AN3983

Demystifying ISA/IEC 62443 and Secure Elements

Introduction

Authors: Matteo Giaconia, Security Pattern and Xavier Bignalet, Microchip Technology Inc.

This application note provides guidance on how Microchip secure element devices can be effectively used as building blocks in the creation of ISA/IEC 62443-compliant products.

This document is targeting engineers and managers tasked to obtain ISA/IEC 62443-compatible or certified products.

In the context of ISA/IEC 62443, Microchip components ATECC608 and TA100 can be acknowledged as technology enablers on the path to reaching compliance and certification of Industrial and Automation Control System (IACS) products according to the standard (with specific reference to part 62443-4-2 of the all-encompassing ISA/IEC 62443 standard: “Technical Security Requirements for IACS components”), as clarified in this document.

© 2021 Microchip Technology Inc.
and its subsidiaries

Table of Contents

© 2021 Microchip Technology Inc.
and its subsidiaries

1. About ISA/IEC 62443

ISA/IEC 62443 is a series of standards, technical specifications and technical reports totalling about 800 pages that came to be from an initiative of the International Society of Automation (ISA) Committee on Security for IACS (ISA99) in 2007, and was later produced by the International Electrotechnical Commission (IEC).

ISA/IEC 62443 is meant to address the security needs of industrial automation and control systems that make use of operational technology (OT) and that have increasingly been facing cyberattacks over the past few years. The consequences are diverse, spanning from the compromise of high value assets that are strategic for national safety (e.g., outages in energy distribution, transportation networks or healthcare industries), to the loss of revenue (e.g., manufacturing), to directly jeopardizing human lives (e.g., electrocution, chemical product exposure, fatal equipment failure, etc.).

These security needs and the threats they arise from are not aligned to those of more traditional information technology (IT) systems due to the many differences in the characteristics of the two types of systems, in terms of:

- Performance requirements (such as throughput or response time)
- Availability requirements (tolerance to outages, need for continuous operation, plant certifications, etc.)
- Operating environment characteristics (e.g., type of operating system used, technology refresh rate, system upgradeability)
- Risk management goals (fault tolerance, prevention of negative HSE consequences)

As a result of all these particularities, the existing security standards that were originally developed for applying to the IT context (such as those belonging to the ISO 27000 series) are not suited to efficiently nor effectively address IACS security requirements.

1.1 The Structure and Contents of the ISA/IEC 62443 Series

The ISA/IEC 62443 series of standards is made up of 14 work products (Standards, Technical Specifications and Technical Reports) that are logically grouped in four tiers:

- Tier 1: General
- Tier 2: Policies and Procedures
- Tier 3: System
- Tier 4: Component

Additionally, the 62443 series introduces three roles:

- **Asset Owner** (AO): This is the end user and operator of an industrial automation control system.
- **System Integrator** (SI): This is the entity in charge of the integration and configuration of the subsystems and components that constitute an IACS and of its deployment in the intended environment.
- **Product Supplier** (PS): The manufacturer of an industrial product (an embedded device such as a PLC or an RTU, a network device such as a firewall, a host device such as a PC or a software application).

The first tier of the standard (62443-1), named “General”, includes those work products that are general in nature, introducing foundational concepts, models and terms that are used throughout the series. It includes 4 work products:

- 62443-1-1: Concepts and Models
- 62443-1-2: Master Glossary of Terms and Abbreviations
- 62443-1-3: System Security Conformance Metrics
- 62443-1-4: IACS Security Lifecycle and Use Cases

This first tier is equally relevant to all roles defined by the standard.

© 2021 Microchip Technology Inc.
and its subsidiaries

Figure 1-1. ISA/IEC 62443 Tier Structure

The second tier (62443-2), named “Policies and Procedures”, focuses on the people and processes aspects of an effective security program and its scope is that of addressing plant operations. It includes five work products:

- 62443-2-1: Security Program Requirements for IACS Asset Owners
- 62443-2-2: Implementation Guidance for an IACS Security Management System
- 62443-2-3: Patch Management in the IACS Environment.
- 62443-2-4: Requirements for IACS Solution Suppliers
- 62443-2-5: Implementation Guidance for IACS Asset Owners

This second tier is most relevant to Asset Owners.

