AN13874

Protecting IP cameras with NXP secure solutions

Rev. 1.0 — 21 June 2023 Application note

Document Information

Information	Content
Keywords	Cameras, IP Cameras, C2PA EdgeLock, SE05x, A5000
Abstract	Protecting IP Cameras: From Serious Security Risk to Trusted Asset, with One IC

Table 1. Revision history

Revision number	Date	Description
1.0	20230621	Initial version

1 IP cameras – A risky business through all device Life-Cycle

Security is always an important consideration when designing for the Internet of Things (IoT). Since any connected device, small or large, is a potential entry point to a broader network. But with IP cameras, security must take center stage.

Internet-connected video cameras make an ideal target for attack. They are often used in sensitive applications, such as security and surveillance, which attract hackers. Since the very early production, camera manufacturers tend to use the connection of the IP camera for their own purposes. From secure manufacturing in untrusted supply chain, to late-stage configurations, and periodic maintenance. All these sessions can be hijacked or abused too. Just to provide a concrete example the IP camera might be manufactured at an untrusted facility, security credentials can be tampered with prior to shipment.

In industrial use cases, IP cameras play an essential role for business processes. This role means business-critical tasks, such as in-field updates, smart analytics, and periodic maintenance. So any disruption of the cameras functioning may cause sever industrial processes disruption.

What is more, installation in unsupervised locations creates opportunities for physical attacks. And, because IP cameras have a relatively high degree of functionality, they are attractive targets for use in network strikes. Such as Distributed Denial of Service (DDoS) attacks.

At nearly every point in the Life-Cycle of the IP camera, there are opportunities for manipulation or theft. During installation, hackers can steal the private information used for legitimate access. Every session with the cloud presents an opportunity to spoof the authentication process. Any video transmission can be stolen or modified as part of a deepfake attack. The rise of fake images, created by artificial intelligence (AI), makes it all the more important to be able to verify the origin and validity of footage.

Finally, in smart home environments, cameras are directly connected to the smart home network and they might represent an entry point for attackers to the households.

Given so many points of risk, it is best to view security in an IP camera as a starting point for design. Approaching security as a design element relevant to every aspect of functionality.

1.1 Protecting IP Cameras: From serious security risk to trusted asset, with one EdgeLock® IC

NXP provides scalable, flexible, and secure solutions to develop future-proof and secure cameras.

Enabling top-notch security on cameras, is as easy as integrating the **NXP EdgeLock SE05x/A5000 secure element**: A ready-to-use SE solution. Tailor-made for the IoT, that provides a secure CC EAL 6+, AVA_VAN.5 certified tamper-resistant hardware, to protect mission critical cryptographic credentials as well as a secure environment to offload cryptographic operations. EdgeLock SE05x/A5000 is pre-provisioned with keys and credentials in a highly secure, and controlled environment, therefore relieving device manufacturers from setting up a complex and expensive Public Key Infrastructure (PKI). It also comes with a pre-installed applet and a Plug & Trust middleware package that eases the integration of the secure element in the device MCU/MPU.

As a matter of fact, the NXP EdgeLock secure element family is a turnkey solution that gives developers an easier path to security certification while making security an essential part of the design, relevant to every aspect of functionality.

By delivering certified security with tamper resistance, along with Common Criteria EAL 6+ certification as well as protection from the latest attack scenarios, including advanced hardware attacks. The EdgeLock SE050/ SE051, and A5000 delivers Life-Cycle protection for cameras.

Hardware-based security ensures safe operation. Including secure key and credential storage, verified proof of origin, and safe execution of secure algorithms, and protects the essential steps in IP camera operations:

• Secure cloud onboarding – By delivering end-to-end security, from chip to edge to cloud, the EdgeLock SE050 makes onboarding a zero-touch event. Keys are never exposed to any party during the lifetime of the device.

• Device-to-device authentication and attestation: The EdgeLock SE050 supports mutual authentication, ensuring only authorized devices access the network, and uses encryption to attest the authenticity of data.

• Late-stage parameter configuration: EdgeLock SE05x variants integrate an ISO/IEC 1443 interface, for use with NFC, so smartphones or contactless readers can safely configure the IP camera by installing a specific setup or loading data.

• Wi-Fi credential operation: The EdgeLock SE050 protects the Wi-Fi credentials, including WPA2 passphrases and secret keys, used to authenticate and validate devices before allowing them to use a WLAN or Wi-Fi connection.

