling for consumers. In response, NIST developed NISTIR 8425 (described above) and a NIST Cybersecurity White Paper titled "Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products [5]".

Most recently, the US government announced a US National Label for Consumer IoT Cybersecurity [6]. This label will reward products that meet the requirements of NISTIR 8425 by permitting them to display a US government label and be listed in a US government registry indicating that their cybersecurity has been tested and certified as compliant with US government standards. Although this US National Label will be optional to start with, it may eventually become a de facto or de jure requirement.

The European Union (EU) has been bolder in defining mandatory requirements for IoT cybersecurity. A revision to the Radio Equipment Directive (RED) will require all devices with a radio to comply with certain cybersecurity requirements in order to be sold in the EU [7]. Because of delays in developing and agreeing on these requirements, the effective date for these RED requirements is being pushed back from 2024 to 2025. Beyond the RED revisions, the EU Cyber Resilience Act (CRA) will impose even more strict requirements [8]. Although the details of the RED and CRA requirements are still being negotiated, these EU mandates will clearly become a powerful force boosting IoT cybersecurity.

Beyond the US and EU, dozens of countries have created or are creating IoT cybersecurity requirements. Table 3 summarizes some of these requirements.

Table 3 Summary of IoT device specification usage by region

Region	IoT device security spec	Mandatory/voluntary	Certification	Labeling	Key standard referenced
Asia					
Australia	Under development	Voluntary	Yes	Yes	ETSI EN 303 645
China	Yes	Mandatory	No	No	None
India	Yes	Voluntary	Yes	Yes	ETSI EN 303 645
Japan	Yes	Voluntary	No	No	NIST, ETSI EN 303 645
Singapore	Yes	Voluntary	Yes	Yes	ETSI EN 303 645
South Korea	Yes	Voluntary	Yes	Yes	ITU X.1352
Thailand	Under development	Voluntary	No	No	None
Vietnam	Yes	Voluntary	No	No	ETSI EN 303 645
Europe					
France	Yes	Voluntary	No	No	ETSI EN 303 645
Germany	Yes	Voluntary	Yes	Yes	ETSI EN 303 645
Spain	No	Voluntary	No	No	None
UK	Yes	Mandatory	Yes	Yes	ETSI EN 303 645
Americas					
Brazil	Yes	Mandatory	Yes	Yes	ETSI EN 303 645, ISO/IEC 27402
US	Yes	Voluntary	Yes	Yes	NIST IR 8425

Source: Omdia Report: Consumer IoT Device Cybersecurity Standards, Policies, and Certification Schemes [9] (February 2023).

While the NIST and ETSI guidelines prevail at the moment, new requirements come along every year. This should be no surprise. History shows that there is always a race between cybersecurity attackers and defenders. In the next decade, the requirements for IoT cybersecurity will surely continue to rise rapidly until they reach fairly high levels. Wise product designers will build into their products a generous margin of cybersecurity beyond today's minimums so that they can continue to satisfy the ever-rising bar of requirements that must be met to sell their products globally. As a beneficial and not insignificant effect, their products and customers will be well protected against cyber attacks.

To avoid premature product obsolescence and meet the increasingly stringent requirements, product manufacturers need to design-in the most rigorous cybersecurity solutions today. No company wants to be left with a product that must be radically redesigned to meet new IoT cybersecurity requirements so that it can continue to be sold.

3 IoT defenses

Different security defenses are required in many facets of the IoT to avoid weaknesses for exploitation to satisfy security requirements. Figure 2 identifies 10 key areas for security, many of which are identified in the existing regulations described above.