The third tier (62443-3), named “System”, focuses on technology-related aspects of security for systems, describing the guiding principles for performing implementation and integration to achieve security. It includes 3 work products:

- 62443-3-1: Security Technologies for IACS
- 62443-3-2: Security Risk Assessment and System Design
- 62443-3-3: System Security Requirements and Security Levels

The fourth tier (62443-4), named “Component”, focuses on specific security-related requirements for products and components, covering both the technical contents of those products and the processes employed to manage them throughout their lifecycle. It includes two work products:

- 62443-4-1: Secure Product Development Lifecycle Requirements
- 62443-4-2: Technical Security Requirements for IACS Components

This fourth tier is most relevant to Product Suppliers. It is important to note that the content of Tier 4 was built with the goal of abstracting the component and its features from any specifics pertaining to the final automation project’s implementation (it is focused on the component’s capabilities).

© 2021 Microchip Technology Inc. and its subsidiaries

1.2 The ISA/IEC 62443 Approach to Security

The ISA/IEC 62443 series illustrates a comprehensive approach to security in the industrial domain, stressing the importance of:

- Applying risk-management methods whenever defining and handling both processes and technical features.
- Addressing all aspects of security as part of an integrated framework (including physical security, personnel security, cybersecurity).

This holistic approach originates from the need of serving the end user's concerns (the Asset Owner's perspective is central).

One of the cornerstones this approach is built on is the concept of "Security Levels" (SLs).

The ISA/IEC 62443 series introduces qualitative definitions for security levels (SL), characterized by the level of protection that is provided against attacks.

Figure 1-2. ISA/IEC 62443 Security Levels

The ISA/IEC 62443 approach expects an Asset Owner to perform a risk assessment activity when defining the IACS for implementation. The outcome of this risk assessment activity is a "Target Security Level" (SL-T) for the IACS as a whole.

Based on this SL-T, the AO (with the aid of System Integrators), then, performs procurement of subsystems and components and implements the IACS in the specific destination environment. Each component and subsystem is characterized by a "Capability Security Level" (SL-C).

The system implementation is, then, evaluated by the AO to verify whether the "Achieved Security Level" (SL-A) meets the requirements previously set forth (checking whether SL-A is greater or equal to SL-T). Compensating countermeasures (both technical and procedural) are repeatedly applied at the system level or in processes and procedures until the goal is fully achieved.

Using components whose development process and technical contents are certified according to the ISA/IEC 62443 Tier 4 standards allows Asset Owners and System Integrators to perform their IACS integration, implementation and risk management activities more efficiently, more effectively and with a greater degree of confidence in the security of the resulting system.

© 2021 Microchip Technology Inc. and its subsidiaries

2. ISA/IEC 62443 for Product Suppliers

To build products that are certifiable according to ISA/IEC 62443, Product Suppliers must consider the contents of the two work products belonging to Tier 4 of the standard:

- The Product Supplier's processes must meet the requirements set forth in part 4-1 of the standard ("Secure Product Development Lifecycle Requirements"), which defines a set of "Practices" and ranks the readiness of the PS's processes in terms of "Maturity Levels".
- The specific product that certification is sought for needs to meet the technical requirements set forth in part 4-2 of the standard ("Technical Security Requirements for IACS Components"), which defines a set of "Foundational Requirements" and ranks the security capabilities of the PS's product in terms of "Security Levels".

The content of this document is mainly focused on how to address the latter and aimed to simplify the 200-page part 4-2 of the standard by highlighting how Microchip secure elements and Security Pattern can help your product meet compliance.

2.1 How to Comply to ISA/IEC 62443-4-2

The qualitative definition of Security Levels is provided in 1.2. The ISA/IEC 62443 Approach to Security.

A quantitative evaluation of a product's SL-C (Capability Security Level) needs to be performed to assign a specific level to the product. This quantitative evaluation is based on a list of Component Requirements (CRs) and associated Requirement Enhancements (REs), which are grouped in categories that are called Foundational Requirements.

The standard defines seven Foundational Requirements (FR1-to-7):

FR1	Identification and Authentication Control (IAC)
FR2	Use Control (UC)
FR3	System Integrity (SI)
FR4	Data Confidentiality (DC)
FR5	Restricted Data Flow (RDF)
FR6	Timely Response to Events (TRE)
FR7	Resource Availability (RA)

Each Foundational Requirement is simply a logical grouping of individual sets each made up of one Component Requirement and, eventually, some Requirement Enhancements.

The standard provides tables that illustrate which CRs/REs are needed to reach each SL.