Furthermore, to support FIPS certification, for example, the EdgeLock SE050 is available as a module that serves as a ready-to-use certified platform with security Level 3 for the OS and app, and security Level 4 for the physical security of the hardware.

To support Matter certification, dedicated EdgeLock secure element and secure authenticator provide full, turnkey Matter security. These Plug & Trust security components, which connect to any type of processor using a standard I^2C interface, provision Matter attestation keys, and certificates to the device and provide hardware-accelerated execution of Matter authentication protocols for interoperability.

Last but not least, to abstract the complexity of key and certificate management in secure elements and authenticators, NXP offers **EdgeLock 2GO**: a fully managed cloud platform that allows customers to create and manage secure objects, such as symmetric roots of trusts, key-pairs, and certificates, which are then securely provisioned (either remotely or locally) into the secure elements of IoT devices. This fully managed cloud platform gives customers the flexibility to securely manage the credentials of EVSEs already deployed in the field and to update the credentials quickly and easily to meet new security requirements or react to security incidents.

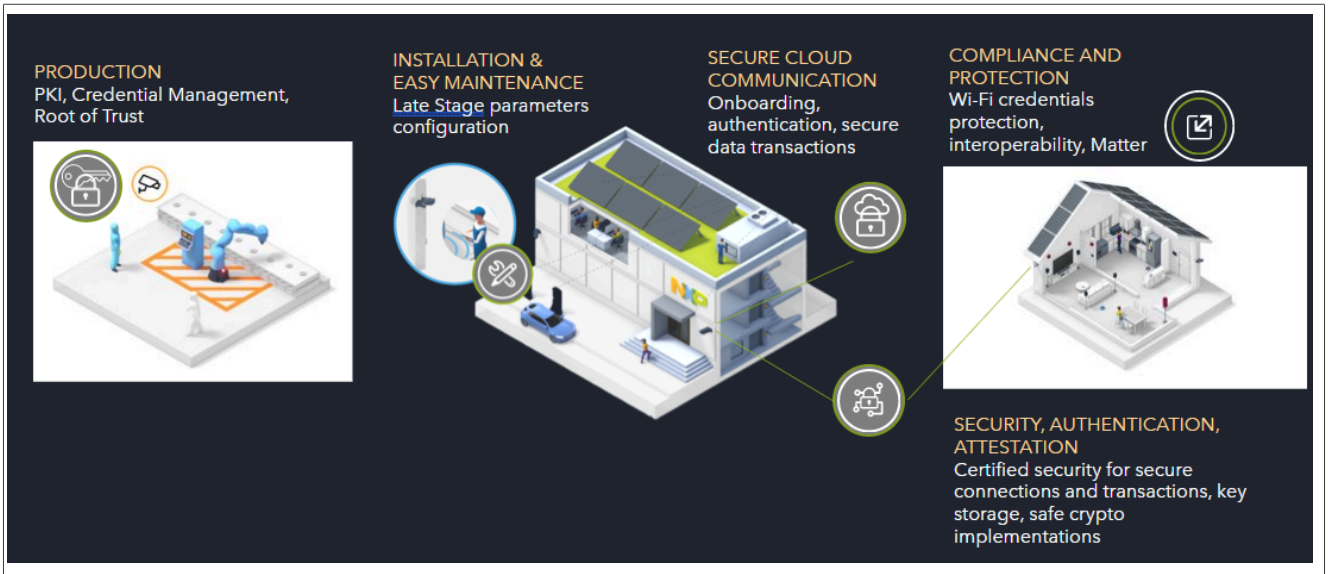

Figure 1. Examples that need protection

2 Key operations for camera

When designed into an IP camera, the EdgeLock SE050 protects a number of key operations: secure cloud onboarding, device-to-device authentication, attestation, late-stage parameter configuration, and Wi-Fi credential protection. The following security considerations are essential to guarantee the secure operation of IP Camera throughout their Life-Cycle.

2.1 Secure cloud onboarding

Connectivity to central systems is a main functionality of IP cameras. Having individual credentials in the devices allows these central systems to accept only connections from trusted devices. The EdgeLock SE05x is designed to provide a tamper-resistant platform to store credentials safely, needed for device authentication and registration to public or private clouds.