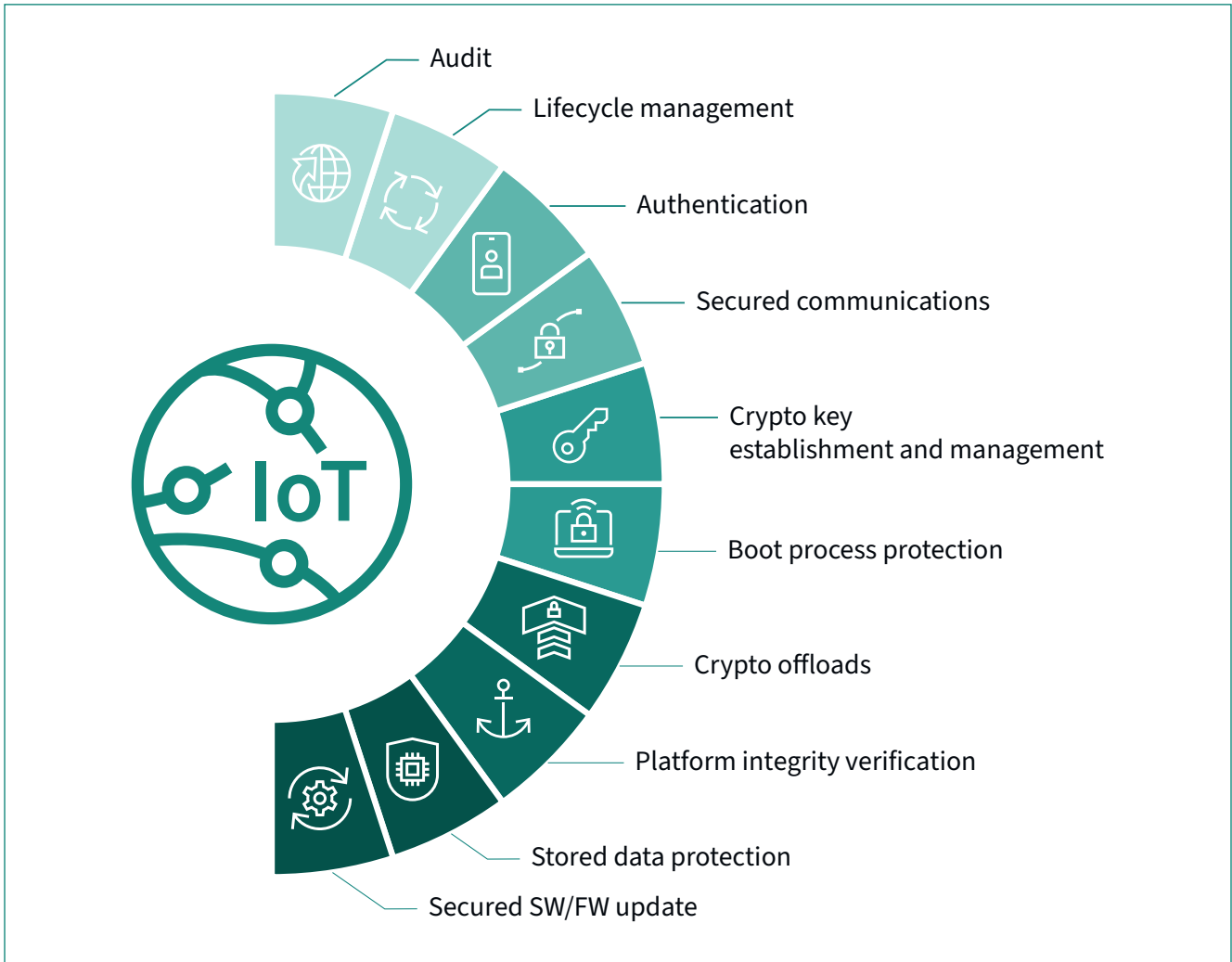







Figure 2 A broad range of defenses exist to protect IoT devices.

Security hardware makes it easier for product manufacturers to design and produce secured IoT devices that comply with IoT security regulations and can continue to do so in the future. Furthermore, security hardware can make it easier for end-users to install and use these devices. Infineon offers a wide range of security hardware products, allowing designers to choose the product that best meets the needs of their application. Figure 3 shows the range of security features in Infineon's AIROC™, Programmable System-On-Chip™ (PSoC™), OPTIGA™ Trust and OPTIGA™ TPM solutions.

	AIROC™	PSoC 62	PSoC 64	OPTIGA™ Trust M	OPTIGA™ TPM
					
Primary function	Communication & MCU	MCU	MCU	Security	Security
Secured connectivity	✓	✓	✓✓	✓✓✓	✓✓✓
Secured cloud authentication	✓	✓	✓✓	✓✓✓	✓✓✓
Secured software update over-the-air	✓	✓	✓✓	✓✓✓	✓✓✓✓
Physical attack resistance		✓	✓✓	✓✓✓	✓✓✓




Figure 3 Infineon’s hardware-based security products span a range of capabilities.

4 How to meet the toughest regulations

A careful look at ETSI EN 303 645 and NISTIR 8425 shows that many requirements are best met with hardware security. The choice of hardware over software-based security will not change with new legislation and regulations. In fact, future regulations will add requirements for features like secured boot that are not required today but already supported in hardware.