The table below provides a quantitative evaluation example based on requirement number 7 (strength of password-based authentication) of the first foundational requirement category (Identification and Authentication Control).

There are two REs associated with this CR. The tick marks appearing in the table indicate whether the CR or RE is needed to reach a given SL.

	SL1	SL2	SL3	SL4
CR1.7 – Strength of Password-Based Authentication	✔	✔	✔	✔
RE1.7.1 – Password Generation and Lifetime Restrictions for Human Users			✔	✔
RE1.7.2 – Password Lifetime Restrictions for All Users				✔

As an example evaluation:

- If the component does not satisfy the base CR, its SL will be 0.
- If the component satisfies only the base CR, its SL will be 2.
- If the component satisfies the base CR and the first RE(1), its SL will be 3.

© 2021 Microchip Technology Inc. and its subsidiaries

- If the component satisfies the base CR, both RE(1) and RE(2), its SL will be 4.

This evaluation must be repeated across all CR/RE groups belonging to each FR category. The total SL for the product under consideration is the minimum SL achieved over all these evaluations. In conclusion, to meet a targeted security level (SL), all the requirements must be met.

2.2 How Our Products Can Help

The ATECC608 is a technology enabler that provides IACS product suppliers with the means to satisfy the component requirements mandated by ISA/IEC 62443-4-2. Below is a list of cryptographic features and security protection of the ATECC608 that will be later mapped against the ISA/IEC 62443 specification.

Table Naming	Features
SHA256	SHA-256 & HMAC Hash including off-chip context save/restore.
Secure Key Storage	JIL High secure storage for up to 16 keys, certificates or data.
ECDSA	ECDSA: FIPS186-3 Elliptic Curve Digital Signature (Sign/verify).
ECDH	ECDH: FIPS SP800-56A Elliptic Curve Diffie-Hellman.
ECCP256	NIST Standard P256 Elliptic Curve Support.
PRF/HDKF	Turnkey PRF/HKDF Calculation for TLS 1.2 & 1.3.
Ephemeral Key	Ephemeral Key Generation and Key Agreement in SRAM.
Message Encryption	Small Message Encryption with Keys Entirely Protected.
AEC128/GCM	AES-128: Encrypt/Decrypt, Galois Field Multiply for GCM.
RNG	Internal High-Quality NIST SP 800-90A/B/C Random Number Generator (RNG).
Key Rotation	Private Key Rotation and public key attestation are effectively possible and pre-configured in the ATECC608 TrustFLEX for convenience Public Key Rotation is also effectively possible and and pre-configured in the ATECC608 TrustFLEX for convenience. It will be an essential feature for late stage key provisioning.
Tamper Protection	Physical Tamper and Side Channel Attack Protection.
Secure Key Provisioning	Microchip in-house Secure Key Provisioning leveraging HSM network and Late Stage Provisioning possible.
Secure Boot	ECC-P256 ECDSA Verify for Signature Verification.
Key Disable	The secure element has the capability to Disable Key following logic conditions defined by the developer.
Secure Key Provisioning	Microchip in-house Secure Key Provisioning service allows customers to leverage our factory equipped with Hardware Secure Module (HSM) and isolate cryptographic keys from third party manufacturers. Late Stage Provisioning is possible (contact Microchip).

The ISA/IEC 62443 is calling for “secure key storage” or protection of the cryptographic keys. This is not a vague term in security but rather a specific feature the silicon is designed with. A secure key storage or the act of protecting keys consists of implementing a physical secure boundary wherein both the crypto-operations and cryptographic keys live. If keys and algorithms are not in that same secure boundary, the keys will be exposed at some point during transactions. This is where the essence of secure elements like the ATECC608 start to bring their contribution to a successful certification. Secure elements are secure key storage devices tested against the Joint Interpretation Library (JIL) rating scale from the Common Criteria practices to evaluate its robustness to protect keys.

Following the value of secure key storage, loading keys in such a device location following a secure manufacturing process comes up immediately as the next question. Microchip has factories equipped with a network of managed hardware security modules (HSM) that enable our customers to leverage our secure key provisioning service. By onboarding the secure element with this service, customers follow a controlled secret key exchange process that

© 2021 Microchip Technology Inc. and its subsidiaries

binds the credentials securely stored in the device to their own chain of trust or their client's chain of trust without exposing the various cryptographic keys to any third party such as contract manufacturers. In complementary fashion, Microchip's secure element can enable late-stage provisioning when an end-customer desires to activate the cryptographic keys late in the provisioning process.