EdgeLock SE05x helps to set up a trusted TLS connection to onboard devices to the cloud without writing security code or exposing credentials or keys.

The listed application notes describe the platform-specific secure authentication to all major cloud platforms. AN12400 - Secure connection to OEM cloud depicts an authenticated connection to general central services using mutually authenticated TLS.

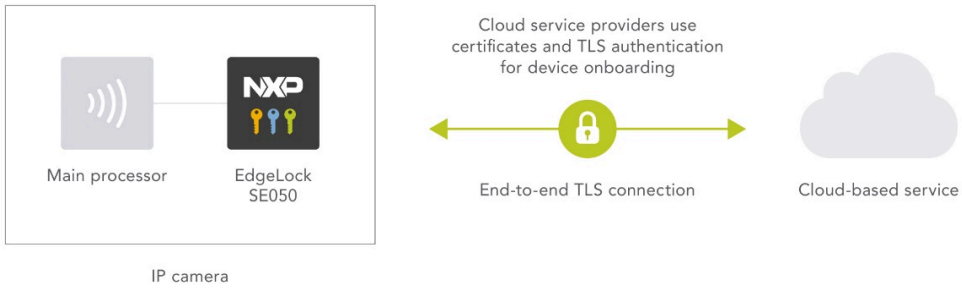

Figure 2. Secure cloud onboarding

Table 2. Support documentation

App note	Title
AN12404	Secure connection to AWS IoT Core
AN12401	Secure connection to Google Cloud Platform
AN12402	Secure connection to Azure IoT Hub
AN12403	Secure connection to IBM Watson IoT
AN12400	Secure connection to OEM cloud

2.2 Device to device authentication

IoT networks can have a demand on direct device to device communication, and authentication to be able to work without or at least less dependence on central services. The connections between devices can be secured either like in the cloud connection case with mutually authenticated TLS or with custom authentication methods like described in AN12399 - Device-to-device authentication. The AN12399 describes how to implement a strong mutual authentication mechanisms using digital certificates.

Figure 3. Device to device authentication

Table 3. Support documentation

App note	Title
AN12400	Secure connection to OEM cloud
AN12399	Device-to-device authentication

2.3 Secure attestation

Secure attestation is a means to undeniably prove to a third party that a piece of data has originated in a trusted environment. For example, an SE such as EdgeLock SE05x. When data is requested from the SE, the user can request attestation for the returned data. The SE attests the origin of the data by signing it with a chip-unique key-pair (attestation key-pair) that is securely stored inside the SE and cannot be used for other purposes.

The data to be attested can be for example data being sent from a trusted subsystem connected to the I^2C controller of the secure element (the subsystem can as such only be controlled by the secure element) or it can be keys or data from within the secure element. With data attestation a third party can check if a key or data presented to it was either:

- generated inside the secure element
- injected via secure trust provisioning at NXP
- injected externally (possibly known to others)

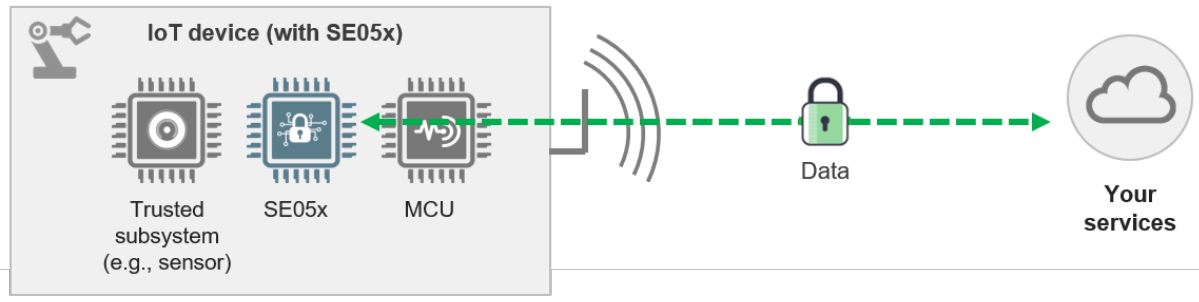

Figure 4. IoT device attestation with EdgeLock SE05x

Table 4. Support documentation

App note	Title
AN13254	Secure attestation with EdgeLock SE05x

2.4 Late stage parameters configuration

The EdgeLock SE05x comes with an integrated, fully ISO/IEC14443 A compliant interface. This interface allows you to perform a secure and convenient late stage parameter configuration of industrial IoT devices already deployed in the field using an NFC reader. The SE05x ISO/IEC 14443 an interface is passive and noes not require any power from the host. Connecting a small loop antenna to the two antenna pins of the SE05x is enough.