How specifically can hardware security help product developers to meet the requirements of government regulations? Look at NIST IR 8425. Item 1 in the NISTIR 8425 list (Table 1) indicates the need for unique identity.

The PSoC™ 64 and OPTIGA™ solutions include a unique cryptographic key pair and certificate stored in hardware – the strongest concept of unique identity available. By integrating a PSoC™ 64 or OPTIGA™ solution into an IoT device, device manufacturers can quickly and easily meet these government requirements and probably any future ones relating to IoT device identity. Beyond this, the OPTIGA™ family of security solutions can be used for item 2, which requires that only authorized entities can change device configuration. The best way to implement this is with strong hardware-based authentication of users, servers, and other devices.

Item 3 in NISTIR 8425 requires secured communications and storage. The best place to store sensitive data is in a security-enabled chip, as supported by the AIROC™, PSoC™, and OPTIGA™ solutions.

Securely storing and communicating large amounts of data typically is performed with bulk encryption implemented on the main processor (e.g., PSoC™ 6) for maximum throughput. Even in those cases, OPTIGA™ products can play several essential roles. First, generating an encryption key requires high-quality entropy (cryptographic randomness) which the OPTIGA™ solutions are designed to provide. Second, secured communications are meaningless without strong authentication to prevent attackers from posing a man-in-the-middle (MitM) attack. Hardware-based identity is valuable there. Third, secured storage requires a place to store the encryption key or key-encryption key, which is supported by the OPTIGA™ solutions.

Restricting access to interfaces, protocols, and services (Item 4) is similar to item 2 in that it requires support for strong authentication so that access requests can be verified. Beyond this, hardware security can provide tamper-resistant access controls which can resist even more sophisticated attacks.

Item 5 in NISTIR 8425 requires support for updating software on IoT devices. Installing security updates is as important for IoT devices as it is for phones and computers. To prevent the installation of malicious updates, the signature of each update needs to be checked. The best way to do this is by using a verification key stored in hardware, like a PSoC™ or OPTIGA™ solution.

The best way to report device cybersecurity state (Item 6 in NISTIR 8425) is with techniques like remote attestation, which employ the hardware security capabilities of a PSoC™ 6 or OPTIGA™ security solutions to prevent malware from subverting the reporting process. With remote attestation, the cloud can monitor the device to verify it is running the latest and proper software.

ETSI EN 303 645 adds several requirements that go beyond those included in NISTIR 8425. Checking software integrity (Item 7 in ETSI EN 303 645) is typically performed during the boot sequence. As the device boots up, the PSoC™ or AIROC™ uses a key (preferably stored in hardware such as an OPTIGA™ solution) and checks the signature on all of its software before running it.

There are a variety of ways to make systems resilient to outages (Item 9 in ETSI EN 303 645). One simple way is by having everything residing local to the system, so if the internet goes out, the device still works. This requires the device to be secured and not require the cloud for its security. The built-in hardware-based security performs this task.

The best way to make it easy for consumers to delete personal data (Item 11 in ETSI EN 303 645) is to encrypt personal data with a key and store that key in a secured location. When the consumer no longer needs to access the information, because of a sale or even end of life of the device, deleting the key eliminates the possibility of using it to decrypt the personal encrypted data. Unlike erasing data with software, which can allow a determined attacker to retrieve and restore data, the destruction of an encryption key in hardware instantly renders the encrypted data completely meaningless.

While easy installation and maintenance (Item 12 in ETSI EN 303 645) sounds simple, making it easy for the consumer to securely install an IoT device is often quite difficult. The PSoC™ 64 and OPTIGA™ family of security solutions are designed to integrate quickly and securely with all the major IoT clouds such as Microsoft Azure, Amazon AWS, Google Cloud and more. The device manufacturer gets a chip that is ready for easy cloud integration.

Finally, validating input data (Item 13 in ETSI EN 303 645) is always good advice. However, validation has proven devilishly difficult for IoT devices. Daily news reports show that even thoroughly vetted software can be vulnerable to malicious packets that may cause a buffer to overwrite and compromise the device thus giving it access to all data and keys accessible to the main processor. For this reason, long-term keys and critical secrets should not be accessible to the main processor. PSoC™ 6 and OPTIGA™ solutions offer a protected place for such secrets.

5 Certifying compliance with global requirements

How can manufacturers show that their products comply with the dozens of national and regional requirements coming from governments around the world? Must they submit their products separately to each government for certification through each national or regional program? The costs of obtaining these many certifications would be exorbitant!