The table below refers to the component requirements defined in ISA/IEC 62443-4-2, and provides indications on how the ATECC608 can act as a technology enabler to help the client's product meet each of the requirements. The Security Level (SL) is specified for each CR and Cryptographic feature listed in the table below.

The ISA/IEC 62443 standard defines the requirements for four types of components:

- Embedded Devices (EDR)
- Software Applications (SAR)
- Host Devices (HDR)
- Network Devices (NDR).

Those component requirements that apply to all types of components are marked as "CR", while the other requirements are marked according to the component type that they apply to (respectively: EDR, SAR, HDR, NDR).

When reading the table below, keep in mind the RE is associated to the CR of the same base paragraph. For example, "CR 1.1 RE(1) Unique identification and authentication" is part of the "CR1.1 Human user identification and authentication".

© 2021 Microchip Technology Inc.
and its subsidiaries

Functional Requirement		Associated Requirements:																		
Component Requirement (CR)	Component Requirement Enhancement (RE)	SAR EDR HDR HDR Requirements	SAR EDR HDR HDR Enhancements	Title	NIST SP 800-90A/B/C (RNG)	ECC-P256	ECDSA P256 FIPS 186-3 (Sign/verify)	ECDH FIPS SP800-56A	Ephemeral key and key agreement in SRAM	PRF/HKDF for TLS 1.2 & 1.3	SHA-256 & HMAC with save/restore	AES-128: GCM, Encrypt/Decrypt	Message encryption with protected keys	JIL High secure key storage	Tamper protection	Key rotation	Key disable	Secureboot	Secure key provisioning	Features and Usage
CR. 1.1				Human User Identification and Authentication							1									Hash functionality combined with the secure key storage capabilities enable robust management of integrity checks on password files.
	CR 1.1 RE (1)			Unique Identification and Authentication							2									Hash functionality combined with the secure key storage capabilities enable robust management of integrity checks on password files.
CR 1.2				Software Process and Device Identification and Authentication	2	2	2	2						2	2				2	JIL High Secure storage of keys and certificates, and digital signature verification and generation capabilities enable secure identification and authentication.
	CR 1.2 RE(1)			Unique Identification and Authentication	3	3	3	3						3	3				3	JIL High Secure storage of keys and certificates, and digital signature verification and generation capabilities enable secure identification and authentication.
CR 1.5				Authenticator Management					1	1		1	1	1	1	1	1		1	Cryptographic key generation and secure storage capabilities enable robust initialization and lifecycle management for keys via hardware.
	CR 1.5 RE(1)			Hardware Security for Authenticators					3	3		3	3	3	3	3	3		3	Cryptographic key generation and secure storage capabilities enable robust initialization and lifecycle management for keys via hardware.
CR 2.4		SAR 2.4 EDR 2.4 HDR 2.4 NDR 2.4		Mobile Code		1	1	1			1	1		1	1	1	1		1	Hash functionality and secure storage capabilities enable robust management of integrity checks on code and data.
			SAR 2.4 RE(1) EDR 2.4 RE(1) HDR 2.4 RE(1) NDR2.4 RE(1)	Mobile Code Authenticity Check	2	2	2	2						2	2	2	2		2	Secure storage of keys and certificates, and digital signature verification and generation capabilities enable authentication of code and data.
CR2.12				Non-Repudiation	1	1	1	1			1									Hash functionality and secure storage capabilities enable robust management of integrity checks on audit information. Secure storage of keys and certificates, and digital signature verification and generation capabilities enable authentication of audit information.
CR2.12	CR2.12 RE(1)			Non-Repudiation for All Users	4	4	4	4			4									Hash functionality and secure storage capabilities enable robust management of integrity checks on audit information. Secure storage of keys and certificates, and digital signature verification and generation capabilities enable authentication of audit information.
CR3.1				Communication Integrity							1									Secure storage of keys and certificates, and digital signature verification and generation capabilities enable assurance of integrity and authenticity of transmitted information. Cryptographic engines for standard symmetric-key and asymmetric-key algorithms and for hashing enable support of common communication cypher suites.
Index Value : 1 = SL1 2 = SL2 3 = SL3 4 = SL4																				