As such, EdgeLock SE05x acts like a bridge between the IoT device and the contactless reader.

The AN12664 describes how to leverage EdgeLock SE05x to enable a secure, and convenient late-stage parameter configuration of IoT devices in the factory, before shipment, or in the field.

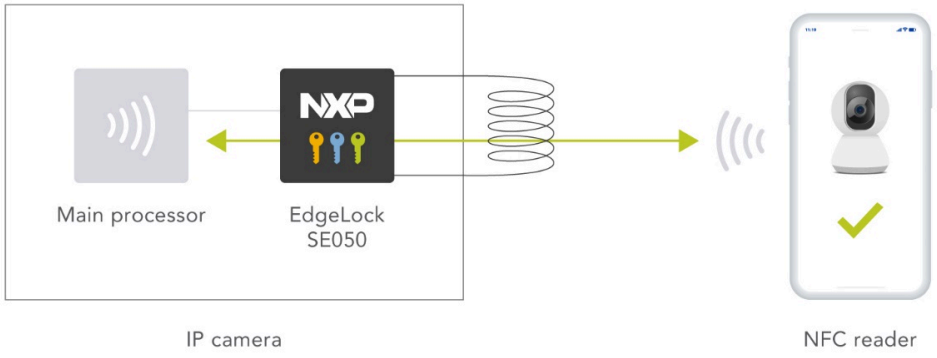

Figure 5. Late stage parameters configuration

Table 5. Support documentation

App note	Title
AN12664	NFC late-stage configuration

2.5 Network credentials protection

Security on the connectivity of IP cameras is not limited to the central services itself. In a layered approach as well, the network uses the camera to deliver its data has to be secured. This can be done using standards like 802.1x or 802.11x network authentication. The AN12661 - Wi-Fi credential protection describes this on the example of a Wi-Fi based 802.11x network authentication. The same certificate based principle can be applied to 802.1x based wired networks.

Figure 6. Wi-Fi credentials protection

Table 6. Support documentation

App note	Title
AN12661	Wi-Fi credential protection

3 Meet FIPS, Matter and C2PA security requirements with NXP solutions

3.1 FIPS requirements

The FIPS standards, officially known as the Federal Information Processing Standards, are developed and maintained by the National Institute of Standards and Technology (NIST) and implemented by the US government to regulate information technology and computer security. FIPS compliance is a requirement for products certified for use by government departments and agencies within the US and Canada. Also, because FIPS standards are widely recognized as being state-of-the-art, FIPS compliance is used as a purchasing guideline in the private sector, too.

Insisting on a FIPS-compliant solution gives users operating in the IoT the confidence that their setup is both interoperable and secure. For this reason, many IoT vendors, including those who are not working directly with the US or Canadian governments, now make it a priority to obtain FIPS compliance. They either certify the entire IoT device or, more frequently, select modules of the design. The EdgeLock SE050 offers FIPS certification as a cryptographic module. The module is a FIPS 140-2 ready-to-use certified platform with security Level 3 for the OS and app, and security Level 4 for the physical security of the hardware.

3.2 Smart Home: Matter compliant operation

For IP cameras that operate in Smart Home environments, the new Matter specification offers a number of benefits, from interoperability and ease of installation to high-level protection and privacy. Security is at the heart of Matter. The NXP development platforms offer dedicated EdgeLock® secure element and secure authenticator to provide full, turnkey Matter security. These Plug & Trust security components, which can be connected to any type of processor using a standard I^2C interface, take care of provisioning Matter attestation keys and certificates to the device and provide HW accelerated execution of Matter authentication protocols. These OEMs can simplify and accelerate manufacturing and compliance to Matter security specifications. In particular the generation, and injection of attestation, and commissioning credential, as well as security logistics associated with Matter ecosystem. In addition, OEMs can further leverage the NXP EdgeLock secure element and secure authenticator, which are Common Criteria, certified to protect user data and user privacy, integrity of devices, and secure connections to multiple clouds (including software update servers).