Fortunately, a global approach to IoT product certification is coming from the Connectivity Standards Alliance (CSA), the group that developed the Matter standard [10]. CSA is developing a global IoT product cybersecurity certification program that includes a superset of all the national and regional requirements. With this program, manufacturers can get their product certified once to show compliance with all the national and regional programs.

Even better, the CSA program will recognize the cybersecurity certifications already obtained by hardware and software components in the IoT product. Thus, if an IoT product includes security certified Infineon chips, there is no need to duplicate those certifications. The IoT product that includes the Infineon chips gets the benefit of the security certifications that the chips have.

To give a specific example, an IoT product that uses Infineon's unique identity features not only gains the benefit of this feature's functionality (a pre-built unique identity solution) but also avoids the need to get this feature recertified.

6 Security for today and the future

After years of attackers exploiting IoT device weaknesses, governments around the world are finally starting to take preventive action. Excellent directions for what is needed to provide security in today's IoT devices are found in guidelines such as the USA's NISTIR 8259 and NISTIR 8425, as well as the EU's ETSI EN 303 645. As demonstrated by the EU's RED and CRA, one may reasonably expect these rules to tighten over time or be extended as more security is needed. To avoid premature product obsolescence, device manufacturers should adopt strong hardware-based security solutions like the AIROC™, PSoC™ and OPTIGA™ technologies that can be used to meet the increasingly stringent requirements for IoT security emerging from governments all around the world.

Doing the best job possible for designing an IoT product starts with hardware-based security to provide best-in-class security and preparation for the most rigorous security requirements --- both today and in the future.

PSoC™ is a registered trademark of Infineon Technologies AG. OPTIGA™, AIROC™ and Programmable System-On-Chip are trademarks of Infineon Technologies AG.

References

- [1] Security for IoT Device Manufacturers: NIST Publishes NISTIRs 8259 and 8259A: <https://www.nist.gov/news-events/news/2020/06/security-iot-device-manufacturers-nist-publishes-nistirs-8259-and-8259a>
- [2] ETSI EN 303 645 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
- [3] National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems: <https://csrc.nist.gov/publications/detail/nistir/8259d/draft>
- [4] Executive order on improving the nation's cybersecurity, and Security Memorandum on improving cybersecurity for critical infrastructure control systems: <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>
- [5] Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf>
- [6] OCT 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/20/statement-by-nsc-spokesperson-adrienne-watson-on-the-biden-harris-administrations-effort-to-secure-household-internet-enabled-devices/>
- [7] Radio Equipment Directive (RED) https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en
- [8] Cyber Resilience Act <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act>
- [9] Consumer IoT Device Cybersecurity Standards, Policies, and Certification Schemes, <https://csa-iot.org/wp-content/uploads/2023/02/Consumer-IoT-Device-Cybersecurity-Standards-Policies-and-Certification-Schemes.pdf>
- [10] The Foundation for Connected Things <https://csa-iot.org/all-solutions/matter/>

Where to Buy

Infiniteon distribution partners and sales offices:

www.infineon.com/WhereToBuy

Service Hotline

Infiniteon offers its toll-free **0800/4001** service hotline as one central number, available 24/7 in English, Mandarin and German.

Germany	0800 951 951 951 (German/English)
China, mainland	4001 200 951 (Mandarin/English)
India	000 800 4402 951 (English)
USA	1-866 951 9519 (English/German)
Other countries	00* 800 951 951 951 (English/German)
Direct access	+49 89 234-0 (interconnection fee, German/English)

*Please note: Some countries may require you to dial a code other than "00" to access this international number, please visit www.infineon.com/service for your country!

Published by
Infineon Technologies AG
Am Campeon 1-15, 85579 Neubiberg
Germany

© 2023 Infineon Technologies AG.
All rights reserved.

Public

Date: 07/2023



Stay connected!



Scan QR code and explore offering
www.infineon.com

Please note!

This Document is for information purposes only and any information given herein shall in no event be regarded as a warranty, guarantee or description of any functionality, conditions and/or quality of our products or any suitability for a particular purpose. With regard to the technical specifications of our products, we kindly ask you to refer to the relevant product data sheets provided by us. Our customers and their technical departments are required to evaluate the suitability of our products for the intended application.

We reserve the right to change this document and/or the information given herein at any time.

Additional information

For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices, please contact your nearest Infineon Technologies office (www.infineon.com).

Warnings

Due to technical requirements, our products may contain dangerous substances. For information on the types in question, please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life-endangering applications, including but not limited to medical, nuclear, military, life-critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.