© 2021 Microchip Technology Inc. and its subsidiaries

.....continued

Functional Requirement		Associated Requirements:																		
Component Requirement (CR)	Component Requirement Enhancement (RE)	SAR EDR HDR HDR Requirements	SAR EDR HDR HDR Enhancements	Title	NIST SP 800-90A/B/C (RNG)	ECC-P256	ECDSA P256 FIPS186-3 (Sign/verify)	ECDH FIPS SP800-56A	Ephemeral key and key agreement in SRAM	PRF/HKDF for TLS 1.2 & 1.3	SHA-256 & HMAC with save/restore	AES-128: GCM, Encrypt/Decrypt	Message encryption with protected keys	JIL High secure key storage	Tamper protection	Key rotation	Key disable	Secureboot	Secure key provisioning	Features and Usage
CR3.1	CR3.1 RE(1)			Communication Authentication	2	2	2	2		2		2	2	2	2	2	2		2	Networking key management support enables support for standard cryptographic communication protocols such as TLS.
CR3.4				Software and Information Integrity							1			1	1	1	1		1	Hash functionality and secure storage capabilities enable robust management of integrity checks on code and data.
CR3.4	CR3.4 RE(1)			Authenticity of Software and Information		2	2	2						2	2	2	2		2	Secure storage of keys and certificates, and digital signature verification and generation capabilities enable authentication of code and data.
CR3.8				Session Integrity	2				2	2		2	2							Networking key management support and the internal RNG provide the capability to generate robust unique session identifiers.
CR3.10			EDRE3.10.1, HDRE3.10.1, NDRE3.10.1	Update Authenticity and Integrity		2	2	2			2	2	2	2	2	2	2	2	2	Secure storage of keys and certificates, digital signature verification and generation capabilities, HW support for asymmetric and symmetric algorithms and for hashing functions enable authentication and integrity verification of SW updates.
CR3.12		EDR3.12 HDR3.12 NDR3.12		Provisioning Product Supplier Roots of Trust										2	2	2	2		2	Secure storage capabilities are available for protecting product supplier roots of trust.
CR3.13		EDR3.13 HDR3.13 NDR3.13		Provisioning Asset Owner Roots of Trust										2	2	2	2		2	Secure storage capabilities are available for protecting asset owner roots of trust.
CR3.14		EDR3.14 HDR3.14 NDR3.14		Integrity of Boot Process		1	1											1		Secure boot support is provided through internal signature validation mechanisms and secure storage of digests/signatures.
CR3.14			EDRE3.14.1, HDRE3.14.1, NDRE3.14.1	Authenticity of the Boot Process		2	2											2		Secure boot support is provided through internal signature validation mechanisms and secure storage of digests/signatures.
CR4.1				Information Confidentiality		1	1	1			1	1		1	1	1	1		1	Secure encrypted storage is directly provided for up to 16 keys, certificates or data. Additionally, HW support for symmetric algorithms and key storage capabilities enable encryption of externally stored data.
CR4.3				Use of Cryptography		1	1	1			1	1								Secure encrypted storage is directly provided for up to 16 keys, certificates or data. Additionally, HW support for symmetric algorithms and key storage capabilities enable encryption of externally stored data.
CR4.3	CR7.3 RE(1)			Backup Integrity Verification							2			2	2	2	2		2	Hash functionality and secure storage capabilities enable robust management of integrity checks on backup data.
CR7.4				Control System Recovery and Reconstitution							1			1	1	1	1		1	Hash functionality and secure storage capabilities enable robust management of integrity checks on backup data.