3.3 Coalition for content provenance and authenticity (C2PA)

For media creator, it is becoming more and more critical to attest and establish the origin of the created media in order to ensure trust.

The origin of content (also known as provenance) can be used for authenticity and integrity of the content. To address this issue, the Coalition for Content Provenance and Authenticity (C2PA) has developed a **technical specification** which describes a trust model for storing and accessing cryptographically verifiable content.This trust model is based on the concept of C2PA Manifest which is a set of information about the provenance of an asset. Manifests should contain a timestamp.

Here we describe a use case where a manifest is used:

- Take a photograph with their C2PA enabled camera
- The Camera creates a manifest using on-camera stored credentials
- The manifest is used to prove authenticity and origin of picture
  The Manifest contains Assertions like:
  - camera info
  - thumbnail of image
  - hashes binding picture to manifest
- Camera generates a claim containing list of assertions
- The Claim is digitally signed and the entire manifest embedded into output JPEG

3.3.1 Leveraging EdgeLock Secure Element and Authenticator for C2PA

The EdgeLock® secure element and secure authenticator can be used to meet C2PA security requirements.

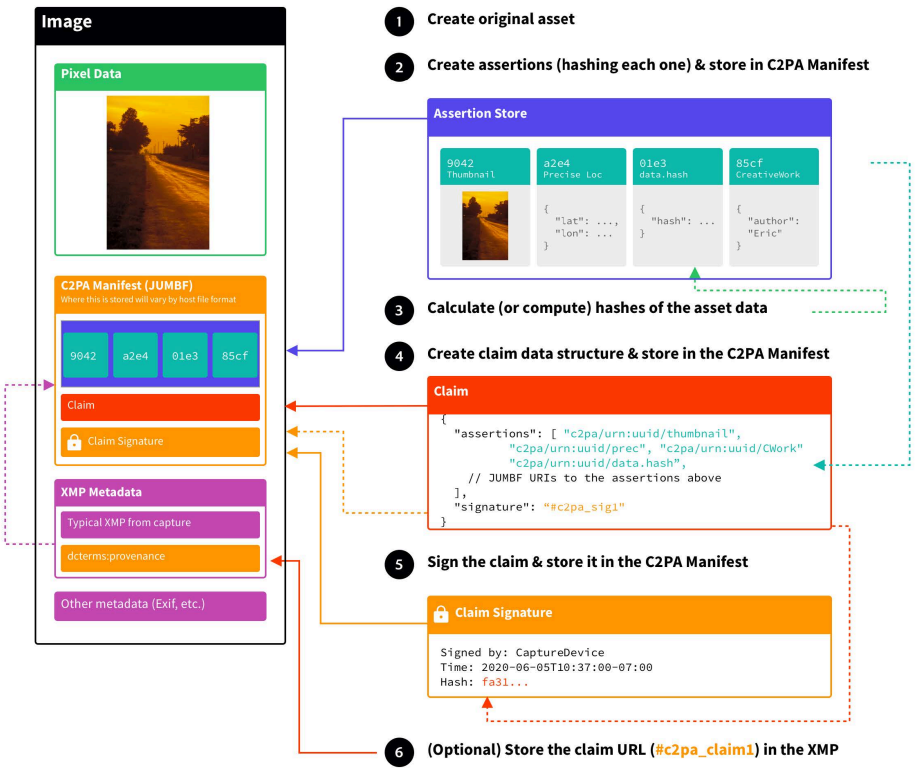

Figure 7. Manifest example
[1]

[1] The image is from: *C2PA Technical Specification, page 34*, release 1.0,2022-07-26 owned by the Coalition for Content Provenance and Authenticity.

To summarize: the Secure Element or Secure Authentication can be used for the following use cases:

- Create signatures for the claim
  - ECDSA with SHA-256 (which is called sES256 in the standard)
  - The SE05x supports all C2PA needed algorithms
- Store public key of Time Stamp Authority (TSA)
  - The camera can use the key to verify the timestamp token

4 Legal information

4.1 Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

4.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Suitability for use in non-automotive qualified products — Unless this data sheet expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

Translations — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

NXP B.V. - NXP B.V. is not an operating company and it does not distribute or sell products.

4.3 Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

NXP — wordmark and logo are trademarks of NXP B.V.

Tables

Figures

Contents

For more information, please visit: http://www.nxp.com

Date of release: 21 June 2023
Document identifier: AN13874-IP Cameras