Index Value : 1 = SL1 2 = SL2 3 = SL3 4 = SL4

© 2021 Microchip Technology Inc. and its subsidiaries

3. Conclusion

1. **The cryptographic algorithm's requirements:** Cryptographic accelerators alone do not solve security and this is what the ISA/IEC 62443 is demonstrating. Where the ATECC608 parts excel is their very low power consumption (30 nA) in Sleep mode, which is where most of the device lifetime will be. Combine that benefit with its hardware-based crypto accelerators, reducing execution time, and the device becomes an outstanding solution for power budget optimization by offloading the heavy cryptographic operations to the ATECC608.
2. **The JIL High secure key storage:** This is where Microchip secure elements stand out to help meet ISA/IEC 62443 compliance. Cryptographic algorithms are just mathematical operations. Without the protection of their associated keys, there is virtually no security. Essentially, every time a cryptographic algorithm is called for, secure key storage becomes a must-have. The ATECC608 was tested following Common Criteria testing practices on secure key storage. The rating is on the JIL scale. With a JIL High, the highest JIL grade possible for secure key storage, the ATECC608 brings a high level of confidence that keys will be protected at a very effective price point.
3. **Secure Key Provisioning:** Similarly, the same analogy can be drawn between secure key storage and secure key provisioning. Handling the cryptographic keys following a secure manufacturing process is essential to preserve as much isolation as possible between keys and any outside variable. This is a benefit that the ISA/IEC62443-4-1 standard also emphasizes. Microchip offers an in-house secure key provisioning service where the cryptographic keys will be loaded on the customer's behalf. The Microchip Trust Platform will be the starting point.
4. **CryptoAuthLib Library:** An essential element that will bring flexibility to the choice of microcontroller or microprocessor (consider using PKCS11). The CryptoAuthLib Library offers a hardware abstraction layer (HAL) where the I^2C or SWI drivers will exist and keep the secure element agnostic of the microcontroller or microprocessor.

© 2021 Microchip Technology Inc.
and its subsidiaries

4. How Our Resources and Our Partner Security Pattern Can Help

The ISA/IEC 62443 standard stresses the need to address security holistically: security cannot be achieved through technology alone. Security is certainly about technology, but it is also about people and processes.

As a natural consequence of this approach, compliance of a product supplier's processes to the ISA/IEC 62443-4-1 standard (“Secure Product Development Lifecycle Requirements”) was made a prerequisite for achieving CSA [1] and EDSA [2] product certification according to part 4-2 of the standard.

Complying to ISA/IEC 62443-4-1 implies adopting a series of robust processes that guarantee that products are indeed managed by product suppliers with a level of security that is commensurate to their technological content, in line with their customers' expectations and sustainable throughout the products lifecycle. These requirements are fully in-line with common recommendations and good practices for security.

These are some of the key activities that the standard requires from product suppliers:

- The application of security-by-design principles, including defense in depth
- The proper definition and tracking of security requirements, starting from conception and on to design, implementation, testing, managing of field issues and decommissioning
- The application of risk management practices to the design of secure components (with threat modeling activities being an integral part of this risk-centric approach)
- The training of their personnel in those areas of security that are relevant as per the definition of each employee's role and responsibility in product definition, development and management

Security Pattern, as Certified Microchip Security partner, can:

- Support manufacturers of industrial components in understanding their products’ security requirements and how these relate to the ISA/IEC 62443 standard, by means of focused consultancies or introductory trainings.
- Aid in the definition and refinement of security-related product requirements (including platform selection/ definition).
- Guide Product Suppliers in making proper applicative use of Microchip components and their rich set of security features.
- Help Product Suppliers, during product development phases, in the definition of their system, the streamlining of their production flow (considering security of the supply chain and of third-party suppliers), the development of their software.
- Provide technologies and expertise for public key infrastructure setup, digital certificates management, secure boot, etc.
- Aid in implementing and executing the Product Supplier’s internal processes according to ISA/IEC 62443-4-1 requirements, providing a structure for their documentation that is compliant to ISA/IEC 62443 standard requirements.
- Perform product gap analysis vs. the ISA/IEC 62443-4-2 component requirements.
- Support the technical discussions with the selected ISA/IEC 62443 certification body.
- Deliver training sessions tailored to meet the needs of Product Suppliers’ personnel, which Practice 1 of the standard mandates security expertise upkeep and assessment for.

Notes:

1. www.isasecure.org/en-US/Certification/IEC-62443-CSA-Certification#tab1
2. www.isasecure.org/en-US/Certification/IEC-62443-CSA-Certification#tab2

© 2021 Microchip Technology Inc. and its subsidiaries

5. Get Started with the ATECC608 and Security Pattern

Visit our approved Security Design Partner Security Pattern's website for consulting and design services.

Visit the Microchip website for more information:

- Overview of the Trust Platform for CryptoAuthentication™ and understanding where to start to leverage Microchip Secure Key Provisioning service
- Github repository for the CryptoAuthLib library
- Details on the pre-provisioned Trust&GO ISA/IEC 62443 secure element for TLS or LoRaWan networks
- Details on the pre-configured TrustFLEX ISA/IEC 62443 secure element
- Details on the fully customizable TrustCUSTOM ISA/IEC 62443 secure element

© 2021 Microchip Technology Inc.
and its subsidiaries

6. Revision History

Revision	Date	Section	Description
A	04/2021	Document	Initial Revision
B	12/2021	1.1. The Structure and Contents of the ISA/IEC 62443 Series	Corrected Figure 1-1 graphic

The Microchip Website

Microchip provides online support via our website at www.microchip.com/. This website is used to make files and information easily available to customers. Some of the content available includes:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQs), technical support requests, online discussion groups, Microchip design partner program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Product Change Notification Service

Microchip's product change notification service helps keep customers current on Microchip products. Subscribers will receive email notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, go to www.microchip.com/pcn and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Embedded Solutions Engineer (ESE)
- Technical Support

Customers should contact their distributor, representative or ESE for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in this document.

Technical support is available through the website at: www.microchip.com/support

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip products:

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner, within operating specifications, and under normal conditions.
- Microchip values and aggressively protects its intellectual property rights. Attempts to breach the code protection features of Microchip product is strictly prohibited and may violate the Digital Millennium Copyright Act.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is "unbreakable". Code protection is constantly evolving. Microchip is committed to continuously improving the code protection features of our products.

Legal Notice

This publication and the information herein may be used only with Microchip products, including to design, test, and integrate Microchip products with your application. Use of this information in any other manner violates these terms. Information regarding device applications is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. Contact your local Microchip sales office for additional support or, obtain additional support at www.microchip.com/en-us/support/design-help/client-support-services.

© 2021 Microchip Technology Inc. and its subsidiaries

THIS INFORMATION IS PROVIDED BY MICROCHIP "AS IS". MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, OR WARRANTIES RELATED TO ITS CONDITION, QUALITY, OR PERFORMANCE.

IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, OR CONSEQUENTIAL LOSS, DAMAGE, COST, OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE INFORMATION OR ITS USE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIP'S TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THE INFORMATION OR ITS USE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THE INFORMATION.

Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

Trademarks

The Microchip name and logo, the Microchip logo, Adaptec, AnyRate, AVR, AVR logo, AVR Freaks, BesTime, BitCloud, CryptoMemory, CryptoRF, dsPIC, flexPWR, HELDO, IGLOO, JukeBlox, KeeLoq, Kleer, LANCheck, LinkMD, maXStylus, maXTouch, MediaLB, megaAVR, Microsemi, Microsemi logo, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, PolarFire, Prochip Designer, QTouch, SAM-BA, SenGenuity, SpyNIC, SST, SST Logo, SuperFlash, Symmetricom, SyncServer, Tachyon, TimeSource, tinyAVR, UNI/O, Vectron, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

AgileSwitch, APT, ClockWorks, The Embedded Control Solutions Company, EtherSynch, Flashtec, Hyper Speed Control, HyperLight Load, IntelliMOS, Libero, motorBench, mTouch, Powermite 3, Precision Edge, ProASIC, ProASIC Plus, ProASIC Plus logo, Quiet- Wire, SmartFusion, SyncWorld, Temux, TimeCesium, TimeHub, TimePictra, TimeProvider, TrueTime, WinPath, and ZL are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Adjacent Key Suppression, AKS, Analog-for-the-Digital Age, Any Capacitor, AnyIn, AnyOut, Augmented Switching, BlueSky, BodyCom, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, Espresso T1S, EtherGREEN, GridTime, IdealBridge, In-Circuit Serial Programming, ICSP, INICnet, Intelligent Paralleling, Inter-Chip Connectivity, JitterBlocker, Knob-on-Display, maxCrypto, maxView, memBrain, Mindi, MiWi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, NVM Express, NVMe, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, PowerSmart, PureSilicon, QMatrix, REAL ICE, Ripple Blocker, RTAX, RTG4, SAM-ICE, Serial Quad I/O, simpleMAP, SimpliPHY, SmartBuffer, SmartHLS, SMART-I.S., storClad, SQI, SuperSwitcher, SuperSwitcher II, Switchtec, SynchroPHY, Total Endurance, TSHARC, USBCheck, VariSense, VectorBlox, VeriPHY, ViewSpan, WiperLock, XpressConnect, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

The Adaptec logo, Frequency on Demand, Silicon Storage Technology, Symmcom, and Trusted Time are registered trademarks of Microchip Technology Inc. in other countries.

GestIC is a registered trademark of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

All other trademarks mentioned herein are property of their respective companies.

© 2021, Microchip Technology Incorporated and its subsidiaries. All Rights Reserved.

ISBN: 978-1-5224-9466-9

Quality Management System

For information regarding Microchip's Quality Management Systems, please visit www.microchip.com/quality.

© 2021 Microchip Technology Inc.
and its subsidiaries

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: www.microchip.com/support Web Address: www.microchip.com **Atlanta** Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455 **Austin, TX** Tel: 512-257-3370 **Boston** Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088 **Chicago** Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075 **Dallas** Addison, TX Tel: 972-818-7423 Fax: 972-818-2924 **Detroit** Novi, MI Tel: 248-848-4000 **Houston, TX** Tel: 281-894-5983 **Indianapolis** Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380 **Los Angeles** Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 **Raleigh, NC** Tel: 919-844-7510 **New York, NY** Tel: 631-435-6000 **San Jose, CA** Tel: 408-735-9110 Tel: 408-436-4270 **Canada - Toronto** Tel: 905-695-1980 Fax: 905-695-2078	**Australia - Sydney** Tel: 61-2-9868-6733 **China - Beijing** Tel: 86-10-8569-7000 **China - Chengdu** Tel: 86-28-8665-5511 **China - Chongqing** Tel: 86-23-8980-9588 **China - Dongguan** Tel: 86-769-8702-9880 **China - Guangzhou** Tel: 86-20-8755-8029 **China - Hangzhou** Tel: 86-571-8792-8115 **China - Hong Kong SAR** Tel: 852-2943-5100 **China - Nanjing** Tel: 86-25-8473-2460 **China - Qingdao** Tel: 86-532-8502-7355 **China - Shanghai** Tel: 86-21-3326-8000 **China - Shenyang** Tel: 86-24-2334-2829 **China - Shenzhen** Tel: 86-755-8864-2200 **China - Suzhou** Tel: 86-186-6233-1526 **China - Wuhan** Tel: 86-27-5980-5300 **China - Xian** Tel: 86-29-8833-7252 **China - Xiamen** Tel: 86-592-2388138 **China - Zhuhai** Tel: 86-756-3210040	**India - Bangalore** Tel: 91-80-3090-4444 **India - New Delhi** Tel: 91-11-4160-8631 **India - Pune** Tel: 91-20-4121-0141 **Japan - Osaka** Tel: 81-6-6152-7160 **Japan - Tokyo** Tel: 81-3-6880- 3770 **Korea - Daegu** Tel: 82-53-744-4301 **Korea - Seoul** Tel: 82-2-554-7200 **Malaysia - Kuala Lumpur** Tel: 60-3-7651-7906 **Malaysia - Penang** Tel: 60-4-227-8870 **Philippines - Manila** Tel: 63-2-634-9065 **Singapore** Tel: 65-6334-8870 **Taiwan - Hsin Chu** Tel: 886-3-577-8366 **Taiwan - Kaohsiung** Tel: 886-7-213-7830 **Taiwan - Taipei** Tel: 886-2-2508-8600 **Thailand - Bangkok** Tel: 66-2-694-1351 **Vietnam - Ho Chi Minh** Tel: 84-28-5448-2100	**Austria - Wels** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 **Denmark - Copenhagen** Tel: 45-4485-5910 Fax: 45-4485-2829 **Finland - Espoo** Tel: 358-9-4520-820 **France - Paris** Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 **Germany - Garching** Tel: 49-8931-9700 **Germany - Haan** Tel: 49-2129-3766400 **Germany - Heilbronn** Tel: 49-7131-72400 **Germany - Karlsruhe** Tel: 49-721-625370 **Germany - Munich** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 **Germany - Rosenheim** Tel: 49-8031-354-560 **Israel - Ra'anana** Tel: 972-9-744-7705 **Italy - Milan** Tel: 39-0331-742611 Fax: 39-0331-466781 **Italy - Padova** Tel: 39-049-7625286 **Netherlands - Drunen** Tel: 31-416-690399 Fax: 31-416-690340 **Norway - Trondheim** Tel: 47-72884388 **Poland - Warsaw** Tel: 48-22-3325737 **Romania - Bucharest** Tel: 40-21-407-87-50 **Spain - Madrid** Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 **Sweden - Gothenberg** Tel: 46-31-704-60-40 **Sweden - Stockholm** Tel: 46-8-5090-4654 **UK - Wokingham** Tel: 44-118-921-5800 Fax: 44-118-921-5820

© 2021 Microchip Technology Inc.
and its subsidiaries